Army Regulation 215–8
AFI 34-211(I)

Morale, Welfare, and Recreation

Army and Air Force Exchange Service Operations

Headquarters
Departments of the Army,
and the Air Force
Washington, DC
5 October 2012

UNCLASSIFIED

SUMMARY of CHANGE

AR 215–8/AFI 34–211(I)
Army and Air Force Exchange Service Operations

This administrative revision, dated 7 January 2013-

- Corrects an administrative editing error to reflect new Army and Air Force Exchange Service internal management (para 1-9*b*).

- Makes administrative changes (throughout).

This major revision, dated 5 October 2012--

- Consolidates Army and Air Force Exchange Service funding policies (chap 3).

- Adds additional patronage categories for unlimited exchange privileges (table 7-1).

- Implements appropriated funding and support rules from DODI 1015.15, DODI 1330.09, DODI 1330.21, and Office of the Under Secretary of Defense (Personnel and Readiness) policy memorandum, subject: Funding Sources for Nonappropriated Fund Instrumentality (NAFI) Facilities, dated 4 December 2007 (throughout).

- Incorporates policy changes set forth in Army Directive 2012-15 and GO 2012-10 (throughout).

- Prescribes policies for providing Army and Air Force exchange services to the Army and the Air Force worldwide (throughout).

- Makes administrative changes (throughout).

Headquarters
Departments of the Army,
and the Air Force
Washington, DC
5 October 2012

*Army Regulation 215–8
AFI 34-211(I)

Effective 5 November 2012

Morale, Welfare, and Recreation

Army and Air Force Exchange Service Operations

By Order of the Secretary of the Army, and Air Force:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

EDEN J. MURRIE, Brig Gen, USAF
Director of Services
DCS, Manpower, Personnel and Services

History. This publication is an administrative revision.

Summary. This regulation implements DODI 1330.09 and DODI 1330.21, and it prescribes policies for providing exchange services to Army and Air Force activities worldwide. Also, this regulation implements the appropriated funding and/or support rules contained in DODI 1015.15.

Applicability. This regulation applies to the following, unless otherwise stated: the active Army, the Army National Guard/ Army National Guard of the United States, and the U.S. Army Reserve; and the active Air Force, Air National Guard, and Air Force Reserve.

Proponent and exception authority. The proponent of this regulation is the Assistant Chief of Staff for Installation Management. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions, in accordance with AR 11–2, but it does not identify key management controls that must be evaluated. These controls and management control checklists are contained in exchange operating procedures/Exchange Service regulations issued by the director and chief executive officer of the Army and Air Force Exchange Service.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Assistant Chief of Staff for Installation Management (DAIM–ISS), 600 Army Pentagon, Washington, DC 20310–0600.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Assistant Chief of Staff for Installation Management (DAIM–ISS), 600 Army Pentagon, Washington, DC 20310–0600.

Committee management. AR 15–1 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the U.S. Army Resources and Programs Agency, Department of the Army Committee Management Office (AARP–ZA), 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060–5527. Further, if it is determined that an established "group" identified within this regulation, later takes on the characteristics of a committee, as found in AR 15–1, then the proponent will follow all AR 15–1 requirements for establishing and continuing the group as a committee.

Distribution. This publication is available in electronic media only and is intended for command level C for the Army and F for the Air Force.

*This regulation supersedes AR 215–8, dated 30 July 2008.

Contents (Listed by paragraph and page number)

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Chapter 1
Purpose, Objectives, Organization, and Legal Status

1–1. Purpose
This regulation contains the operating policy of the Army and Air Force Exchange Service (AAFES). If inconsistencies exist between this regulation and other departmental regulations governing nonappropriated fund (NAF) activities, military exchanges, or the military resale system, this regulation will prevail with regard to AAFES operations, pending resolution by the appropriate official, if necessary.

1–2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Abbreviations and special terms
Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities
Responsibilities are listed in chapter 2.

1–5. Authority for Army and Air Force Exchange Service
The Secretary of Defense has vested in the Secretary of the Army and the Secretary of the Air Force all functions, powers, and duties relating to exchange activities within their respective military departments. This authority is held jointly and equally.

1–6. Army and Air Force Exchange Service mission
AAFES has a dual and enduring mission of providing quality merchandise and services to its customers at competitively low prices and of generating earnings which provide a dividend to support morale, welfare, and recreation (MWR) programs.

1–7. Objectives
The Secretary of the Army and the Secretary of the Air Force will—

a. Establish a centrally directed and jointly operated, worldwide, exchange system.

b. Establish uniform standards of service that meet the needs of the Army and the Air Force.

c. Use all available resources (facilities, funds, and personnel) to achieve an economical and efficient operation with a sound capital structure.

d. Use accepted business methods and uniform practices to meet mission requirements.

1–8. Dividend distribution
The AAFES Board of Directors (BOD) will declare dividends based on earnings, available funds, and required capital to the Army and the Air Force in support of their military MWR programs. Dividends are based on Army and Air Force distribution formulas. Any distributions to garrisons and installations are meant for an officially established and recognized military MWR nonappropriated fund instrumentality (NAFI).

1–9. Army and Air Force Exchange Service organization
a. AAFES is established as a Joint NAFI.

b. As a Joint NAFI, AAFES has a governing council known as a BOD. The composition of the AAFES BOD is detailed in AR 15–110/AFI 34–203(I). The AAFES director and chief executive officer, on behalf of the AAFES BOD, has primary interdepartmental responsibility for the worldwide administration and operation of AAFES activities. The director and chief executive officer will appoint the executive secretary for the AAFES BOD.

c. AAFES is categorized by DODI 1015.15 as a Program Group II, NAFI, Category C, revenue-generating program.

1–10. Command relationships, policy, and operating procedures
a. AAFES is a Joint NAFI of the Army and the Air Force and is under the jurisdiction of the Chief of Staff of the Army and the Chief of Staff of the Air Force. AAFES consists of all activities, personnel, property, and NAF activities that provide exchange services to the Army and the Air Force and other governmental agencies identified in this regulation.

b. The AAFES BOD directs AAFES and is responsible to the Secretary of the Army and the Secretary of the Air Force through their respective Chiefs of Staff.

c. The departmental staffs of the Services develop general policy governing AAFES. This policy is published in Joint Army regulations and Air Force instructions. The Army is responsible for developing, staffing, and administering

publication of AAFES policy. The AAFES director and chief executive officer issues exchange operating procedures (EOPs) and exchange service regulations.

1–11. Legal status

a. AAFES is an instrumentality of the United States. It is entitled to the immunities and privileges enjoyed by the Federal Government under the Constitution, federal statutes, federal legal precedents, established principles of international law, and international treaties and agreements.

b. AAFES is immune from direct state taxation and state laws and regulations that would interfere with its performance of its federal functions. Pursuant to Section 104, Title 4, United States Code (4 USC 104), Congress specifically permits the collection of state taxes on gasoline and other fuels sold through exchanges on U.S. military or other reservations, when such fuels are not for the exclusive use of the United States.

c. Suits by or against AAFES, or its individual activities, in tort or in contract, are suits by or against the United States. Claims, judgments, and compromise settlements of court actions against the United States, arising out of AAFES activities and sounding in tort, are payable solely out of AAFES funds. Judgments and compromise settlements of court actions against the United States, arising out of AAFES activities sounding in contract, will be obligated out of appropriated funds (APFs) of the United States, and AAFES will reimburse the United States.

d. As an instrumentality of the Federal Government, AAFES (and its employees) is bound by DOD 5500.07–R.

1–12. Freedom of Information Act requests

Freedom of Information Act (FOIA) requests for AAFES documents must be submitted in writing to the AAFES headquarters (HQ) at HQ, AAFES, General Counsel (FOIA), P.O. Box 650060, Dallas, TX 75265–0060. Requests will be processed in accordance with applicable federal laws and regulations. The servicing general counsel, or designee, is the Initial Denial Authority for FOIA requests.

Chapter 2
Responsibilities

2–1. Secretary of the Army and Secretary of the Air Force

The Secretary of the Army and the Secretary of the Air Force have oversight responsibility of the AAFES BOD and exchange operations.

2–2. Assistant Chief of Staff for Installation Management (Army) and Deputy Chief of Staff for Manpower, Personnel and Services (Air Force)

The following administrative agent responsibilities rests with the ACSIM (Army). The ACSIM, in coordination with the AF/A1 (Director of Services (AF/A1S)), will—

a. Oversee policy development and interpretation of AAFES operations.

b. Revise and update this regulation with necessary coordination among the Army, Air Force, and AAFES.

2–3. Army region directors of Installation Management Commands and commanders of Air Force major commands

Army region directors of IMCOMs and commanders of Air Force major commands (MAJCOMs) will—

a. Designate an appropriate staff element to act as liaison with the AAFES director and chief executive officer.

b. Authorize the establishment of exchanges at installations under their command, providing exchange service at locations other than military installations when doing so is consistent with departmental operational requirements.

c. Evaluate the responsiveness of services to customer needs and command requirements and adequacy of patronage controls.

d. Enforce departmental resale policy, including acting on disagreements between garrison and installation commanders and exchange general managers (GMs) that involve local MWR versus AAFES operation of resale and service outlets.

e. Provide logistical and administrative support, including—

(1) Granting proprietary approval for AAFES work on real property. (This authority may be delegated to a subordinate command.)

(2) Ensuring that AAFES-funded projects involving work on real property are reviewed for technical sufficiency.

f. Provide port handling and transportation for the movement of AAFES merchandise, supplies, and equipment from continental United States (CONUS) ports to overseas ports and return, and between overseas ports. (This will be provided on a non-reimbursable basis per applicable departmental regulations.)

g. Provide support services, such as transportation, facilities, operating personnel, security, medical, and finance support for exchange operations in contingency and wartime operations or emergencies. Develop contingency plans, in

conjunction with the AAFES director and chief executive officer for exchange support, during emergencies, mobilizations, and wartime operations.

h. In addition to the above, overseas Army IMCOM region directors and Air Force MAJCOM commanders will—

(1) Coordinate with the AAFES regional commander to ensure that exchange merchandise and services are included in agreements with the host country for reduced freight rates, customs clearances, and tax exemptions.

(2) Set hours of work, rates of pay, and employment benefits for non-U.S. citizens employed at AAFES activities (when they have the responsibility for those purposes), according to treaties, agreements, and laws of the host country and in consultation with designated AAFES representatives.

(3) Implement and enforce ration controls where needed or required.

2–4. Army garrison and/or Air Force installation commanders

In command organizations where the term garrison/installation commander is not applicable, Army commands, Army service component commands, direct reporting units, and Air Force MAJCOMs will assign the following responsibilities to the most appropriate command element. Garrison and installation commanders will—

a. Provide AAFES activities adequate and suitable buildings and facilities, and applicable services. Buildings may be provided from existing structures or construction of facilities (see chap 4). At remote and isolated locations, APF support is afforded the same level of support provided to category B, military MWR programs, as outlined in AR 215–1 and AFI 65–106.

b. Provide facilities and services on a non-reimbursable basis (see app B which outlines the APF support to various elements of expense).

c. Initiate installation support agreements. For administrative purposes only, DODI 4000.19 will be referenced for this process.

d. Include AAFES activities in command information programs and other community information services.

e. Provide the same logistical support for AAFES civilian personnel as is provided to other NAF employees, including DD Form 2574 (Armed Forces Exchange Services Identification and Privilege Card) and other appropriate forms of identification. This support will not differ materially from that enjoyed by civilian personnel of the classified federal service.

f. Provide essential logistical and administrative support for military personnel assigned to AAFES, including the administration of military justice.

g. Evaluate the responsiveness of AAFES to command requirements, convey results to exchange management and the GM, and recommend changes as appropriate.

h. Enforce local rules for dress, appearance, and uniform regulations for patrons using exchange facilities, consistent with applicable departmental regulations.

i. Liaise with exchange personnel.

j. Ensure that decisions based on needs, mission readiness, and community requirements (including recommended hours of operation) are coordinated with exchange management and the GM.

k. Enforce departmental resale policy (see chap 6 and applicable departmental regulations).

l. Act on proposals for garrison and installation entities and NAFIs to open resale and service outlets; and review periodically or as required by Army IMCOM, G–9 (Family and MWR Programs)/Air Force Services the continued need for these outlets (see para 6–14*e* of this regulation for guidance on AAFES operation of MWR sales operations on a management fee basis).

m. Review the need for new exchange concession, agency, and vending services, and review source lists per paragraph 9–1*d* of this regulation.

n. Advise the GM of all claim matters that affect exchange operations.

o. Issue identification documents, per applicable departmental regulations and criteria outlined in chapter 7, to persons authorized to purchase at exchanges, to enter exchanges for official business without the privilege of purchase, or to act as an agent of an authorized patron.

p. Ensure disciplinary actions, when appropriate, are taken against persons who violate patron privileges (see para 7–6). If abuse of privileges is found after appropriate review, garrison and installation commanders or other informed officials will take appropriate action, to include revoking or suspending exchange privileges.

q. Ensure the identification card issuing office maintains a current listing of locally reported lost and stolen identification cards and provides this to exchange management.

2–5. Director and Chief Executive Officer, Army and Air Force Exchange Service

The AAFES director and chief executive officer's position is filled by an NF–6. The civilian director and chief executive officer, AAFES will—

a. Manage all AAFES activities and issue EOPs and exchange service regulations to fulfill policies in this regulation and to establish new policies. Authority vested in the AAFES director and chief executive officer by this regulation may be delegated, unless stated otherwise.

b. Supervise AAFES personnel, property, and funds worldwide.

c. Operate, manage, and supervise exchange activities worldwide.

d. Submit an annual report, through the AAFES BOD, to the Secretary of the Army and the Secretary of the Air Force. This report will include—

(1) An annual audit statement issued by a certified public accountant (CPA).

(2) A summary of exchange operations for the prior fiscal year.

e. Provide clearance for personnel within a specific area of control for access to classified Department of Defense (DOD) information, according to applicable departmental regulations.

f. Plan for and support Army and Air Force mobilization, contingency, and wartime operations or other emergency situations within the capabilities and limitations of AAFES.

g. Prescribe uniform check cashing procedures and controls, procedures for enforcing patronage eligibility and identification control, and establish stock assortment criteria for all categories of retail merchandise.

h. Act on requests or appeals from military commanders to open exchange activities when GMs and region senior vice presidents or overseas region commanders have declined requested services.

i. Administer the AAFES capital expenditure program as directed by the AAFES BOD.

j. Report, annually, to DOD on the customer satisfaction index and the results of standardized market basket price survey.

k. Under authority granted, suspend or remove privileges from patrons who abuse catalog and Internet ordering systems controlled and managed by AAFES (see para 7–6*e*).

2–6. Deputy Director, Army and Air Force Exchange Service

The deputy director's position is filled by a general officer alternating between the Army and the Air Force. The deputy director will assist the director and chief executive officer, AAFES in the overall operation of AAFES.

2–7. Chief Operating Officer, Army and Air Force Exchange Service

The chief operating officer, AAFES, will—

a. Assist the director and chief executive officer, AAFES in directing the overall operation of AAFES.

b. Supervise operational elements.

c. Directly support all AAFES operations worldwide.

2–8. Overseas region commanders, Army and Air Force Exchange Service

Overseas region commanders will direct all operational aspects of AAFES activities assigned to their area of responsibility.

2–9. Region senior vice presidents, Army and Air Force Exchange Service

Region senior vice presidents will direct overall operations of AAFES facilities within their assigned geographical areas.

2–10. Headquarters staff, Army and Air Force Exchange Service

The AAFES HQ staff will formulate and execute procedures to implement the operating policy in this regulation and EOPs and exchange service regulations as issued by the AAFES director and chief executive officer. The AAFES HQ staff includes senior vice presidents, vice presidents, division directors, AAFES chief of staff, and special staff directors (for example, inspector general (IG), general counsel, Audit Agency, and Equal Employment Opportunity (EEO)).

2–11. General managers, Army and Air Force Exchange Service

GMs, AAFES will—

a. Manage all exchange operations and administrative support activities for exchanges in their assigned geographical areas.

b. Ensure the primacy of AAFES as the source of all non-food merchandise and patron services on military installations, except where military and civilian MWR, lodging, and other NAFIs (for example, museums, veterinary offices, and prisons) engage in resale that is directly related to their programs.

c. Enter into agreements with garrison and installation commanders to manage designated sales operations.

d. Set hours of operation in coordination with the garrison and installation commanders.

e. Ensure alleged crimes are reported to loss prevention personnel for coordination with the appropriate law enforcement agency; provost marshal; U.S. Army Criminal Investigation Command element; or Air Force Office of Special Investigations.

Chapter 3
Funding

3–1. Funding of Army and Air Force Exchange Service activities

As a Program Group II, NAFI, Category C, revenue-generating activity, AAFES will use its revenue-generating capability to fund ongoing operations and capital improvement projects. Within the limits established by law and DODI 1015.15, AAFES can be provided limited APF support as outlined below and in appendix B of this regulation.

3–2. Appropriated funds

a. The basic financial standard for AAFES programs is to use APFs to fund 100 percent of costs for which it is authorized. Appropriated funding will be used to the maximum extent possible to fund those elements of expense authorized by DODI 1015.15, paragraphs 6.2 and 6.3 and enclosures 4 and 5; and Office of the Under Secretary of Defense (Personnel and Readiness) memorandum, subject: Funding Sources for Nonappropriated Fund Instrumentality (NAFI) Facilities, dated 4 December 2007 (until it is incorporated into the DODI 1015.15). Details are summarized in appendix B of this regulation.

b. AAFES facility construction funding.

(1) Appropriations must be used for AAFES facilities modernization and construction (minor or major) for—

(a) Exchange facilities required in areas of military conflict, wartime deployments, and in support of contingency, humanitarian, and peacekeeping operations.

(b) Exchange facilities required as integral parts of air terminal, hospital, housing, or other military construction projects.

(c) Exchange-operated laundries, dry cleaning plants, bakeries, dairies, or similar facilities operated by AAFES in support of military conflict, wartime deployments, and in support of contingency, humanitarian, and peacekeeping operations.

(d) Administrative, storage, and maintenance facilities outside the United States.

(2) Appropriations must be used for major and minor facility construction determined by the Army/Air Force to

(a) Establish, activate, or expand a military installation, including base realignment and closures (BRAC) and global restationing requirements. Expansion must be the result of a mission change or influx of new units or systems and result in a 25 percent increase in authorized and assigned personnel strength within a 2–year time span.

(b) Relocate facilities for convenience of the government.

(c) Replace facilities denied by country-to-country agreements.

(d) Restore facilities and improvements destroyed by acts of nature, fire, or terrorism.

(e) Incorporate antiterrorism and force protection measures required under DODI 2000.16.

(f) Correct deficiencies in life, safety, and force protection measures.

(g) Meet Americans with Disabilities Act of 1990 requirements.

c. APFs will be used for heating, ventilation, and air conditioning systems capitalized and transferred as part of a capital improvement, repair, or renovation project that is classified as real property installed and building equipment.

d. APFs may be used to purchase commercially-owned buildings only to the extent authorized by Congress.

e. The policy on the funding of BRAC sites and use of the BRAC reserve account is outlined in DODI 1015.15, paragraph 6.12.

3–3. Use of Army and Air Force Exchange Service funds

a. AAFES NAFs will be used in accordance with appendix B of this regulation and DODI 1015.15, paragraphs 6.2 and 6.3 and enclosures 4 and 5.

b. AAFES NAFs will not be used for authorized APF expenditures unless authorized APFs are not available. Certification of non-availability of APFs must be obtained from the respective Service's responsible resource office. The above will not apply where this regulation prohibits the use of NAFs. NAFs will not be used instead of authorized APF support as a matter of convenience.

c. AAFES funds may be used for—

(1) New construction of facilities (including purchase and erection of pre-engineered or portable buildings), subject to prior approval by the AAFES director and chief executive officer or AAFES BOD, as appropriate (see app B for APF and NAF authorizations).

(2) Access roads, curbing, and utilities (when appropriated funds are not available), which serve only AAFES facilities.

(3) Relocation of utility main lines running through the site and the removal of existing improvements below the 6–inch level as negotiated with the garrison and installation.

(4) Alteration, modification, deletion, or extension of existing facilities (including buildings and outside improvements such as parking lots and utility systems) when APFs are not available for utility relocation to make them suitable for exchange use.

(5) Acquisition and installation of exchange operating equipment.

(6) Heating and air conditioning beyond what is provided by the installation facility and base engineer, in accordance with appendix B. Heating and air conditioning purchased with NAFs will normally consist of only those systems which are not classified as real property installed and building equipment (self-contained, pre-packaged, window-installed, and like-type units).

(7) Work within the interiors of buildings, if that work is required solely for purposes peculiar to exchange operations.

(8) The sustainment, restoration, and modernization of AAFES structures to which AAFES holds title is funded with exchange funds. This includes interior finish, such as paint, floors, ceilings, special lighting, and building modifications and alterations solely for purposes directly applicable to exchange operations.

(9) Leasing of facilities on an exception basis only.

(a) The AAFES director and chief executive officer approves exceptions up to $199,999 annually.

(b) With AAFES BOD approval, AAFES may request a review and approval by the Assistant Secretary of the Army (Manpower and Reserve Affairs) or the Assistant Secretary of the Air Force (Manpower and Reserve Affairs) concerned before contract award for lease amounts with an annual cost of $200,000 to $500,000.

(c) The Assistant Secretary of the Army (Manpower and Reserve Affairs) or the Assistant Secretary of the Air Force (Manpower and Reserve Affairs) reviews and approves lease amounts with an annual cost of $500,000 to $1 million before contract award.

(d) Leases with an annual cost of $1 million or more require AAFES to comply with the land moratorium requirement contained in DODI 4165.71.

(e) Exceptions are considered in CONUS, Alaska, Hawaii, and U.S. territories when existing buildings under military control are not available or are inadequate. Exceptions are considered in all other locations when existing buildings under military control are inadequate and APFs are not available within the timeframe required.

(10) Services obtained through government sources are as follows:

(a) AAFES may obtain construction services or architectural and engineering services through other government sources on a reimbursable basis.

(b) AAFES funds may be certified and made available for payment to other government sources on an individual basis or through a bulk funding method where funds are certified in advance and made available on an as needed basis.

(11) Purchase of commercially owned buildings located on government property.

(12) When garrisons and installations cannot provide architectural and engineering services without adding additional manpower authorizations, AAFES will use AAFES funds to perform the work, or contract for it, and add the cost to the project (see table B–1).

3–4. Deviation from funding policy

a. Unique situations or exigencies that need immediate or more specific attention may require deviation or exception to the basic funding policy outlined above. Any deviations or exceptions to use AAFES NAFs in lieu of appropriations, must be approved by the Under Secretary of Defense for Personnel and Readiness in coordination with the Under Secretary of Defense (Comptroller) on a case-by-case basis.

b. Deviations or exceptions will be submitted to the Army or the Air Force, as applicable, at the following address:

(1) Army: Assistant Chief of Staff for Installation Management (DAIM–ISS), 600 Army Pentagon, Washington, DC 20310–0600.

(2) Air Force: Deputy Chief of Staff for Manpower, Personnel and Services, Director of Services (AF/A1S), 1770 Air Force Pentagon, Washington, DC 20330–1770.

c. The above Army or Air Force organizations must satisfy the following Office of the Secretary of Defense criteria:

(1) The project is included in the military construction (major and minor construction) or APF modernization budget submission to the Under Secretary of Defense (Comptroller).

(2) The project was not included in the President's budget submission to Congress or was not approved by Congress.

(3) Failure to build the facility will seriously impact the quality of life of military personnel and their families.

(4) The Army or the Air Force certifies that the project is of higher priority than all other non-funded NAF construction (major and minor) and modernization requirements.

(5) The Service's headquarters concerned and AAFES will endorse the use of AAFES NAFs.

Chapter 4
Facilities and Equipment

4–1. Scope
This chapter governs AAFES expenditures related to facilities, equipment, and sustainment, restoration, and modernization of facilities and equipment. When local circumstances warrant exception to the provisions of this chapter, the AAFES director and chief executive officer may authorize alternatives if consistent with applicable departmental regulations.

4–2. Construction project approval and reporting
AAFES-funded projects are designed, constructed, and approved according to the standards set by DOD, Department of the Army (DA), Department of the Air Force, and relevant AAFES EOPs and exchange service regulations. All AAFES project approval authority and the authority to obligate AAFES funds delegated within AAFES emanates from the AAFES BOD.

4–3. Reporting construction projects
a. The AAFES director and chief executive officer reports annually to the Services and DOD on construction projects that have new construction costs exceeding $750,000 and—

(1) Are planned for construction award within 1 year following the year of DOD and Congressional release.

(2) Were previously reported, but have not been placed under contract or started, during the planned period noted in paragraph (1), above.

b. The AAFES director and chief executive officer will resubmit projects previously approved by the DOD when—

(1) The scope of the approved new construction changes by more than 10 percent.

(2) The amount of the approved construction award amount increases by more than 25 percent.

c. Until DOD advises the AAFES director and chief executive officer that reporting and approval requirements are satisfied, AAFES will not place any project requiring reporting to DOD under construction contract or start construction.

4–4. New construction, alterations, and additions by the private sector
a. AAFES will forward projects involving the erection of structures by private individuals or commercial concerns (see DODI 1015.13) for facilities/activities traditionally associated with AAFES (see DODI 1330.21) through the garrison and installation to the appropriate IMCOM region director (Army)/MAJCOM commander (Air Force) and Service Secretary for approval prior to submitting to the AAFES BOD.

b. Removal of structures and buildings erected by the private sector are subject to the provisions of applicable departmental regulations.

4–5. Army and Air Force Exchange Service contracting for appropriated funds or combined appropriated funds, and Army and Air Force Exchange Service projects
When APFs are used in a construction project that is managed and contracted by AAFES, both the APF and NAF funding sources and related scopes of work will retain their separate identity in the contract documents and in their respective records of account. Projects involving APFs will be executed only upon completion of a memorandum of agreement (MOA) between AAFES and the APF agency and funding source, and notification to AAFES that the availability of APFs has been certified.

4–6. Titles to structures and installed property and equipment
a. Government title. Structures other than portable and relocatable buildings erected with proper authority on military installations and paid for from AAFES funds or erected by the private sector pursuant to a contract with AAFES, become the property of the government and are carried on records of DA or Department of the Air Force, as appropriate, in accordance with existing departmental regulations. Military installations accept newly erected structures, extension, alteration, and improvement of government facilities paid for from AAFES funds upon completion of final inspection and receipt of transfer documents. This includes real property installed and building equipment.

b. Army and Air Force Exchange Service title. AAFES retains title to—

(1) Facilities acquired with AAFES funds that are not located on active duty, Guard, or Reserve military installations.

(2) Portable and relocatable buildings acquired and erected solely with AAFES funds.

(3) Portable buildings erected under contract. Private individuals or commercial concerns may retain title to a portable building erected by them under contract, with prior approval of the AAFES director and chief executive officer.

(4) Accountability for all installed property purchased wholly with AAFES funds remain with AAFES, where the property is movable or severable without causing substantial physical damage or injury to the structure or land. The

determination as to moveability or severability of the installed property will be accomplished in coordination with the facilities engineer or base civil engineer.

(5) Installed equipment purchased wholly with AAFES funds, is attached to or integrated with any public structure or land, and cannot be separated from that structure or land. When it is desired that title to and accountability for the equipment be retained by AAFES, a written permit will be obtained from the garrison and installation commanders identifying the property and the authority for retention of title and accountability by AAFES for that property. The facility or base civil engineer will be furnished with a copy of the permit. Equipment covered by the permit may be removed by AAFES, provided that the public structure or land to which the property was affixed is restored by AAFES to the condition existing at the time the property was originally affixed to it, fair wear and tear excepted.

c. Unit titles. Units to which AAFES retains title will be maintained by AAFES.

4–7. Use of Army and Air Force Exchange Service facilities

Structures erected with AAFES funds or private funds (for AAFES use) will not be used for other than AAFES purposes without prior approval by the AAFES director and chief executive officer and the department concerned.

a. Improvements. If another NAF agency takes over a facility improved with AAFES funds, that agency will normally reimburse AAFES for the un-depreciated value of AAFES-funded construction and installed property.

b. New facilities. Exchanges established on state-operated installation will be operated and controlled by AAFES. A memorandum of understanding (MOU) will be established providing the authority for continued use of facilities improved or erected with AAFES funds. The MOU will contain language that specifically states AAFES will agree to release a facility, improved or erected with AAFES funds when the installation reimburses AAFES for the un-depreciated value of the facility improvement or construction. Where AAFES has made a substantial investment, relocation will not be required unless an alternate and suitable facility is provided by the garrison and installation. Facilities erected with AAFES funds cannot be used for purposes other than AAFES without prior approval by the AAFES director.

4–8. Smoke-free facilities

The policies on smoke-free facilities are contained in the respective Army and Air Force regulations and instructions.

Chapter 5
Personnel

5–1. Policies and practices

a. AAFES civilian personnel are Federal employees of an instrumentality of the United States within DOD. Because they are compensated from NAFs, they are distinguished from other civilian employees of the Armed Services who are compensated from APFs. As such, they are removed from the provisions of laws or regulations administered by the U.S. Office of Personnel Management, except in the case of wage fixing for prevailing-rate employees covered under the provisions of Public Law (PL) 92–392 and application of the Fair Labor Standards Act (as amended by PL 93–259).

b. Personnel policy and practices are subject to DOD policy governing NAF personnel (DODI 1400.25, Volume 1401) and applicable statutes, union collective bargaining agreements, and guidance from the AAFES BOD.

c. The AAFES director and chief executive officer is expressly delegated the authority to make those decisions and take those actions which are the responsibilities of the head of a DOD component with respect to AAFES NAF civilian personnel policy covered in DODI 1400.25, Volume 1401. This delegation is subject to, and must be exercised in accordance with, higher level directives and policy as promulgated within the DOD and applicable collective bargaining obligations.

d. Practices apply to all AAFES employees in the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and the territories and possessions of the United States; all U.S. citizens and U.S. national employees worldwide; and all U.S. permanent resident alien employees worldwide.

e. AAFES employees are advised of policies, programs, and procedures in writing. This includes, but is not limited to—

(1) Manpower requirements worldwide, allocation of grades and/or bands of positions, and pay and compensation practices.

(2) Employee benefits programs.

(3) Employee leave practices.

(4) Grievance rights and responsibilities, adverse action and administrative appeals process, and business-based action practices.

(5) Professional development and training requirements.

5–2. Overseas entitlements

When available, AAFES employees in overseas areas recruited from the United States, receive government quarters and family housing entitlements and allowances subject to controls in DODI 1400.25, Volume 1412, under applicable federal law. These employees and their dependents have access to the same medical health services provided APF personnel and access to Department of Defense Dependent Schools under the provisions of applicable federal law. United States citizens receive allowances and differentials as defined by federal regulations.

5–3. Employment of United States citizens in foreign countries

United States citizens and U.S. nationals will be employed in a pay system authorized by DODI 1400.25, Volume 1405 for DOD NAF employees. On the prior approval of the AAFES director and chief executive officer, in special circumstances, these employees may be hired under a special contract of employment.

5–4. Travel and transportation

a. AAFES civilian employees who are authorized payment of travel and transportation expenses shall be paid in accordance with the DOD Joint Travel Regulations, Volume 2. Expenses for essential travel and transportation of AAFES employees, their authorized Family members, and household goods and effects are not to exceed those prescribed in DOD Joint Travel Regulations, Volume 2, and are in accordance with implementing instructions issued by the AAFES director and chief executive officer.

b. AAFES employees do not authorize their own official travel. Official travel will be authorized by ordering-issuing officials designated, in writing, by the AAFES director and chief executive officer.

5–5. Executive management program

a. The executive management program exists to fulfill AAFES continuing requirement for executive employees who are readily available to meet worldwide short-term and long-term executive personnel requirements. The AAFES director and chief executive officer will administer the executive management program worldwide, pursuant to written rules and procedures, published by the director and chief executive officer, under the guidance of the AAFES BOD.

b. The AAFES director and chief executive officer will periodically review and establish, as necessary, the number and grade level of positions to be included in the executive management program. Benefits established by the AAFES director and chief executive officer must be uniform for all executive management program employees.

c. Employees participating in the executive management program must sign a written agreement (mobility statement) obligating them to accept transfer or assignment worldwide within 30 days. Temporary exceptions may be granted by the AAFES director and chief executive officer.

d. The AAFES director and chief executive officer or designee, may withdraw executive management program status for—

(1) Failure to fulfill executive management program obligations as per written agreement with AAFES.

(2) Unsatisfactory performance.

(3) Misconduct of a disciplinary nature, on or off the job.

e. Benefits to executive management program employees are as follows:

(1) Retention priority as a result of business-based action.

(2) Longer notice periods based on length of service in case of certain separations.

(3) Triple indemnity accidental death and supplementary life insurance benefits under the AAFES Group Insurance Plan.

(4) Supplemental retirement benefits and retention of personal grade, regardless of assignment.

5–6. Grievances, adverse actions, and administrative appeals

a. Principles of discipline. Principles of discipline are as follows:

(1) Maintenance of discipline will be achieved, to the maximum extent possible, through cooperation, fairness, good supervisory practices, and adherence to reasonable standards of conduct.

(2) Supervisors should, when appropriate, admonish and counsel employees as the first step in constructive discipline to prevent breaches of regulation and standards of conduct and to prevent repetition of offenses.

(3) Reasonable and timely penalties will be imposed on employees whose conduct is detrimental to the efficiency of AAFES.

(4) Responsible judgment must be exercised in selecting among the variety of disciplinary penalties that may be imposed. The following must be considered in reaching a decision on the action to be taken:

(a) The seriousness of the offense.

(b) The past record of the employee.

(c) The circumstances contributing to the offense.

(d) The probable effectiveness of the penalty in stimulating improvement.

(e) The reasonableness of the penalty.

(f) The time period since a previous-like offense.

(g) The influence of the penalty on the morale of other employees.

(5) There may be factors and considerations other than those mentioned above that are pertinent to the selection of the penalty. The action selected should be reasonable and of such nature as to promote the efficiency of AAFES.

(6) Disciplinary action and official investigation of an incident should be initiated on a timely basis.

(7) If an employee has been disciplined for an offense, no further disciplinary action will be proposed against that employee for the same offense.

(8) When management considers that formal disciplinary action may be required to correct misconduct on the part of a subordinate employee, management should obtain all available information concerning the alleged misconduct and discuss the incident with the employee to—

(a) Ensure all the relevant facts are known to both parties.

(b) Afford the employee the opportunity to explain the basis for their actions.

(c) Advise the employee that disciplinary action is under consideration.

b. Grievances. The AAFES director and chief executive officer will develop a prompt and equitable grievance process and will issue instructions and procedures to administer this process worldwide, subject to the requirements of DOD 1401.01–M, in circumstances where a labor organization has exclusive recognition.

c. Adverse actions. An adverse action may be either a non-disciplinary or a disciplinary-type action.

(1) Non-disciplinary actions are administrative actions taken by management that do not fall within the definition of a disciplinary action, but cause dissatisfaction with the employee. These actions include, but are not limited to—

(a) Counseling.

(b) Warning letter.

(c) Downgrade or separation for unsatisfactory performance.

(d) Downgrade or separation for business based action.

(e) Downgrade or reduction in compensation based on reorganization, reallocation, or conversion.

(f) Administrative separation (for disqualification; during probationary period; for disability; business based action or death; on expiration of temporary employment; based upon resignation, abandonment of position or declination of transfer; for retirement; from leave without pay or intermittent employment; or for unsatisfactory performance).

(2) Disciplinary actions are taken by management as a result of an employee's conduct, action, or lack of action when action should have been taken. Authorized disciplinary actions include—

(a) Oral reprimand.

(b) Written reprimand.

(c) Suspension.

(d) Disciplinary downgrade.

(e) Disciplinary pay reduction.

(f) Separation for cause.

(g) Withdrawal of executive management program (except for declination of transfer, which is non-disciplinary).

(3) Disciplinary actions are based on the following:

(a) Conduct on the job involving insubordination; violation of laws, regulations, rules, or policies/procedures; or other conduct incompatible with maximum employee efficiency.

(b) Conduct off the job which reflects discredit on AAFES, interferes with job performance, or involves violation of laws.

(c) Activities and conduct which AAFES personnel are prohibited from engaging.

d. Advance notice of an adverse action. When required by EOP 15–10, an advance notice of an adverse action will be in writing by the management official and will identify the specific adverse action with the effective date and details of the adverse action. The employee also will be advised of their right to reply, to whom to reply, and time limit for a response, and that consideration would be given to their response before a final decision is made. Advance notice is not required for counseling entries, warning periods, oral or written reprimands, or for separations for resignation, declination of transfer, retirement, from temporary or intermittent employment, from the probationary period unless for cause or for abandonment of position.

e. Employee response to notice of adverse action. The employee may respond orally or in writing to the management official who provided the advance notice of an adverse action. The employee may provide documentation and may be accompanied by a representative. Any expenses involved in refuting the advance notice of an adverse action are borne by the employee. The response does not include the right to a hearing with testimony from witnesses, but is an opportunity to refute the advance notice.

f. Final decision. After consideration of an employee response to the advance notice of adverse action, a final decision will be made. The final decision will be in writing and will reference the advance notice of adverse action; it will advise the employee of consideration of their response, if a response is received; state the action to be taken and

the basis for the action and effective date. The employee will be provided the final decision and advised of the right to appeal the final decision and the time limit for a response.

g. Appeal of final decision. When required by EOP 15–10, the employee may appeal the final decision to the appellate authority. The employee will be provided with the procedures for appeals. The appeal may contain relevant documents and must state the basis for the appeal in sufficient detail. Counseling entries, warning periods, and separations for resignation, declination of transfer, disqualification, retirement, temporary or intermittent employment, probationary period unless for cause, abandonment of position, or for leave without pay are not appealable. Oral and written reprimands are grievable, but are not appealable unless issued by a principle management official.

h. Appellate authority determination. The appellate authority is the director and chief executive officer, AAFES, or designee. However, if the director and chief executive officer, AAFES is the management official who made the final decision, the appellate authority is the chairperson of the AAFES BOD. The appellate authority's determination on the final decision will be rendered after securing the legal advice of the applicable general counsel. The written determination will include a statement that the determination by the appellate authority is final and not subject to further appeal or review. Copies of the determination will be provided applicable officials.

i. Exchange Operating Procedure 15–10. Chapter 6 of EOP 15–10 outlines the above process in detail. It covers the procedures for all adverse actions, time limits for responses, issuing authorities, AAFES grievance procedures, and AAFES adverse action appeals for nonbargaining unit employees.

5–7. Labor management relations

a. With regard to labor management relations, the AAFES director and chief executive officer makes all decisions and takes actions that are the responsibility of the head of a DOD component. Title 5, USC 7101 and implementing DODIs apply to AAFES labor-management policies (see DODI 1400.25).

b. AAFES recognizes the employee's right to form, join, or assist any labor organization or to refrain from such activity. This right is freely given without fear of penalty or reprisal.

5–8. Employee associations

The voluntary organization of employee associates to provide recreational, welfare, and social activities for its membership is authorized and regulated under DODI 1000.15 (see also AR 210–22 and AFI 34–223). Support and relations are regulated under DOD 5500.07–R.

5–9. Memberships in organizations

a. Memberships paid from AAFES funds are limited to those necessary for liaison with local civic, service, and business associations of sufficient prestige to make participation desirable from a community relations or professional development viewpoint. Funding of memberships may be authorized by the responsible HQ, AAFES staff director.

b. Memberships are in the name of AAFES or an element of the AAFES organization, not an AAFES employee.

c. All such membership activities must be in accordance with the requirements of the DOD Joint Ethics Regulation.

5–10. Equal Employment Opportunity programs

The AAFES director and chief executive officer will administer EEO programs for civilian applicants and employees of AAFES.

5–11. Law suits against individual employees

An AAFES employee sued for acts or omissions by the employee within the scope of employment is entitled to have the U.S. Government substituted as the party defendant in most cases. Where this is not the case, the employee may request representation by the Department of Justice in accordance with applicable departmental regulations. Such requests are forwarded through the AAFES general counsel.

5–12. Fiduciary responsibilities

Military personnel and AAFES employees paid with NAFs and APFs have an individual fiduciary responsibility for properly using AAFES resources and for preventing waste, loss, mismanagement, or unauthorized use of such funds.

a. Reporting of suspected violations at the lowest organization level is encouraged. However, reports may be made to senior management, IGs, or to the DOD hotline.

b. According to 10 USC 2783, AAFES NAF personnel who violate regulations governing the management and use of NAFs are subject to the same penalties as under federal laws that govern the misuse of appropriations by APF personnel. Violations by military personnel are punishable under the Uniform Code of Military Justice.

c. The use of APF shall be consistent with the provisions of 31 USC 1301, which requires that funds be used only for the purposes for which they were appropriated. Military personnel and AAFES employees, paid with NAFs and APF, are subject to the limitations, exceptions, and penalties governing the use of APF as contained in 31 USC Chapter 13.

5–13. Security clearance and investigations for assigned personnel

a. Army or Air Force regulations and instructions concerning NAF civilian personnel security investigations and adjudications apply to AAFES employees at Army and Air Force installations, respectively.

b. Authority and procedures governing security investigations and clearances of assigned AAFES personnel will be in accordance with AR 380–67, AFI 31–501, and DOD 5200.2–R. The AAFES director and chief executive officer has the authority to identify security clearance jurisdiction over HQ, AAFES and its subordinate activities. The Services clearance adjudication facilities shall adjudicate security clearances for assigned AAFES personnel who are under their jurisdiction or installations. The determination whether an individual is qualified to fill a designated position of trust will be adjudicated by AAFES loss prevention, unless otherwise identified by regulatory guidance.

5–14. Falsification of records

a. Any employee who, for the purpose of concealing or misrepresenting a material fact, willfully or unlawfully alters, falsifies, or destroys, or causes to be altered, falsified, or destroyed official AAFES or other government documents, records, or files, regardless of motive, is subject to separation for cause or other disciplinary action.

b. Any employee who knowingly and willfully prices or sells, or causes to be priced or sold, merchandise or services contrary to the established sale price, regardless of motive, is subject to separation for cause or other disciplinary action.

5–15. Employees to furnish required reports and information

It is each employee's duty to report and furnish information, whether favorable or unfavorable, regarding matters of official interest (as defined in glossary) as may be lawfully required by competent authority, including supervisors and investigative officials. Refusal to furnish required reports or information, or deliberate concealment or misrepresentation of material facts in a report or statement, will constitute grounds for separation for cause or other disciplinary action.

5–16. Arrest, indictment, or conviction for criminal offenses

a. Conviction of a felony, and in some instances of a lesser crime, may constitute a basis for disciplinary action, including termination of employment. The mere fact of an arrest or indictment on a charge of a criminal offense is not a basis for disciplinary action. However, the alleged misconduct itself, stated in specific terms, may be the basis for disciplinary action, regardless of any arrest, indictment, conviction, or even acquittal in judicial proceedings. Disciplinary action on charges of misconduct or delinquency need not wait upon a conviction of an employee for a criminal offense. Likewise, an employee's acquittal on an indictment charging him with committing a criminal offense does not invalidate prior disciplinary action or prohibit subsequent disciplinary action for the cause that resulted in the arrest or indictment, as long as the disciplinary action is independent of the judicial proceedings and is factually supported by available evidence.

b. Any employee arrested or indicted for any offense, including driving while intoxicated and vehicular homicide or related charges, but excluding minor traffic violations, will report the arrest or indictment to the human resources manager whether or not the conduct resulting in the arrest or indictment occurs on or off duty.

c. Refusal or failure of an employee to make a report of arrest or indictment will constitute grounds for separation for cause or other disciplinary action.

5–17. Separation for cause

An employee may be separated for cause. In separations involving suspected employee theft, pilferage, or damage and loss of AAFES property due to the employee's negligence, final pay may be withheld pending a determination of the employee's liability.

5–18. Separation based on resignation

a. Separate an employee based on resignation per the following:

(1) The employee will submit a written resignation to their supervisor.

(2) The employee should give the reason for resigning and the effective date.

(3) The employee should give AAFES notice when possible. If notice is not given, a notation will be made on the employee's communication record. The notation will indicate the employee's reasons for not giving notice and whether the notice was acceptable to AAFES.

b. The employee will be separated on the date indicated in the written resignation unless the employee is separated per another paragraph (for example, para 5–17, above) prior to this date.

c. A copy of the personnel request separating the employee based on resignation will be furnished to the employee. No advance notice of separation based on resignation will be given.

d. An employee who has received an advance notice of separation for cause or unsatisfactory performance may resign from employment to avoid separation prior to the proposed effective date of separation. The resignation request will note that the employee resigned to avoid separation for cause or unsatisfactory performance, as appropriate. In

cases where actual or suspected employee theft or damage to AAFES property is involved, the employee's final pay may be withheld pending a determination of the employees liability.

Chapter 6
Exchange Operations

Section I
Exchange Establishment

6–1. Exchange service establishment

a. An exchange operation may be established at any federal or state installation and other locations where DOD military personnel are assigned. All AAFES resale outlets (including contractor operated) will be operated and controlled either directly or indirectly by AAFES, regardless of location. Criteria to consider when establishing an exchange include, but are not limited to—

(1) Estimated number of assigned and present active duty military personnel located within a 25–mile radius of the proposed exchange outlet.

(2) Estimated number of eligible Family members residing in the area.

(3) Estimated number of other eligible patrons (for example, retirees) residing in the area.

(4) Location and distance to the nearest DOD installation with an exchange outlet.

(5) Economic viability to maintain an exchange.

(6) Mission requirements.

(7) Military resale requirements.

b. At state-operated installations, an MOA will be executed between a designee of the State Adjutant General's office and the supporting GM, AAFES. Requests to establish an exchange will include the following:

(1) Number of assigned and present active duty military personnel (include National Guard and Reserve personnel on continuous active duty in excess of 179 days) located within a 25–mile radius of the proposed exchange outlet.

(2) Number of eligible Family members residing in the area.

(3) Estimated number of other eligible exchange patrons (retirees) residing in the area.

(4) Name, location, and distance in miles to the nearest DOD installation with an exchange outlet.

(5) The written opinion of the AAFES region director as to the economic feasibility of the proposed outlet.

(6) A statement by the appropriate Reserve Component commander that the site available for the proposed exchange facility is excess to mission requirements.

(7) A written statement by the State Adjutant General that state and local taxing authorities interpose no objection to the sale of exchange merchandise to authorized patrons free of taxes. (This guidance is applicable to state-operated installations only.)

c. Requests for permanent exchange outlets at National Guard and Reserve installations will be processed as follows:

(1) Proposed outlets at Reserve installations will be submitted through command channels to the responsible military department at the following address:

(a) Assistant Chief of Staff for Installation Management (DAIM–ISS), 600 Army Pentagon, Washington, DC 20310–0600.

(b) Deputy Chief of Staff for Manpower, Personnel and Services, Director of Services (AF/A1S), 1770 AF Pentagon, Washington, DC 20330–1770.

(2) Requests for proposed outlets at state-operated Army and Air National Guard installations will be submitted through normal command channels to Chief, National Guard Bureau (NGB–ZA), 2500 Army Pentagon, Washington, DC 20310–0500.

(3) Each request will be supported by a proposed agreement and must—

(a) Be executed by the State Adjutant General concerned and HQ, AAFES representative or designee.

(b) Include specific provisions for financing capital investment and for exercising patronage control.

(4) The National Guard Bureau, in its endorsement, will evaluate the need for the proposed exchange outlet. The National Guard Bureau will then forward the request, together with the agreement, signed by the State Adjutant General, to the appropriate address in paragraph (1), above. Approvals will be granted only by the military departments concerned, subject to the signing of the agreement by HQ, AAFES.

d. Exchanges permanently established at Army and Air National Guard and Army and Air Force Reserve sites will be evaluated biennially by HQ, AAFES to ensure that they continue to satisfy a valid resale requirement in a cost effective manner. The evaluation is applicable to all off-base exchange outlets (outlets not located on active DOD military installations), notwithstanding that these outlets may be branches or annexes of main exchanges.

e. HQ, AAFES will provide the results of the biennial evaluation to the responsible command exercising command and control over those Army and Air Force National Guard and Reserve installations having exchange outlets.

f. The responsible command will review the updated listing of Army and Air Force National Guard and Reserve exchange outlets, as reported in the AAFES evaluation, and forward the report with appropriate comment, for information purposes to the military department concerned (see addressees in *c*, above).

g. The evaluation cycle is set for 1 July each even numbered year, with a reporting date to the respective military departments no later than 15 August.

h. The AAFES director and chief executive officer determines whether a new exchange will be operated as a separate outlet, that is, an Army and Air Force Exchange Service Imprest Fund Activity (AIFA) or other type of operation (see para 6–2).

i. A sample format of an MOA between the State Adjutant General's office and the supporting GM, AAFES is at figure 6–1.

DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

MEMORANDUM OF AGREEMENT

BETWEEN

ADJUTANT GENERAL OF THE STATE OF (MAINE)

AND

THE ARMY AND AIR FORCE EXCHANGE SERVICE

SUBJECT: Operation of an Exchange Facility for the National Guard at (Site)

1. This memorandum of agreement (MOA) is entered into by the above parties for the operation of an exchange facility at (garrison/installation). The parties to this agreement agree to the conditions contained in this agreement.

2. The Army and Air Force Exchange Service (AAFES) has determined that the operation of an exchange activity at (garrison/installation) is economically feasible, and the State has determined that the establishment of the exchange facility will not create unfair competition with local commercial interests.

3. The State agrees to provide a suitable (as determined by the AAFES engineering representatives) facility for the operation of an exchange to include retail, storage, and administrative space. The State agrees to finance any capital investment necessary to renovate or convert such facility into a suitable exchange activity.

4. The AAFES agrees to operate the facility for the sale of authorized goods and services according to the applicable military departmental regulations. The State agrees to exercise patronage control for the exchange facility and to designate an active duty officer to serve as the "garrison/installation commander" for discharging the responsibilities prescribed by the military departments.

5. The State agrees to provide all necessary utilities cost and sewage cost.

6. The State agrees to provide custodial support; maintenance and repair of the building with State funds, except for repairs to equipment and interior finishes of the exchange facility for which AAFES will be responsible; and appropriate fire protection and security for funds and property. Subject to the availability of appropriated funds, AAFES will be reimbursed by the State for loss or damage to merchandise or equipment.

Figure 6–1. Sample of a memorandum of agreement

7. The AAFES will be authorized to install all necessary equipment and furnishings for the operation of an exchange, and title to all items purchased with AAFES funds (except installed property that becomes a part of the building) will remain with AAFES. AAFES agrees to perform no structural additions or alterations without the written approval of the designated garrison/installation commander.

8. The establishment of this exchange will be evaluated biennially, to ensure that it meets the minimum criteria for continued operations.

9. Dividends from the operation of exchange operations will be distributed to the Army and Air Force on the same basis as dividends are distributed from active component exchange operations. The Army and Air Force may share these dividends with the Guard unit in accordance with the respective Service's policies.

10. This agreement may be terminated upon the disestablishment of the military activity, upon failure of revalidation, or upon 90-day written notice by either party.

Appropriate AAFES representative
(Name, title, and date)

Appropriate State representative
(Name, title, and date)

Figure 6–1. Sample of a memorandum of agreement-continued

6–2. Exchange support in theater operations

a. AAFES is the national level provider of military exchange items and services. When requested and resourced by the supported commander, AAFES serves as a supporting organization providing military exchange items and services to U.S. forces, and other authorized customers, deployed for or conducting humanitarian or contingency operations and exercises. In a contingency theater of operations or military exercises, where regular AAFES facilities are not available, commanders may request AAFES support as follows:

(1) *Army and Air Force Exchange Service Imprest Fund Activitiy.* An AIFA is a unit-operated activity usually at a small or remote site where a regular direct operation exchange cannot be provided. Units operating an AIFA will be given a change fund, purchase merchandise for stocking and restocking from AAFES only, and sell at AAFES set prices.

(a) The AAFES director and chief executive officer issues operating procedures to activate, operate, and deactivate the AIFA.

(b) Unit commanders appoint a commissioned or warrant officer or senior noncommissioned officer to supervise the AIFA, be accountable for the AAFES assets loaned, and to furnish all administrative and logistical support necessary to operate the AIFA.

(2) *Tactical field exchange.* A tactical field exchange (TFE) is operated by the military usually in remote locations. TFE operators are trained by AAFES personnel. The TFE operates using AAFES standard operating procedures, and merchandise is pushed to these facilities by AAFES distribution centers with APF support as required in the theater of operation.

(3) *Direct operating exchange-tactical.* A direct operating exchange-tactical (DOX-T) is operated by AAFES civilian personnel. The DOX-T operates using AAFES operating procedures, and merchandise will be procured through AAFES distribution channels with APF support as required in the theater of operation. AAFES normally will not operate a DOX-T or deploy AAFES associates in non-permissive or combat environments.

(4) *Alternate operations.* When it is impractical to provide service by AIFA, TFE, or DOX-T, service may be by

(a) Mobile service or vending machines.

(b) Group representation at the nearest exchange, if vending or mobile service is not practical. (Group representation

is sending a representative of several exchange patrons to the nearest exchange outlet, where purchases for the group are made.)

(c) Mail-order or e-commerce arrangements.

b. The decision to operate or deploy AAFES personnel in non-permissive or combat environments rests with the AAFES director and chief executive officer. All AAFES support requires administrative and logistical support from the requesting command. The requirement for exchange support, as well as any administrative or logistical support to the exchange is set forth as specified tasks in contingency operations plans or field exercise directives. Such support also may be formalized in MOAs between AAFES and the military command being supported or their higher headquarters.

6–3. Alternatives to regular exchange service operations

a. Army National Guard, Air National Guard, Army Reserve, and Reserve Officers' Training Corps units normally receive exchange support through existing exchange outlets during their annual field training period. If these outlets are not available, an AIFA may be used during the training period (see para 6–2*a*(1)).

b. When it is impractical to provide service by AIFA, then TFE or DOX-T service may be provided (see para 6–2*a*(2) and para 6–2*a*(3)).

c. Issues of exchange merchandise required by military activities for gratuitous issue during emergency actions may be furnished by exchanges to the requiring activity on a reimbursable basis, to include merchandise cost, freight, packing, and any applicable administrative costs.

6–4. Exchanges on closed installations

a. Exchanges may operate on closed installations in the United States and its territories and possessions under specific criteria. Policy and the criteria are found in DODI 1330.21.

b. Combined commissary and exchange stores may be operated on closed garrisons and installations. Policy is found in DODI 1330.21.

6–5. Transfer of activities

An exchange or organizational activity may be transferred between AAFES and another NAFI. When an activity is transferred, the AAFES director and chief executive officer and the commander or head of the other NAFI, will establish an agreement with provisions for transferring assets and granting entitlements and benefits to the employees whose positions will be transferred. If an agreement cannot be reached, the departments involved will determine the provisions of transfer. Transfers between AAFES and APF government agencies will be as permitted by applicable law and must be reviewed by the AAFES general counsel before implementation.

Section II
Other Exchange Service Operations

6–6. Motion picture service

Policy on entertainment motion picture services is contained in chapter 12.

6–7. Military clothing sales stores

a. Military clothing sales stores (MCSS) are APF activities managed by the AAFES director and chief executive officer, pursuant to applicable departmental regulations and the MOU between AAFES and the military departments.

b. The military departments will reimburse AAFES for all costs associated with MCSS construction, facility improvement, operation, and management as stipulated in the respective Service's MOU.

c. The MCSS are also governed by AR 700–84 and AFMAN 23–110, Volume 1.

6–8. School food service

AAFES operates the DOD School Meal Program in accordance with AAFES/DOD Education Activity MOA under the provisions of DODD 1015.5. Program operating costs are covered by United States Department of Agriculture subsidies, student meal prices, and the DOD Education Activity. Facilities and equipment are provided and maintained by the installation on a non-reimbursable basis. The GM, AAFES will provide the garrison and installation commanders with a request for replacement or procurement of the DOD School Meal Program equipment prior to the fiscal year (October), so necessary equipment can be budgeted, ordered, and installed during the schools' summer break, and in order to prevent disruption of service.

6–9. Army and Air Force Exchange Service loss activities

Exchange activities will not normally be operated at a loss. The AAFES director and chief executive officer will establish procedures to review losing operations and criteria that are the basis for continuing operations.

Section III
Financial Services

6–10. Contracts and agreements

Subject to the provisions of DODI 1000.11 and DOD 7000.14–R, Financial Management Regulations, Volume 5, AAFES may enter into contracts or other agreements to provide check cashing, automated teller machines, and other authorized financial services to authorized patrons in exchange facilities.

6–11. Check cashing

a. Use of AAFES funds for check cashing services is within the limits of cash working funds prescribed by the AAFES director and chief executive officer.

b. When on-base banking facilities are available, exchange check cashing service may be offered before, during, and after banking hours, if this does not violate existing agreements among the bank, the U.S. Department of the Treasury, and the installation command. (Exchange check cashing service does not relieve an authorized banking facility of its obligation to furnish the service.)

c. Checks drawn on foreign banks and payable in foreign currency are not cashed or accepted as payment for merchandise.

d. The AAFES does not cash checks drawn in foreign currencies on U.S. banks or on their overseas subsidiaries.

e. Outside the continental United States (OCONUS) dollar checks issued by foreign banks authorized to act as military banking facilities are accepted for cashing and for payment of merchandise. (Such checks are not accepted in CONUS exchanges, unless issued by foreign subsidiaries of U.S. banks acting as military banking facilities in CONUS.)

f. The AAFES director and chief executive officer establishes procedures, limitations, and controls for cashing checks and for payment for merchandise or service.

6–12. Processing dishonored checks

a. Instructions for processing dishonored check claims are issued by the AAFES director and chief executive officer.

b. Upon receipt of a dishonored check, a demand for restitution is made on the maker and prior endorsers. The amount requested includes a fee to cover the Exchange's cost of collections and any other service and penalty charges that may be passed on by banks.

(1) If military personnel do not make restitution within 30 days, the matter is reported to the individual's unit commander and garrison and installation commanders/check control officer.

(2) If restitution is not made within 60 days, the debt may be submitted for further collection action, to include processing of involuntary pay withholdings and Treasury Offset Program, which may include, but is not limited to—

(a) Tax refund offsets.

(b) Federal salary pay, including military pay.

(c) Contractor and vendor payments.

(d) Certain federal benefits payments, such as social security, veteran benefits, disability benefits, and employee travel pay.

(e) Other federal payments, including certain loans.

(3) Administrative wage garnishments of non-government civilian wages.

c. When checks are returned as dishonored, check cashing privileges are suspended.

(1) Exchange credit program privileges may be suspended only if such action is consistent with applicable federal law and regulations.

(2) Privileges are restored when full voluntary restitution is received from all outstanding debts and service/penalty charges.

(3) The AAFES director and chief executive officer, or designee, has the authority to set policy for the suspension of check cashing privileges in cases of repeated presentation of dishonored checks, nonpayment or involuntary collection of unpaid dishonored check debts and dishonored check fees.

6–13. Exchange credit program

AAFES may sell merchandise and services on a deferred payment basis as authorized by DODI 1330.09 and DODI 1330.21. The AAFES director and chief executive officer establishes procedures, limitations, and controls for exchange credit products that may be used by authorized patrons to purchase merchandise and services. The AAFES BOD may authorize the AAFES director and chief executive officer, or designee, to enter into commercial borrowing agreements or issue commercial paper to fund this program in accordance with applicable legal authority.

Section IV
Resale Activities

6–14. Exchange service

a. AAFES is the primary resale activity on Army and Air Force installations, and other locations where AAFES operations are established for the military community, for non-food merchandise and patron services. AAFES operation of any vending machines at authorized locations is exempt from the Randolph-Sheppard Act (AR 210–25/AFI 34–206). Exchanges support forward deployments, ships at sea, emergency and disaster relief efforts, international exercises, and contingency operations.

b. Resolution of disagreements concerning the primacy of AAFES resale authority or AAFES ability to provide requested merchandise and services resides with the appropriate region director IMCOM (Army) or commander MAJCOM (Air Force).

c. Authorized AAFES resale activities are listed in appendix C of this regulation and DODI 1330.21.

d. The AAFES director and chief executive officer determines what is sold in AAFES facilities, either directly or by concessionaire, subject to limitations in appendix C. CONUS-only restrictions are listed in appendix D. Merchandise restrictions apply to direct sales (including special order and catalog or e-commerce sales) and indirect or concession activities.

e. Garrisons and installation commanders may enter into MOAs, MOUs, or installation support agreements with AAFES to manage designated MWR sales operations. Agreements generally include provisions for applicable management fees, audit trails that account for receipts and disbursements, and submission of monthly income and expense statements. Such agreements can be signed by the GM, AAFES after proper coordination with HQ, AAFES, Army IMCOM, G–9 (Family and MWR Programs)/Air Force Services. Operations that may be managed by AAFES if most beneficial to the NAFI and with local command agreements, include but are not limited to—

(1) Amusement machines.

(2) Service and vending machines in military clubs, civilian employee NAF activities, bowling centers, and similar activities.

(3) Commodity concession contracts and short-term sales agreements for overseas military clubs, Armed Forces Recreation Centers, and other lodging facilities.

(4) Any other resale activity connected with MWR functions which appropriately may be performed under an MOA/MOU/installation support agreement with AAFES.

6–15. Resale by nonappropriated fund instrumentalities, other than the Exchange Service

MWR programs may engage in resale activities and services that are directly related to their program as defined in MWR departmental regulations. Such resale activities, including membership clubs (open messes), restaurants, cafeterias, and snack bars incidental to MWR programs, must be NAF-operated, NAF-managed, or NAF-contracted. Otherwise, military exchanges will be the primary source of resale merchandise and services on DOD installations. MWR programs will obtain, in advance, written right of first refusal from AAFES to operate any other resale or service activity.

Section V
Non-Army and Air Force Exchange Service Operations

6–16. Commercial solicitation

Commercial solicitation on Army/Air Force garrisons/installations is governed by DODI 1344.07, AR 210–7 (for Army), AFI 36–2702 (for Air Force), and as permitted by applicable law. The garrison/installation commander may authorize solicitation privileges in coordination with the local GM, AAFES, even though the merchandise sold or services provided by these companies are similar to that available through AAFES. Commercial solicitation agreements will receive a legal review by the servicing staff judge advocate (SJA).

6–17. Home-based business

Home enterprises on Army installations are governed by AR 210–7. Such enterprises include sales or services customarily conducted in a domestic setting and do not compete with an installation's officially sanctioned commerce, that is the Exchange and MWR resale operations. Home-based businesses on Air Force installations are governed by AFI 32–6001.

6–18. Non-incidental morale, welfare, and recreation operations

MWR programs may operate any AAFES resale operation only after obtaining, in advance, written right of first refusal from AAFES. Any restrictions or prohibitions pertaining to AAFES operation also apply to MWR operation. Such resale activities must be NAF-operated, NAF-managed, or NAF-contracted.

6–19. Non-morale, welfare, and recreation entities

Any private venture that includes the acquisition or construction of privatized military family housing or privatized military unaccompanied housing is prohibited from providing merchandise or services in direct competition with AAFES unless AAFES relinquishes its authority in writing.

6–20. Civilian welfare fund and post restaurant

Resale operations are provided in AR 215–7 and AFJI 34–122.

Section VI
Prohibitions

6–21. Contributions and donations

a. AAFES will not contribute funds, merchandise, or services (financial, procurement, contracting, and so forth) to any charity or other organization. This does not prohibit

(1) Providing gift certificates and gift cards to military MWR programs for promotional purposes, as long as recipients of such certificates and cards are authorized patrons.

(2) Transferring no-value inventory items to the garrison or installation MWR entity and fund or other installation governmental entities without charge.

b. Collection jars or other displays for donation of money or items are not permitted in AAFES facilities.

6–22. Other

Other prohibitions are at appendix E of this regulation, as implemented from DODI 1330.21.

Chapter 7
Patrons, Privileges, and Identification

7–1. Privileges within continental United States

Limited and unlimited privileges in CONUS, Alaska, Hawaii, and all U.S. commonwealths, possessions, and territories are outlined in table 7–1 and table 7–2.

7–2. Privileges in foreign (overseas) areas

a. Exchange privileges in foreign or overseas areas are neither automatic nor uniform. AAFES does not determine shopping privileges or access to duty-free items. Overseas commanders will extend exchange privileges based solely on the applicable international agreements.

b. If consistent with applicable international agreements, privileges will be extended to the following:

(1) All uniformed personnel assigned or on temporary duty (TDY) to that overseas area.

(2) U.S. citizen employees of the U.S. Government (including those paid from NAFs), U.S. citizen employees of firms under contract to the DOD, and Red Cross personnel assigned with an activity of the military Services. This includes DOD civilian employees in a TDY status.

(3) Military personnel of foreign nations on active duty, when the major overseas commander determines that the granting of such privileges is in the best interests of the United States.

(4) Family members of persons specified in paragraphs (1), (2), and (3), above.

(5) Unauthorized persons stranded on an installation may purchase small quantities of gasoline, oil, other automotive items, or items necessary for an individual's health.

(6) Official organizations or activities of the Armed Forces which are composed of personnel on active military duty, including NAFIs.

(7) Overseas commanders may extend privileges to certain officials of the United Services Organization (USO) when it will not impair the military mission.

(8) Uniformed personnel, U.S. Government civilians, and their respective Family members, when traveling on leave to foreign and overseas areas, have only those privileges afforded/extended by international agreements and the local command. Privileges are determined by pertinent international agreement and the local chain of command.

(9) International agreements may limit privileges of military retirees in foreign overseas areas.

(10) Specific categories of personnel or organizations authorized by the responsible commander when determined to be in the best interests of the mission of the command concerned. If private organizations are authorized exchange privileges, they will not be authorized to make purchases on credit.

7–3. Purchases for patrons unable to shop for themselves

a. An authorized patron entitled to exchange privileges may have a person (referred to as an agent) accompany them to assist in shopping, or shop on behalf of the patron, when the patron—

(1) Is incapable or unable to shop due to medical conditions, or the patron is a minor child.

(2) Lacks available transportation or is experiencing some other similar type of hardship.

b. Patrons who are bed-ridden or physically unable to do their own shopping may choose an agent to shop for them. Items of purchase are limited to those items that will be used exclusively by the patron.

c. In these cases, the garrison and installation commanders will issue a letter of authorization to that designated agent. The letter of authorization applies only to the installations under the control of the signing authority. A sample of a letter of authorization to accompany a patron is found at figure 7–1.

DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

(Office Symbol) (date)

MEMORANDUM FOR GENERAL MANAGER, XYZ EXCHANGE

SUBJECT: Authorization to Make Exchange Purchases

1. (Name), whose status is described below, is entitled to exchange privileges indicated during the period (beginning date) to (ending date).

2. Status: (Include only one category, for example)

a. Agent of (name typed), an eligible minor child.
b. Agent of (name typed), an eligible handicapped patron.

3. Privileges: (Include only one category)

a. Unlimited.
b. Limited to purchase of books, supplies, and materials related to the military service school educational process and environment. These items may be purchased only from (name of exchange).

(Signature of Bearer)

(Signature of Issuing Authority)

(Date of Issue)

Figure 7–1. Sample of letter of authorization

7–4. Identification

a. Purchases of merchandise or services from an AAFES activity requires identification of individuals who are not in military uniform (excluding para *b*, below). Identification will be made prior to purchase. Commanders will issue proper identification documents to persons authorized exchange privileges. Such identification includes—

(1) Complete regulation U.S. military uniform.

(2) An official Uniformed Services Identification Card or common access card. Specific information regarding identification cards is contained in AFI 36–3026_IP, Volume 1/AR 600–8–14 and DODI 1000.13.

(3) DD Form 2574, an exchange identification card is issued to authorized patrons of exchanges who do not otherwise require the Armed Services Identification Card for benefits or identification purposes.

(4) An official identification card issued by the military Service of which the patron is affiliated.

(5) Official DOD issuances (DD Form 4 (Enlistment/Reenlistment Document Armed Forces of the United States), DD Form 1610 (Request and Authorization for TDY Travel of DOD Personnel), and DD Form 1618 (Department of Defense (DOD) Transportation Agreement Transfer of Civilian Employees to and Within Continental United States)).

(6) The Defense Enrollment Eligibility Reporting System may be used to verify authorized Armed Services Exchange catalog customers.

b. Identification cards are not required from personnel as listed in table 7–2, category 9, who are authorized to patronize only exchange food facilities (fountain, snack bar, and cafeteria).

c. Civilian students and faculty members of Service schools may use the Exchange with a picture identification.

7–5. Visitors

a. Garrison and installation commanders may permit visitors of authorized patrons to accompany the patron as a guest unless the commander determines otherwise based upon local conditions. Visitors will not have purchasing privileges, except as noted in table 7–2, category 11. In foreign or overseas areas, the access privilege of visitors will be controlled as directed by the region director IMCOM (Army)/commander MAJCOM (Air Force) concerned and based on limitations imposed by host government agreements.

b. Guests may attend all motion picture services, provided they are accompanied by authorized patrons.

7–6. Abuse of privileges

a. Garrison and installation commanders may ask the GM, AAFES or exchange manager to conduct periodic unannounced checks of exchange patron identification.

b. The GM, AAFES will inform garrison and installation commanders of any abuses of exchange privileges. Garrison/installation commanders will take appropriate action to include revoking or suspending exchange privileges. The garrison and installation commanders may also request local modifications of exchange patron control procedures deemed necessary to prevent abuse of exchange privileges. Disputes over patron control procedures may be forwarded by garrison and installation commanders through command channels, including appropriate department staff element, to the AAFES director and chief executive officer for resolution. If the dispute over patron control procedures is not resolved to command satisfaction, it may be presented to the AAFES executive secretary for the AAFES BOD for resolution by the AAFES BOD.

c. Exchange patrons are prohibited from the following:

(1) Making (or purchasing for the purpose of making) a sale, exchange, or transfer or other disposition of exchange merchandise or services to unauthorized patrons (customary gifts of a personal nature are permissible).

(2) Using exchange merchandise or services to produce income.

(3) Making purchases for the purpose of resale by, or on behalf of, an installation private organization or other non-governmental entity.

d. Other abuses include, but are not limited to—

(1) Theft of exchange merchandise or other assets by shoplifting, employee pilferage, or other means, by any person having exchange privileges. The final disposition of each case of shoplifting or employee theft will be provided by the local command to the GM, AAFES, for forwarding to HQ, AAFES, Loss Prevention Office.

(2) Intentional or repeated presentation of dishonored checks, or failing to make prompt restitution on dishonored checks or other indebtedness determined to be owed to AAFES. Actions taken with regard to amounts owed to AAFES under exchange credit programs will comply with applicable Federal law and regulations.

e. Garrison and installation commanders may revoke exchange privileges for any period deemed appropriate, except in the case of shoplifting, employee pilferage, or intentional presentations of dishonored checks. In these cases, exchange privileges will be revoked for a minimum period of 6 months. As an exception, active duty uniformed personnel may be allowed controlled access to the Exchange to satisfy personal appearance, health, and sanitary requirements. On appeal, the garrison and installation commander who revoked the privileges, or the next higher commander, may reinstate exchange privileges for cogent and compelling reasons. The AAFES director and chief

executive officer may revoke catalog and Internet privileges for abuse of those privileges, for any period deemed appropriate. Revocation of catalog and Internet privileges shall not affect a patron's garrison and installation exchange privileges.

f. Pursuant to the Federal Claims Collection Act, AAFES can pursue losses and administrative costs directly relating to shoplifting, theft detection, and theft prevention as claims of the United States recoverable from shoplifters through federal debt collection methods.

7–7. Catalog service to replace lost or damaged items

Authorized patrons reassigned to CONUS may purchase from the AAFES catalog or e-commerce programs, those items that are identified for purchase only while stationed or TDY overseas in order to replace items lost or destroyed during a government-sponsored shipment from an overseas duty assignment to CONUS, provided the customer

a. Places the order, attaching the SF 95 (Claim for Damage, Injury, or Death) and reassignment orders to the catalog order.

b. Is responsible for payment of the sell price, shipping and handling fees, and all customs duties upon entry into the United States.

7–8. Patronage exceptions

The Secretary of the Army and the Secretary of the Air Force of the military departments may grant deviations with regard to authorized patron access for individuals or classes and groups of persons at specific garrisons and installations. Delegation of this authority outside the Secretariat concerned is prohibited. Deviations may be granted, when based on alleviating individual hardships. General criteria for requesting deviations by garrisons and installations are at appendix F.

7–9. Unlimited exchange access (except as noted)

Table 7–1 lists the individuals, organizations, and activities in the United States and all U.S. possessions and territories of the United States, and, as noted, outside the United States, entitled to unlimited exchange service benefits.

Table 7–1
Unlimited exchange service privileges

Category	Status
1. Uniformed or retired uniformed personnel, either on active duty or serving in any category of their Reserve Component.	a. All members of the Army, Navy, Air Force, Marine Corps, Coast Guard; commissioned officers of the National Oceanic and Atmospheric Administration (NOAA) and its predecessors; and commissioned officers of the Public Health Service. b. Former members of the Lighthouse Services and personnel of the Emergency Officers' Retired List of the Army, Navy, Air Force, and Marine Corps, and members or former members of Reserve Components who, but for age, would be eligible for retired pay. c. Enlisted personnel transferred to the Fleet Reserve of the Navy and Fleet Marine Corps Reserve after 16 or more years of active military service. (These personnel are equivalent to Army and Air Force retired enlisted personnel.)
2. Involuntarily separated Servicemembers under other than adverse conditions. Appropriate Separation Program Designation codes will be used to allow issuance of DD Form 2765 (Department of Defense/Uniformed Services Identification and Privilege Card). a. Servicemembers involuntarily separated from active duty. b. Servicemembers involuntarily separated from the Selected Reserve of the Ready Reserve as a result of BRAC or Global Defense Posture Realignment.	Continued use of AAFES facilities in the same manner as a member on active duty during the 2–year period beginning on the date of the involuntary separation of the Servicemember. Applicable period begins on 1 October 2007, ending on 31 December 2012 (10 USC 1146).
3. Servicemembers receiving sole survivorship (see glossary for definition) discharge granted after 11 September 2001. DD Form 2765 is issued as identification.	Continued use of AAFES facilities in the same manner as a member on active duty during the 2–year period beginning on the later of the following dates: a. Date of separation of the member. b. Date on which the member is first notified of entitlement of exchange facility use (10 USC 1146).
4. Congressional Medal of Honor recipients.	All
5. Honorably discharged veterans.	When— a. Classified by the Department of Veterans Affairs as being 100 percent disabled. b. Hospitalized where exchange facilities are available.

Table 7–1
Unlimited exchange service privileges—Continued

Category	Status
6. Surviving spouses and Family members of veterans who were posthumously determined to possess Service-connected disabilities rated as 100 percent or total.	See glossary for definition of Family member.
7. Military members of foreign nations.	a. Active duty officers and enlisted personnel of foreign nations, when on duty with the U.S. military Services under competent orders issued by the U.S. Army, Navy, Air Force, or Marine Corps. (Purchase of uniforms will be limited by the provisions of AR 12–15/ SECNAVINST 4950.4B/AFI 16–105.) b. Excluded are active duty military personnel of foreign nations, retired, or on leave in the United States, or when attending U.S. schools, but not under orders issued by the Army, Navy, Air Force, or Marine Corps. c. Overseas, when determined by the region director IMCOM/MAJCOM that the granting of such privileges is in the best interests of the United States and such persons are connected with, or their activities are related to, the performance of functions of the U.S. military establishment.
8. National Guard not in federal service.	When called or ordered to duty in response to a federally declared disaster or national emergency, during the period of such duty, on the same basis as active duty members of the Armed Forces.
9. Red Cross personnel.	U.S. citizens assigned to duty outside the United States and Puerto Rico with an activity of the military Service. Uniform items are not authorized.
10. U.S. civilian DOD employees.	When stationed outside the United States, except when assigned to U.S. territories and possessions. Uniform items are not authorized.
11. U.S. employees of firms under contract to the DOD.	When employed outside the United States, except when assigned to U.S. territories and possessions. Uniform items are not authorized.
12. Wage marine personnel and retired wage marine personnel, including noncommissioned ships' officers and crewmembers of the NOAA.	All
13. Authorized Family members of personnel in categories 1 through 12, above.	See glossary for definition of Family member.
14. Contract surgeons.	During the period of their contract with The Surgeon General.
15. Official DOD activities.	For activity purchase and use only (not for individual purchases or use). All purchases authorized for government-wide purchase card use. All purchases authorized by 10 USC 2492. All other purchases based on sole source justification.
16. Non-DOD federal departments and agencies.	a. For federal department or agency purchases and use only (not for individual purchases or use). b. When it is determined by the local commander that the desired supplies or services cannot be conveniently obtained elsewhere and the supplies or services can be furnished without unduly impairing the service to exchange patrons. c. All purchases authorized by 10 USC 2492.
17. Dependents of members of the Armed Forces, commissioned officers of the Public Health Service, and commissioned officers of the NOAA, separated for dependent abuse.	A dependent or former dependent entitled to transition compensation under 10 USC 1059, if not eligible under another provision of law, while receiving payments for transition compensation.
18. United Service Organizations.	a. USO personnel stationed outside the United States. b. USO clubs and agencies may purchase supplies for use in club snack bars, which support active duty military members and their families. c. Overseas, garrison and installation commanders may extend privileges to USO area executives (directors, assistant directors) who are U.S. citizens on invitational travel orders, when it is in the capacity of the Exchange and does not impair the Exchange military mission. d. Uniform items are not authorized.
19. Agents.	Persons authorized in writing by the garrison and installation commander to shop for an authorized patron or official organization or activity entitled to unlimited exchange privileges. Agents are not authorized to shop for themselves.

Table 7–1
Unlimited exchange service privileges—Continued

Category	Status
20. Delayed Entry Program participants.	Authorized to use exchange facilities during interim period before entering active duty.
21. Armed Services Young Men's Christian Association.	In overseas areas, garrison and installation commanders may extend privileges to Armed Services Young Men's Christian Associations branch or unit directors and assistant directors for their personal and family needs and for use in Armed Services Young Men's Christian Association programs that support active duty military members and their families, when it is in the capability of AAFES and does not impair the military mission. Uniform items are not authorized.
22. United Seaman's Service.	Support to the United Seaman's Service personnel for personal and family needs, and for supplies and services necessary to accomplish the United Seaman's Service mission when economic conditions or isolated locations are such that support is not available from local civilian sources, cannot be imported from other sources, or is available from local civilian sources or by importation only at prohibitive cost. The local commander may authorize access when available without detriment to DOD mission accomplishment.

7–10. Limited exchange privileges

Limited exchange access applies to the United States and all U.S. territories and possessions (except as noted). Generally, it excludes tobacco products, alcoholic beverages, and military uniforms. Table 7–2 lists individuals, organizations, and activities entitled to purchases from AAFES.

Table 7–2
Limited exchange access

Category	Status (except as noted)
1. U.S. Government civilian employees and full-time paid staff of the Red Cross, residing on military installations within the United States and Puerto Rico.	a. No uniform items. b. No state tax-free tobacco items. c. Tax-free alcoholic beverages may be purchased, but not removed from the garrison and installation.
2. Armed Forces exchange employees.	a. Current employees, retired employees with 20 or more years of service, and employees on 100 percent disability retirement from the Exchange Service. Includes all privileges of the exchange, where employed. b. No uniform items. c. No state tax-free tobacco items. d. No tax-free alcoholic beverages. e. Unlimited privileges overseas, except for uniform items. f. Overseas sales to exchange employees must not violate status of forces agreement (SOFA) or international agreements.
3. DOD civilian employees on evacuation orders.	Employees who are directly affected by an emergency evacuation are authorized to use the Exchange Service for the duration of the evacuation period at their safe haven location, as determined by the pertinent garrison and installation commander in the United States.
4. Authorized Family members of personnel in listed in 1, 2, and 3 of this table.	See glossary for definition of Family member.
5. DOD civilian employees (see para F–4 and para F–5 for reporting requirement).	a. Garrison and installation commanders may authorize exchange and commissary access to such employees and their Family members when the employees are assigned to U.S. territories and possessions under a valid transportation agreement, as defined in Title 41, Chapter 302, Code of Federal Regulations (41 CFR, Chapter 302). (Access does not include DOD civilian employees locally hired in U.S. territories and possessions or those without a valid transportation agreement.) b. No uniform items. c. No state tax-free tobacco items. d. No tax-free alcoholic beverages.

Table 7–2
Limited exchange access—Continued

Category	Status (except as noted)
6. Employees of firms under contract to the U.S. Government and their Family members (see para F–4 and para F–5 for reporting requirement).	a. Garrison and installation commanders concerned may grant exchange and commissary access for either individuals or classes and groups of such employees, and their Family members, who are assigned to U.S. territories or possessions, provided specific criteria in footnote 1 are met. b. No uniform items. c. No state tax-free tobacco items. d. No tax-free alcoholic beverages.
7. Non-DOD U.S. federal civilian employees (see para F–4 and para F–5 for reporting requirement).	a. The Secretary of the Army, the Secretary of Air Force, and combatant commanders may grant non-DOD U.S. federal employees and their Family members serving in U.S. territories and possessions access to the military exchanges when all the criteria at footnote 2, below, are met. Local commanders will execute a separate support agreement with the non-DOD U.S. federal employee's agency. b. No uniform items. c. No state tax-free tobacco items. d. No tax-free alcoholic beverages.
8. DOD civilian employees in TDY status.	a. In the United States when occupying government quarters on military installations, and identified by copies of their TDY orders and on-base billeting authorization. b. Outside the United States when identified by copies of their TDY orders. c. No uniform items. d. No state tax-free tobacco items. e. No tax-free alcoholic beverages.
9. Civilian employees of the U.S. Government working on, but residing off military installations.	All food and beverages sold at any AAFES food activity, if consumed on post.
10. Uniformed and non-uniformed personnel working in recognized welfare service organization offices within an activity of the military Service.	All food and beverages sold at any AAFES food activity, if consumed on post.
11. Visitors to military installations (also see para 7–5).	All food and beverages sold at any AAFES food activity, if consumed on post.
12. Contract technical services personnel in travel status and Army, Navy, and Air Force Academy applicants.	a. When occupying government quarters on a military installation. b. No uniform items. c. No state tax-free tobacco items. d. No tax-free alcoholic beverages.
13. Foreign national active duty officers and enlisted members, when visiting U.S. military installations on unofficial business.	a. Entitled to all exchange privileges, except that merchandise sold to such personnel will be restricted to quantities required for their personal use. b. AR 12–15/SECNAVINST 4950.4B/AFI 16–105 and AFMAN 23–110, Volume 1, will govern the sale of uniform items.
14. Servicemembers of the Civil Air Patrol in a travel status and occupying government quarters on a DOD installation.	a. For purchases other than uniforms, they will be identified with their current membership card, their travel authorization, and evidence they are occupying government quarters on the installation. b. Purchase of uniforms, when Civil Air Patrol membership card is shown. c. No state tax-free tobacco items. d. No tax-free alcohol beverages.
15. Civil Air Patrol cadets.	a. Purchase of uniforms, when Civil Air Patrol membership card is shown. b. All food and beverage sold at any AAFES food activity, if consumed on post.
16. Members of the Reserve Officers' Training Corps and Junior Reserve Officers' Training Corps.	a. When visiting installations under orders as part of a Service orientation program. b. No state tax-free tobacco items. c. No tax-free alcoholic beverages.
17. Members of the Naval Sea Cadet Corps.	a. On 2–week summer training duty, if occupying government quarters on a military installation. b. No distinctive uniform items. c. No state tax-free tobacco items. d. No tax-free alcoholic beverages.

Table 7–2
Limited exchange access—Continued

Category	Status (except as noted)
18. Coast Guard Auxiliary members.	a. When identified by the Coast Guard Auxiliary Membership Card (USCG Form CG–2650). b. Uniform articles and accessories authorized by Coast Guard Auxiliary directives.
19. Civilian students and faculty members at Service schools.	Books, supplies, and materials related to the educational process, only at AAFES facilities which support the school.
20. Persons suffering from hardship.	Exchange employees may sell to otherwise unauthorized persons stranded on an installation, small quantities of gasoline, oil, other automotive items, or items necessary for an individual's health.
21. DOD civilian employees using government authorized vehicles for official business.	Gasoline for use in vehicles, upon presentation of military travel orders that authorize the leasing or use of the government vehicle.

Notes:

[1] The employee exclusively serves DOD and was hired in the 50 states, the District of Columbia, or a U.S. territory or possession other than the one to which the employee is assigned; due to specific difficulties faced by the employee to obtain services from civilian or other federal agencies, such as unhealthful conditions, hostile or imminent danger, or extraordinarily difficult living conditions; granting exchange and commissary privileges is in the best interest of the U.S. Government; and the denial of privileges would impair efficient DOD operations.

[2] The employee is assigned under a service agreement, as defined in 41 CFR, Chapter 302–2.12 or a tour renewal agreement (41 CFR, Chapter 302–3.209); granting access will alleviate individual hardship due to extraordinarily difficult living conditions, excessive physical hardship, or notably unhealthful conditions; and granting access will fit into and support a web of security precautions essential to ensure the safety and security of the individual employee who is subject to current and specific threat conditions, such as hostile or imminent danger. Delegation of this authority outside of the Secretariat or Combatant Command Headquarters concerned is prohibited.

Chapter 8
Stock assortment, sales, pricing, advertising, and promotions

Section I
Stock assortment and pricing

8–1. Retail stock assortment

a. The AAFES director and chief executive officer prescribes the AAFES master stock assortment for each retail department. HQ, AAFES sets stock assortments and stock structures for outlets within the parameters of the master stock assortment. This includes a variety of price-lines, nationally accepted brands identified to satisfy customer demand to the maximum extent, and private label merchandise.

b. All exchanges stock and sell retail merchandise consistent with retail industry standards and the AAFES master stock assortment (subject to the restrictions in app E). Only the Principal Deputy Under Secretary of Defense (Personnel and Readiness) (PDUSD(PR)) can make changes to the restrictions.

c. The AAFES director and chief executive officer prescribes limitations regarding stocking and special order of specific categories or items when deemed necessary.

(1) Overseas and offshore exchanges may stock high-demand merchandise not authorized for resale in CONUS exchanges (see app E).

(2) Merchandise sold in overseas exchanges for delivery in CONUS, either directly or through a concessionaire or agency arrangement, is subject to the limitations for CONUS exchanges (see app E), except—

(a) As specifically approved by the PDUSD(PR).

(b) This restriction does not apply to gift items located in the CONUS mail-order warehouse.

(c) U.S. manufactured automobiles and motorcycles may be sold for delivery in CONUS.

8–2. Retail pricing and markups

a. Basis for AAFES pricing and markups—

(1) The principle that exchange privileges are a vital form of non-pay compensation that helps military personnel sustain an acceptable American standard of living, regardless of location.

(2) The need to maintain a financially independent organization capable of generating a source of funding for the support of Army and Air Force MWR programs.

b. The AAFES director and chief executive officer is responsible for and has authority to establish—

(1) Generally, uniform prices.

(2) Standard markups that support AAFES' mission and service objectives.

(3) Internal operating procedures concerning pricing strategies that are considered proprietary to AAFES, not to be disseminated outside exchange channels.

c. Special order prices include the cost of transportation or postage and other related handling costs, unless specifically exempted by the AAFES director and chief executive officer.

8–3. Fees and prices

Fees and prices are determined according to EOPs and exchange service regulations issued by the AAFES director and chief executive officer.

8–4. International Balance of Payments Program

Policy on the purchasing, sale, and pricing of foreign merchandise and services by overseas resale NAFIs is found in DODI 7060.03.

Section II
Sales and Trade Names

8–5. Vending sales of tobacco and alcohol

For additional alcoholic beverages sales, see chapter 11.

a. Continental United States, Alaska, or Hawaii—

(1) State tax-free tobacco products are not sold through vending machines.

(2) State tax-free beer may be sold through vending machines in military quarters and mess or dining halls, when authorized by garrison and installation commanders. Such sales must comply with applicable departmental and command directives.

b. In offshore and overseas areas, sales of beer and tobacco products through vending machines are authorized when such sales comply with departmental and command directives and host country agreements and when authorized by the commander concerned.

8–6. Tobacco products

a. Tobacco products (including smokeless tobacco) will not be sold to anyone under 18 years of age.

b. A customer's identification will be checked if the buyer appears to be under 21 years of age.

c. Military retail outlets will not enter into any new merchandise display or promotion agreements, or exercise any options in existing agreements, that provide for any increase in total tobacco shelf space. This provision does not prohibit couponing, or incentives that allocate tobacco shelf space among brands so long as total tobacco shelf space is not increased. Self-service promotional displays will not be used outside of the tobacco department. Incentives to increase the total number of tobacco displays will not be accepted, except to reallocate existing tobacco shelf space among tobacco brands, provided that the total amount of tobacco shelf space is not increased.

d. Exchanges will endeavor to display tobacco cessation products in areas that provide visibility and opportunity to customers who desire to change their tobacco habit. AAFES will support pricing of smoking cessation products below the local competitive price.

e. Exchange merchandise categories for tobacco products may be consigned and sold in commissary stores as exchange items.

f. State tax-free tobacco products will be sold only to those individuals, organizations, and activities entitled to unlimited exchange privileges. Common sense must be used in determining the quantities of state tax-free tobacco products sold are reasonable and for the use of authorized exchange patrons.

8–7. Special sales

a. Coupon books. The use of coupon books in lieu of currency is—

(1) Prohibited in CONUS, except at the U.S. Disciplinary Barracks.

(2) Permitted overseas (and encouraged where local nationals have snack bar privileges). Petroleum, oil, and lubrication coupons are used to purchase gasoline overseas.

b. Pog gift certificates. The use of pog gift certificates in lieu of currency is—

(1) Permitted in CONUS for Servicemembers returning from contingency operations where host countries restrict the use of U.S. coinage or U.S. coinage is not readily available.

(2) Permitted overseas in contingency operations where host countries restrict the use of U.S. coinage or U.S. coinage is not readily available.

c. Layaway sales. Layaway sales are conducted according to EOPs and exchange service regulations.

d. Credit sales. Authority for credit card policies, procedures, limitations, and controls governing acceptance of credit cards rests with the AAFES director and chief executive officer.

e. Special orders. Special orders, using prescribed markup procedures, may be permitted on items available outside of the stock assortment, if available from manufacturers.

f. Financing. Financing service is allowed for the sale of new DOD authorized automobiles and motorcycles in

overseas exchanges. Financing must be done by a U.S. finance company, financial institution, or credit union per applicable departmental regulations.

8–8. Organization or activity sales

a. Types.

(1) *Procurement sales.* AAFES sale of institutional-use merchandise and supplies, services, motor vehicles, equipment, and other retail merchandise not on the AAFES stock assortment.

(2) *Bulk sales.* AAFES sale of supplies, merchandise, and equipment usually in original containers issued from AAFES storage.

(3) *Convenience sales.* AAFES sale of regular exchange stock selected from stock located in an AAFES resale facility.

b. Condition of sale. Above sales are restricted to activities of the U.S. Armed Forces and authorized official organizations determined by the AAFES director and chief executive officer. Prices will be set according to procedures published by the AAFES director and chief executive officer.

8–9. Stock assortment limitation

Limitations and controls on the sale of any item of exchange merchandise may be authorized by the AAFES director and chief executive officer. This is different from ration controls imposed per paragraph 2–3*h*(3). Many times these limitations are operational constraints caused by limits imposed on the availability of supply. Garrison and installation commanders may also ask the GM, AAFES to establish limitations when local conditions warrant such action. To resolve disputes over limitations on goods sold, garrison and installation commanders will forward requests for resolution through command channels, including appropriate department staff elements, to the AAFES director and chief executive officer. Any dispute over limitations on goods sold not resolved at command level may be presented to the executive secretary, AAFES, for resolution by the AAFES BOD.

8–10. Refunds and adjustments

Refunds and exchanges will be authorized in accordance with EOPs and exchange service regulations for merchandise and service that does not meet customer satisfaction. Procedures will be consistent with industry practices.

8–11. Contractor/concessionaire operations

a. Authorized exchange revenue-generating activities are listed in appendix C and DODI 1330.21, enclosure 3.

b. AAFES resale activities may be operated directly by AAFES or by AAFES contractors. Either direct or contractor-operated activities may be operated pursuant to franchise agreements with commercial franchisors. Method of operation will be determined by AAFES, based on a comparison of the financial return and alternative costs of comparable service.

(1) Limitations or restrictions on AAFES sales apply to contractually-operated activities.

(2) Commodity and service concessionaires do not sell merchandise in direct competition with items sold in exchange stores, unless authorized by the AAFES director and chief executive officer and rendered by the terms of the contract. Concessionaire sales may be subject to state and local taxes.

(3) An AAFES contractor or concessionaire selling or providing authorized services is entitled to the same APF support that AAFES is entitled to when providing like services.

c. Service and vending machines are exchange-controlled except for those machines maintained under concessionaire contracts or provided by military MWR programs and off-post Army Reserve Training Centers. Vending machines located in military MWR facilities (see AR 215–1 and AFI 34–206) may be operated by AAFES under a management fee basis as outlined in paragraph 6–14*e*, of this regulation.

8–12. Sanitation

Standards of sanitation prescribed in applicable departmental regulations apply to all exchange activities.

8–13. Use of Army and Air Force Exchange Service trademarks

a. AAFES registers and maintains its own trademarks with the U.S. Patent and Trademark Office. AAFES possesses common law property rights, and formal trademark registration rights, in the terms and abbreviations shown below and any combination of them to include domain names used by AAFES. This list does not include all of AAFES registered trademarks.

(1) Army and Air Force Exchange Service.

(2) AAFES.

(3) Army and Air Force Exchange Service, Europe.

(4) AAFES, Europe.

(5) AAFES–EUR.

(6) Army and Air Force Exchange Service, Pacific.

(7) AAFES, Pacific.
(8) AAFES–PAC.
(9) Post Exchange.
(10) PX.
(11) Base Exchange.
(12) BX.
(13) AAFES.com.

b. Use of the trade names, domain names, abbreviations, terms, or references to AAFES or its exchanges, by and for any person, business, or publication in any type advertisement or promotional campaign is not authorized without the prior approval of the AAFES director and chief executive officer. AAFES personnel will ensure that proper protective language is included in all publications containing AAFES registered trademarks or services marks. Any incidents of such unauthorized use, advertising, or promotions will be reported to the AAFES general counsel.

Section III
Advertising and Promotions

8–14. Advertising

a. The use of AAFES premises, facilities, or personnel by firms or their representatives for any type of advertising, promotion, or solicitation purposes is prohibited.

b. Use of AAFES premises, facilities, personnel, and funds by AAFES for advertising or promotional purposes is authorized on a restrictive basis, as approved by the AAFES director and chief executive officer.

c. AAFES advertising will not reflect unfavorably on the Federal Government, DOD, the Army, or the Air Force. AAFES advertising is based on reaching bona fide users, in accordance with patronage policy issued in this regulation.

d. AAFES media is not distributed off military installations or outside of AAFES facilities, except for mailings to authorized patrons and dissemination of AAFES benefit information at recruiting locations. Patrons living and working off-base should be aware of the products and services available in the Exchange.

e. AAFES activities may contribute articles and stories as unpaid information items in base newspapers, plan-of-the-day publications, Armed Forces Radio and Television Service, installation cable television, Internet sites, and other media intended primarily for distribution to authorized AAFES patrons.

f. AAFES may pay to advertise AAFES goods, services, and entertainment events in—

(1) DOD media, including installation cable television. These advertisements may include brand names, item prices, films, theater admission prices, and names of commercial sponsors, companies, vendors, or distributors involved with special events.

(2) Non-DOD media, if the chosen media is circulated to, written for, or geared to an audience consisting primarily of military personnel and other authorized exchange patrons. When non-DOD media is used for advertising that may be heard, seen, or read by other than authorized patrons, a disclaimer will be used similar to: This offer or event is open only to authorized patrons. (This policy will not be interpreted to apply to publications distributed to a more general audience.) This phrase is not required for advertising AAFES events that are open to the private sector (see para (3), below). Both economic and non-economic factors will be evaluated before engaging non-DOD media to advertise exchange services, products, and events.

(3) Appropriate civilian local and national media, when AAFES is holding or participating in special events (such as automobile shows) that are open to the public and private sector and held on a military installation or in an AAFES facility subject to the following:

(a) Such events do not directly compete with other MWR programs or similar events offered in the local civilian community.

(b) Merchandise will not be advertised, however, event-related merchandise, souvenirs, and food and beverages consumed on the premises may be sold at the event.

(c) Open events and event advertising will be coordinated in advance with the local public affairs office.

(d) Open events are infrequent, not weekly or monthly, and enhance community relations.

(e) OCONUS advertising conforms to existing SOFA, regulations, command policy, and local laws.

(4) Advertisements, premiums, coupons, and samples (except for tobacco, alcohol, and adult-oriented products) may be distributed directly to authorized patrons. A disclaimer is not required.

g. Official channels are not used for distribution of ads and promotional materials that are primarily advertising devices. Such media may be placed in locations on the installation for personal pickup, if a disclaimer is attached.

h. AAFES may sell space for commercial advertising in any media (for example printed and electronic) produced for or prepared by AAFES subject to the following:

(1) A disclaimer is included that the advertisement does not constitute AAFES, DOD, Army, Air Force, or Federal Government endorsement. The phrase PAID ADVERTISEMENT is displayed prominently.

(2) Advertising is limited to only those products and services AAFES is authorized to sell.

(3) Publication of paid commercial advertising by AAFES is bound by similar standards that apply to civilian enterprise publications.

(4) Acceptance of paid commercial advertising on Armed Forces Radio and Television Service, local command channels, or any APF electronic media is prohibited.

(5) Prominent displays containing commercial advertising complies with applicable Service regulations governing signage on military installations.

(6) Advertising will be rejected if it—

(a) Undermines, or appears to undermine, an environment conducive to successful mission performance and preservation of loyalty, morale, and discipline.

(b) Is considered in poor taste or contrary to DOD policy.

(c) Contains advertising for any establishment placed off limits by the garrison and installation commander, or from contractors who are suspended or debarred from doing business with the Federal Government.

(d) Competes directly with AAFES sales of merchandise or services, unless approved by the AAFES U.S. region or overseas senior vice president.

8–15. Promoting

a. See paragraphs 8–14*a* and 8–14*b* related to the use of AAFES premises, facilities, personnel, and funds.

b. Mailings (written or electronic) of announcements promoting exchange products and services are permitted only to authorized patrons. Such mailings may contain advertisements for specific commercial products, commodities, or services provided by or for any private individual, firm, or corporation, and are permitted only to those who voluntarily agree to receive such mailings. Mailings may include advertisements or promotions on behalf of other DOD organizations, including other exchanges, other MWR programs, and the commissary, if such advertising meets the standards in this regulation and is the result of a cooperative effort between AAFES and the other DOD programs. The cost of promotional mailing and postage is NAF funded. A mechanism shall be adopted so those individuals who had consented to such mailings may remove their names from the list. All customers are informed of their right to have names removed from mailing lists, upon their request.

c. Ads, premiums, coupons, samples, and similar promotions (like those used in the commercial sector) may be distributed directly to authorized patrons unless specifically prohibited by DOD policy. The distribution of free samples of tobacco products is prohibited.

d. AAFES may accept premiums with a value of $10 or less when voluntarily initiated and prepared by vendors. AAFES may accept such funds as part of promotional discounts offered by AAFES vendors, under contracts for purchase of retail merchandise by AAFES. Materials prepared as part of such discounts may be at vendor's expense. Funds are not solicited from vendors or other non-DOD sources to offset costs of premiums.

e. AAFES gift certificates and gift cards and merchandise for use in customer promotions and contests are not sold to, or put into the possession of, vendors or vendor representatives.

f. Point of sale displays and promotional material, such as reduced price and special offer coupons, may be used.

g. Vendor may provide merchandising assistance and training of exchange sales personnel. Equipment which combines display and utility, such as retail merchandise counter dispensers of light bulbs or shoestrings, is authorized as prescribed by the AAFES director and chief executive officer when useful and not considered to be primarily advertising devices.

h. In-store demonstrations may be provided by vendors on the use or application of products stocked.

i. Vendor may provide free clinics for inspection and servicing of a vendor's products.

j. The AAFES may participate in national and local coupon redemption programs available to the general public, as well as the military community.

k. The AAFES may accept promotional displays of products being featured in AAFES programs.

8–16. Web sites

AAFES may establish, operate, and maintain unclassified Web sites in accordance with policies and procedures prescribed for official and unofficial Web sites.

8–17. Public affairs

The AAFES public affairs officer is responsible for advising and informing the AAFES director and chief executive officer of the public affairs impact and applications inherent in daily, planned, contingency, or wartime operations. The public affairs officer serves as the AAFES spokesperson for response to media queries and crisis communications concerning AAFES operations as well as ensuring information for public dissemination is reviewed for compliance with policy requirements. The public affairs officer prepares the public affairs annex or portions of operations orders, plans, and standard operating procedures. Additionally, the public affairs officer serves in an advisory capacity to the

media and works closely with the staff to ensure that liaison activities support the AAFES mission and director and chief executive officer's intent.

Chapter 9
Procurement

9–1. General

a. AAFES contracts will be solicited, evaluated, and awarded in keeping with DODD 4105.67, and procedures issued by the AAFES director and chief executive officer. Competitive negotiation, as distinguished from sealed bidding, will be used to the maximum extent practicable.

b. Each contractual relationship will be documented, in writing, on a prescribed AAFES form.

c. AAFES will not negotiate, purchase, or otherwise conduct any procurement business, including in-store or other contract service, with active duty military personnel, U.S. Government employees, NAF employees, or immediate Family members of the above who reside in the same household. Exceptions include—

(1) AAFES director and chief executive officer may waive the prohibition for immediate Family members.

(2) In overseas areas only, contracts for court reporting on a fee basis may be awarded to immediate Family members, if the overseas region commander determines, in writing, that—

(a) Insufficient competition exists without using Family members as sources.

(b) There is no conflict or apparent conflict of interest.

(c) An exception is otherwise in the best interest of AAFES.

(3) Individuals acting in an official capacity as outlined in paragraph *e*, below.

d. Source lists will include only those sources, which are not debarred, suspended, or ineligible in accordance with applicable Congressional mandates, federal law and regulations, and AAFES purchasing procedures. Garrison/installation commanders or designees will review source lists and may recommend deleting a source in writing to the GM, AAFES. They may also recommend adding a qualified local source. Recommendations for suspension or debarment of individuals and firms doing business with AAFES will be prepared by the cognizant contracting officer and submitted to the AAFES general counsel for review and appropriate action.

e. AAFES may enter into contracts or other agreements with other NAFIs, DOD elements or other federal departments, agencies, or instrumentalities, pursuant to 10 USC 2492, to provide those goods and services specifically authorized for exchanges. Under this authority, AAFES may also provide services inherent to their internal operation. AAFES will not enter into contracts or agreements with other NAFIs, DOD elements, or other federal departments, agencies, or instrumentalities for the provision of goods and services that will result in the loss of jobs created pursuant to the Randolph-Sheppard Act, or small business programs. Before entering into a contract or other agreement, AAFES will ensure that the contract or agreement will financially benefit AAFES, considering fixed and variable direct and overhead costs (including depreciation).

f. Other government activities referenced above may consider AAFES as a provider of such goods and services prior to the initiation of the competitive procurement process. However, if the competitive procurement process by other government activities has been initiated, pursuant to the above authority, AAFES may submit bids or proposals in response to the competitive procurement.

9–2. Authority

a. The AAFES director and chief executive officer is vested with the responsibility and authority for worldwide AAFES procurement of merchandise, supplies, motion picture services, facilities, equipment, architect-engineering services, construction, and renovation of equipment and facilities. The official assigned responsibility for procurement management, HQ, AAFES, is sub-delegated the procurement authority of the AAFES director and chief executive officer to manage procurement policies, procedures, and authority as outlined herein. Procurement, including preliminary communications and negotiations, will be done only through, or as authorized by, the AAFES director and chief executive officer or designee.

b. The procurement authority of the AAFES director and chief executive officer includes—

(1) Authority to negotiate, execute, approve, and administer contracts and amendments or changes to them.

(2) Authority to appoint contracting officers.

(3) Authority to issue uniform purchasing instructions and standard contract forms. The AAFES director and chief executive officer may approve deviations from the instructions and forms when consistent with applicable departmental regulations.

c. Only duly appointed AAFES contracting officers who have been specifically delegated the authority to execute contracts will perform AAFES procurement.

d. The HQ, AAFES will procure all feature length entertainment motion pictures for AAFES exhibition at AAFES theaters on Army and Air Force installations, to include contingency locations.

e. Aside from the automatic sub-delegation stated in paragraph *a*, above, the AAFES director and chief executive officer's procurement authority may be further delegated. All delegations are written and may be contained in AAFES purchasing procedures. Delegations may be by categories of personnel or to individuals. Authority of delegation will be as set forth in AAFES purchasing procedures.

f. A certificate of appointment will designate AAFES contracting officers. Appointing officials are delegated authority to issue certificates of appointment in purchasing procedures issued by the AAFES director and chief executive officer.

(1) The AAFES is not obligated to recognize or ratify actions by AAFES personnel who do not have certificates of appointment, or actions by personnel that exceed the limits of appointment. The AAFES personnel may be liable for unauthorized procurement actions and may be subject to administrative actions to include disciplinary actions.

(2) When issuing certificates of appointment, the appointing official considers the appointee's experience, training, education, business acumen, judgment, character, reputation, and ethics.

(3) Termination of contracting officer's authority will be automatic upon termination of the individual. Other types of terminations of authority will be in writing.

9–3. Mandatory contract clauses

Clauses that must be included in all AAFES contracts are listed below. If language is not specified in this regulation, as shown by quotation marks below, the AAFES director and chief executive officer issues required language in AAFES purchasing procedures, subject to review and approval by the AAFES general counsel. If language is specified below, all deviations must be approved in advance by the AAFES director and chief executive officer with concurrence of the AAFES general counsel.

a. Legal status. "The Army and Air Force Exchange Service (AAFES), including its activities, offices and individual exchanges, is an integral part of the Departments of the Army and Air Force and an instrumentality of the United States Government. AAFES contracts are United States contracts; however, they do not obligate appropriated funds of the United States except for a judgment or compromise settlement in suits brought under the provisions of the Contract Disputes Act of 1978, as amended, in which event AAFES will reimburse the United States Government. AAFES procurement policy is established by applicable directives and instructions promulgated by DOD. The Federal Acquisition Regulation (FAR) does not apply to AAFES."

b. Disputes. A clause implementing the Contract Disputes Act of 1978, as amended.

c. Representations. "Contractor will not represent themselves to be an agent or representative of AAFES, another instrumentality, or an agency of the United States."

d. Advertisements. "Contractor will not represent in any manner, expressly or by implication, that products purchased under this contract are approved or endorsed by any element of the United States, including AAFES. All contractor advertisements that refer to AAFES or military exchanges will contain a statement that the advertisement was neither paid for nor sponsored, in whole, or in part, by AAFES, the military Exchange system, or the U.S. Government."

e. Examination of records.

(1) This clause applies if the amount of the contract exceeds $10,000 and the contract was entered into by means of negotiation. The contractor agrees that the contracting officer or their duly authorized representative will have the right to examine and audit the books and records of the contractor directly pertaining to the contract during the period of the contract and until the expiration of 3 years after the final payment under the contract. The contractor agrees to include this clause in all subcontracts that exceed $10,000.

(2) Government Accountability Office may be substituted for contracting officer or his duly authorized representative when the prospective contractor does not accept the standard wording of the examination clause.

(3) Contracts awarded to foreign contractors may exclude the examination clause when its use is precluded by the laws of the country involved, subject to the approval of the servicing AAFES general counsel (HQ, AAFES and AAFESEurope). Contract files will in such circumstances be documented to show the basis for exclusion of the clause.

f. Hold harmless clause. A clause providing that the contractor will hold harmless the United States and AAFES from any claims or legal actions arising from the contractor's activities. Such clause will not give the contractor the right to control defense of any suit brought against AAFES or the United States.

g. Defining clause. A clause defining the term "contracting officer" and any other personnel authorized to act on behalf of AAFES with regard to the contract.

h. Insurance. Insurance clauses appropriate for the contract.

i. Gratuity and contingent fee. A gratuities and contingent fee clause.

j. Assignment of Claims Act. A clause prohibiting the assignment of AAFES contracts under the Assignment of Claims Act.

k. Labor. Clauses implementing labor and socioeconomic laws and regulations applicable to AAFES contracts, including, but not limited to—

(1) EEO requirements.

(2) Department of Labor requirements.

(3) Service Contract Act.

(4) Davis-Bacon Act.

(5) Contract Work Hours and Safety Standards Act.

l. Construction. Applicable clauses from the Copeland Anti-Kickback Act and the Miller Act. The Miller Act clauses may be omitted if the performance and payment bond requirements are waived.

m. Termination. A contract termination clause.

9–4. Minority business concerns

a. Certain contracts for concession services, not currently available on a military installation, may be set aside for minority business concerns. The Minority Business Development Agency identifies the eligible concerns and the AAFES director and chief executive officer issues purchasing procedures for contract awards. The definition of "concession services" for purposes of this provision will be as contained in AAFES purchasing procedures.

(1) Each nominated minority concern is eligible for only one reserved contract at a time. If the nominee is a franchisee or subsidiary of a minority business enterprise, the one contract limitation will apply to the franchiser or parent firm as if it and the franchisee or subsidiaries were one entity. If a nominated firm is determined ineligible for a reserved contract under this provision, it will be included on the source list for competitive solicitation of the service if otherwise eligible.

(2) Any follow-on contracts for the same service will not be set aside for the incumbent minority business concern. The concern will be placed on the source list, subject to AAFES purchasing procedures concerning eligible sources.

(3) Before making awards to minority business concerns under this program, the contracting officer must determine that price and fees are fair and reasonable.

b. Contracting officers award contracts for equipment or expense items under $1,000 (or construction or renovation not exceeding $2,000) to responsible minority businesses, when AAFES requirements can be met and prices are determined to be fair and reasonable. Contracts will be awarded to these firms without competition and according to purchasing procedures issued by the AAFES director and chief executive officer.

9–5. Services, agency, concession, and vending agreements

a. Contractually operated activities operate under one of the following types of contracts, as defined in the glossary:

(1) Services.

(2) Agency.

(3) Concession.

(4) Vending.

b. These contracts may be for a period not to exceed 5 years. The AAFES director and chief executive officer may approve an initial contract period, or a combination of initial contract period and renewal options exceeding 5 years, but not more than 25 years total. Such approval may be granted only when—

(1) The contract investment is largely unrecoverable within 5 years; or

(2) It is necessary in order to allow a reasonable return on investment to AAFES; or

(3) It is necessary for the life cycle cost of a particular product or service to include product upgrades, enhancement, and maintenance support; or

(4) It is of such magnitude that a longer period is necessary in order to allow a reasonable return to AAFES and the contractor or in order to permit amortization consistent with industry standards.

c. These contracts may contain provisions permitting the contracting officer to extend the contract without resorting to competitive solicitation. To extend the contract without competition, the contracting officer must find that the issuance of a competitive solicitation will not be to the advantage of AAFES. Such contracts must be opened to competitive solicitation not less frequently than once every 5 years, unless a longer period has been approved per paragraph *b*, above, or prior approval for extension beyond a 5–year period has been granted, in writing, by the AAFES director and chief executive officer. The authority to approve contract extensions for a period beyond 5 years may be delegated by the AAFES director and chief executive officer to officials who are assigned responsibility for HQ, AAFES procurement management, without power of redelegation.

d. Short-term concession contracts may be awarded noncompetitively by GMs for the sale of unique merchandise or services that are not normally sold in AAFES exchanges. Authority to award these contracts may not be delegated to subordinate exchange personnel. Short-term concessionaires may sell only cash and carry merchandise and shall not be allowed to take customer orders that cannot be filled by the last day of the sales period during which the order is taken. Short-term concessionaires may not sell or provide customer services except as incidental to the sale of merchandise.

9–6. Procurement of retail merchandise

a. Retail merchandise is selected consistent with industry standards and federal laws and regulations applicable to AAFES (see chap 11 for procurement of alcoholic beverages).

b. Purchases of merchandise for resale will not be made under extended credit arrangements or on a consignment basis, except as authorized, in writing, by the AAFES director and chief executive officer.

c. Interested suppliers will be treated fairly. If their merchandise is not selected for purchase, they will be advised of the reason.

9–7. Procurement of fixtures, equipment, and supplies

Procurement of AAFES fixtures, equipment, and supplies is accomplished in accordance with purchasing procedures issued by the AAFES director and chief executive officer. The AAFES is authorized to purchase, on a reimbursable basis, expense-type supply items in the operation of exchange activities from Army and Air Force installation-level stocks.

9–8. Military uniforms

Purchase of articles of uniform and insignia will be from sources approved and certified in accordance with applicable quality control procedures of the Departments of the Army and the Air Force and purchasing procedures issued by the AAFES director and chief executive officer.

9–9. Sources of supply

HQ, AAFES will issue contracts for requirements that are common among AAFES exchanges. The CONUS and overseas regions may also establish contracts for items that are not available from a HQ-established source, consistent with purchasing procedures issued by the AAFES director and chief executive officer.

9–10. Quality assurance program

The AAFES director and chief executive officer establishes and maintains a quality assurance program to ensure high standards of merchandise, services, equipment, and supplies sold or used worldwide.

9–11. Procurement for contractors

a. Region senior vice presidents or overseas region commanders may authorize AAFES procurement, or transfers of AAFES-owned merchandise, supplies, or equipment, to contractors, on a reimbursable basis, when determined that it will result in better service and lower prices to the customer or it will contribute to uniformity in operations. This does not authorize tax-free purchases for private organizations. However, such transfers will not be made if they are in violation of applicable international agreements in overseas regions.

b. The AAFES director and chief executive officer issues operating procedures for AAFES procurement or transfers of AAFES-owned goods to contractors.

9–12. Liability as an agent

Where an AAFES activity acts in an agency capacity for a vendor or a supplier, its liability will be limited to that of an agent, and it will not bind itself to perform any of the obligations of the principal.

Chapter 10
Transportation

10–1. Mode of transportation

a. The AAFES director and chief executive officer is responsible for traffic management as it concerns movements of AAFES goods.

b. The mode of transportation of AAFES cargo destined for overseas is determined by AAFES in accordance with applicable departmental transportation regulations. When costs of transporting AAFES cargo are paid from NAFs, AAFES, at its option, may use the Defense Transportation System or contract for commercial transportation.

10–2. Ocean shipments

a. Surface shipments. The oceanic surface movements of exchange cargo will be financed per applicable departmental transportation regulations.

b. Shipments through port terminals. Movement of AAFES merchandise, equipment, and supplies through military ocean terminals will be per applicable departmental transportation regulations. AAFES liaison personnel may be stationed at military terminals to assist in the management of the movement and control of AAFES supplies.

10–3. Inland movement

The funding and mode of transportation of AAFES merchandise, equipment, and supplies within CONUS and not destined for OCONUS is the responsibility of AAFES.

10–4. Air transport

a. Military airlift. AAFES will coordinate, as necessary, with U.S. Transportation Command for movement of AAFES cargo via military aircraft. Requirements for military airlift from CONUS in connection with essential exchange merchandise, equipment, or supplies in all categories will be confined to high value, emergency type or seasonal items when other modes of transport are not reasonably available at reasonable cost or will not meet the delivery requirements. Air shipments will be limited to sufficient quantities for immediate needs with the balance directed by water or other means of transport.

b. Commercial air shipments. Per applicable DODDs and DODIs, when it is determined to be more cost effective and efficient than military airlifts or to satisfy emergency requirements, AAFES may use tailored, commercial air service for expedited movement of highly perishable, time-sensitive commodities.

10–5. Mail shipments to destinations outside the continental United States

AAFES small package shipments (such as catalog and Internet sales) of merchandise, supplies, or equipment may be mailed from CONUS to OCONUS exchanges through the military postal channels (Army/Air Force Post Office or Fleet Post Office).

10–6. Funding

a. DA is responsible for the appropriation funded fiscal requirements associated with the overseas transportation of AAFES cargo. Responsibilities include the programming and budgeting of operation and maintenance funding to support overseas transportation and port handling of AAFES cargo.

b. Appendix B provides guidance on the authorized use of APF and NAF funding for transportation-related expenses.

Chapter 11
Alcoholic Beverage Sales

11–1. Class Six Program

a. AAFES is the single manager of packaged alcoholic beverage stores (historically called Class Six) and the primary wholesaler of alcoholic beverages on Army and Air Force installations and other locations where AAFES has exchange outlets.

b. AAFES will operate the Class Six Program for the sale of alcoholic beverages.

c. Packaged non-alcoholic, alcoholic beverage substitutes are sold only in exchange facilities and only to those customers authorized to purchase alcoholic beverages.

d. For all locations, garrison and installation commanders, in coordination with AAFES, authorize where Class Six stores are sited. AAFES will coordinate proposed Class Six facility closures and consolidations with the garrison installation commander. There will be no expansion of distilled spirits or wine products to traditional AAFES activities without agreement of the garrison and installation commander. Once introduced, AAFES will manage products as any other category of merchandise.

e. The AAFES director and chief executive officer prescribes the alcoholic beverage stock assortment using similar criteria as any other category of merchandise.

f. Outside of the United States, wines and malt beverages produced in the United States receive equitable distribution, selection, and price when compared with wines and malt beverages produced in the host nation.

g. Outside of the United States, the sale of packaged alcoholic beverages with an alcoholic content of more than 7 percent by volume may be approved by the Exchange Service director/chief executive officer provided such sales do not contradict treaties, SOFA, and local government agreements.

h. All beverages sold by AAFES will be labeled according to the Alcoholic Beverage Labeling Act of 1988, as amended.

i. Credit cards may be accepted for alcoholic beverage purchases.

j. The price of bulk/case items must be displayed by signage or through individual pricing methods.

k. Garrisons and installations will not enter into competition with AAFES operations. Sale of packaged alcoholic beverages by other authorized MWR programs for off-premise consumption will be restricted to time periods when AAFES-operated retail activities are closed and at no less than AAFES prices. Sales of beer and wine products incidental to party contracts or take-out food/beverage operations are excluded from the foregoing. Take-out beverage sales for personal and individual use are normally limited to sales of 4–packs, 6–packs, or similar small quantities. Other exceptions must be approved jointly by the respective Services and AAFES.

11–2. Promotions

a. AAFES sponsored promotions of alcoholic products are not authorized. For example, there will be no distribution of coupons and free samples to promote or advertise the sale or consumption of specific brands of alcohol.

b. Commercially sponsored promotions are authorized for Class Six stores, if—

(1) The promotion is not targeted exclusively to the military community.

(2) The promotion is of the type available to the general public.

c. Beverage tastings, sponsored either by AAFES or vendors, are authorized if patronage controls and all restrictions concerning the sale of alcoholic beverages are enforced during tastings.

11–3. Controls

a. Packaged alcohol beverage outlets are operated solely for the benefit of authorized purchasers. Members of the uniformed Services and other authorized purchasers will not sell, exchange, or otherwise divert packaged alcoholic beverages to unauthorized personnel or for purposes that violate federal, state, or local laws, or SOFAs.

b. Garrison and installation commanders remain responsible for ensuring that the use of alcoholic beverages is consistent with the DOD controls in paragraph *a*, above. Garrison/installation commanders, with the coordination of the GM, AAFES, remain responsible for reviewing the amount of alcoholic beverages purchased in packaged alcohol beverage outlets against the number of authorized purchasers.

11–4. Packaged alcoholic beverage outlet establishment

a. The Secretary of the Army and the Secretary of the Air Force must approve the establishment of all Class Six stores (selling alcohol with 7 percent or more alcoholic content by volume) on garrisons and installations in the United States. Exchanges may sell wine, malt beverages, wine coolers, and other low alcoholic beverages with less than 7 percent alcoholic content by volume without establishing a Class Six store.

b. Before requesting the establishment of a Class Six facility in the United States, many factors must be considered, primarily the importance of profits to provide, maintain, and operate MWR programs, to lighten the financial burden on Soldiers/Airmen, and support and complement community programs for Soldiers/Airmen and their families. Other factors include—

(1) The estimated number of authorized patrons.

(2) The availability of wholesome family social clubs to military personnel in the local civilian community and limitations on non-military sources.

(3) Geographical inconveniences.

(4) Disciplinary and control problems caused by restrictions imposed by local laws and regulations.

(5) Highway safety.

(6) Location and distance of nearest package store and reasons that the use of that facility is not feasible.

(7) A digest of attitudes of community officials, local businesses, and civic organizations toward establishment of a Class Six outlet. This digest consists of a summary of any written comments received from individuals and agents such as local mayors, heads of prominent civic groups, or chambers of commerce, state legislators, members of Congress, or other government officials. The names of the community authorities and civic organizations, including the circumstances of the contacts and the dates on which they occurred are included unless letters from local contacts are submitted. Speculative assessments of prospective community attitudes will not satisfy this requirement.

c. Local commands, in coordination with AAFES, wishing to establish a Class Six store will submit requests through their command channels to HQ, AAFES. HQ, AAFES will submit the request to the Army IMCOM, G–9 (Family and MWR Programs) or Air Force Services, per applicable departmental regulations (AR 215–1 or AFI 34–219). A request for approval will be submitted to the Secretary of the Army or the Secretary of the Air Force, as applicable. Requests must include all of the information detailed in paragraph *b*, above. The Secretary of the Army or the Secretary of the Air Force, as applicable, will notify the responsible Assistant Secretary of Defense and Congress. HQ, AAFES will be notified upon approval by the Service Secretary, as applicable.

d. Where a package store operation is authorized for a garrison and installation, the Exchange may operate in an independent facility or merge the alcoholic beverage operation with other exchange activities provided the garrison and installation commander concurs, the stock and displays are segregated, and all inventory controls, ration controls, and signage required for alcoholic beverages are in effect.

11–5. Triennial review

a. A review of packaged alcoholic beverage store operations in the United Sates is required every 3 years by the Service Secretary concerned. The review is to determine the need for continued operation. The evaluation will consider such factors as—

(1) Number of authorized patrons.

(2) Contributions of profits to providing, maintaining, and operating military MWR programs.

(3) Availability of wholesome family social clubs to military personnel in the local civilian community.

(4) Geographic inconveniences.
(5) Limitations of non-military sources.
(6) Disciplinary and control problems.
(7) Highway safety.

b. The above factors are generally the same as those for establishing such operations, prescribed in AR 215–1 and AFI 34–219.

c. If any of the above factors are adversely affected, consideration will be given to closing the packaged alcoholic beverage store operation.

11–6. Purchase eligibility

a. United States and the District of Columbia. The authorized age for the purchase of alcoholic beverages in AAFES U.S. facilities is consistent with the law of the state in which the garrison and installation is located. As states enact new drinking age laws, the timing of revised garrison and installation drinking age policy shall coincide with implementation of the new state laws by state and local authority. Exceptions to this guidance are as provided in applicable departmental regulations.

b. Overseas. The authorized age for the purchase of alcoholic beverages in AAFES overseas facilities is 18 years or older. This applies to all authorized patrons. Decisions on a higher minimum age will be based on treaties and international agreements and policies of the local command.

c. Proof of eligibility. All patrons are required to show purchase eligibility before a sale is made. An exception is patrons in full regulation uniform need no identification unless there is doubt as to active duty status or age. Special procedures for ration control regulations may be required, if applicable.

11–7. Alcohol seller training

All employees involved in selling alcohol will be trained on subjects such as the effects of alcohol, how to identify intoxication, and what to do when a person becomes intoxicated. Employees selling alcohol are required to sign a dram shop certification, which will be documented in their personnel file.

11–8. Procurement procedures

a. The AAFES procures alcoholic beverages under the most advantageous contract unless applicable federal laws and regulations restrict procurement.

b. Within the 48 contiguous states of the United States and the District of Columbia, AAFES may procure alcoholic beverages containing distilled spirits (does not include malt beverages and wine) from the most competitive source, price and other factors considered.

c. In Hawaii and Alaska, alcoholic beverages containing distilled spirits must be procured from a source within the respective state in which the garrison and installation is located.

d. Malt beverages and wine must be procured from a source within the respective state in which the garrison and installation is located (includes the District of Columbia).

e. If an installation is located in more than one state, then the source may be in any state in which the garrison and installation is located.

f. Consignment sales of alcoholic beverages are prohibited. AAFES must own the product sold.

11–9. Alcohol sales to morale, welfare, and recreation/nonappropriated fund activities

a. The AAFES provides requested products to authorized MWR/NAF activities selling alcoholic beverages by the drink, on a priority basis.

b. Any AAFES sales (from Class Six or warehouse) to MWR/NAF activities will be at landed cost.

c. MWR/NAF activities are not authorized to resell packaged alcoholic beverages for less than full AAFES retail price.

d. If permitted by departmental regulations, sales of alcoholic beverages to non-MWR/NAF activities will be at no less than full AAFES retail price, or as determined by the AAFES director and chief executive officer. Headquarters of the Army and Air Force may grant exceptions for official government functions when alcohol is purchased with APFs by other U.S. Government agencies.

Chapter 12
Motion Picture Service

12–1. Establishment and operational requirements of entertainment motion picture theaters

A written request for establishment of motion picture service will be submitted to appropriate CONUS region director

or overseas region commander through command channels, sufficiently in advance of requirement for service, with information as follows:

a. Name, mailing, and message addresses of requesting unit.

b. Name, grade, and telephone numbers (military and civilian) of unit officer to be contacted regarding the establishment of service.

c. Telephone numbers (military and civilian) of unit commander's offices.

d. Present and projected military and Family member strength, number of civilians authorized to attend the theater, and will attendance be sufficient to support this service.

e. Distance (in miles) from nearest civilian theater. If overseas service is requested, distance from nearest English language civilian theater, if there is one in the host nation.

f. Distance (in miles) from nearest videocassette or U.S. forces military theater.

g. Accessibility of post office or other methods of transporting video cassettes or films.

h. If cinema motion picture service is desired and a theater building is to be used, the following items should be considered:

(1) Facility available, including type of building, floor plan, longitudinal and horizontal sections of auditorium, and sizes, types, and locations of entrance and exit doors.

(2) Accurate projection room dimensions, including the type of construction, and the location of the projection and observation portholes.

(3) Voltage, cycle, and phase of electric power.

(4) Adequate seating and sanitary facilities for the seating capacity, appropriate lighting, and a building suitable for presenting motion pictures.

i. If cinema motion picture is desired and a multi-purpose building not designed for motion picture showings is to be used, the following items should be considered:

(1) Type of building.

(2) Distance, in feet, from screen to proposed location of projector.

(3) Ceiling height, in feet, at screen location.

(4) Indication of any lighting fixtures or other obstructions that would interfere with projection.

(5) Distance, in feet, from proposed location of projectors to power outlet.

(6) Indication of whether projector, screen, and speaker will be left in position from one performance to another, or whether they will be removed to permit other activity in the building.

j. If videocassette service is desired, the following items should be considered:

(1) Type of building.

(2) Room location.

(3) Type of storage security for cassettes.

(4) Check-out security procedures for cassettes.

(5) Type of viewing and playback of videocassette equipment.

(6) Estimated number of reviewers for each movie.

k. Request for service for field training exercises or maneuvers will be submitted reasonably in advance of requirements and will include the following additional information:

(1) Identification of all units served.

(2) Rotation period of each unit to be served.

(3) Unit strength or average number of troops in the field each week.

(4) Distances of troop billeting or bivouac areas to nearest military and commercial theaters.

(5) Duration of requirement for film service.

12–2. Type of film service

Based on the information provided in paragraph 12–1, the AAFES director and chief executive officer will determine the type of service to be provided. The service originally provided may be changed at any time conditions warrant.

12–3. Film showings

a. HQ, AAFES will procure all feature length cinema motion pictures for AAFES exhibition at theaters on Army and Air Force garrisons and installations, to include contingency locations.

b. AAFES has the exclusive authority to obtain films from industry distributing companies.

c. Film ratings established by the motion picture industry are used.

d. Other than films obtained from the motion picture industry, AAFES may exhibit national anthem trailers. These trailers will be supplied by the local command.

e. Motion picture films, videocassettes, and digital versatile discs will not be shown to support fund-raising activities.

f. Films are exhibited only with subjects scheduled by AAFES, only in officially authorized theaters, and only at authorized performances.

g. Motion picture facilities are intended for the purpose of motion picture entertainment; all non-military uses are subordinate. The facility will be known as an entertainment motion picture theater only during the period when used for the paid admission exhibition of cinema motion pictures.

h. Garrison and installation commanders will provide APFs to equip, operate, and maintain theater facilities to include seating. Maintenance of facilities includes maintenance of the grounds and structures or the outdoor areas approved for presenting entertainment motion picture programs. Commanders will use APFs to equip, operate, and maintain theater facilities for all purposes except when they are used for showing entertainment motion picture programs.

i. Marquees, theater changeable letter signs, one sheet display frames, and sound and projection equipment will be used for approved performances of entertainment motion picture films only.

j. Garrison and installation commanders will appoint a building custodian for the theater facility when it is used for purposes other than a paid admission theater.

k. The cancellation of motion picture showings to promote attendance at other recreational or athletic activities or the observance of religious holidays is not authorized.

l. Guests may attend motion picture theaters, provided they are accompanied by personnel authorized exchange privileges.

12–4. Additional theater expenses

AAFES will pay all personnel costs in the routine operation of paid admission entertainment motion picture theaters. AAFES will also pay for the purchase of operating equipment and supplies. AAFES will pay janitorial services only for the periods when the theater is used to show AAFES cinema motion pictures. When the theater is used for other purposes, the commander (Army or Air Force supply agency) will provide janitorial services, to include expendable articles of regular issue needed to maintain and clean the theater.

12–5. Admission charges

a. Admission charges will be established by the AAFES director and chief executive officer.

b. All cinema motion pictures will be shown on a paid admission basis, noting provisions referenced in paragraph 12–7, for special shows.

c. Videocassette showings are to be on a free admission basis, unless paid admission service is approved by the AAFES director and chief executive officer.

d. Free admission videocassette showings may be established under the following circumstances:

(1) Where the present and projected population is such that paid admission service is not economically feasible.

(2) When military personnel are engaged in field training exercises or maneuvers for a period exceeding 7 days.

(3) Equipment, supplies, personnel, and servicing costs required will be provided by the garrison and installation commander with APFs.

(4) When theater facilities are not available.

(5) Free admission videocassette service will not be set up within 3 miles of, or at, any place considered to be in competition with a paid admission Army, Air Force, or commercial theater, unless approved by the AAFES director and chief executive officer.

(6) A maximum of two programs a week on a free admission basis may be provided at military confinement facilities. Attendance will be restricted to military prisoners and essential attendants.

12–6. Exhibition

a. Entertainment videocassette or cinema motion picture programs will consist only of subjects scheduled by AAFES and will be exhibited only in officially authorized theaters. No part of a motion picture program may be used at other than authorized performances.

b. Television films and non-entertainment motion pictures and slides in such subjects as orientation, training, appeals for funds, appeals for attendance at activities, appeals to support a cause, recruitment, or those of a purely educational nature will not be used in connection with regularly-scheduled entertainment motion picture programs.

c. Requests will not be made upon motion picture companies or their agents or employees for free admission or paid admission showings of any film subject. Any offers of a film subject for free admission or paid admission showings will be rejected unless a unit at a particular installation participated in making the picture. In these cases, the commander will inform HQ, AAFES of the arrangements that were made with the producer so that the showing may be cleared with the appropriate distributing company.

12–7. Special shows and other uses

a. Showing of films for special programs. Showings of cinema motion pictures without an individual admission charge are authorized for organization day programs or special programs in which the organization participates as a

whole. These may be held when paid for from funds available to the organization, based on the actual attendance and the established admission rates.

b. Showing of films in other facilities. After formal concurrence from AAFES, garrisons and installations are authorized to obligate or spend NAFs for the rental or purchase of any motion picture films for entertainment recreational showings in MWR/NAF activities. The garrison and installation is responsible for obtaining the required public performance license for such showings. Commercially sponsored films (including television films) not of feature length, and available without cost, may be shown in recreation centers and military clubs (open messes). These showings will start a half hour after the scheduled opening performance at the Army and Air Force theaters and will not be held more frequently than twice a week. Films used for this purpose will not include those that are normally included in Army and Air Force theater programs.

c. Utilization for training purposes. Occasionally, requests are received from installations for authority to exhibit, on a free admission basis, AAFES-scheduled motion pictures (or portions) that may be considered to have training or orientation value. AAFES does not hold title to the films. Such requests will not be approved.

d. Utilization for benefit purposes. Entertainment motion picture films and videocassettes will not be used to support fund-raising activities.

12–8. Leasing arrangement

a. Entertainment motion picture films and videocassettes distributed by AAFES are leased from commercial distributors authorized to do so under film and videocassette copyrights. AAFES has a property right, as a lessee, only during the license period specified in the rental contracts.

b. The taking, damaging, destruction, or unauthorized use of motion pictures and videocassettes leased by AAFES could subject individuals to civilian liability, and to criminal prosecution.

Chapter 13
Claims and Incidents of Misconduct and Losses

13–1. Tort and tort-type claims

a. Tort and tort-type claims arising from AAFES operations will be investigated, processed, and settled in accordance with applicable departmental regulations.

b. Awards on administrative claims will be paid from AAFES self-insurance funds.

c. The GM, AAFES will notify, immediately, the servicing SJA of any incident likely to result in a claim for personal injury or property damage. Servicing legal offices will notify the Office of the AAFES General Counsel, General and Revenue Recovery Law Branch, within 3 duty days of receiving a claim SF 95 against AAFES. For cases such as serious vehicular incidents occurring off-post, the SJA should consider requesting investigative assistance from AAFES regional loss prevention personnel. These requests may be submitted through the AAFES general counsel. The GM, AAFES will also notify the garrison and installation of any corrective measures necessary to prevent potential incidents from occurring.

13–2. Other claims

a. The Military Personnel and Civilian Employees' Claims Act of 1964 provides for AAFES civilian personnel benefits, except that payment of claims will be made only from AAFES self-insurance funds or per applicable insurance contracts.

(1) Personal property claims of AAFES civilian employees for loss or damage incident to their Service, inclusive of those arising out of the authorized permanent change of station (PCS) movement or storage of household effects, personal effects, and privately owned vehicles, will be investigated, processed, and settled per AR 27–20 and AFI 51–502.

(2) AAFES employees may, at their own expense, insure against any damages or losses in excess of limits of applicable regulations.

b. Cash payment, services, or replacement will settle customer complaints arising out of operations of AAFES activities in kind. Any such claims that cannot be satisfactorily settled in this manner, or any claim of this nature that includes a demand for consequential damages (such as personal injury or property damage other than to the article purchased, serviced, lost, or damaged), will be investigated, processed, and settled by the same authorities and procedures applicable to tort and tort-type claims.

c. Claims arising out of, or related to, AAFES contracts will be processed according to applicable federal law, contract provisions, and AAFES EOPs and exchange service regulations.

d. The following miscellaneous claims will be processed in accordance with EOPs and exchange service regulations issued by the AAFES director and chief executive officer:

(1) Marine cargo losses.

(2) Claims against vendors, commercial carriers, and the U.S. Postal Service.
(3) Claims arising out of workmen's compensation.
(4) Group insurance and retirement annuity insurance.

13–3. Criminal investigations

AAFES personnel will comply with applicable departmental regulations concerning criminal investigations.

a. The overseas region commanders, HQ, AAFES chief of staff, U.S. region and overseas senior vice presidents, and GMs will report the following incidents promptly to the servicing military or civilian law enforcement authority for investigation or referral to U.S. Army Criminal Investigation Command, AFOSI, and Federal Bureau of Investigation, as appropriate: arson, assault, burglary, embezzlement, forgery, homicide, larceny, robbery, shoplifting, and other acts of criminal misconduct involving exchange operations. Incidents requiring criminal investigations in offshore and overseas areas will be reported as indicated above, except when alternate procedures are established by host country agreements or local command directives.

b. Irregularities involving standards of conduct, other than criminal misconduct, of exchange personnel, contractors, suppliers, their agents, and representatives will be promptly reported to the servicing Loss Prevention Office or HQ, AAFES, Office of Inspector General Fraud, Waste, Abuse, or Mismanagement Hotline.

c. All AAFES personnel are responsible for reporting any incidents or suspicion of incidents of misconduct or irregularities involving AAFES operations. Reports are given to an immediate supervisor, or higher official, if any person in the chain of command is suspected of involvement. Failure to report such incidents constitutes grounds for separation for cause or other disciplinary action. Incidents can also be reported to the HQ, AAFES Office of Inspector General Fraud, Waste, Abuse, or Mismanagement Hotline.

d. Incident reports and reports of investigations covering the incidents above will be furnished to HQ, AAFES, Loss Prevention Office, per applicable departmental regulations, EOPs, and exchange service regulations issued by the AAFES director and chief executive officer.

13–4. Pecuniary loss investigations

a. An investigation into pecuniary loss is conducted by an officer (military or civilian) appointed by the AAFES director and chief executive officer. At the discretion of the AAFES chief financial officer (CFO), if no qualified commissioned officer assigned to duty with AAFES or no AAFES civilian employee is reasonably available, or it is determined that an investigating officer outside of AAFES would be advisable, the AAFES director and chief executive officer may appoint any qualified commissioned officer made available by the local garrison and installation commander.

b. Reports of investigation will be prepared in the format and processed per procedures prescribed by the AAFES director and chief executive officer.

c. Loss or damage of APF property is processed per applicable departmental regulations.

13–5. Other non-criminal investigations

The AAFES director and chief executive officer, or the overseas commanders, have authority to appoint investigating officers to investigate non-criminal conduct of AAFES associates and assigned military members. This authority may be delegated to the deputy director, AAFES, and may not be further delegated. All investigations shall be coordinated with the servicing general counsel. This provision does not restrict the mission of the Loss Prevention Directorate, who routinely conducts investigations into acts of misconduct, unethical behavior, and other matters of official interest. The authority to initiate loss prevention conducted investigations rests with the vice president, loss prevention, or other authorized designee.

13–6. Restitution and collection

Restitution and collection action, as specified below, is taken when a recommendation of pecuniary liability by an investigating officer has been approved, or when the CFO has made an administrative determination that an individual is pecuniary liable or accountable for a loss or shortage. The CFO may delegate this authority. An administrative determination of indebtedness in favor of a constituent element of AAFES is a determination that the indebtedness is due and owed AAFES. The AAFES, its constituent exchanges, and other exchange facilities constitute a single integrated fiscal entity. The following procedures apply to restitution or collection (they do not apply to dishonored checks):

a. The individual concerned receives a written request for payment, with a copy of the report of internal management review or investigation or other documentation upon which pecuniary liability is based. The request will show the basis for the liability, provide notice that an administrative determination has been made that the individual is liable to AAFES, and include appeal rights specified in paragraph 13–7.

(1) If the individual concerned is a military member assigned to a remote location or employed by an AIFA, the request for payment is submitted to the individual's commanding officer, with a copy of the report of internal management review or investigation or other documentation upon which pecuniary liability is based.

(2) If the individual concerned is an AAFES civilian employee and refuses to pay the indebtedness voluntarily, the amount of the claim is deducted from any money AAFES owes the employee. Collection of claims against AAFES foreign national personnel in overseas areas is according to local laws.

(3) If the individual concerned is an active duty Servicemember, the GM, AAFES, having been unable to effect voluntary collection, will report the indebtedness, with all relevant information, to the individual's unit commander. If the unit commander cannot effect voluntary cash settlement in a timely basis, the Exchange—

(a) Prepares the appropriate departmental form naming the Exchange as claimant.

(b) Submits the appropriate form to the servicing finance and accounting office as certification and payment.

(4) If the individual concerned is a retired Servicemember and indebtedness is not voluntarily collected, the claim is submitted to the appropriate retired pay branch for collection. The finance office records the indebtedness on the individual's pay and forwards collected amounts to the Exchange concerned.

(5) If the individual concerned is a civilian employee paid from APFs, and the debt is not voluntarily collected, the appropriate civilian personnel officer or the garrison and installation commanders will be asked to assist in collecting the debt. Documentation supporting the indebtedness will be forwarded with the request.

(6) If the individual concerned is an AAFES employee paid from NAFs, and the debt is not voluntarily collected, the responsible manager will send collection notification to the payroll office unless there is an appeal. A copy of the collection notification is sent to the employee. The amount deducted in any one pay period must be reasonable in terms of net pay and, generally, should be sufficient to satisfy the debt in 5 to 10 pay periods.

b. Consistent with applicable laws and regulations, AAFES may use all available means to collect valid debts to AAFES.

13–7. Appeals

a. Except for losses resulting from dishonored checks, when a person is notified of an approved report of investigation or determination of pecuniary liability for a loss, reconsideration may be requested. A written request for reconsideration to the AAFES CFO, with supporting explanation, must be submitted within 30 days after receipt of the notice of assessment of pecuniary liability. The appeal must state specifically the alleged errors or irregularities relied upon.

b. In coordination with AAFES general counsel review, the CFO will reconsider the earlier action and give full consideration to the request and any other matter presented in support thereof. The appellant will be advised promptly of one of the following results:

(1) The action is revoked and a refund of any previous collection will be issued.

(2) A new or revised report of investigation will be completed.

(3) The request is denied and will be submitted to the AAFES director and chief executive officer for final decision.

c. If the request is denied, the CFO will submit a memorandum stating the basis for denial to the AAFES director and chief executive officer. This, with the following documents attached, will constitute the appeal of the CFO's decision to decline to change the assessment upon reconsideration.

(1) A copy of the request for reconsideration.

(2) All correspondence and other pertinent material.

(3) A copy of the approved report of investigation.

d. AAFES director and chief executive officer's decision on an appeal is final. The CFO will notify the appellant of the decision.

Chapter 14
Financial Planning, Accounting, and Accountability

14–1. Financial management

a. The financial objectives of AAFES are programmed and controlled by the Annual Financial Plan prepared by the AAFES director and chief executive officer and approved by the AAFES BOD. The plan includes projected income and expenses, the proposed capital program, the capital requirements schedule, and actual operating data to permit an analysis of projected data worldwide.

b. Quarterly, and at the close of each fiscal year, the AAFES director and chief executive officer issues a statement of financial position worldwide. Separate statements of financial position will not be prepared by any exchange, CONUS region, or exchange system within AAFES.

c. Exchange operating statements showing sales and other income costs, expenses, profits, depreciation, and significant statistical data will be prepared monthly as prescribed by the AAFES director and chief executive officer.

d. The AAFES director and chief executive officer publishes a uniform chart of accounts used worldwide, deviations from which are permitted only with prior written approval of the AAFES director and chief executive officer.

e. As prescribed by the AAFES director and chief executive officer, financial statements will be maintained to show AAFES assets and liabilities for management control of resources and operations.

f. To provide timely and essential management information and ensure adequate internal controls, finance and accounting will maintain standard accounting records as prescribed by the AAFES director and chief executive officer.

14–2. Financial management reports

a. The AAFES director and chief executive officer submits the financial management report, required by DODI 1015.15 for the preceding AAFES fiscal year to designated officials of the Departments of the Army and Air Force. AAFES financial report is audited by an external audit firm. The AAFES BOD submits this report annually to the Secretary of the Army and the Secretary of the Air Force.

b. Annually, the Departments of the Army and the Air Force will submit to AAFES data on APF costs and expenses in support of AAFES. This will be included in the report required by applicable departmental regulations and the annual report to both the Secretary of the Army and the Secretary of the Air Force.

c. The Army IMCOM, G–9 (Family and MWR Programs) forwards AAFES report to the PUSD(PR) after obtaining Air Force (AF/A1S) coordination.

14–3. Accountability

a. In normal practice, sales are made and accounted for in U.S. dollars or dollar instruments. The AAFES director and chief executive officer may authorize sales in foreign currencies in overseas areas.

b. Selling activities account for merchandise at retail value, using the retail inventory method. Accounting for other merchandise, supplies, equipment, and vehicles is at cost value.

c. Accountability and responsibility for AAFES assets worldwide is prescribed in EOPs and exchange service regulations.

d. Assignment and relief of accountable individuals on a temporary or permanent assignment basis will be documented as stipulated in EOPs and exchange service regulations issued by the AAFES director and chief executive officer.

14–4. Physical inventories

a. The AAFES director and chief executive officer designates the dates for worldwide physical inventories of cash, merchandise, and supplies. Such inventories will be taken at least annually. Fixed assets will be inventoried as directed by the AAFES director and chief executive officer.

(1) The AAFES director and chief executive officer delegates authority to the region senior vice president and vice president to appoint disinterested (not within the direct chain of command or permanently assigned to that location) chief and branch inventory inspectors, in writing.

(2) Appointed inventory inspectors are required to recheck assigned exchange inventories.

(3) Chief and branch inventory inspectors will control the use of inventory sheets.

(4) Chief and branch inventory inspectors will be disinterested AAFES employees. If sufficient exchange personnel are not available, the military commander provides the necessary personnel.

(5) When accountability variances occur as a result of the official annual physical inventory, adjustments will be made to the ledger. An adjustment to the ledger does not eliminate the requisite actions prescribed for asset write-offs, losses, restitution, and collections.

b. The AAFES director and chief executive officer, overseas region commanders, region senior vice presidents, or GMs may direct an inventory in case of catastrophe (for example, fire, flood, storm), burglary or theft, hostile action, or evidence of unsatisfactory accountability. When inventories other than the annual inventory are taken, variance will be maintained in a memorandum format.

14–5. Write-off of assets

a. Approval. The AAFES director and chief executive officer may approve write-off of AAFES assets. Write-off procedures, including delegations of write-off authority, will be contained in EOPs and exchange service regulations. Write-offs will be supported by documentation and justification initiated by the accountable and responsible individual.

(1) When a fixed asset is surplus to AAFES requirements and cannot be disposed of by trade-in or sale for reuse, it will be written off. The amount of the write-off will be acquisition cost less applicable accumulated depreciation.

(2) Write-off of accounts receivable, including Military Star Card payment charges, expired gasoline credit card charges, and vendor debit balances, will be initiated if and when considered uncollectable or expired.

b. Merchandise, supplies, or other inventory items of no value will be marked down to zero and disposed of by one of the following methods:

(1) *Transfer.* Transfer to an installation MWR fund/garrison MWR entity, the garrison and installation chaplain, other governmental entities, or the Defense Reutilization and Marketing Office. Receipt is issued for the no-value inventories. If the no-value inventory is sold by Defense Reutilization and Marketing Office, 90 percent of the proceeds of the sale will be sent to the Exchange.

(2) *Destruction.* The AAFES director and chief executive officer appoints an AAFES employee as a disinterested party to witness and certify.

14–6. Insurance

AAFES self-insurance funds are reserved to pay for losses not commercially insured. The AAFES director and chief executive officer issues policy concerning insurance coverage.

a. Named insured. Insurance policies covering claims against AAFES will expressly name the United States of America and AAFES as named insured. As appropriate, other AAFES elements may be listed as named insured to protect the interests of the United States against claims arising out of the activities of AAFES.

b. Legal proceedings. The legal status of AAFES, as a U.S. Government instrumentality, will not be interposed as a defense in any legal proceedings in which the insurer's liability is in any way concerned, unless so requested in writing by the AAFES director and chief executive officer, after obtaining approval of the appropriate SJA.

c. Subrogation. No subrogation action will be taken against the United States.

d. Contractor's insurance and bonds. The AAFES director and chief executive officer issues policy prescribing the types of insurance required of all businesses under contract with AAFES. Required insurance will be funded by the contracted business.

Chapter 15
Taxes

15–1. Federal taxes

a. Reporting and remittance of federal taxes, including claims for exemptions, refunds, and drawback of duties, will conform to applicable federal laws, regulations, EOPs, and exchange service regulations issued by the AAFES director and chief executive officer.

b. The U.S. Department of the Treasury may issue levies against the pay of exchange personnel.

c. Exchanges located in CONUS, Alaska, Hawaii, and U.S. possessions, are subject to occupational taxes if imposed by the U.S. Department of the Treasury.

d. AAFES must pay federal excise taxes on items that are subject to the taxes unless the purchase is for immediate export from the United States. In such case, the purchase by AAFES can be made tax-free if the appropriate exemption certificate prescribed by the U.S. Department of the Treasury is completed by the appropriate AAFES official and given to the vendor of the item.

e. Drawback of duties is allowed upon the exportation of articles manufactured or produced in the United States wholly or in part with the use of imported or substituted merchandise.

15–2. State, territorial, and local taxes

a. As an instrumentality of the United States, AAFES is entitled to the same immunity accorded the U.S. Government from the taxes of states, the District of Columbia, territories and possessions of the United States, the Commonwealth of Puerto Rico, and their political subdivisions.

b. Sales by exchanges are immune from state sales and use taxes. Purchases by exchanges are immune from direct state taxation.

c. The immunity of AAFES from direct state taxation does not extend to indirect taxation (taxes the legal incidence of which is on the wholesaler, manufacturer, importer, and the like, unless the state by law or regulation has granted an exemption on sales to the United States).

d. Concessionaires and other independent contractors are not entitled to claim AAFES immunity from taxation. Concessionaires must collect and remit applicable sales and use taxes as required by state jurisdictional law; contractors may be liable for sales and use taxes as provided by jurisdictional law.

e. State and territorial income taxes will be withheld from compensation of all civilian employees whose regular place of employment is within the state or territory.

(1) Taxes will be withheld when an agreement exists between the Secretary of the Treasury and the state or territory, pursuant to applicable federal law or regulation.

(2) On the request, and with the authorization of a civilian employee, and otherwise subject to withholding of pay under these agreements, voluntary withholding of income tax may be made in favor of the state of residence if that state has entered into such a withholding agreement.

f. Where the Secretary of the Treasury has entered into an agreement with a city to withhold from the pay of federal employees city income or employment taxes, AAFES is subject to such withholding requirements.

g. Taxes of a state, the District of Columbia, or a territory of the United States upon or measured by sales, purchases, storage, or use (except U.S. Government use) of gasoline or other motor fuels will be collected and paid according to applicable federal law.

h. Exchanges located in foreign countries, including occupied areas and the Trust Territory of the Pacific Islands, will not pay to, nor collect for, any foreign country or political subdivision of a foreign country any tax, unless the United States has consented to that levy or collection by international agreement.

i. Except as permitted by this regulation, or required by applicable law, taxes will not be paid or collected without the express authorization of the AAFES director and chief executive officer. Inquiries, questions, tax levies, and any other matter concerning taxation will be promptly forwarded to the AAFES general counsel.

j. AAFES is authorized to conduct negotiations with taxing authorities, except that no formal administrative contest or litigation will be undertaken without express authorization of the AAFES general counsel in coordination with the Department of Justice or the local U.S. Attorney's Office (28 USC 516) and, as necessary, the appropriate Army or Air Force litigating division or Office of the General Counsel.

15–3. U.S. Department of the Treasury records retention policy

All records relating to payments to individuals and firms must be retained for at least 4 years and must be available for review by the U.S. Department of the Treasury, if required. CONUS operators should consult their local U.S. Department of the Treasury office when forms, publications, or assistance is needed. Overseas local offices should be consulted for the address and telephone number of the nearest office of the U.S. Department of the Treasury representative.

15–4. Federal occupation taxes

a. Exchanges located in CONUS, Alaska, Hawaii, and U.S. territories are subject to the following U.S. Department of the Treasury occupation taxes:

(1) *Wholesale dealer in liquor*. For the purpose of this tax, a military reservation constitutes one location under the same proprietorship so that only one tax is due regardless of the number of outlets that an exchange operates within the geographical limits of the reservation. The wholesale dealer's tax is paid where AAFES sells to another organization authorized to purchase from the Class Six store.

(2) *Retail dealer in liquor, unless the tax has been paid under paragraph (1), above.* For the purpose of this tax, a military reservation constitutes one location under the same proprietorship so that only one tax is due irrespective of the number of outlets that an exchange operates within the geographical limits of the reservation.

b. The AAFES director and chief executive officer issues procedures relating to obtaining wholesale and retail dealer liquor tax licenses for Class Six stores.

15–5. State tax exemptions

a. The sale by AAFES of merchandise including soft drinks, alcoholic and malt beverages, and tobacco products is exempt from state taxes. This exemption applies to all Army and Air Force installations, organizations, activities, and personnel within the United States and its territories.

b. The immunity of AAFES from direct state taxation does not extend to indirect taxes whose legal incidence is on a party other than the Exchange (such as a manufacturer, importer, processor, or wholesaler).

c. Several states have granted military exemptions from excise taxes that would otherwise be applicable to alcoholic beverages and tobacco products, and soft drinks procured by exchanges for resale to authorized patrons. This exemption is enjoyed as a privilege and not as a matter of legal right and is, therefore, to be respected and observed through full compliance with applicable restrictions, including the prohibition against unauthorized sale or disposition.

15–6. Sale of state tax-free items

a. State tax-free alcoholic and malt beverages may be sold for on-premises consumption at exchange food service outlets to those persons and organizations authorized to use food service outlets.

b. State tax-free packaged alcoholic beverages will be sold only to individuals, organizations, and activities entitled to unlimited exchange privileges and civilian employees of the Federal Government who work and permanently reside on the garrison and installation. The aforementioned civilians are prohibited, however, from removing state tax-free beverages from the military installation.

c. State tax-free tobacco products shall be sold only to those individuals, organizations, and activities entitled to unlimited exchange privileges.

d. The AAFES director and chief executive officer prescribes and enforces necessary controls to ensure that no sales are made to persons who lack prescribed identification. The garrison and installation commander, in coordination with the GM, AAFES may establish reasonable purchase quantity limitations and will ensure that restrictions and limitations governing the sale and disposition of state tax-free items are strictly enforced. Garrison/installation commanders will cooperate with state tax officials and will investigate all complaints. Garrison/installation commanders may take appropriate action for abuse of exchange privileges related to purchase of tax-free items, to include revoking or suspending exchange privileges.

Chapter 16
Audits and Inspections

16–1. Audits

a. The AAFES Audit Division fulfills all internal audit functions required by DOD regulations. The Audit Division staff will have access to all books of accounts, records, and documents needed to audit AAFES operations, accounting, internal controls, other audits, and funds. Operating procedures will be issued by the AAFES director and chief executive officer.

(1) The U.S. Army Audit Agency is designated to evaluate the adequacy of AAFES internal audit function. The Army Auditor General is the principal point of contact for the peer review function and for reporting results to the AAFES director and chief executive officer and to the Audit Committee of the AAFES BOD. Peer reviews are in consultation with, and with the assistance of, the U.S. Air Force Auditor General.

(2) The Department of Defense Inspector General (DODIG) and the Office of the Assistant Inspector General for Audit Policy and Oversight, with the assistance of representatives from the DOD internal audit organizations may also conduct external quality control peer reviews of the AAFES Audit Division.

b. The General Accountability Office (GAO), or authorized representatives, have access to all books of accounts, records, and documents needed to audit AAFES operations, accounting, internal controls, other audits, and funds. Representatives from the GAO coordinate their reviews of AAFES operations with the AAFES Audit Division. All levels of AAFES management will cooperate with GAO representatives and advise the AAFES Audit Division of any direct contact by GAO representatives.

c. The DODIG auditors are authorized to have access to all books of accounts, records, and documents needed to audit operations and funds of AAFES. Auditors coordinate their reviews of AAFES operations with the AAFES Audit Division. All levels of AAFES management will cooperate with the auditors and advise the AAFES Audit Division of DODIG contacts.

d. AAFES contracts with a CPA firm to perform annual examinations of its financial statements. The CPA's work must meet the standards specified in the government auditing standards issued by the Comptroller General of the United States. CPA work is subject to U.S. Army Audit Agency review to ensure that government auditing standards are met.

16–2. Inspector General

a. AAFES will maintain an IG office operating under the regulatory policies and procedures of the DODIG. The AAFES director and chief executive officer will issue operating procedures.

b. The IG, AAFES, in compliance with applicable departmental guidelines, will—

(1) Operate the AAFES Fraud, Waste, Abuse, or Mismanagement Hotline program.

(2) Conduct inquiries to resolve assistance complaints and perform investigations as directed by the AAFES director and chief executive officer.

(3) Inspect AAFES facilities and operations reporting findings/observations (including, but not limited to, operational efficiency, employee morale and effectiveness, and chain of command relationships) to the AAFES director and chief executive officer on a scheduled and unscheduled basis.

(4) Be the primary point of contact with external IG officials for non-audit actions.

(5) Obtain DOD and DA or Air Force IG assistance, as necessary, for Service or Joint support on significant issues beyond AAFES control.

16–3. Inspector General inquiries and investigations

a. The IG may investigate or conduct investigative IG inquiries into allegations of violations of policy, regulation, or law and mismanagement, unethical behavior, or misconduct which, if true, may be of concern to the directing authority (see para 13–3 for processing of criminal misconduct).

b. The IG will provide results of IG investigations into allegations contained in paragraph *a*, above, to the AAFES director and chief executive officer for any action deemed appropriate.

c. Allegations against AAFES senior officials will be forwarded to the DODIG. Senior officials are defined as active duty military officers in grades O–7 and above, or selected for promotion to grade O–7; current and former members of the Senior Executive Service; other current and former DOD civilian employees whose positions are deemed equivalent to that of a member of the Senior Executive Service (for example, senior level employees and NAF senior executives) (see DODD 5505.06).

d. Investigation of allegations against senior officials, not cited elsewhere in this regulation, will be administered in accordance with the applicable component IG regulation of that senior official or by the IG, AAFES, if civilian.

e. Any allegation of misconduct may be investigated, at the direction of the AAFES director and chief executive officer, under the purview of IG procedures, departmental investigation procedures, or director and chief executive

officer's inquiry procedure. This includes command inquiries conducted by IG or loss prevention personnel, as well as inquiries conducted by NAF civilian personnel.

16–4. Department and command inspections

a. The IG, Army and the IG, Air Force jointly inspect AAFES, as directed by the applicable Service's Chief of Staff. Lead responsibility alternates between the departments. The IG of the lead department submits departmental inspections through the AAFES BOD to the AAFES director and chief executive officer.

b. The IG, AAFES will conduct inspections below department level. The IG, AAFES will develop an annual program based on the AAFES director and chief executive officer's guidance and provide the inspection results to the AAFES director and chief executive officer.

16–5. Release of Army and Air Force Exchange Service inspector general records

Release and use of IG, AAFES records outside AAFES requires the approval of the AAFES director and chief executive officer or higher authority. The IG, AAFES is designated the initial denial authority for all IG, AAFES records requested under the FOIA.

Appendix A
References

Section I
Required Publications

Army publications are available at http://www.apd.army.mil. Air Force publications are available at http://www.e-publishing.af.mil. DOD publications are available at http://www.dtic.mil/whs/directives.

AR 15–110/AFI 34–203(I)
Board of Directors, Army and Air Force Exchange Service (Cited in para 1–9*b*.)

AR 215–1
Military Morale, Welfare, and Recreation Programs and Nonappropriated Fund Instrumentalities (Cited in paras 2–4*a*, 8–11*c*, 11–4*c*, 11–5*b*, B–2, and table B–1, footnote 1.)

AFI 65–106
Appropriated Fund Support of Morale, Welfare, and Recreation and Nonappropriated Fund Instrumentalities (Cited in paras 2–4*a*, B–2, and table B–1, footnote 1.)

DOD 5500.07–R
Joint Ethics Regulation (JER) (Cited in paras 1–11*d*, 5–8.)

DODI 1015.15
Establishment, Management, and Control of Nonappropriated Fund Instrumentalities and Financial Management of Supporting Resources (Cited in paras 1–9*c*, 3–1, 3–2*a*, 3–2*e*, 3–3*a*, 14–2*a*, B–1, B–2, B–3, and table B–1, item 8b(1) and footnote 5.)

DODI 1330.21
Armed Services Exchange Regulations (Cited in paras 4–4*a*, 6–4*a*, 6–4*b*, 6–13, 6–14*c*, 6–22, 8–11*a*, B–1, C–1, D–2, and F–5.)

DODI 7060.03
International Balance of Payments—Nonappropriated Fund Activities (Cited in para 8–4.)

Section II
Related Publications

A related publication is a source of additional information. The user does not have to read a related publication to understand this publication.

AR 11–2
Managers' Internal Control Program

AR 12–15/SECNAVINST 4950.4B/AFI 16–105
Joint Security Cooperation Education and Training

AR 15–1
Committee Management

AR 25–30
The Army Publishing Program

AR 27–20
Claims

AR 195–2
Criminal Investigation Activities

AR 200–1
Environmental Protection and Enhancement

AR 210–7
Personal Commercial Solicitation on Army Installations

AR 210–22
Private Organizations on Department of the Army Installations

AR 210–25
Vending Facility Program for the Blind on Federal Property

AR 215–7
Civilian Nonappropriated Funds and Morale, Welfare, and Recreation Activities

AR 380–67
Personnel Security Program

AR 700–84
Issue and Sale of Personal Clothing

AFI 31–501
Personnel Security Program Management

AFI 32–6001
Family Housing Management

AFI 34–206
Vending Facility Program for the Blind on Air Force Property

AFI 34–219
Alcoholic Beverage Program

AFI 34–223
Private Organizations (PO) Program

AFI 34–262
Services Program and Use Eligibility

AFI 36–2702
Personal Commercial Solicitation on Air Force Installations

AFI 36–3026_IP, Vol 1/AR 600–8–14
Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel

AFI 51–502
Personnel and Government Recovery Claims

AFI 71–101 (Volume 1)
Criminal Investigations Program

AFJI 34–122
Civilian Nonappropriated Funds and Morale, Welfare, and Recreation Activities

AFMAN 23–110 (Volume 1)
USAF Supply Manual

AFPD 36–29
Military Standards

DOD 1401.01–M
Personnel Policy Manual for Nonappropriated Fund Instrumentalities

DOD 5200.2–R
Personnel Security Program

DOD 7000.14–R
Department of Defense Financial Management Regulations (FMRS): Volumes 2A and 2B, Budget Formulation and Presentation; Volume 5, Disbursing Policy and Procedures; and Volume 13, Nonappropriated Fund Policy and Procedures

DODD 1015.5
DOD Student Meal Program

DODD 4105.67
Nonappropriated Fund (NAF) Procurement Policy

DODD 5505.06
Investigations of Allegations Against Senior Officials of the Department of Defense

DODI 1000.11
Financial Institutions on DOD Installations

DODI 1000.13
Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals

DODI 1000.15
Procedures and Support for Non-Federal Entities Authorized to Operate on DOD Installations

DODI 1015.10
Military Morale, Welfare, and Recreation (MWR) Programs

DODI 1015.12
Lodging Program Resource Management

DODI 1015.13
DOD Procedures for Implementing Public-Private Ventures (PPVs) for Morale, Welfare and Recreation (MWR), and Armed Services Exchange Category C Revenue-Generating Activities

DODI 1330.09
Armed Services Exchange Policy

DODI 1344.07
Personal Commercial Solicitation on DOD Installations

DODI 1400.25
DOD Civilian Personnel Management

DODI 1401.1
Personnel Policy for Nonappropriated Fund Instrumentalities (NAFIs)

DODI 1401.25
DOD Civilian Personnel Management

DODI 2000.16
DOD Antiterrorism (AT) Standards

DODI 4000.19
Interservice and Intragovernmental Support

DODI 4105.70
Sale or Rental of Sexually Explicit Material on DOD Property

DODI 4165.71
Real Property Acquisition

DODI 7600.6
Audit of Nonappropriated Fund Instrumentalities and Related Activities

DODI 7700.18
Commissary Surcharge, Nonappropriated Fund (NAF) and Privately Financed Construction Reporting Procedures

EO 13149
Greening the Government Though Federal Fleet and Transportation Efficiency

EOP 15–10
Exchange Operating Procedures: Managing Human Resources

JTR
Joint Travel Regulations, Volume 2

PL 87–581
Contract Work Hours and Safety Standards Act

PL 88–558
Military Personnel and Civilian Employees' Claims Act of 1964

PL 89–286
Service Contract Act of 1965

PL 89–508
Federal Claims Collection Act of 1966

PL 92–392
Federal Wage System

PL 93–259
Fair Labor Standards Amendments of 1974

PL 95–563
Contract Disputes Act of 1978

Under Secretary of Defense (Personnel and Readiness) policy memorandum
Funding Sources for Nonappropriated Fund Instrumentality (NAFI) Facilities, dated 4 December 2007 (Available from the Assistant Chief of Staff Installation Management (DAIM–ISS), 600 Army Pentagon, Washington, DC 20310–0600.)

41 CFR, Chapter 302
Relocation Allowances

4 USC 104
Tax on motor fuel sold on military or other reservations—reports to State taxing authority

5 USC 552
Freedom of Information Reform Act of 1986: Public information; agency rules, opinions, orders, records, and proceedings

5 USC 7101
Findings and purpose

10 USC Chapter 49
Miscellaneous Prohibitions and Penalties

10 USC 1059
Dependents of members separated for dependent abuse: transitional compensation; commissary and exchange benefits

10 USC 1146
Commissary and exchange benefits

10 USC 2481
Defense commissary and exchange systems: existence and purpose

10 USC 2492
Nonappropriated fund instrumentalities: contracts with other agencies and instrumentalities to provide and obtain goods and services

10 USC 2643
Commissary and exchange services: transportation overseas

10 USC 2783
Nonappropriated fund instrumentalities: financial management and use of nonappropriated funds

10 USC 3911
Twenty years or more: regular or reserve commissioned officers (Army)

10 USC 6323
Officers: 20 years

10 USC 8911
Twenty years or more: regular or reserve commissioned officers (Air Force)

10 USC Chapter 61
Retirement or Separation for Physical Disability

10 USC Chapter 1223
Retired Pay for Non-Regular Service

18 USC 874
Kickbacks from public works employees (*Copeland Anti-Kickback Act*)

20 USC 107
Operation of vending facilities (*Randolph-Sheppard Act*)

27 USC 201
Federal Alcohol Administration Act (*Alcoholic Beverage Labeling Act of 1988*)

27 USC 215
Labeling Requirement

28 USC 516
Conduct of litigation reserved to Department of Justice

31 USC Chapter 13
Appropriations

31 USC 3727
Assignment of Claims (*Assignment of Claims Act of 1940*)

33 USC
Navigation and Navigable Waters

38 USC
Veterans' Benefits

40 USC 3131
Bonds of contractors of public buildings or works (*Miller Act*)

40 USC 3141
Definitions (*Davis-Bacon Act*)

40 USC Chapter 37
Contract Work Hours and Safety Standards

41 USC
Public Contracts

42 USC 6374
Alternative fuel use by light duty Federal vehicles

42 USC 7586
Centrally fueled fleets

42 USC 12101
Equal Opportunity for Individuals with Disabilities (*Americans with Disabilities Act of 1990*)

47 USC 548
Development of competition and diversity in video programming distribution

Section III
Prescribed Forms

Unless otherwise indicated, DD Forms are available at http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.

DD Form 2574
Armed Forces Exchange Service Identification and Privilege Card (Available through normal forms supply channels.) (Cited in paras 2–4*e*, 7–4*a*(3).)

Section IV
Referenced Forms

Unless otherwise indicated, DA forms are available at http://www.apd.army.mil; DD forms are available at http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm; Standard Forms (SFs) are available at http://www.gsa.gov/.

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 4
Enlistment/Reenlistment Document Armed Forces of the United States

DD Form 1610
Request and Authorization for TDY Travel of DOD Personnel

DD Form 1618
Department of Defense (DOD) Transportation Agreement Transfer of Civilian Employees to and Within Continental United States

DD Form 2765
Department of Defense/Uniformed Services Identification and Privilege Card

SF 95
Claim for Damage, Injury, or Death

CG–2650
USCG Auxiliary Membership Card

Appendix B
Funding Authorizations

B–1. Appropriated fund authorization
DODI 1015.15 and DODI 1330.21 authorize APF support to AAFES.

B–2. Remote and isolated locations
At designated remote and isolated locations, AAFES is authorized APF funding under category B rules in accordance with DODI 1015.15. Army designated remote and isolated locations are listed in AR 215–1 and Air Force designated sites are listed in AFI 65–106.

B–3. Base realignment and closures locations
Exchanges at installations identified for closure under BRAC procedures may receive APF support authorized for category B activities (see DODI 1015.15). APFs may finance costs that are a direct result of an approved BRAC action. Those costs include, but are not limited to PCS for NAF employees, exchange unemployment and severance payments associated with NAF personnel, and facilities construction. Exchange BRAC costs are authorized funding from all BRAC accounts (see DODI 1015.15) and other valid appropriations.

B–4. Force protection conditions
During force protection conditions Charlie and Delta, exchanges are authorized APF support for civilian personnel with installation executive control and essential command supervision (ECECS) except for those directly involved in resale activities

B–5. Elements of expense
Table B–1 outlines the elements of expense authorized APF and AAFES NAF support. Also see chapter 3 of this regulation for additional policy on expenditure of APFs and AAFES NAFs.

Table B–1
General funding authorizations for AAFES activities

Elements of expense	APFs (see footnotes 1 and 2 of this table)	AAFES NAFs
1. *Military personnel*.		
a. Active duty military personnel assigned and used on a full-time permanent basis to perform ECECS.	Authorized.	Not applicable.
b. All other personnel.	Not authorized, except as outlined in footnote 3 of this table.	Not applicable, except as outlined in footnote 4 of this table.
2. *Civilian personnel*.		
a. Permanent assignment for ECECS purposes.	Authorized, only per footnote 5.	Authorized.
b. Personnel performing managerial functions or requiring technical and professional qualification. Also personnel accountable for APF resources and protection in the interests of the Federal Government.	Not authorized, except at locations identified in paras B–2, B–3, and B–4, and footnote 5 of this table.	Authorized.
c. Personnel directly and primarily involved in resale.	Not authorized.	Authorized.
d. Additional and collateral duties. Applies to APF employees who are assigned duties on an additional or collateral duty basis. These duties are in addition to the civilian employee's primary duty assignment and may be of an ECECS or operational nature.	Not authorized, except at locations identified in paras B–2, B–3, and B–4, and footnote 5 of this table.	Not applicable.

Table B–1
General funding authorizations for AAFES activities—Continued

Elements of expense	APFs (see footnotes 1 and 2 of this table)	AAFES NAFs
3. *Civilian Personnel Office assistance and administration*. Relates to APF Civilian Personnel Advisory Center/Civilian Personnel Operations Center support for–		
a. Technical advice and counsel that may be provided by the Civilian Personnel Advisory Center/Civilian Personnel Operations Center to assist in the personnel management of employees paid with NAFs.	Authorized.	Not authorized.
b. Day-to-day personnel administration of employees paid with NAFs to include, but not limited to, recruitment, placement, position classification, salary and wage administration, training, personnel records maintenance, employee relations, and personnel matters.	Authorized, when no additional incremental APF costs are incurred.	Authorized.
4. *Family housing overseas*. Applies to those employees who are authorized housing or a housing allowance in overseas areas.		
a. APF personnel.	Authorized.	Not authorized.
b. NAF personnel.	Authorized for APF-authorized NAF positions.	Authorized.
5. *Personnel evacuation expenses*. Includes evacuation payments, evacuation transportation to and from safe haven locations, and per diem and subsistence allowances for those employees ordered to evacuate by the commanding officer or other DOD authority.		
a. APF personnel.	Authorized.	Not authorized.
b. NAF personnel.	Authorized.	Authorized, only when APFs are not available or sufficient.
6. *Travel of personnel*. Applies to personnel employed by or assigned or detailed to AAFES programs and activities.		
a. PCS. Applies to the relocation of APF and NAF personnel assigned on a full-time permanent basis.	Authorized for APF personnel and APF authorized AAFES NAF personnel as a direct result of an approved BRAC action.	Not authorized for APF personnel. Authorized for AAFES NAF personnel.
b. TDY and temporary assigned duty travel for military and APF civilian personnel and for AAFES NAF personnel.	Authorized for military and APF civilian personnel. Authorized for AAFES NAF personnel, when directed by the DOD and relates to APF business.	Authorized for personnel engaged in internal AAFES operations.
7. *Government-owned, motor pool-controlled*. Use of government-owned, motor pool-controlled passenger vehicles by AAFES activities.	Authorized when assisting in ECECS functions.	AAFES NAFs are authorized and will reimburse APF when government-owned vehicles are used for other than ECECS functions.
8. *Transportation of AAFES goods*.		
a. Purchased with APFs.	Authorized.	Not authorized.
b. Purchased with NAFs.		
(*1*) Transoceanic movement expenses of transporting supplies and products from CONUS sea and aerial ports of embarkation to OCONUS final AAFES retail facility (see chap 10).	Authorized.	Not authorized (per DODI 1015.15 as implemented by 10 USC 2643).

Table B–1
General funding authorizations for AAFES activities—Continued

Elements of expense	APFs (see footnotes 1 and 2 of this table)	AAFES NAFs
(*2*) Movement of U.S. and foreign goods within foreign areas when commercial transportation is not available, or in contingency areas.	Authorized.	Authorized when APFs are not available.
(*3*) Transoceanic movement of goods from OCONUS sea and aerial ports of embarkation to first destination CONUS or bulk breakdown point.	Authorized.	Authorized when APFs are not available.
(*4*) Movement of U.S. goods between DOD installations because of base closures, or to safeguard goods under emergency conditions, for example, threat of hostile force or natural disaster.	Authorized.	Authorized when APFs are not available.
(*5*) All other transportation of NAF goods.	Not authorized, except on a reimbursable basis; initial APF funding permitted only when NAF will reimburse APF.	Authorized.
9. *Household goods*.		
a. APF personnel.	Authorized.	Not authorized.
b. AAFES personnel.	Authorized for APF-authorized AAFES NAF positions. Initial APF funding is permitted for other AAFES NAF positions only when AAFES will reimburse APF (except at BRAC locations that are authorized APFs).	Authorized.
10. *Utilities*. Applies to heat, steam, water, gas, electricity, air conditioning, and other utility services for facilities used primarily for AAFES purposes.	Authorized in CONUS and OCONUS.	Authorized for costs in CONUS when APFs are not available. Not authorized OCONUS and for remote and isolated locations (CONUS and OCONUS) (see footnote 6 of this table).
11. *Rents*. Applies to the use and possession of non-DOD lands, buildings, and other improvements and installed equipment for a specified period through contract, lease agreement, or other legal instrument when authority is granted through appropriate channels.	Not authorized, except upon specific approval by the Secretary of the Army/Air Force concerned.	Not authorized, except upon specific approval by the Secretary of the Army/Air Force concerned and in accordance with real property acquisition regulations of the Army and Air Force.
12. *Communications*.		
a. *Electronic communications*. Applies to electronic communications (telephone, teletype, television, fax, Internet), Defense Switched Network, public address systems, and other electronic media) provided to AAFES.	Authorized in support of ECECS functions, statistical data gathering, communications with other DOD and government agencies, and OCONUS.	Authorized when supporting the operational function of the activity, such as procurement of items for resale and collection of income for merchandise or services sold in CONUS.
b. *Postal service and postage*. Official communications within and between government agencies and individuals, communications with commercial agencies, persons, private commercial agencies, not related to the sale of goods and services.	Authorized.	Authorized for all other correspondence related to the operation of AAFES, sale of goods and services, such as the inventory procurement and sales, collection of income, advertising, and AAFES equipment maintenance. (Does not preclude use of Army Post Office/Fleet Post Office for unofficial mail.)
13. *Equipment maintenance*.		
a. *Government-owned equipment*. Applies to maintenance, repair, overhaul, or rework of equipment.	Authorized, except for surplus and excess government equipment.	Authorized.
b. *Equipment acquired with NAF*. Applies to maintenance, repair, overhaul, or rework of equipment acquired with NAF.	Authorized for equipment acquired with NAFs, but authorized for purchase with APFs where the title transfers to the government.	Authorized.

Table B–1
General funding authorizations for AAFES activities—Continued

Elements of expense	APFs (see footnotes 1 and 2 of this table)	AAFES NAFs
c. *Real property installed equipment/building equipment*. This includes permanently attached real property generally installed as a part of a construction project, that cannot be removed from the structure without physically damaging the structure and without which the facility (structure) would be unable to operate as designed.	Authorized.	NAFs authorized only when a certification of non-availability of funds is signed by the garrison and installation commander.
14. *Printing and reproduction*. Applies to printing and reproduction such as work done on printing presses, lithographing, and other duplicating, related binding operations, photography, electronic media, microfilming, formats and forms, editing, and graphics.	Authorized for all costs except those related to the sale of merchandise or services and to the internal operation of AAFES.	Authorized.
15. *Education and training*. Pertains to the advancement of job knowledge, development of skills, and improvement of abilities of AAFES personnel.	Authorized for APF positions and APF-authorized AAFES NAF positions and for Army/Air Force-approved training that is not job unique such as management and leader development courses, quality training, health and safety, sexual harassment, and so forth.	Authorized for AAFES NAF personnel. Not authorized for APF non-tuition courses.
16. *Auditing services*. Relates to the independent examination, review, and evaluation of the records, controls, practices, and procedures in the area of financial and operational management of AAFES by DOD components' audit organizations or independent public accountants.	Authorized in accordance with DODI 7600.6.	Authorized in accordance with DODI 7600.6.
17. *Data automation*. Applies to automatic data processing system development or operation (personnel, equipment, supplies) needed for either ECECS or internal operation of AAFES.	Authorized for services required for ECECS and to discharge a commander's supervisory responsibility for management review and analysis.	Authorized for costs related to internal management of AAFES NAF resources.
18. *Financial management services*. Relates to those services that reflect the preparation of APF and AAFES NAF budgets; provide accounting for financial management data; facilitate the preparation of financial reports; and provide for management review and analysis to ensure proper control over all the resources that support AAFES.	Authorized to provide technical guidance and assistance in preparing budgets, financial and analytical data required for ECECS. Not authorized for AAFES NAF accounting and analytical functions.	Authorized for all costs related to AAFES NAF accounting and analytical functions required for the operation of AAFES.
19. *Legal services*. Applies to that service and assistance provided by or through The Judge Advocate General or general counsel.	Authorized.	Authorized for AAFES internal legal staffing.
20. *Procurement office assistance and administration*.		
(a) *Assistance*. Applies to technical advice and assistance that may be provided by the procurement office to assist AAFES management in the procurement of goods and services with NAFs.	Authorized.	Not applicable.
(b) *Administration*. Applies to the functions of procurement (source development, preparation of procurement documents, negotiation of prices, contract administration and audit, and related procurement functions) being performed by the procurement office in the procurement of goods and services with NAFs.	Authorized when no additional incremental APF costs are incurred and when existing APF contracts may be used to purchase the item or services.	Authorized.

Table B–1
General funding authorizations for AAFES activities—Continued

Elements of expense	APFs (see footnotes 1 and 2 of this table)	AAFES NAFs
21. *Custodial and janitorial services*. Applies to the manpower, supplies, and equipment provided by the installation engineer, the public works department, or by contract.	Authorized for locations identified in paras B–2, B–3, and B–4. Not authorized all other locations.	Authorized when APFs are not available or not sufficient at locations identified in paras B–2, B–3, and B–4. Authorized all other locations.
22. *Other services*. Relates to those services of a protective or sanitary nature normally supplied as a command function. Such services include, but are not limited to fire protection, including acquisition and installation of extinguishers and sprinkler and alarm systems; security protection, including physical security of buildings (such as alarm systems and security bars), personnel background investigations under the provisions of DOD 5200.2–R and protection of funds; pest control; sewage disposal; environmental compliance and remediation; trash and garbage removal; snow removal; safety; medical, veterinary and sanitary inspections; rescue operations.	Authorized for all costs associated with protecting the health and safety of participants and employees and with protecting AAFES NAF resources. Trash and garbage removal are not authorized for AAFES activities in CONUS. Trash and garbage removal are authorized OCONUS. Authorized for sewage disposal.	Trash and garbage removal are authorized for AAFES activities in CONUS. Otherwise, authorized only when APFs are not available or sufficient.
23. *Minor construction and modernization*. These terms are defined in the glossary. Also see terms for restoration, sustainment, real property, construction project, construction costs, and construction.	Authorized only per footnotes 7, 8, and 9 of this table.	Authorized. Not authorized for conditions outlined in footnotes 7, 8, and 9 of this table.
24. *Sustainment and restoration*. These terms are defined in the glossary.	Authorized.	Authorized when APFs are not available or sufficient.
25. *Routine grounds maintenance*. Applies to work required to maintain surrounding building grounds.	Authorized.	Authorized when APFs are not available or sufficient.
26. *Supplies*. Applies to supply items (expendables) that are consumed or lose their identity when used, or whose low value does not require the same accountability required for equipment. Included in this group are clothing, tentage, organizational tools, administrative and housekeeping supplies (other than in #21 of this table), petroleum fuels, lubricants, preservatives, coolants, oil derivatives.	Authorized for supplies required for ECECS.	Authorized.
27. *Investment equipment*. Relates to the acquisition and use of equipment that meets the criteria of investment items, as defined in DOD 7000.14–R (Volume 2A).	Not authorized, (except for use of surplus/excess government equipment) unless permitted by footnote 10 of this table.	Authorized.
28. *Equipment*. Includes the acquisition cost of any item of equipment, furniture, or furnishing that does not meet the criteria of an investment cost as defined in DOD 7000.14–R (Volume 2A).	Authorized for equipment required for ECECS and surplus/excess government equipment at all other locations and per footnote 10 of this table.	Authorized.
29. *Other operating expenses*. Includes the cost of types of resources not otherwise provided for, such as investments and loans, grants, subsidies and contributions, insurance claims and indemnities, interest and dividends, and payments instead of taxes, if such resources are included in operations appropriations.	Authorized for costs incurred incident to the performance of functions related to ECECS or as specifically authorized by statute or DOD publication.	Authorized.

Table B–1
General funding authorizations for AAFES activities—Continued

Elements of expense	APFs (see footnotes 1 and 2 of this table)	AAFES NAFs
30. *Architecture and engineering services*. Applies to professional services that include the necessary consultations, preparation of preliminary studies, analyses, cost estimates, working drawings, specifications, interior design and decoration, and the inspection and supervision services required for the construction, alteration, or restoration of real property facilities.	Authorized for APF construction and NAF construction when no additional manpower authorizations are required.	Authorized for NAF construction, except for inspection and supervision services required for government acceptance of the facility (see also para 3–3*c*(10)*(a)*).
31. *Major construction*. See glossary for a definition of this term.	Not authorized unless permitted by footnotes 7, 8, and 9 of this table.	Authorized. Not authorized for conditions in footnotes 7, 8, and 9 of this table.
32. *Purchase of real property*. Relates to the acquisition cost of land, buildings, and other fixed improvements.	Authorized only to the extent approved by Congress.	Not authorized, except for the purchase of commercially owned buildings located on government property.
33. *Merchandise, service, and equipment for resale or rent*. Pertains to that procured by AAFES for resale or rent to authorized patrons or related to the sale of merchandise or services.	Not authorized, unless permitted per footnotes 10 and 11 of this table.	Authorized.

Notes:

[1] AAFES activities at designated remote and isolated locations are authorized APF funding under category B rules (AR 215–1 and AFI 65–106).

[2] During Force Protection conditions at Charlie and Delta, AAFES activities are authorized APF support for civilian personnel with installation management and supervisory functions (excluding personnel directly and primarily involved in resale), utilities, rents, and custodian and janitorial services.

[3] Active duty military personnel performing ECECS are authorized in sufficient numbers for AAFES programs to provide a trained cadre to meet wartime and deployment requirements and to perform managerial functions.

[4] Enlisted personnel may be employed during non-duty hours by NAFIs as part-time NAF-paid employees.

[5] APFs authorized for civilian personnel in sufficient numbers to provide a trained cadre to perform ECECS and managerial functions to meet exchange wartime deployment requirements in support of contingency, humanitarian, and peacekeeping operations. APF civilian positions may be provided by permanent assignment utilization and the assignment of additional or collateral duties, in lieu of military positions authorized by #1*b* of this table and footnote 3, above. Where NAF positions are utilized, APF support is authorized for NAF expenditures incurred for compensation and benefits, travel of personnel, transportation of household goods, and education and training. APF support will be executed under an MOA as prescribed in DODI 1015.15, pertaining to MWR utilization, support, and accountability and uniform funding and management practices.

[6] Rates charged shall not include incremental or prorated share of overhead, maintenance, and repair to utility systems, or capital investments in the installation's utility infrastructure system unless otherwise specified by an MOU or installation support agreement.

[7] APFs must be used for all AAFES facility construction (major and minor) determined by the applicable military Service to be required to establish, activate, or expand a military installation, including BRAC and global re-stationing requirements; relocation for convenience of the government; replacement of facilities denied by country-to-country agreements; and restoration of facilities and improvements destroyed by acts of nature, fire, or terrorism; antiterrorism/force protection measures required under DODI 2000.16, and to correct life, safety, and Americans with Disabilities Act of 1990 and force protection deficiencies. Expansion must be the result of a mission change or influx of new units or systems, and result in a 25 percent increase in authorized and assigned personnel strength within a 2–year time span.

[8] APFs are authorized and will be used for site development costs, archeological and ammunition clearances, environmental assessment and remediation, water purification, demolition, excessive utility connections, and road services.

[9] APFs must be used for exchange administrative, storage, and maintenance facilities OCONUS; NAFs will be used for these facilities inside the United States. APFs must be used for facilities required in areas of military conflict or as integral parts of air terminal, hospital, housing, or other military construction projects. APFs must be used for all exchange-operated laundries, dry cleaning plants, bakeries, dairies, or similar facilities operated by exchanges when in support of a military mission (see para 3–4 for deviations/exceptions to use of NAFs in lieu of APFs). For all other exchange facilities, NAFs will be used.

[10] APFs are authorized for losses caused by acts of nature; losses during wartime deployments, and in support of contingency, humanitarian, and peacekeeping operations; and for equipment required to be in compliance with the Americans with Disabilities Act of 1990.

[11] APFs are authorized for military clothing and other APF-funded items sold in military exchanges on a cost-reimbursable basis.

Appendix C
Authorized Army and Air Force Exchange Service Resale Activities

C–1. Army and Air Force Exchange Service primary activities

AAFES is authorized to operate the below listed revenue-generating activities on military installations; in areas of military conflict; in military air terminals, hospitals, and housing areas (including government-owned, government-leased, or government-contracted); and in support of military operations. Any differences in this appendix and DODI 1330.21 are resolved in favor of DODI 1330.21.

a. Retail stores.

b. Mail-order, catalog, and e-commerce services.

c. Automobile services, including garages, fuel sales, car washes, and service stations.

d. Restaurants, cafeterias, and snack bars, and name-brand fast food outlets, including nationally and regionally recognized franchises and exchange signature brands.

e. Packaged beverage stores.

f. Barber and beauty services, including nail salons, day spas.

g. Flower shops.

h. Laundry, dry cleaning, and pressing plants and services.

i. Alteration and tailor services.

j. Product repair services, such as watch, shoe, radio, television, computer and electronic repair.

k. Photographic studios.

l. Vending machines.

m. Personal services.

n. Newsstands.

o. Unofficial telecommunication services (including, but not limited to, pay telephone stations and telephone calling centers).

p. Military clothing sales operations.

q. Exchange credit programs.

r. Tax preparation services.

s. Exchange marts.

t. Motion picture theaters.

u. Rental of merchandise. Rental of any merchandise AAFES is authorized to sell.

v. The Secretary of the Army and the Secretary of the Air Force may prescribe in their regulations a selection of food and beverages, including malt beverages, wines, and other alcoholic beverages. Food items will supplement the primary full-line grocery service provided by the commissary system.

w. Pet services, including, but not limited to, pet grooming services.

C–2. Departmental authorized activities

The Secretary of the Army and the Secretary of the Air Force may authorize the exchanges to operate the activities listed below. Requests for AAFES operation will be forwarded for approval to the respective Army and Air Force military department at the appropriate addresses in paragraph 6–1 of this regulation.

a. Membership clubs (open messes), restaurants, cafeterias, and snack bars incidental to MWR programs. Includes national name-brand casual dining (full table service) restaurants as replacements for existing military MWR food operations.

b. Lodging operations in categories A, B, and C, as permitted in DODI 1015.12, enclosure 3. Authorized users of these facilities are outlined in DODI 1015.12, paragraph 4.

c. School lunch programs.

d. Amusement machines. AAFES will own and operate, or contract for, amusement machines located in AAFES-operated outlets, and at the discretion of the garrison and installation commander in other locations. Displacement of AAFES-controlled amusement machines, or transfer of amusement machines to AAFES control, will be planned and coordinated with local AAFES management for orderly transition, to preclude disruption of service, financial loss, or conflict with expiration terms of contracts.

e. Recreational, social, and family support activities.

f. Animal kennels (services for boarding pets).

g. Personal Information Services. Personal Information Services is defined as Internet, telephone, or television services for which an individual user pays a fee to obtain service for personal use.

C–3. Additional authorized activities with special requirements

a. Fresh meat and produce departments. The garrison and installation commander may request the local GM, AAFES to sell fresh meat, fresh poultry, fresh seafood, fresh fruit, and produce when no commissary store is available on the installation or when fresh meat and produce are not available within a reasonable distance at a reasonable price, or in satisfactory quality and quantity. Other necessary grocery items may be sold without limitation in the number of items or container size.

b. Self-storage activities. These activities provide rental space in facilities and temporary rental storage units on military installations and government-owned or government-leased military housing areas for the temporary storage of personal possessions of authorized patrons. This does not include vehicle storage facilities, which are an authorized MWR operation. Proposals to establish and operate self-storage activities (major or minor construction or public-private ventures) shall be submitted 60 days in advance to the PDUSD(PR) for Congressional notification. Reporting requirements for construction and public-private ventures are found in DODI 7700.18. Such notification will document

the lack of adequate commercial facilities in the area around the installation or government-owned or government-leased military housing area and provide both a description of the process used to notify the local business community and the responses received. DOD components shall not establish and operate permanently constructed self-storage activities to include placing proposals under contract until the PDUSD(PR) approves the proposal and notifies Congress.

c. Medical and dental services including pharmacies. Medical services include, but are not limited to dental, optometry, audiology, and pharmacy activities.

(1) Proposals for medical services at specific locations must be submitted 60 days in advance to PDUSD(PR) for Congressional notification. The PDUSD(PR) must approve the offering of new medical and dental services and shall notify Congress of such approval. Congressional notification and PDUSD(PR) approval must be obtained before exchanges initiate construction or contract action, including entering into any license agreement with private practitioners.

(2) Proposals must include the garrison's/installation's name and location; statements that solicitations will include small businesses from the surrounding communities and that no military doctors will be used in the clinic; that the garrison and installation commander and local military health care facility commander support the project; the number of customers to be served; projected sales and financial return to the DOD, and AAFES; projected customer savings; a statement that space available for the service meets DOD military medical space requirements; a detailed site specific description of the contract award process, the contract requirements, the length of the contract, the scope of services to be offered; and specific benefits to Servicemembers. While there is no requirement that local business leaders agree with the new service, the local business community and government officials must be made aware of the initiative and the proposal must include their views.

(3) An MOA with the Army and Air Force Surgeon Generals are required for all health care services provided.

(4) Renotification is not required for renewal of a previously-approved specific medical concession at a specific location.

d. Optical shops. Services may not include eye exams or any medical procedures.

e. Magazines and periodicals. Magazines and periodicals are authorized exchange sale items. DODI 4105.70 governs the sale or rental of sexually explicit material on DOD property.

f. Firearms and ammunition. Firearms and ammunition are authorized exchange sale items. Firearms will be sold in compliance with federal laws and regulations. Overseas activities shall conform to all applicable SOFA requirements, as well as any requirements imposed by bilateral agreements between the United States and the host nation.

g. Name-brand fast-food operations. When establishing name-brand commercial fast-food operations, concession operations are preferred for military bases in the United States, and exchange direct-run operations are the preferred method for bases overseas. Both economic and non-economic factors shall be evaluated to decide on the method of operation that best meets the Exchange mission for each location. In addition, the following factors shall be considered in the aggregate: financial risk, customer service, employment opportunities, management control, operational risk, and investment opportunities. Primary consideration will be given to the overall quality of life and welfare of the active duty military community. Notice of deviations from the preferred method that result in major construction projects as defined in DODI 7700.18 will accompany the major construction program submitted to the PDUSD(PR) and include the evaluation of economic and non-economic factors.

h. New car sales. Only Armed Services exchanges are permitted to sell, publicize, or display new or factory certified cars or motorcycles on overseas DOD installations. This does not preclude brief periods of publicity and display of foreign cars or motorcycles as sponsor recognition authorized for military MWR programs. AAFES may sell automobiles and motorcycles only to authorized patrons who are stationed or are assigned overseas for 30 consecutive days or more. Orders may be taken for U.S.-made automobiles, foreign name-plated vehicles with at least 75 percent U.S. or Canadian content, and motorcycles. Sales may be made for stateside delivery or for in-country delivery where permitted under the SOFA.

i. Alternative fuels. The AAFES may sell alternative fuels to the general public in compliance with 42 USC 6374, 42 USC 7586, and Executive Order 13149.

j. Cable television services. AAFES may provide cable television services in compliance with 47 USC 548.

k. Home services. The AAFES is authorized to operate home services on or off DOD garrisons and installations, including, but not limited to, maid service, lawn care, and fence construction under concession contracts.

l. Automobile rental. AAFES is authorized to operate short-term automobile, truck, and trailer rental services on a concession basis. Leasing of vehicles is not authorized, nor is the sale of used vehicles.

m. Logistical facilities. AAFES is authorized to operate logistical, administration, storage, and maintenance facilities in support of the Exchange mission.

n. Plants. AAFES is authorized to operate laundries, dry cleaning plants, bakeries, dairies, or similar facilities in support of a military mission.

o. Taxicab and bus services. These services may be provided only to authorized patrons or civilians employed on military garrisons and installations. Each trip must either start or end on the military garrison and installation. Any travel off the installation must be incidental to providing transportation to or from the military garrison and installation.

p. Used media. Used media of any type, including, but not limited to, books, magazines, videos, recorded music, or computer software will not be sold unless specifically authorized by the AAFES director and chief executive officer. This does not apply to previously rented videos which may be sold by AAFES or its concessionaires when clearly identified as such.

q. Services. AAFES will not provide services that require the customer to sign a separate contract with a service provider, except as approved by the AAFES director and chief executive officer.

r. Live animals. AAFES will not sell live animals, including fish, birds, or reptiles unless specifically authorized by the AAFES director and chief executive officer.

s. Tattooing/body piercing. AAFES will not offer any form of permanent tattooing or body piercing (other than ear piercing consistent with standard industry retail practices) unless approved in advance by the AAFES director and chief executive officer.

t. Vendor-owned equipment. AAFES will not use vendor-owned equipment except as authorized by the AAFES director and chief executive officer.

u. Insurance contracts. AAFES may sell, place, solicit, or service insurance contracts of any description to authorized patrons as a customer service only as specifically authorized by the AAFES director and chief executive officer and with the approval of the AAFES BOD.

v. Personal information services. Applies to Army garrisons only and provides for an AAFES and Army IMCOM, G–9 (Family and MWR Programs) noncompetitive partnership agreement to provide Internet, telephone, or television services for which an individual user pays a fee to obtain service. The partnership will operate under a mutually agreed upon MOU.

Appendix D
Continental United States Only Merchandise Restrictions

D–1. Sale restrictions

Exchanges in CONUS will not sell—

a. Diamond settings with individual stones that exceed one and one-half carat.

b. Jewelry other than diamond jewelry with per unit (piece) cost to the Exchange in excess of the cost price of 2 ounces of gold.

c. Finished furniture with per unit (piece) cost to the Exchange in excess of $1,100.

(1) Exchanges in CONUS may not undertake new capital construction or renovation of an exchange facility of any kind for the purpose, in whole or in part, of providing additional space in which to sell finished furniture.

(2) At any location at which AAFES proposes to sell finished furniture, the GM, AAFES or garrison and installation commander will consult in advance with local furniture merchants and ascertain in writing whether there are any objections to the introduction of furniture at the Exchange facility.

(3) Any objections, along with a list of locations where exchanges propose to sell finished furniture, will be forwarded to the office of the PDUSD(PR) within 60 days in advance of sales, so that the office can notify the Armed Services Congressional Committees in advance.

(4) The office of the PDUSD(PR) must approve the offering of finished furniture at new locations and will notify the Congress of such approval prior to offering finished furniture at new locations.

d. Decorative housewares and furnishings with per unit (piece) cost to the Exchange Service in excess of $500.

e. Small appliances with per unit (piece) cost to the Exchange in excess of $150, except that there is no cost limitation on floor polishers, food processors, fans, coffee makers, humidifiers, dehumidifiers, air purifiers, microwave ovens, refrigerators, rotisseries, roasters, broilers, and vacuum cleaners.

f. Recreational boats with per unit (piece) cost to the Exchange in excess of $750.

g. Sports, recreational, garden, and manual arts equipment and supplies, photographic supplies and film with per unit (piece) cost to the Exchange Service in excess of $500. There is no cost limitation on aquatic equipment; bicycles; cameras and projectors; camera and projector accessories; fishing equipment; golf club sets; guns and gun accessories; physical fitness exercise equipment; power tools; outdoor power equipment, including lawn mowers, edgers, and snow blowers; ski equipment; surfboards; and tents.

D–2. Changes to sale restrictions

Differences between the above restrictions and those contained in DODI 1330.21, enclosure 4, are resolved in favor of those contained in DODI 1330.21, enclosure 4.

Appendix E
Prohibited Exchange Activities

E–1. Prohibitions

AAFES is not authorized to—

a. Sell or solicit the sale of real estate to authorized patrons, either as a retail item or a service.

b. Operate pawnshops, adults-only entertainment centers, or childcare centers.

c. Sell, lease, or display new cars on installations except overseas (see app C for new car sales overseas).

d. Sell or lease space in AAFES facilities. The AAFES in-store bank, automated teller machine, and concession and franchise agreements are not leases as contemplated by this prohibition.

e. Provide paid or free babysitting services, non-sports or non-therapeutic massage (whether clothed or unclothed), legal services, financial planning services, or funeral and mortuary services.

f. Sell or solicit the sale of stocks, bonds, mutual funds, or other investment instruments.

g. Use service or equipment items that contain product promotional advertisement, except where the product name is an integral part of the display. (Examples: packaged cereal and dessert displays, table condiments, gasoline pumps, and gasoline pylons.)

h. Authorize credit sales except as provided in this regulation.

i. Stock or sell drug abuse paraphernalia.

j. Sell or rent media of any type if it contains sexually explicit material (see DODI 4105.70).

k. Operate gambling devices in the United States and U.S. territories and possessions.

E–2. Continental United States restrictions

See appendix D for restrictions applicable to CONUS only.

Appendix F
Exceptions to the Armed Services Exchange Service regulations

F–1. Exceptions to exchange patronage within the 50 United States (to include the District of Columbia)

Garrison/installation commanders within the 50 United States (to include the District of Columbia) may request (through command channels) approval of deviations to the Armed Services Exchange regulations with regard to patronage privileges for individuals or classes and groups of persons. Exceptions for patronage privileges are approved only by the appropriate Secretary of the Army or the Secretary of the Air Force. Delegation of this authority is prohibited.

a. The garrison and installation commander must sign the request, and commanders at all levels must ensure that requests are fully responsive to the requirements prescribed herein.

b. The Army IMCOM or the Air Force MAJCOM recipients will conduct a judicious review of the respective garrison and installation request to determine if it should be forwarded.

c. If forwarded, requests will be submitted to—

(1) Army: Assistant Chief of Staff for Installation Management (DAIM–ISS), 600 Army Pentagon, Washington, DC 20310–0600.

(2) Air Force: Deputy Chief of Staff for Manpower, Personnel and Services, Director of Services (AF/A1S), 1770 Air Force Pentagon, Washington, DC 20330–1770.

F–2. Evaluation criteria

The Secretary of the Army and the Secretary of the Air Force will approve exceptions for patronage privileges only under the most stringent circumstances.

a. Requests for exceptions will be submitted and evaluated primarily on the basis of the geographic isolation of the garrison and installation concerned. Such requests will be strictly limited to those items necessary to ensure a reasonable standard of living to DOD civilian and contract personnel and their families assigned to the isolated location.

b. Requests for exchange privilege exceptions will be submitted and evaluated solely on the basis of their necessity for alleviating conditions of personal hardship.

F–3. Justification

Requests for exceptions will include the following:

a. A by-name listing of civilians or classes and groups of persons (to include the number of individuals within the class/group) and their Family members at the specific installation for who exchange privileges are being requested.

b. The personal hardships being experienced, described in detail.

c. The reasons why commercial retail facilities cannot be used will be explained.

F–4. Exceptions to exchange and commissary patronage—U.S. territories and possessions

a. DOD civilian employees and their dependents may be granted limited exchange and commissary access by the garrison and installation commander in accordance with table 7–2. DOD civilian employees must be assigned under a valid transportation agreement (as defined in 41 CFR, Chapter 302). An annual report of all approved exceptions is required for the 12–month period prior to 30 January.

b. Employees of firms under contract to the U.S. Government and their dependents may be granted limited exchange and commissary access by the garrison and installation commander in accordance with table 7–2. Employees must be hired in the 50 states or the District of Columbia and must exclusively serve the DOD. An annual report of all approved exceptions is required for the 12–month period prior to 30 January.

c. Non-DOD federal employees and their dependents may be granted limited exchange and commissary access by the Secretary of the Army or the Secretary of the Air Force and combatant commanders in accordance with table 7–2. Delegation of this authority outside the Secretariat or Combatant Command Headquarters concerned is prohibited. Employees must be assigned under a service agreement or tour renewal agreement (defined in 41 CFR, Chapter 302). Requests will be sent to the garrison and installation commander by the federal agency and then forwarded through command channels to the appropriate address in paragraph F–1, for consideration and processing to the applicable Secretariat. An annual report of all approved exceptions is required for the 12–month period prior to 30 January.

F–5. Reports

A report of deviations granted by the garrison and installation commander and appropriate Army/Air Force Secretariat is required by DODI 1330.21. Deviations approved by commanders allowing access to exchanges and commissaries (see para F–4*a* and para F–4*b*) will be submitted through command channels to the appropriate Army/Air Force at the address in paragraph F–1. The report must include the names of the employee and Family members and the justification required in paragraph F–4*a* and paragraph F–4*b*. This report will be compiled with approvals granted by the Army/Air Force Secretariat and submitted to the Office of the Secretary of Defense by Headquarters, Department of the Army and Headquarters, Department of the Air Force (see para F–1).

Glossary

Section I
Abbreviations

AAFES
Army and Air Force Exchange Service

AARP–ZA
Department of the Army Committee Management Office

ACOM
Army Command

ACSIM
Assistant Chief of Staff for Installation Management

AF/A1
Air Force: Deputy Chief of Staff for Manpower, Personnel and Services

AF/A1S
Air Force: Deputy Chief of Staff for Manpower, Personnel and Services, Director of Services

AFI
Air Force Instruction

AFJI
Air Force Joint Instruction

AFMAN
Air Force Manual

AFPD
Air Force Policy Directive

AIFA
AAFES Imprest Fund Activity

APFs or APF
appropriated funds or appropriated fund

AR
Army regulation

BOD
board of directors

BRAC
base realignment and closures

CFO
chief financial officer

CFR
Code of Federal Regulations

CONUS
continental United States

CPA
certified public accountant

DA
Department of the Army

DAIM–ISS
Assistant Chief of Staff for Installation Management (Soldier and Family Support Division)

DC
District of Columbia

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DODIG
Department of Defense Inspector General

DOX-T
direct operating exchange-tactical

ECECS
executive control and essential command supervision

EEO
Equal Employment Opportunity

EOP
exchange operating procedure

FAR
Federal Acquisition Regulation

FOIA
Freedom of Information Act

GAO
General Accountability Office

GM
general manager

HQ
Headquarters

HQDA
Headquarters, Department of the Army

IG
inspector general

IMCOM
Installation Management Command

MAJCOM
major command (Air Force)

MCSS
military clothing sales store

MOA
memorandum of agreement

MOU
memorandum of understanding

MWR
morale, welfare, and recreation

NAF or NAFs
nonappropriated fund or nonappropriated funds

NAFI or NAFIs
nonappropriated fund instrumentality or nonappropriated fund instrumentalities

NOAA
National Oceanic and Atmospheric Administration

OCONUS
outside the continental United States

PCS
permanent change of station

PL
Public Law

PDUSD(PR)
Principal Deputy Under Secretary of Defense (Personnel and Readiness)

SF
standard form

SJA
staff judge advocate

SOFA
status of forces agreement

TDY
temporary duty

TFE
tactical field exchange

U.S.
United States

USC
United States Code

USO
United Services Organization

VA
Virginia

Section II
Terms

Adverse action
An action taken against an employee that is contrary to the employee's best interests; it can be appealed under the procedures in EOP 15–10.

Agent
A specific named person authorized on a temporary basis (not exceeding 1 year unless extended for continuing hardship) by the commanding officer, at the command level designated by the Army/Air Force concerned to shop for an authorized patron in extreme hardship cases; or when no adult dependent member is capable of shopping due to sickness or stationing away from their household.

Air Force Services
An organization whose mission is to increase combat capability and improve productivity through programs promoting readiness, esprit de corps, and quality of life for Air Force people. Programs include physical fitness, peacetime and wartime troop feeding, mortuary affairs, Armed Forces entertainment, Air Force protocol, lodging, libraries, child development centers, youth centers, and a wide spectrum of recreation activities.

Alcoholic beverage
Beverages including wines, malt beverages, and distilled spirits.

Amusement machine
Electronic machine that accepts coins to play and provides entertainment or pleasurable diversions. This does not include Army Recreation Machine Program or Air Force Services Gaming machines.

Annex
A facility reporting directly to a branch and which, for accounting, management, and operational and administrative control, is considered to be a component of that branch.

Army and Air Force Exchange Service Imprest Fund Activity
An activity that furnishes exchange support to a small military unit where it is impractical to establish a regular exchange outlet.

Branch
An activity for which separate asset and financial accountability exists.

Business based action
Non-disciplinary, involuntary action taken to adjust personnel resources.

Complaint
An expression of dissatisfaction.

Construction
Includes major and minor construction and modifications (see definitions at major and minor construction).

Construction costs
The direct cost for labor, material, installed equipment integral to the facility, supervision, inspection and overhead, and profit required in order to construct a facility. It includes design costs when part of a design/build construction contract. It does not include design costs prior to construction contract award or the cost of collateral equipment.

Construction project
The erection, installation, or assembly of a new facility; the addition, expansion, extension, alteration, conversion, or replacement of an existing facility; or the relocation of a facility from one place to another. Includes equipment installed and made a part of such facilities, and related site preparation, demolition, excavation, filling, and landscaping, or other improvements.

Continental United States
The 48 contiguous states and the District of Columbia.

Contracting officer
A person authorized to execute and administer contracts on behalf of AAFES, within the limits imposed in their designation, and to make determination and findings with respect thereto.

Contracts
Contracts include all contractual arrangements prescribed by the AAFES director and chief executive officer, in AAFES purchasing procedures, including—

a. Agency contract. A contract whereby AAFES performs certain services as an agent for another who is dealing with AAFES customers.

b. Concessionaire contract. A contract between AAFES and another, known as a concessionaire, whereby the concessionaire performs certain authorized exchange activities on a military installation.

c. Vending machine contract (rental basis). A contract whereby a contractor rents to AAFES and services vending machines that vend merchandise owned by AAFES on a military installation.

d. Installment contract. An agreement whereby, in consideration of the purchase of property or equipment, the purchase price is divided into parts payable over a period of time.

e. Service contract. A contract whereby a contractor performs a service for AAFES off a military installation, such as laundry, dry cleaning, photo processing, and repair service. This type contract may also include procurement of direct services such as janitorial and window cleaning service, or financial services provided by a financial institution.

Dram shop certification
Required by employees selling alcohol to ensure they are aware of their liability in serving alcohol to underage patrons or serving alcohol to someone who appears drunk under the influence.

Exchange (post exchange/base exchange)
The organizational grouping of businesses and services that provide exchange services on Army and Air Force military installations and other locations where AAFES operates.

Expense supplies
Materials and articles, exclusive of motor vehicles, equipment, and other fixed assets that are used or consumed in performing administrative or customer services.

Facility
A general term used to designate any separate unit of real property at which exchange selling and administrative or support functions are performed.

Family member
An individual whose relationship to the sponsor leads to entitlements, benefits, or access administered by the Uniformed Services. Family members include—

a. Dependent children 21 or over. Children, including adopted children, stepchildren, and wards, who are 21 years of age or older, unmarried, and dependent upon the sponsor for over half of their support and either incapable of self-support because of a mental or physical handicap; or have not passed their 23rd birthday and are enrolled in a full-time course of study at an institution of higher education.

b. Dependent children under 21. Unmarried children under 21 years of age, including pre-adoptive children, adopted children, stepchildren, foster children, and wards dependent on the sponsor for over half of their support.

c. Lawful spouse. If separated, a dependent spouse retains privileges until a final divorce decree is issued.

d. Orphans. Surviving unmarried children of a deceased uniformed Servicemember or retired member of a Uniformed Service, who are either adopted or natural born and under the age of 21, or who are over 21 and incapable of self-support; or under 23 and enrolled in a full-time course of study. The surviving children must have been dependents under the Family member definitions at the time of the death of the parent or parents.

e. Parents. Father, mother, stepparent, parent by adoption, and parents-in-law, who depend on the sponsor for over half of their support. The surviving dependent parents of a member of the Armed Services who dies while on active duty are included.

f. Surviving Family member. Children or parents of a sponsor who are dependent on the surviving spouse for over half their support.

g. Surviving spouse. A widow or widower of a sponsor who has not remarried or who, if remarried, has reverted through divorce, annulment, or the demise of the spouse, to an unmarried status.

h. Unmarried children. Unmarried children, including pre-adoptive children, adopted children, stepchildren, foster children, and wards not having passed their 23rd birthday and enrolled in a full-time course of study at an institution of higher education and dependent on the sponsor for over half of their support.

i. Un-remarried former spouse. An un-remarried former spouse of a member or former member of the Uniformed

Services, who (on the date of the final decree of divorce, dissolution, or annulment) had been married to the member or former member for a period of at least 20 years during which period the member or former member performed at least 20 years of service creditable for retired or retainer pay, or equivalent pay.

Fixed assets
Buildings and improvements, motor vehicles, equipment, and other fixed assets owned and capitalized by AAFES.

a. Building and improvements. AAFES investment in renovation and construction of facilities.

b. Equipment. Any item not for resale that meets the dollar thresholds as established by the AAFES director and chief executive officer in the EOP that has a life expectancy of 1 year or more, including—

(1) Vehicles used exclusively for sale of food, merchandise, or services. (These vehicles will be considered motor vehicles for insurance purposes.)

(2) Equipment designed for use in depots, warehouses, stockrooms, and port operations, such as forklifts, tow motors, tow tractors, and trailer movers.

(3) Equipment designed for earth moving, lawn cutting, and snow removal.

c. Motor vehicles. Passenger, cargo, and special purpose vehicles designed for use on public highways.

d. Other fixed assets. Multiple or groups of similar items not for resale that do not meet the dollar threshold for being classified as equipment (see para *b*, above), but that meet the established categories and dollar thresholds for being capitalized.

Garrison
For purposes of this regulation, the Army uses garrison to define any real property or area that is controlled, owned, or leased by DA.

Garrison commander
For the purpose of this regulation, garrison commanders are responsible for exchange operations at Army locations, such as a base, camp, post, station, yard, center, home port facility for any ship, or other activity under the jurisdiction of the DOD, including leased facilities.

General manager (GM)
An AAFES civilian employee who is responsible to a region senior vice president for the operational supervision of AAFES activities located on a garrison and installation that is part of a region.

Grievance
A complaint that has been reduced to writing (this definition applies only to proceedings within the purview of this regulation and EOP 15–10).

Inside the United States
The 50 United States and the District of Columbia.

Installation
For the purpose of this regulation, the Air Force uses installation to define any real property or area that is controlled, owned, or leased by the Department of the Air Force.

Installation commander
For purposes of this regulation, installation commanders are responsible for exchange operations at Air Force locations, such as a base, camp, post, station, yard, center, home port facility for any ship, or other activity under the jurisdiction of the DOD, including leased facilities.

Landed cost
Vendor invoice plus warehousing and applicable transportation costs.

Limited privileges
Generally, purchasing privileges exclude tax-free alcoholic beverages, tobacco products, and military uniforms. Other limitations are explained in table 7–2.

Major construction
A construction project with a construction component cost that exceeds $750,000.

Matters of official interest
Any matter that concerns or affects AAFES business, personnel, customers and reputation; either on-duty conduct, or off-duty conduct that has a nexus to AAFES or has any implications regarding the employee's ability to perform their

job. This includes, but is not limited to, activities on AAFES premises and involving AAFES merchandise, funds, or property; interactions between activities of, or actions by and affecting AAFES personnel whether in their official capacity or in any way affecting AAFES; information about or concerning customers including transactional information and financial activities; and any matter affecting AAFES' reputation in the community, within the government, or with its customers.

Media
Any method used to convey an advertising message; it includes newspapers, magazines, trade, and professional journals, special printed matter, circulars, flyers, posters, signs, radio, television, and other promotional devices such as decals, table tents, or activity calendars.

Merchandise
Items of consumer goods purchased and offered for sale to authorized customers through retail, food, service, and vending outlets.

Minor construction
A construction project with a construction component cost between $200,000 and $750,000.

Modernization
Includes alterations of facilities solely to implement new or higher standards (including regulatory changes) to accommodate new functions, or to replace building components that typically last more than 50 years (such as foundation, structural members).

Morale, welfare, and recreation (MWR) programs
Those military MWR programs located on DOD installations or on property controlled (by lease or other means) by the DOD or furnished by a DOD contractor that provide mission sustainment, community support, and other revenue-generating programs for authorized DOD personnel. They include the programs listed in respective Army and Air Force regulations and instructions, as implemented from DODI 1015.10. Private organizations are not MWR programs.

Nonappropriated fund (NAF)
Cash and other assets received from sources other than Congressional appropriations. NAFs are government funds used for the collective benefit of those who generate them. These funds are separate and apart from funds that are recorded in the books of the Treasurer of the United States.

Nonappropriated fund instrumentality (NAFI)
A U.S. Government organization and fiscal entity that performs essential government functions. It is not a federal agency. It acts in its own name to provide, or assist other DOD organizations in providing MWR and other programs for military personnel, their families, and authorized civilians. It is established and maintained individually or jointly by two or more DOD components. As a fiscal entity, it maintains custody of and control over its NAFs, equipment, facilities, land, and other assets. It is responsible for the prudent administration, safeguarding, preservation, and maintenance of those APF resources made available to carry out its function. With its NAFs, it contributes to the MWR programs of other authorized organizational entities, when so authorized. It is not incorporated under the laws of any state or the District of Columbia and enjoys the legal status of an instrumentality of the United States. NAFIs are not persons subject to federal trade and antitrust laws, and they are not subject to state regulation or control in absence of specific authorization in a federal statute.

Outside the continental United States (OCONUS)
Areas other than the 48 contiguous states and the District of Columbia. Includes Alaska, Hawaii, the Commonwealths of Puerto Rico and the Northern Mariana Islands, and the U.S. territories and possessions.

Outside the United States
All locations except the 50 United States and the District of Columbia.

Overseas
Areas other than the 50 United States and the District of Columbia.

Packaged alcoholic beverage
An alcoholic beverage in an unopened container for consumption at a location other than the place of sale.

Pog
An artificial coin used in combat, mobilization, contingency areas where U.S. coinage is not readily available.

Premium
Items furnished without charge to advertise an activity, product, service, or event or to serve as an inducement to buy.

Principal management official
Individuals with the delegated authority for administrative and disciplinary actions involving a loss of pay or grade, to include separations. Specific delegations are contained in EOP 15–10.

Procurement
All functions pertaining to purchasing, renting, leasing, or otherwise obtaining merchandise, equipment, supplies, facilities, and services.

Purchasing activity
An organizational element assigned the responsibility for purchasing merchandise, equipment, supplies, facilities, or services.

Real property
Lands, buildings, structures, utilities systems, improvements, and appurtenances thereto. Includes equipment attached to and made part of buildings and structures (such as heating systems) but not movable equipment (such as plant equipment).

Remote and isolated locations
Sites identified as remote and isolated locations in accordance with DODI 1015.10 and the DOD approved list of military locations. Also see departmental regulations.

Reserve Components
The Army National Guard, the Army National Guard of the United States, the Air National Guard, the Air National Guard of the United States, the Army Reserve, the Naval Reserve, the Marine Corps Reserve, the Air Force Reserve, the Coast Guard Reserve, and the Reserve Officers of the Public Health Service. Members of the Reserve Components include all individuals in any category of the foregoing, whether on active or inactive status, to include any retirees who would be eligible for retired pay except for the fact that they have not reached age 60.

Restoration
Includes the restoration of facilities damaged by inadequate sustainment, excessive age, natural disaster, fire, accident, or other causes.

Retired uniformed military personnel
The term retired uniformed personnel includes—

a. All retired personnel carried on the official retired lists (Active and Reserve) of the Uniformed Services, who are retired with pay, granted retirement pay for physical disability, or entitled to retirement pay whether or not such pay is waived, or pending due to age requirement.

b. Members of the Retired Reserve who are eligible for retired pay at age 60, but have not yet reached age 60.

c. Personnel on the emergency officers' retired list of the Army, the Navy, the Air Force, and the Marine Corps who retired under 38 USC, (reference (l)).

d. Officers, crews of vessels, light keepers, and depot keepers of the former Lighthouse Service who retired under 33 USC (reference (m)).

e. Retired noncommissioned ships' officers and crewmembers of the NOAA and its predecessors, who either were on active duty as a vessel employee on 19 July 1963, and whose employment as such vessel employee was continuous from that date until the date of retirement, or who had retired as a vessel employee on or before 19 July, 1963.

Sole survivorship
A member of the Armed Forces who is discharged from the Armed Forces at their request based on the member being the only surviving child in a family in which the father or mother, or one or more siblings, was killed, died as a result of wounds, accident, or disease, is in a captured or missing in action status, or is permanently disabled while serving honorably in the Armed Forces.

State tax-free items
Soft drinks, alcoholic beverages, and tobacco products which are purchased and resold by AAFES free of state and local excise taxes.

Sustainment
Includes maintenance and repair activities necessary to keep an inventory of facilities in good working order. It includes regularly scheduled adjustments and inspections, preventive maintenance tasks, and emergency response and service calls for minor repairs. It also includes major repairs or replacement of facility components (usually accomplished by contract) that are expected to occur periodically throughout the life cycle of facilities. This work includes regular roof replacement, refinishing of wall surfaces, repairing and replacement of heating and cooling systems, replacing tile and carpeting, and similar types of work. It does not include environmental compliance costs, facility leases, or other tasks associated with facilities operations (such as custodial services, grounds services, waste disposal, and the provision of central utilities).

Tactical field exchange (TFE)
An exchange activity established for a temporary period to support a military contingency operation or training exercise.

Uniformed personnel
Members of the Army, Navy, Air Force, Marine Corps, and Coast Guard; cadets and midshipmen of the Army, Navy, Air Force, and Coast Guard academies; commissioned officers of the NOAA; commissioned officers of the Public Health Service; and members of the Reserve Components while on extended active duty.

Uniformed Services
The Army, Navy, Air Force, Marine Corps, Coast Guard; commissioned officers of the Public Health Service; and active duty and retired commissioned officers of vessels of the NOAA and its predecessors, the Coast and Geodetic Survey, and the Environmental Science Services Administration.

U.S. Government employee
A federal civilian employee of DOD directly hired and paid from APFs or NAFs.

U.S. territories and possessions
Includes Guam, the Commonwealth of Puerto Rico, the American Virgin Islands, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Section III
Special Abbreviations and Terms
This section contains no entries.

10 USC 3013: Secretary of the Army
Text contains those laws in effect on February 22, 2016

From Title 10-ARMED FORCES
Subtitle B-Army
PART I-ORGANIZATION
CHAPTER 303-DEPARTMENT OF THE ARMY
Jump To:
Source Credit
Prior Provisions
Amendments
Miscellaneous

§3013. Secretary of the Army

(a)(1) There is a Secretary of the Army, appointed from civilian life by the President, by and with the advice and consent of the Senate. The Secretary is the head of the Department of the Army.

(2) A person may not be appointed as Secretary of the Army within five years after relief from active duty as a commissioned officer of a regular component of an armed force.

(b) Subject to the authority, direction, and control of the Secretary of Defense and subject to the provisions of chapter 6 of this title, the Secretary of the Army is responsible for, and has the authority necessary to conduct, all affairs of the Department of the Army, including the following functions:

(1) Recruiting.
(2) Organizing.
(3) Supplying.
(4) Equipping (including research and development).
(5) Training.
(6) Servicing.
(7) Mobilizing.
(8) Demobilizing.
(9) Administering (including the morale and welfare of personnel).
(10) Maintaining.
(11) The construction, outfitting, and repair of military equipment.
(12) The construction, maintenance, and repair of buildings, structures, and utilities and the acquisition of real property and interests in real property necessary to carry out the responsibilities specified in this section.

(c) Subject to the authority, direction, and control of the Secretary of Defense, the Secretary of the Army is also responsible to the Secretary of Defense for-

(1) the functioning and efficiency of the Department of the Army;
(2) the formulation of policies and programs by the Department of the Army that are fully consistent with national security objectives and policies established by the President or the Secretary of Defense;
(3) the effective and timely implementation of policy, program, and budget decisions and instructions of the President or the Secretary of Defense relating to the functions of the Department of the Army;
(4) carrying out the functions of the Department of the Army so as to fulfill the current and future operational requirements of the unified and specified combatant commands;
(5) effective cooperation and coordination between the Department of the Army and the other military departments and agencies of the Department of Defense to provide for more effective, efficient, and economical administration and to eliminate duplication;
(6) the presentation and justification of the positions of the Department of the Army on the plans, programs, and policies of the Department of Defense; and
(7) the effective supervision and control of the intelligence activities of the Department of the Army.

(d) The Secretary of the Army is also responsible for such other activities as may be prescribed by law or by the President or Secretary of Defense.

(e) After first informing the Secretary of Defense, the Secretary of the Army may make such recommendations to Congress relating to the Department of Defense as he considers appropriate.

(f) The Secretary of the Army may assign such of his functions, powers, and duties as he considers appropriate to the Under Secretary of the Army and to the Assistant Secretaries of the Army. Officers of the Army shall, as directed by the Secretary, report on any matter to the Secretary, the Under Secretary, or any Assistant Secretary.

(g) The Secretary of the Army may-

(1) assign, detail, and prescribe the duties of members of the Army and civilian personnel of the Department of the Army;
(2) change the title of any officer or activity of the Department of the Army not prescribed by law; and
(3) prescribe regulations to carry out his functions, powers, and duties under this title.

(Added Pub. L. 99–433, title V, §501(a)(5), Oct. 1, 1986, 100 Stat. 1035 ; amended Pub. L. 99–661, div. A, title V, §534, Nov. 14, 1986, 100 Stat. 3873 ; Pub. L. 108–136, div. A, title IX, §901, Nov. 24, 2003, 117 Stat. 1558 .)

PRIOR PROVISIONS

A prior section 3013, acts Aug. 10, 1956, ch. 1041, 70A Stat. 157, §3012; Sept. 2, 1958, Pub. L. 85–861, §1 (57), 72 Stat. 1462 ; Sept. 7, 1962, Pub. L. 87–651, title II, §211, 76 Stat. 524 ; Aug. 14, 1964, Pub. L. 88–426, title III, §§305(2), 306(j)(1), 78 Stat. 422 , 431; Nov. 2, 1966, Pub. L. 89–718, §22, 80 Stat. 1118 ; renumbered §3013, Oct. 1, 1986, Pub. L. 99–433, title V, §501(a)(2), 100 Stat. 1034 , related to Secretary of the Army, powers and duties, and delegations, prior to repeal by Pub. L. 99–433, §501(a)(5).

Another prior section 3013 was renumbered section 3014 of this title and subsequently repealed.

AMENDMENTS

2003-Subsec. (c)(4). Pub. L. 108–136 struck out "(to the maximum extent practicable)" after "fulfill".

1986-Subsec. (a)(2). Pub. L. 99–661 substituted "five years" for "10 years".

PILOT PROGRAM FOR THE HUMAN TERRAIN SYSTEM

Pub. L. 113–291, div. A, title X, §1075, Dec. 19, 2014, 128 Stat. 3519 , provided that:

"(a) Pilot Program Required.-The Secretary of the Army may carry out a pilot program under which the Secretary utilizes Human Terrain System assets in the United States Pacific Command area of responsibility to support phase 0 shaping operations and the theater security cooperation plans of the Commander of the United States Pacific Command.

"(b) Reports.-

"(1) Initial report.-Not later than one year after the date of the enactment of this Act [Dec. 19, 2014], the Secretary of the Army shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the status of the pilot program under this section. Such report shall include the independent analysis and recommendations of the Commander of the United States Pacific Command regarding the effectiveness of the program and how it could be improved.

"(2) Final report.-Not later than December 1, 2016, the Secretary of the Army shall submit to the congressional defense committees a final report on the pilot program. Such report shall include an analysis of the comparative value of human terrain information relative to other analytic tools and techniques, recommendations regarding expanding the program to include other combatant commands, and any improvements to the program and necessary resources that would enable expanding the program.

"(c) Termination.-The authority to carry out a pilot program under this section shall terminate on September 30, 2016."

EXPANSION OF FIRST SERGEANTS BARRACKS INITIATIVE

Pub. L. 111–84, div. B, title XXVIII, §2807, Oct. 28, 2009, 123 Stat. 2663 , provided that:

"(a) Expansion of Initiative.-Not later than September 30, 2011, the Secretary of the Army shall expand the First Sergeants Barracks Initiative (FSBI) to include all Army installations in order to improve the quality of life and living environments for single soldiers.

"(b) Progress Reports.-Not later than February 15, 2010, and February 15, 2011, the Secretary of the Army shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report describing the progress made in expanding the First Sergeants Barracks Initiative to all Army installations."

SELECTION OF MILITARY INSTALLATIONS TO SERVE AS LOCATIONS OF BRIGADE COMBAT TEAMS

Pub. L. 111–84, div. B, title XXVIII, §2825, Oct. 28, 2009, 123 Stat. 2668 , provided that: "In selecting the military installations at which brigade combat teams will be stationed, the Secretary of the Army shall take into consideration the availability and proximity of training spaces for the units and the capacity of the installations to support the units."

ARMY TRAINING STRATEGY FOR BRIGADE-BASED COMBAT TEAMS AND FUNCTIONAL SUPPORTING BRIGADES

Pub. L. 109–163, div. A, title III, §353, Jan. 6, 2006, 119 Stat. 3203 , provided that:

"(a) Training Strategy.-

"(1) Strategy required.-The Secretary of the Army shall develop and implement a strategy for the training

of brigade-based combat teams and functional supporting brigades in order to ensure the readiness of such teams and brigades.

"(2) Elements.-The training strategy under paragraph (1) shall include the following:

"(A) A statement of the purpose of training for brigade-based combat teams and functional supporting brigades.

"(B) Performance goals for both active-component and reserve-component brigade-based combat teams and functional supporting brigades, including goals for live, virtual, and constructive training.

"(C) Metrics to quantify training performance against the performance goals specified under subparagraph (B).

"(D) A process to report the status of collective training to Army leadership for monitoring the training performance of brigade-based combat teams and functional supporting brigades.

"(E) A model to quantify, and to forecast, operation and maintenance funding required for each fiscal year to attain the performance goals specified under subparagraph (B).

"(3) Timing of implementation.-The Secretary of the Army shall develop and implement the training strategy under paragraph (1) as soon as practicable.

"(b) Report.-

"(1) Report required.-Not later than one year after the date of the enactment of this Act [Jan. 6, 2006], the Secretary of the Army shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the training strategy developed under subsection (a).

"(2) Elements.-The report under paragraph (1) shall include the following:

"(A) A discussion of the training strategy developed under subsection (a), including a description of the performance goals and metrics developed under that subsection.

"(B) A discussion and description of the training ranges and other essential elements required to support the training strategy.

"(C) A list of the funding requirements, shown by fiscal year and set forth in a format consistent with the future-years defense program to accompany the budget of the President under section 221 of title 10, United States Code, necessary to meet the requirements of the training ranges and other essential elements described under subparagraph (B).

"(D) A schedule for the implementation of the training strategy.

"(c) Comptroller General Review of Implementation.-

"(1) In general.-The Comptroller General shall monitor the implementation of the training strategy developed under subsection (a).

"(2) Report.-Not later than 180 days after the date on which the Secretary of the Army submits the report under subsection (b), the Comptroller General shall submit to the congressional defense committees a report containing the assessment of the Comptroller General of the current progress of the Army in implementing the training strategy."

ARMY TRANSFORMATION TO BRIGADE STRUCTURE

Pub. L. 108–375, div. A, title V, §595(c), Oct. 28, 2004, 118 Stat. 1937 , provided that: "The Secretary of the Army shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives an annual report on the status of the internal transformation of the Army from a division-orientated force to a brigade-orientated force. Such report shall be submitted not later than March 31 of each year, except that the requirement to submit such annual report shall terminate when the Secretary of the Army submits to those committees the Secretary's certification that the transformation of the Army to a brigade-orientated force has been completed. Upon the submission of such certification, the Secretary shall publish in the Federal Register notice of that certification and that the statutory requirement to submit an annual report under this subsection has terminated."

DEMONSTRATION PROJECT FOR USE OF ARMY INSTALLATIONS TO PROVIDE PRERELEASE EMPLOYMENT TRAINING TO NONVIOLENT OFFENDERS IN STATE PENAL SYSTEMS

Pub. L. 103–337, div. A, title X, §1065, Oct. 5, 1994, 108 Stat. 2849 , provided that:

"(a) Demonstration Project Authorized.-The Secretary of the Army may conduct a demonstration project to test the feasibility of using Army facilities to provide employment training to nonviolent offenders in a State penal system before their release from incarceration. The demonstration project shall be limited to not more than three military installations under the jurisdiction of the Secretary.

"(b) Sources of Training.-The Secretary may enter into a cooperative agreement with one or more private, nonprofit organizations for purposes of providing at the military installations included in the demonstration

project the prerelease employment training authorized under subsection (a) or may provide such training directly at such installations by agreement with the State concerned.

"(c) Use of Facilities.-Under a cooperative agreement entered into under subsection (b), the Secretary may lease or otherwise make available to a nonprofit organization participating in the demonstration project at a military installation included in the demonstration project any real property or facilities at the installation that the Secretary considers to be appropriate for use to provide the prerelease employment training authorized under subsection (a). Notwithstanding section 2667(b)(4) of title 10, United States Code, the use of such real property or facilities may be permitted with or without reimbursement.

"(d) Acceptance of Services.-Notwithstanding section 1342 of title 31, United States Code, the Secretary may accept voluntary services provided by persons participating in the prerelease employment training authorized under subsection (a).

"(e) Liability and Indemnification.-(1) The Secretary may not enter into a cooperative agreement under subsection (b) with a nonprofit organization for the participation of that organization in the demonstration project unless the agreement includes provisions that the nonprofit organization shall-

"(A) be liable for any loss or damage to Federal Government property that may result from, or in connection with, the provision of prerelease employment training by the organization under the demonstration project; and

"(B) hold harmless and indemnify the United States from and against any suit, claim, demand, action, or liability arising out of any claim for personal injury or property damage that may result from or in connection with the demonstration project.

"(2) The Secretary may not enter into an agreement under subsection (b) with the State concerned for the provision of prerelease employment training directly by the Secretary unless the agreement with the State concerned includes provisions that the State shall-

"(A) be liable for any loss or damage to Federal Government property that may result from, or in connection with, the provision of the training except to the extent that the loss or damage results from a wrongful act or omission of Federal Government personnel; and

"(B) hold harmless and indemnify the United States from and against any suit, claim, demand, action, or liability arising out of any claim for personal injury or property damage that may result from, or in connection with, the provision of the training except to the extent that the personal injury or property damage results from a wrongful act or omission of Federal Government personnel.

"(f) Report.-Not later than two years after the date of the enactment of this Act [Oct. 5, 1994], the Secretary shall submit to Congress a report evaluating the success of the demonstration project and containing such recommendations with regard to the termination, continuation, or expansion of the demonstration project as the Secretary considers appropriate."

ORDER OF SUCCESSION

For order of succession in event of death, permanent disability, or resignation of Secretary of the Army, see Ex. Ord. No. 12908, Apr. 22, 1994, 59 F.R. 21907, listed in a table under section 3345 of Title 5.

10 USC 8013: Secretary of the Air Force
Text contains those laws in effect on February 22, 2016

From Title 10-ARMED FORCES
Subtitle D-Air Force
PART I-ORGANIZATION
CHAPTER 803-DEPARTMENT OF THE AIR FORCE

Jump To:
Source Credit
Prior Provisions
Amendments
Miscellaneous

§8013. Secretary of the Air Force

(a)(1) There is a Secretary of the Air Force, appointed from civilian life by the President, by and with the advice and consent of the Senate. The Secretary is the head of the Department of the Air Force.

(2) A person may not be appointed as Secretary of the Air Force within five years after relief from active duty as a commissioned officer of a regular component of an armed force.

(b) Subject to the authority, direction, and control of the Secretary of Defense and subject to the provisions of chapter 6 of this title, the Secretary of the Air Force is responsible for, and has the authority necessary to conduct, all affairs of the Department of the Air Force, including the following functions:

(1) Recruiting.
(2) Organizing.
(3) Supplying.
(4) Equipping (including research and development).
(5) Training.
(6) Servicing.
(7) Mobilizing.
(8) Demobilizing.
(9) Administering (including the morale and welfare of personnel).
(10) Maintaining.
(11) The construction, outfitting, and repair of military equipment.
(12) The construction, maintenance, and repair of buildings, structures, and utilities and the acquisition of real property and interests in real property necessary to carry out the responsibilities specified in this section.

(c) Subject to the authority, direction, and control of the Secretary of Defense, the Secretary of the Air Force is also responsible to the Secretary of Defense for-

(1) the functioning and efficiency of the Department of the Air Force;
(2) the formulation of policies and programs by the Department of the Air Force that are fully consistent with national security objectives and policies established by the President or the Secretary of Defense;
(3) the effective and timely implementation of policy, program, and budget decisions and instructions of the President or the Secretary of Defense relating to the functions of the Department of the Air Force;
(4) carrying out the functions of the Department of the Air Force so as to fulfill the current and future operational requirements of the unified and specified combatant commands;
(5) effective cooperation and coordination between the Department of the Air Force and the other military departments and agencies of the Department of Defense to provide for more effective, efficient, and economical administration and to eliminate duplication;
(6) the presentation and justification of the positions of the Department of the Air Force on the plans, programs, and policies of the Department of Defense; and
(7) the effective supervision and control of the intelligence activities of the Department of the Air Force.

(d) The Secretary of the Air Force is also responsible for such other activities as may be prescribed by law or by the President or Secretary of Defense.

(e) After first informing the Secretary of Defense, the Secretary of the Air Force may make such recommendations to Congress relating to the Department of Defense as he considers appropriate.

(f) The Secretary of the Air Force may assign such of his functions, powers, and duties as he considers appropriate to the Under Secretary of the Air Force and to the Assistant Secretaries of the Air Force. Officers of the Air Force shall, as directed by the Secretary, report on any matter to the Secretary, the Under Secretary, or any Assistant Secretary.

(g) The Secretary of the Air Force may-

(1) assign, detail, and prescribe the duties of members of the Air Force and civilian personnel of the Department of the Air Force;
(2) change the title of any officer or activity of the Department of the Air Force not prescribed by law; and

(3) prescribe regulations to carry out his functions, powers, and duties under this title.

(Added Pub. L. 99–433, title V, §521(a)(3), Oct. 1, 1986, 100 Stat. 1055 ; amended Pub. L. 99–661, div. A, title V, §534, Nov. 14, 1986, 100 Stat. 3873 ; Pub. L. 108–136, div. A, title IX, §901, Nov. 24, 2003, 117 Stat. 1558 .)

PRIOR PROVISIONS

A prior section 8013, acts Aug. 10, 1956, ch. 1041, 70A Stat. 488, §8012; Sept. 2, 1958, Pub. L. 85–861, §1(152), 72 Stat. 1513 ; Sept. 7, 1962, Pub. L. 87–651, title II, §211, 76 Stat. 524 ; Aug. 14, 1964, Pub. L. 88–426, title III, §§305(7), 306(j)(7), 78 Stat. 423 , 432; renumbered §8013, Oct. 1, 1986, Pub. L. 99–433, title V, §521(a)(1), 100 Stat. 1055 , related to Secretary of the Air Force, powers and duties, and delegations, prior to repeal by Pub. L. 99–433, §521(a)(3).

Another prior section 8013 was renumbered section 8014 of this title and subsequently repealed.

AMENDMENTS

2003-Subsec. (c)(4). Pub. L. 108–136 struck out "(to the maximum extent practicable)" after "fulfill".

1986-Subsec. (a)(2). Pub. L. 99–661 substituted "five years" for "10 years".

ORDER OF SUCCESSION

For order of succession in event of death, permanent disability, or resignation of Secretary of the Air Force, see Ex. Ord. No. 12909, Apr. 22, 1994, 59 F.R. 21909, listed in a table under section 3345 of Title 5.

RATING CHAINS FOR SYSTEM PROGRAM MANAGERS

Pub. L. 112–239, div. A, title III, §323, Jan. 2, 2013, 126 Stat. 1696 , provided that: "The Secretary of the Air Force, in managing system program management responsibilities for sustainment programs not assigned to a program executive officer or a direct reporting program manager, shall comply with the Department of Defense Instructions regarding assignment of program responsibility."

Army Regulation 380–67

Security

Personnel Security Program

Headquarters
Department of the Army
Washington, DC
24 January 2014

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–67
Personnel Security Program

This rapid action revision, dated 24 January 2014--

- Revises criteria for application of security standards (para 2-4*q*).
- Incorporates the provisions to provide procedural benefits to afford individuals an opportunity to appeal a final adjudicative decisions to a higher level authority (para 8-6*d*).
- Adds performance measures (para 11-5).
- Rescinds appendix on reporting of nonderogatory cases (app E).
- Deletes appendix on guidelines for conducting prenomination personal interviews (app G).
- Deletes appendix on the list of designated countries (app H).
- Updates the National Adjudicative Guidelines (app I).
- Adds internal control evaluation (app M).

Headquarters
Department of the Army
Washington, DC
24 January 2014

*Army Regulation 380–67

Effective 24 February 2014

Security

Personnel Security Program

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army

History. This publication is a rapid action revision. The portions affected by this rapid action revision are listed in the summary of change.

Summary. This regulation implements the DOD and Department of the Army Personnel Security Program and takes precedence over all other departmental issuances affecting these programs. It contains the policies and procedures for access to classified information and assignment in a sensitive position. It also prescribes the investigative scope and adjudicative standards and criteria that are necessary prerequisites for such access or employment. It includes due process procedures for appealing adverse administrative actions rendered in accordance with the provisions of this regulation. This regulation contains all of DOD 5200.2–R and includes all recommendations of the Commission to Review DOD Security Policies and Practices (Stilwell Commission) approved for implementation. Army implementing instructions in this regulation are set in boldface type.

Applicability. This regulation applies to the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. Also, it applies only to Army contractor personnel who require access to sensitive compartmented information in the performance of their duties.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G–2. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix M).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–2, 1000 Army Pentagon, Washington, DC 20310–1000.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G–2, 1000 Army Pentagon, Washington, DC 20310–1000.

Distribution. This regulation is available in electronic media only and is intended for command levels A, B, C, D, and E for the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 380–67, dated 9 September 1988.

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Contents—Continued

Chapter 1
General Provisions

1–1. Purpose

a. To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces and United States Army, acceptance and retention of civilian employees in the Department of Defense (DOD) and Department of the Army (DA), and granting members of the Armed Forces, Army, DA and DOD civilian employees, DA and DOD contractors, and other affiliated persons access to classified information and assignment to sensitive positions are clearly consistent with the interests of national security.

b. This regulation—

(1) Establishes DA and DOD personnel security policies and procedures;

(2) Sets forth the standards, criteria and guidelines upon which personnel security determinations shall be based;

(3) Prescribes the kinds and scopes of personnel security investigation (PSIs) required;

(4) Details the evaluation and adverse action procedures by which personnel security determinations shall be made; and

(5) Assigns overall program management responsibilities.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities

Responsibilities are listed throughout this regulation.

1–5. Objectives

a. This regulation implements the DOD **and DA** Personnel Security Program and takes precedence over all other departmental issuances affecting that program.

b. All provisions of this regulation apply to **DA and** DOD civilian personnel, members of the Armed Forces, excluding the Coast Guard in peacetime, **U.S. Army, DA and** contractor personnel and other personnel who are affiliated with the DOD **and the Army** except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DOD 5220.22–R **(AR 380–49)** and in Department of Defense Directive (DODD) 5220.6 **(AR 380–49)**.

c. The policies and procedures which govern the National Security Agency are prescribed by Public Laws (PL) 88–290 and 86–36, Executive Orders 10450 (EO 10450) and 12333, DODD 5210.45, Director of Central Intelligence Directive (DCID) 1/14 (references (e), (f), (g), (h), (i), and (l), respectively), and regulations of the National Security Agency.

d. Under combat conditions or other military exigencies, an authority in paragraph 1, appendix F, may waive such provisions of this regulation as the circumstances warrant.

e. **This regulation also applies to —**

(1) **Persons employed, hired on an individual basis, or serving on an advisory or consultant basis (including co-op and summer hire students) for whom Army personnel security clearances are required, whether or not such persons are paid from appropriated or nonappropriated funds.**

(2) **Employees of the Army National Guard (ARNG), Army-Air Force Exchange Service, American Red Cross, the United Service Organizations (USO), who are required to have Army personnel security clearances.**

Chapter 2
Policies

Section I
Standards for Access to Classified Information or Assignment to Sensitive Duties

2–1. General

a. Only U.S. citizens shall be granted a personnel security clearance, assigned to sensitive duties, or granted access to classified information unless an authority designated in appendix F has determined that, based on all available information, there are compelling reasons in furtherance of the DOD mission, including, special expertise, to assign an individual who is not a citizen to sensitive duties or grant a limited access authorization to classified information. Non-

U.S. citizens may be employed in the competitive service in sensitive civilian positions only when specifically approved by the Office of Personnel Management (OPM), pursuant to EO 11935. Exceptions to these requirements shall be permitted only for compelling national security reasons.

b. **No person is entitled to knowledge of, possession of, or access to classified defense information solely by virtue of office, position, grade, rank, or security clearance. Such information will be entrusted only to persons whose official military or other governmental duties require it and who have been investigated and cleared for access under the standards prescribed by this regulation. Security clearances indicate that the persons concerned are eligible for access to classified information should their official duties require it.**

2–2. Clearance and sensitive position standard

The personnel security standard that must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

2–3. Military service standard

The personnel security standard that must be applied in determining whether a person is suitable under national security criteria for appointment, enlistment, induction, or retention in the Armed Forces is that, based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States.

Section II
Criteria for Application of Security Standards

2–4. Criteria for application of security standards

The ultimate decision in applying either of the security standards set forth in paragraphs 2–2 and 2–3, above, must be an overall common sense determination based upon all available facts. The criteria for determining eligibility for a clearance or assignment to a sensitive position under the security standard shall include, but not be limited to the following (see app I for further guidance on the application of these factors):

a. Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts thereat or preparation therefore, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

b. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

c. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

d. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State or which seeks to overthrow the Government of the United States, or any State or subdivision thereof by unlawful means.

e. Unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by statute, Executive order, or regulation.

f. Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner which serves or which could be expected to serve the interests of another government in preference to the interests of the United States.

g. Disregard of public law, statutes, EOs, or regulations, including violation of security regulations or practices.

h. Criminal or dishonest conduct.

i. Acts of omission or commission that indicate poor judgment, unreliability, or untrustworthiness.

j. Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case.

k. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be (1) the presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States, or (2) any other circumstances that could cause the applicant to be vulnerable.

l. Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

m. Habitual or episodic use of intoxicants to excess.

n. Illegal or improper use, possession, transfer, or sale of or addiction to any controlled or psychoactive substance, narcotic, cannabis, or other dangerous drug.

o. Any knowing and willful falsification, cover up, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by DOD or any other Federal agency.

p. Failing or refusing to answer or to authorize others to answer questions or provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment. **Refusing or intentionally failing to provide a current personal security questionnaire (PSQ) or omitting material facts in a PSQ or other security form. Refusing to submit to a medical or psychological evaluation when information indicates the individual may have a mental or nervous disorder or be addicted to alcohol or any controlled substance.**

q. Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference may be made solely on the basis of the sexual orientation of the individual.

Section III
Types and Scope of Personnel Security Investigations

2–5. General
The types of PSIs authorized below vary in scope of investigative effort required to meet the purpose of the particular investigation. No other types are authorized. The scope of a PSI may be neither raised nor lowered without the approval of the DUSD(P).

2–6. National agency check/entrance national agency check
Essentially, a national agency check (NAC) is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making a personnel security determination. An entrance national agency check (ENTNAC) is a NAC (scope as outlined in para **B**–1, app B) conducted on inductees and first-term enlistees, but lacking a technical fingerprint search. A NAC is also an integral part of each background investigation (BI), special background investigation (SBI), and periodic reinvestigation (PR). Chapter 3 prescribes when a NAC is required.

2–7. National agency check and written inquiries
The OPM conducts a NAC and written inquiries (NACI) on civilian employees for all departments and agencies of the Federal Government, pursuant to EO 10450. NACIs are considered to meet the investigative requirements of this regulation for a nonsensitive or noncritical-sensitive position and/or up to a SECRET clearance and, in addition to the NAC, include coverage of law enforcement agencies, former employers and supervisors, references, and schools covering the last 5 years.

2–8. DOD national agency check and written inquiries
The Defense Investigative Service (DIS) will conduct a Department of Defense National Agency check with written inquiries (DNACI), consisting of the scope contained in paragraph **B**–2, appendix B, for DOD military and contractor personnel for access to SECRET information. Chapter 3 prescribes when a DNACI is required.

2–9. Background investigation
The BI is the principal type of investigation conducted when an individual requires TOP SECRET clearance or is to be assigned to a critical-sensitive position. The BI normally covers a 5-year period and consists of a subject interview, NAC, local agency check (LAC)s, credit checks, developed character references (3), employment records checks, employment references (3), and select scoping as required to resolve unfavorable or questionable information. (See para**B**–3, app B.) Chapter 3 prescribes when a BI is required.

2–10. Special background investigation
a. An SBI is essentially a BI providing additional coverage both in period of time as well as sources of information, scoped in accordance with the provisions of Director of Central Intelligence Directive (DCID) 1/14 but without the personal interview. While the kind of coverage provided for by the SBI determines eligibility for access to sensitive compartmented information (SCI), DD has adopted this coverage for certain other special access programs. Chapter 3 prescribes when an SBI is required.

b. The OPM, FBI, Central Intelligence Agency (CIA), Secret Service, and the Department of State conduct specially scoped BIs under the provisions of DCID 1/14. Any investigation conducted by one of the above-cited agencies under DCID 1/14 standards is considered to meet the SBI investigative requirements of this regulation.

c. The detailed scope of an SBI is set forth in paragraph **B**–4, appendix B.

2–11. Special investigative inquiry

a. A special investigative inquiry (SII) is a PSI conducted to prove or disprove allegations relating to the criteria outlined in paragraph 2–4 of this regulation, except current criminal activities (see para 2–17*d*, below), that have arisen concerning an individual upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a trustworthiness determination.

b. Special investigative inquiries are scoped as necessary to address the specific matters requiring resolution in the case concerned and generally consist of record checks and/or interviews with potentially knowledgeable persons. An SII may include an interview with the subject of the investigation when necessary to resolve conflicting information and/or to provide an opportunity to refute or mitigate adverse information.

c. In those cases when there is a disagreement between DIS and the requester as to the appropriate scope of the investigation, the matter may be referred to the Deputy Under Secretary of Defense (Policy) (DUSD(P)) for resolution. **Requests for resolution will be forwarded through command channels to HQDA (DAMI–CIS), Washington, DC 20310–1051.**

2–12. Periodic reinvestigation

As referred to in paragraph 3–55 and other national directives, certain categories of duties, clearance, and access require the conduct of a PR every 5 years according to the scope outlined in paragraph **B**–5, appendix B. The PR scope applies to military, civilian, contractor, and foreign national personnel.

2–13. Personal interview

Investigative experience over the years has demonstrated that, given normal circumstances, the subject of a PSI is the best source of accurate and relevant information concerning the matters under consideration. Further, restrictions imposed by the Privacy Act of 1974 dictate that Federal investigative agencies collect information to the greatest extent practicable directly from the subject when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. Accordingly, personal interviews are an integral part of the DOD personnel security program and shall be conducted in accordance with the requirements set forth in the following paragraphs of this section.

a. Background investigation/periodic reinvestigation. A personal interview shall be conducted by a trained DIS agent as part of each BI and PR.

b. Resolving adverse information. A personal interview of the subject shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DOD investigative organizations designated in this regulation to conduct PSIs), when necessary, as part of each special investigative inquiry, as well as during the course of initial or expanded investigations, to resolve or clarify any information which may impugn the subject's moral character, threaten the subject's future Federal employment, raise the question of subject's security clearability, or be otherwise stigmatizing.

c. Hostage situation. A personal interview shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DOD investigative organizations designated in this regulation to conduct PSIs) in those instances in which an individual has immediate family members or other persons bound by ties of affection or obligation who reside in a nation whose interests are inimical to the interests of the United States. (See para 2–18.)

d. Applicants/potential nominees for DOD Military or civilian positions requiring access to sensitive compartmented information or other positions requiring an special background investigation. A personal interview of the individual concerned shall be conducted, to the extent feasible, as part of the selection process for applicants/potential nominees for positions requiring access to SCI or completion of an SBI. The interview shall be conducted by a designee of the component to which the applicant or potential nominee is assigned. Clerical personnel are not authorized to conduct these interviews. Such interviews shall be conducted utilizing resources in the order of priority indicated below:

(1) Existing personnel security screening systems (for example, Air Force Assessment Screening Program, Naval Security Group Personnel Security Interview Program, U.S. Army Personnel Security Screening Program); or

(2) Commander of the nominating organization or such official as they have designated, in writing (for example, deputy commander, executive officer, security officer, security manager, S–2, counterintelligence specialist, personnel security specialist, or personnel officer); or

(3) Agents of investigative agencies in direct support of the component concerned.

e. Administrative procedures.

(1) The personal interview required by paragraph *d*, above, shall be conducted in accordance with appendix G.

(2) For those investigations requested subsequent to the personal interview requirements of paragraph *d*, above, the following procedures apply:

(a) The DD Form 1879 (Request for Personnel Security Investigation) shall be annotated under Item 20 (Remarks) with the statement "Personal Interview Conducted by (cite the duty assignment of the designated official (for example,

commander, security officer, personnel security specialist, and so forth))" in all cases in which an SBI is subsequently requested.

(b) Unfavorable information developed through the personal interview required by paragraph *d*, above, will be detailed in a written report attached to the DD Form 1879 to include full identification of the interviewer. Failure to provide such information may result in conduct of an incomplete investigation by DIS.

(c) Whenever it is determined that it is not feasible to conduct the personal interview required by paragraph *d*, above, prior to requesting the SBI, the DD Form 1879 shall be annotated under Item 20 citing the reason for not conducting the interview.

2–14. Expanded investigation

If adverse or questionable information relevant to a security determination is developed during the conduct of a PSI, regardless of type, the investigation shall be expanded, consistent with the restrictions in paragraph 2–24, to the extent necessary to substantiate or disprove the adverse or questionable information.

Section IV
Authorized Personnel Security Investigative Agencies

2–15. General

The DIS provides a single centrally directed personnel security investigative service to conduct PSIs within the 50 states, District of Columbia, and Commonwealth of Puerto Rico for DOD components, except as provided for in DODD 5100.23. DIS will request the military departments or other appropriate Federal agencies to accomplish DOD investigative requirements in other geographic areas beyond their jurisdiction. No other DOD component shall conduct PSIs unless specifically authorized by the DUSD(P). In certain instances provided for below, the DIS shall refer an investigation to other investigative agencies.

2–16. Subversive affiliations

a. General. In the context of DOD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. Specifically, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:

(1) Overthrowing the Government of the United States or the government of a State;

(2) Substantially impairing for the purpose of influencing U.S. Government policies or decisions:

(a) The functions of the Government of the United States, or

(b) The functions of the government of a State;

(3) Depriving persons of their civil rights under the Constitution or laws of the United States.

b. Military department/Federal Bureau of Investigation jurisdiction. Allegations of activities covered by criteria *a* through *f* of paragraph 2–4 of this regulation are in the exclusive investigative domain of either the counterintelligence agencies of the military departments or the Federal Bureau of Investigation (FBI), depending on the circumstances of the case and the provisions of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the FBI . Whenever allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a PSI conducted by DIS, they shall be referred immediately to either the FBI or to a military department counterintelligence agency, as appropriate.

c. Defense Investigative Service jurisdiction. Allegations of activities limited to those set forth in criterion *g* through *q* of paragraph 2–4 of this regulation shall be investigated by DIS.

2–17. Suitability information

a. General. Most derogatory information developed through PSIs of DOD military or civilian personnel is so- called suitability information, that is, information pertaining to activities or situations covered by criteria *g* through *q* of paragraph 2–4 of this regulation. Almost all unfavorable personnel security determinations made by DOD authorities are based on derogatory suitability information, although such information is often used as a basis for unfavorable administrative actions not of a security nature, such as action under the Uniform Code of Military Justice (UCMJ) or removal from Federal employment under OPM regulations.

b. Preclearance investigation. Derogatory suitability information, except that covered in paragraph *d*, below, developed during the course of a PSI, prior to the issuance of an individual's personnel security clearance, shall be investigated by DIS to the extent necessary to confirm or refute its applicability to criteria in paragraph 2–4, *g* through *q* of this regulation.

c. Postadjudication investigation. Derogatory suitability allegations, except those covered by paragraph *d*, below, arising subsequent to clearance requiring investigation to resolve and to determine the individual's eligibility for continued access to classified information, reinstatement of clearance/access, or retention in a sensitive position shall be referred to DIS to conduct a special investigative inquiry. Reinvestigation of individuals for adjudicative reconsideration due to the passage of time or evidence of favorable behavior shall also be referred to DIS for investigation. In such

cases, completion of the appropriate statement of personal history by the individual constitutes consent to be investigated. Individual consent or completion of a statement of personal history is not required when paragraph 3–56 applies. Postadjudication investigation of allegations of a suitability nature required to support other types of unfavorable personnel security determinations or disciplinary procedures independent of a personnel security determination shall be handled in accordance with applicable component administrative regulations. These latter categories of allegations lie outside the DOD personnel security program and are not a proper investigative function for departmental counterintelligence organizations, component personnel security authorities, or DIS.

d. Allegations of criminal activity. Any allegations of conduct of a nature indicating possible criminal conduct, including any arising during the course of a PSI, shall be referred to the appropriate DOD, military department, or civilian criminal investigative agency. Military department investigative agencies have primary investigative jurisdiction in cases where there is probable cause to believe that the alleged conduct will be the basis for prosecution under the UCMJ. **Such information will be referred to the installation or unit provost marshal and/or security manager or the U.S. Army Criminal Investigation Command for action.**

2–18. Hostage situations

a. General. A hostage situation exists when a member of an individual's immediate family or such other person to whom the individual is bound by obligation or affection resides in a country whose interests are inimical to the interests of the United States. The rationale underlying this category of investigation is based on the possibility that an individual in such a situation might be coerced, influenced, or pressured to act contrary to the best interests of national security.

b. DIS jurisdiction. In the absence of evidence of any coercion, influence, or pressure, hostage investigations are exclusively a personnel security matter, rather than counterintelligence, and all such investigations shall be conducted by DIS.

c. Military department and/or the Federal Bureau of Investigation jurisdiction. Should indications be developed that hostile intelligence is taking any action specifically directed against the individual concerned—or should there exist any other evidence that the individual is actually being coerced, influenced, or pressured by an element inimical to the interests of national security—then the case becomes a counterintelligence matter (outside of the investigative jurisdiction of DIS) to be referred to the appropriate military department or the FBI for investigation.

2–19. Overseas personnel security investigations

Personnel security investigations requiring investigation overseas shall be conducted under the direction and control of DIS by the appropriate military department investigative organization **(AR 381–20 applies).** Only postadjudication investigations involving an overseas subject may be referred by the requester directly to the Military Department investigative organization having investigative responsibility in the overseas area concerned (see app J) with a copy of the investigative request sent to DIS. In such cases, the military department investigative agency will complete the investigation and forward the completed report of investigation directly to DIS, with a copy to the requester.

Section V
Limitations and Restrictions

2–20. Authorized requesters and personnel security determination authorities

Personnel security investigations may be requested and personnel security clearances (including special access authorizations as indicated) granted only by those authorities designated in paragraph 5–1 and appendix F.

2–21. Limit investigations and access

The number of persons cleared for access to classified information shall be kept to a minimum, consistent with the requirements of operations. Special attention shall be given to eliminating unnecessary clearances and requests for PSIs.

2–22. Collection of investigative data

To the greatest extent practicable, personal information relevant to security determinations shall be obtained directly from the subject of a PSI. Such additional information required to make the necessary personnel security determination shall be obtained as appropriate from knowledgeable personal sources, particularly the subject's peers, and through checks of relevant records, including school, employment, credit, medical, and law enforcement records.

2–23. Privacy Act notification

Whenever personal information is solicited from an individual preparatory to the initiation of a PSI, the individual must be informed of (1) the authority (statute or Executive order that authorized solicitation); (2) the principal purpose or purposes for which the information is to be used; (3) the routine uses to be made of the information; (4) whether furnishing such information is mandatory or voluntary; (5) the effect on the individual, if any, of not providing the

information; and (6) that subsequent use of the data may be employed as part of an aperiodic, random process to screen and evaluate continued eligibility for access to classified information.

2–24. Restrictions on investigators

Investigation shall be carried out insofar as possible to collect only as much information as is relevant and necessary for a proper personnel security determination. Questions concerning personal and domestic affairs, national origin, financial matters, and the status of physical health thus should be avoided unless the question is relevant to the criteria of paragraph 2–4 of this regulation. Similarly, the probing of a person's thoughts or beliefs and questions about conduct that have no personnel security implications are unwarranted. When conducting investigations under the provisions of this regulation, investigators shall:

a. Investigate only cases or persons assigned within their official duties.

b. Interview sources only where the interview can take place in reasonably private surroundings.

c. Always present credentials and inform sources of the reasons for the investigation. Inform sources of the subject's accessibility to the information to be provided and to the identity of the sources providing the information. Restrictions on investigators relating to Privacy Act advisements to subjects of PSIs are outlined in paragraph 2–23.

d. Furnish only necessary identity data to a source and refrain from asking questions in such a manner as to indicate that the investigator is in possession of derogatory information concerning the subject of the investigation.

e. Refrain from using, under any circumstances, covert or surreptitious investigative methods, devices, or techniques, including mail covers, physical or photographic surveillance, voice analyzers, inspection of trash, paid informants, wiretaps, or eavesdropping devices.

f. Refrain from accepting any case in which the investigator knows of circumstances that might adversely affect their fairness, impartiality, or objectivity.

g. Refrain from conducting, under any circumstances, physical searches of the subject or their property.

h. Refrain from attempting to evaluate material contained in medical files. Medical files shall be evaluated for personnel security program purposes only by such personnel as are designated by DOD medical authorities. However, review and collection of medical record information may be accomplished by authorized investigative personnel.

2–25. Polygraph restrictions

The polygraph may be used as a personnel security screening measure only in those limited instances authorized by the Secretary of Defense in DODD 5210.48, **(AR 195–6)**.

Chapter 3
Personnel Security Investigative Requirements

Section I
Sensitive Positions

3–1. Designation of sensitive positions

Certain civilian positions within DOD entail duties of such a sensitive nature, including access to classified information, that the misconduct, malfeasance, or nonfeasance of an incumbent in any such position could result in an unacceptably adverse impact upon the national security. These positions are referred to in this regulation as sensitive positions. It is vital to the national security that great care be exercised in the selection of individuals to fill such positions. Similarly, it is important that only positions which truly meet one or more of the criteria set forth in paragraph 3–2 be designated as sensitive. **A sensitive position will not be downgraded or reclassified as nonsensitive solely to aid in recruiting personnel.**

3–2. Criteria for security designation of positions

Each civilian position within DOD shall be categorized, with respect to security sensitivity, as either nonsensitive, noncritical-sensitive, or critical-sensitive.

a. The criteria to be applied in designating a position as sensitive are:

(1) *Critical-sensitive.*

(a) Access to TOP SECRET information.

(b) Development or approval of plans, policies, or programs that affect the overall operations of the DOD or of a DOD component.

(c) Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(d) Investigative and certain investigative support duties, the issuance **or adjudication** of personnel security clearances or access authorizations, or the making of personnel security determinations.

(e) Fiduciary, public contact, or other duties demanding the highest degree of public trust.

(f) Duties falling under special access programs.

(g) Category I automated data processing (ADP) positions.

(h) Any other position so designated by the head of the component or designee.

(2) *Noncritical-sensitive.*

(a) Access to SECRET or CONFIDENTIAL information.

(b) Security police/provost marshal-type duties involving the enforcement of law and security duties involving the protection and safeguarding of DOD personnel and property.

(c) Category II automated data processing positions.

(d) Duties involving education and orientation of DOD personnel.

(e) Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DOD personnel and property.

(f) Any other position so designated by the head of the component or designee.

b. All other positions shall be designated as nonsensitive.

3–3. Authority to designate sensitive positions

The authority to designate sensitive positions is limited to those authorities designated in paragraph **F–7**, appendix F. These authorities shall designate each position within their jurisdiction as to its security sensitivity and maintain these designations current vis-a-vis the specific duties of each position.

3–4. Limitation of sensitive positions

It is the responsibility of those authorities authorized to designate sensitive positions to ensure that (1) only those positions that meet the criteria of paragraph 3–2, above, are designated as sensitive, and (2) the designation of sensitive positions is held to a minimum consistent with mission requirements. Designating authorities shall maintain an accounting of the number of sensitive positions by category, that is, critical or noncritical-sensitive. Such information will be included in the annual report required in chapter 11.

3–5. Billet control system for TOP SECRET

a. To standardize and control the issuance of TOP SECRET clearances within the Department of Defense, a specific designated billet must be established and maintained for all DOD military and civilian positions requiring access to TOP SECRET information. Only persons occupying these billet positions will be authorized TOP SECRET **access**. If an individual departs from a TOP SECRET billet to a billet/position involving a lower level clearance, the TOP SECRET **access** will be administratively rescinded. This TOP SECRET billet requirement is in addition to the existing billet structure maintained for SCI access.

b. Each request to DIS for a BI or SBI that involves access to TOP SECRET or SCI information will require inclusion of the appropriate billet reference, on the request for investigation.

Section II
Civilian Employment

3–6. General

The appointment of each civilian employee in any DOD component is subject to investigation, except for reappointment when the break in employment is less than 12 months. The type of investigation required is set forth in this section according to position sensitivity.

3–7. Nonsensitive positions

In accordance with the OPM Federal Personnel Manual, a NACI shall be requested not later than 3 working days after a person is appointed to a nonsensitive position. Although there is normally no investigation requirement for per diem, intermittent, temporary, or seasonal employees in nonsensitive positions provided such employment does not exceed an aggregate of 120 days in either a single continuous or series of appointments, a NAC may be requested of DIS where deemed appropriate by the employing activity.

3–8. Exceptions to investigative requirements

The following exceptions have been granted DA by the OPM:

a. **When a U.S. citizen or an alien scheduled to work in the United States and its territories or possessions is to be assigned to a nonsensitive position on a temporary basis not to exceed 6 months, a NACI is not automatically required. The commander or head of the activity will decide whether or not it is needed. In no case will this investigation be less than the preemployment inquiries prescribed by CPR 296–31, appendix B, S731–3. Commanders will ensure maximum and proper use of this exception.**

b. **A non-U.S. citizen to be assigned to a nonsensitive position outside the United States and its territories and possessions will be subject to as much of the investigation outlined below as it is feasible to conduct:**

(1) **A check of the national investigative agencies of the foreign government.**

(2) **A check of the appropriate local law enforcement agencies where the person has resided for the past 5 years.**

(3) **A check of the appropriate U.S. military intelligence files.**

c. **The requirement for the "written inquiries" portion of the NACI in connection with summer hire personnel has been waived. A NACI will be required if a summer hire employee is subsequently hired as a permanent employee.**

d. **A NACI will not be requested for a military or civilian family member hired under 5 CFR 213.3106(b)(6). Commanders will ensure that this employment will not be adverse to U.S. interests.**

3–9. Noncritical-sensitive positions

a. An NACI shall be requested and the NAC portion favorably completed before a person is appointed to a noncritical-sensitive position (for exceptions see para 3–10). An ENTNAC, NAC or DNACI conducted during military or contractor employment may also be used for appointment provided a NACI has been requested from OPM and there is no more than 12 months break in service since completion of the investigation.

b. Seasonal employees (including summer hires) normally do not require access to classified information. For those requiring access to classified information, the appropriate investigation is required. The request for the NAC should be submitted to DIS by entering "SH" (summer hire) in red letters approximately 1 inch high on the DD Form 398–2, Personnel Security Questionnaire (National Agency Check). Additionally, to ensure expedited processing by DIS, summer hire requests should be assembled and forwarded to DIS in bundles, when appropriate.

3–10. Critical-sensitive positions

A BI shall be favorably completed prior to appointment to critical-sensitive positions (for exceptions see para 3–10). Certain critical-sensitive positions require a preappointment SBI in accordance with section V of this chapter. Preappointment BIs and SBIs will be conducted by DIS. **Inasmuch as a BI or SBI is of greater scope, a NACI will not be requested from OPM if a BI or SBI for employment in a critical-sensitive position is requested from DIS or a valid BI or SBI exists.**

3–11. Exceptions

a. Noncritical-sensitive. In an emergency, a noncritical-sensitive position may be occupied pending the completion of the NACI if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made a part of the record **in the official personnel folder (OPF). The emergency finding will include a statement of why a delay pending completion of the required investigation will be harmful to the national interest.** In such instances, the position may be filled only after the NACI has been requested.

b. Critical-sensitive. In an emergency, a critical-sensitive position may be occupied pending completion of the BI (or SBI, as appropriate) if the head of the requesting organization **or an authority listed in paragraph F–7*a*, appendix F** finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made a part of the record **in the OPF. The emergency finding will include a statement of why a delay pending completion of the required investigation will be harmful to the national interest.** In such instances, the position may be filled only when the NAC portion of the BI (or SBI) or a previous valid NACI, NAC, or ENTNAC has been completed and favorably adjudicated, **and there has been no break in service in excess of 12 months.**

c. ***Harmful delays.*** **In exceptions *a* and *b* above, a delay in appointment may be considered harmful to national interests if the following apply:**

(1) **Regulatory requirements, mission-essential functions, or responsibilities cannot be met. A detailed explanation will be provided.**

(2) **No other personnel are available on a temporary basis to complete these requirements.**

d. ***Applicability.*** **This policy applies to new appointments and to current incumbents of positions when the sensitivity designation is changed.**

3–12. Mobilization of DOD civilian retirees

The requirements contained in paragraph 3–5 of this section, regarding the type of investigation required by position sensitivity for a DOD civilian retiree's temporary appointment when the break in employment is greater than 12 months, should either be expedited or waived for the purposes of mobilizing selected reemployed annuitants under the provisions of 5 USC, depending upon the degree of sensitivity of the position to which assigned. Particular priority should be afforded to newly assigned personnel assigned to the defense intelligence and security agencies with respect to granting security clearances in an expeditious manner under paragraph 3–5 of this section.

Section III
Military Appointment, Enlistment, and Induction

3–13. General
The appointment, enlistment, and induction of each member of the Armed Forces or their Reserve Components **into any of the components of the U.S. Army** shall be subject to the favorable completion of a PSI. The types of investigation required are set forth in this section.

3–14. Entrance investigation
a. An ENTNAC shall be conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. A DNACI shall be conducted on each commissioned officer, warrant officer, cadet, midshipman, and Reserve Officers Training Candidate, at the time of **or before** appointment. **A SECRET clearance is a condition of appointment. Paragraph 3–303 outlines exceptions.** A full NAC shall be conducted upon reentry of any of the above when there has been a break in service greater than 12 months.

b. If an officer or warrant officer candidate has been the subject of a favorable NAC or ENTNAC and there has not been a break in service of more than 12 months, a new NAC is not authorized **and the NAC or ENTNAC may be used as the authority for commissioning, subject to favorable completion of a DNACI.** This includes ROTC graduates who delay entry onto active duty pending completion of their studies.

c. All derogatory information revealed during the enlistment or appointment process **(including Personnel Security Screening Program processing)** that results in a moral waiver will be fully explained on a written summary attached to the DD Form 398–2 **or DD Form 398.**

3–15. Reserve Components and National Guard
Reserve Components and National Guard personnel not on active duty are subject to the investigative requirements of this chapter.

3–16. Exceptions for certain commissioned officers of Reserve Components
The requirements for entrance investigation shall be rigidly adhered to except as follows. Health professionals, chaplains, and attorneys may be commissioned in the Reserve Components prior to completion of a DNACI provided that:

a. A DNACI is initiated at the time an application for a commission is received; and

b. The applying health professional, chaplain, or attorney agrees in writing that, if the results of the investigation are unfavorable, he or she will be subject to discharge if found to be ineligible to hold a commission. Under this exception, commissions in Reserve Components other than the National Guard may be tendered to immigrant alien health professionals, chaplains, and attorneys; **however, provisions of paragraph 3–21 apply regarding eligibility for access to classified information.**

3–17. Mobilization of military retirees
The requirements contained in paragraph 3–13 of this section, regarding a full NAC upon reentry to active duty of any officer or enlisted regular/reserve military retiree or Individual Ready Reserve**(IRR)**who has been separated from service for a period of greater than 12 months **are** waived for the purposes of partial or full mobilization under provisions of 10 USC, to include the period of prescribed service refresher training. Particular priority should be afforded to military retirees mobilized and assigned to the defense intelligence and security agencies communities. **(See para 7–2 for issuance of interim clearances.)**

3–18. Mobilization exercises
MACOMs may waive the investigative requirements in paragraph 3–19 for any personnel under combat conditions or participating in HQDA-directed mobilization exercises. (See para 7–2*e* for issuance of interim clearances.)

Section IV
Security Clearance

3–19. General
a. The authorities designated in paragraph **F–1,** appendix F, are the only authorities authorized to grant, deny or revoke DOD personnel security clearances. The granting of such clearances shall be limited to only those persons who require access to classified information for mission accomplishment.

b. Military, DOD civilian, and contractor personnel who are employed by or serving in a consultant capacity to the DOD, may be considered for access to classified information only when such access is required in connection with official duties. Such individuals may be granted either a final or interim personnel security clearance provided the investigative requirements set forth below are complied with, and provided further that all available information has

been adjudicated and a finding made that such clearance would be clearly consistent with the interests of national security.

c. **Before issuing any security clearance, final or interim, the commander must verify the following:**

(1) **That the person has had no break in Federal service exceeding 12 months since the completion of the investigation.**

(2) **That the person can prove U.S. citizenship by presenting one of the documents listed in paragraph B–4*d*, appendix B (see para 3–20).**

3–20. Investigative requirements for clearance

a. TOP SECRET.

(1) Final clearance:

(a) BI/**SBI.**

(b) Established billet per paragraph 3–4 (except contractors).

(c) **Favorable review of local personnel, post military police, medical records, and other security records, as appropriate.**

(2) Interim clearance:

(a) Favorable NAC, ENTNAC, DNACI, or NACI completed **within past 5 years.**

(b) Favorable review of DD Form 398/SF–86/OF 612/DD Form 49.

(c) BI or SBI has been initiated.

(d) Favorable review of local personnel, **post or** base military police, medical, and other security records as appropriate.

(e) Established billet per paragraph 3–4 (except contractors).

(f) Provisions of paragraph 3–10 have been met regarding civilian personnel.

(g) **If evidence exists of a BI, SBI, full field investigation, Criminal Investigation Command (CID) character investigation, or comparable investigation not over 4½ years old, provisions of paragraphs (b) and (c), above, are waived and a requesting a final TOP SECRET clearance will be submitted to central clearance facility (CCF) noting that an interim clearance was granted. Such evidence will be attached to the DA Form 5247–R. CCF will check the defense central investigations index (DCII) to find whether or not a later investigation exists that would require withdrawal of a security clearance.**

(h) **Commanders may grant an interim TOP SECRET clearance for 180 days in the name of the Commander, CCF.**

b. SECRET.

(1) Final clearance:

(a) DNACI: Military (except first-term enlistees) and contractor employees.

(b) NACI: Civilian employees.

1. **The NACI is required even though the individual held a valid security clearance based on a NAC, ENTNAC, or DNACI while a member of the Armed Forces.**

2. **Exception: Summer hires, members of cooperative education programs, employees of nonappropriated fund instrumentalities, Army and Air Force Exchange Service employees, Red Cross members, USO employees, and non-Federal employees of the ARNG may be granted a final clearance on the basis of a favorable completed NAC/ENTNAC conducted by the DIS. No interim clearance is authorized for these employees.**

(c) Entrance: First-term enlistees.

(d) **Favorable review of local personnel, post military police, medical, and other security records as appropriate.**

(2) Interim clearance:

(a) When a valid need to access SECRET information is established, an interim SECRET clearance may be issued **for 180 days in the name of the CDR, CCF,** in every case, provided that a DA Form 5247–R has been submitted to CCF, and the steps outlined in paragraphs (b) through (e), below, have been complied with.

(b) Favorable review of DD Form 398–2/SF 85/OF 612/DD Form 48.

(c) NACI, DNACI, or ENTNAC initiated.

(d) Favorable review of local personnel, **post or** base military police, medical, and **other** security records as appropriate.

(e) **NAC or ENTNAC completed or, in an emergency,** provisions of paragraph 3–10 have been complied with regarding civilian personnel.

c. CONFIDENTIAL.

(1) Final clearance:

(a) NAC or ENTNAC: Military and contractor employees (except for Philippine national members of the United States Navy on whom a BI shall be favorably completed).

(b) NACI; Civilian employees (except for summer hires **and others listed in paragraph 3–19*b*(l)(b)(l)*2* who may be granted a final clearance on the basis of a NAC).**

(c) **Favorable review of local personnel, post military police, medical, and other security records as appropriate.**

(2) Interim clearance:

(a) Favorable review of DD Form 398–2/SF 86/OF 612/DD Form 48.

(b) NAC, ENTNAC, or NACI initiated.

(c) Favorable review of local personnel, **post or** base military police, medical, and **other** security records as appropriate.

(d) Provisions of paragraph 3–10 have been complied with regarding civilian personnel.

d. Validity of, previously granted clearances. Clearances granted under less stringent investigative requirements retain their validity; however, if a higher degree of clearance is required, investigative requirements of this regulation will be followed.

3–21. Naturalized U.S. citizens

This paragraph rescinded per DUSD(P) memorandum dated 12 February 1988, subject: Revocation of the Policy, in paragraph 3–20, DOD 5200.2–R.

3–22. Access to classified information by non-U.S. citizens

a. Only U.S. citizens are eligible for a security clearance. Therefore, every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, when there are compelling reasons to grant access to classified information to an immigrant alien or a foreign national in furtherance of the mission of the Department of Defense, such individuals may be granted a "limited access authorization" (LAA) under the following conditions:

(1) The LAAs will be limited to SECRET and CONFIDENTIAL level only; LAAs for TOP SECRET are prohibited.

(2) Access to classified information is not inconsistent with that determined releasable by designated disclosure authorities, in accordance with DODD 5230.11 **(AR 380–10)** to the country of which the individual is a citizen.

(3) Access to classified information must be limited to information relating to a specific program or project.

(4) Favorable completion of a BI (scoped for 10 years); where the full investigative coverage cannot be completed, a counterintelligence scope polygraph examination will be required in accordance with the provisions of DODD 5210.48 **(AR 195–6)**.

(5) Security clearances previously issued to immigrant aliens will be reissued as LAAs. **Immigrant aliens who are eligible for U.S. citizenship and have not tried to become naturalized within 12 months of eligibility will not be considered for an LAA. They will be reported to CCF for action under chapter 8, if appropriate.**

(6) The limited access authorization determination shall be made only by an authority designated in paragraph **F–2**, appendix F.

(7) The LAAs issued by the Unified and Specified Commands shall be reported to the central adjudicative facility of the appropriate Military Department in accordance with the assigned responsibilities in DODD 5100.3 for inclusion in the DCII.

(8) **The LAAs will be limited to persons who have a special skill or technical expertise essential to the national security that is not available from U.S. personnel. LAAs will not be granted to secretarial or clerical personnel or others who perform routine administrative duties.**

(9) **Commanders are reminded that an LAA is not a security clearance but an authorization for access to specific, U.S. classified information required in performance of job duties. Exposure to classified information outside the scope of an approved LAA is a compromise of such information and will be processed according to AR 380–5.**

b. In each case of granting a limited access authorization, a record shall be maintained as to:

(1) The identity (including current citizenship) of the individual to whom the limited access authorization is granted, to include, name and date and place of birth;

(2) Date and type of most recent investigation to include the identity of the investigating agency;

(3) The nature of the specific program material(s) to which access is authorized (delineated as precisely as possible);

(4) The classification level to which access is authorized;

(5) The compelling reasons for granting access to the materials cited in paragraph (3), above, and

(6) Status of the individual (that is, immigrant alien or foreign national).

c. Individuals granted LAAs under the foregoing provisions shall be the subject of a 5-year periodic reinvestigation as set forth in paragraph B–5, appendix B.

d. Foreign nationals who are LAA candidates must agree to submit to a counterintelligence-scope polygraph examination prior to being granted access in accordance with DODD 5210.48 **(AR 195–6)**.

e. If geographical and political situations prevent the full completion of the BI (and/or counterintelligence-scope polygraph), issuance of an LAA shall not be authorized; exceptions to the policy may only be authorized by the DUSD(P).

f. A report on all LAAs in effect, including the data required in paragraphs *b*(l) through (6), above, shall be furnished to the DUSD(P), **DCSINT (DAMI–CIS),** within **30** days after the end of each fiscal year (See para 11–102.)

3–23. Access by persons outside the executive branch

a. Access to classified information by persons outside the executive branch shall be accomplished in accordance with chapter VII, DOD 5200.1–R **(AR 380–5)**. The investigative requirement shall be the same as for the appropriate level of security clearance, except as indicated below.

b. Members of the U.S. Senate and House of Representatives do not require personnel security clearances, They may be granted access to DOD classified information which relates to matters under the jurisdiction of the respective committees to which they are assigned and is needed to perform their duties in connection with such assignments.

c. Congressional staff members requiring access to DOD classified information shall be processed for a security clearance in accordance with DODD 5142.1 and the provisions of this regulation. The Director, Washington Headquarters Services (WHS), will initiate the required investigation (initial or reinvestigation) to DIS, adjudicate the results and grant, deny or revoke the security clearance, as appropriate. The Assistant Secretary of Defense (Legislative Affairs) will be notified by WHS of the completed clearance action.

d. State Governors do not require personnel security clearances. They may be granted access to specifically designated classified information, on a"need-to-know" basis, based upon affirmation by the Secretary of Defense, **the Secretary of the Army (SA), or the Deputy Chief of Staff, G–2 (DCS, G–2)** that access, under the circumstances, serves the national interest. Staff personnel of a Governor's office requiring access into classified information shall be investigated and cleared in accordance with the prescribed procedures of this regulation when the head of a DOD component or single designee, **the SA, or the DCS, G–2** affirms that such clearance serves the national interest. Access shall also be limited to specifically designated classified information on a"need-to-know" basis. **Requests for access by State Governors and/or the staff of a Governor's office will be submitted to HQDA (DAMI–CIS.)**

e. Members of the U.S. Supreme Court, the Federal judiciary and the Supreme Courts of the individual States do not require personnel security clearances. They may be granted access to DOD classified information to the extent necessary to adjudicate cases being heard before these individual courts.

f. Attorneys representing DOD military, civilian or contractor personnel, requiring access to DOD **or DA** classified information to properly represent their clients, shall normally be investigated by DIS and cleared in accordance with the prescribed procedures in paragraph 3–19. This shall be done upon certification of the General Counsel of the DOD component involved in the litigation **or Office of The Judge Advocate General** that access to specified classified information, on the part of the attorney concerned, is necessary to adequately represent their client. In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of paragraph 3–19, access may be granted with the written approval of an authority designated in **paragraph F–1,** appendix F, provided that as a minimum: (a) a favorable name check of the FBI and the DCII has been completed, and (b) a DOD Non-Disclosure Agreement has been executed. **Requests for access for attorneys representing DA military, civilian, or contractor personnel will be submitted through the Office of The Judge Advocate General (DAJA–AL), Washington, DC 20310–2212 to the Office of The Deputy Chief of Staff for Intelligence (DAMI–CIS), Washington, DC 20310–1056.** In postindictment cases, after a judge has invoked the security procedures of **PL 96–456, Stat. 2025,** the Classified Information Procedures Act (CIPA), the Department of Justice may elect to conduct the necessary BI and issue the required security clearance, in coordination with the affected DOD component **or the DA.**

3–24. Restrictions on issuance of personnel security clearances

Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements. Personnel security clearances shall *not* be issued:

a. To persons in nonsensitive positions.

b. To persons whose regular duties do not require authorized access to classified information.

c. For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.

d. To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel, firemen, doctors, nurses, police, ambulance drivers, or similar personnel.

e. To persons working in shipyards whose duties do not require access to classified information.

f. To persons who can be prevented from accessing classified information by being escorted by cleared personnel.

g. To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

h. To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.

i. To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.

j. To perimeter security personnel who have no access to classified information.

k. To drivers, chauffeurs and food service personnel.

3–25. Administrative downgrading

Clearance certificates will not be administratively reduced or invalidated because a person has been assigned to duties that do not require access to the same or lower degree of classified information, the permanent duty station has been changed, or to avoid revocation in the face of credible derogatory information.

3–26. Dual citizenship

Persons claiming both U.S. and foreign citizenship shall be processed under paragraph 3–19, above, and adjudicated in accordance with the"Foreign Preference" standard in appendix I.

3–27. One-time access

Circumstances may arise where an urgent operational or contractual exigency exists for cleared DOD personnel to have one-time or short duration access to classified information at a higher level than is authorized by the existing security clearance. In many instances, the processing time required to upgrade the clearance would preclude timely access to the information. In such situations, and only for compelling reasons in furtherance of the DOD **or DA** mission, an authority referred to in paragraph *a*, below, may grant higher level access on a temporary basis subject to the terms and conditions prescribed below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level clearance. Procedures and conditions for effecting emergency one-time access to the next higher classification level are as follows:

a. Authorization for such one-time access shall be granted by a general officer, a general court martial convening authority or equivalent Senior Executive Service member, after coordination with appropriate security officials.

b. The recipient of the one-time access authorization must be a U.S. citizen, possess a current DOD security clearance, and the access required shall be limited to classified information one level higher than the current clearance.

c. Such access, once granted, shall be canceled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the granting authority.

d. The employee to be afforded the higher level access shall have been continuously employed by a DOD Component or a cleared DOD contractor for the preceding 24-month period. Higher level access is not authorized for part-time employees.

e. Pertinent local records concerning the employee concerned shall be reviewed with favorable results.

f. Whenever possible, access shall be confined to a single instance or, at most, a few occasions. The approval for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval of the granting authority is required. At such time as it is determined that the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been approved, such access shall be canceled at or before 90 days from original date of access.

g. Access at the higher level shall be limited to information under the control and custody of the authorizing official and shall be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision shall be responsible for: (1) recording the higher level information actually revealed, (2) the date(s) such access is afforded, and (3) the daily retrieval of the material accessed.

h. Access at the next higher level shall not be authorized for communications security (COMSEC), SCI, NATO, or foreign government information.

i. The exercise of this provision shall be used sparingly and repeat use within any 12-month period on behalf of the same individual is prohibited. The approving authority shall maintain a record containing the following data with respect to each such access approved:

(1) The name and social security number (SSN) of the employee afforded higher level access.

(2) The level of access authorized.

(3) Justification for the access, to include an explanation of the compelling reason to grant the higher level access and specifically how the DOD mission would be furthered.

(4) An unclassified description of the specific information to which access was authorized and the duration of access along with the date(s) access was afforded.

(5) A listing of the local records reviewed and a statement that no significant adverse information concerning the employee is known to exist.

(6) The approving authority's signature certifying are listed in paragraphs (1) through (5), above.

(7) Copies of any pertinent briefings/debriefings administered to the employee.

3–28. Access by retired flag/general officers

a. Upon determination by an active duty flag/general officer that there are compelling reasons, in furtherance of the Department of Defense **or DA** mission, to grant a retired general officer access to classified information in connection with a specific DOD **or DA** program or mission, for a period not greater than 90 days, the investigative requirements of this regulation may be waived. The access shall be limited to classified information at a level commensurate with the security clearance held at the time of retirement—not including access to SCI. **This level of access may be determined by contacting the CDR, CCF (PCCF–SC).**

b. The flag/general officer approving issuance of the clearance shall provide the **CCF** a written record to be incorporated into the DCII detailing—

(1) All data pertaining to the cleared subject;

(2) The classification of the information to which access was authorized.

c. Such access may be granted only after the compelling reason and the specific aspect of the DOD **or DA** mission which is served by granting such access has been detailed and under the condition that the classified materials involved are not removed from the confines of a Government installation or other area approved for storage of DOD **or DA** classified information.

Section V
Special Access Programs

3–29. General

It is the policy of the Department of Defense to establish, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding established requirements are authorized only when mandated by statute, national regulations, or international agreement. In this connection, there are certain Special Access programs originating at the national or international level that require PSIs and procedures of a special nature. These programs and the special investigative requirements imposed by them are described in this section. A Special Access program is any program designed to control access, distribution, and protection of particularly sensitive information established pursuant to section 4–2 of EO 12356, section 4–2 and prior EOs. DOD 5200.1–R **(AR 380–5)** governs the establishment of Departmental Special Access Programs.

3–30. Sensitive compartmented information

*a. **Investigative requirement.*** The investigative requirement for access to SCI is an SBI (see para **B**–4, app B) including a NAC on the individual's spouse or cohabitant. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family (or other persons to whom the individual is bound by affection or obligation) to the extent necessary to permit a determination by the adjudication agency that the personnel security standards of DCID 1/14 (reference (l)) are met.

(1) **The individual must not be under flagging action under AR 600–8–2.**

(2) **The individual must not be under psychiatric care or participating in any drug or alcohol rehabilitation treatment.**

(3) **The individual must have no pending action under chapter 8 of this regulation.**

(4) **The individual must not be the defendant in any pending civil litigation.**

(5) **The individual and spouse, parents, brother, sister, children, or other persons with whom the individual cohabits or is bound by affection or obligation must be U.S. citizens. Requests for waiver of this criterion must justify a compelling operational requirement and be forwarded to CCF for approval with the SBI packet attached. (See para*d,* below, for specific guidelines concerning foreign national affiliations.)**

(6) **Unresolved or unsubstantiated derogatory allegations should not normally be used to disqualify an individual without a complete investigation. Information of this type will be adjudicated by CCF after completion of the investigation. If the commander decides that the derogatory information clearly warrants denial of SCI access, the nomination and the derogatory information will be forwarded to CCF with the SBI packet attached.**

*b. **Previous investigations.*** A previous investigation conducted within the past 5 years which substantially meets the investigative requirements prescribed by this section may serve as a basis for granting access approval provided that there has been no break in the individual's military service, DOD civilian employment, or access to classified information under the Industrial Security Program greater than 12 months. **If the last SBI is more than 3 years old,** the individual shall submit one copy of an updated PSQ covering the period since the completion of the last SBI **to the servicing special security officer (SSO) for review.**

*c. **Nomination procedures.*** **An individual requiring SCI access should be nominated to CCF as soon as he or she is identified to fill an approved billet. Nominations will be submitted in accordance with AR 380–28. If appropriate, nomination will certify that a review of the PSQ revealed no unfavorable information, or forward a copy of DD Form 398.**

(1) ***"One-time" access.*** **Exceptions are nominations for "one- time" SCI access to attend a conference or**

briefing, or other situation in which temporary (no more than 90 days) SCI access appears warranted. Normal SCI investigative standards (SBI completed within the last 5 years) apply in cases involving one-time access.

(2) ***Exceptional circumstances.*** **Interim SCI access may be granted by the CDR, CCF, before completion of the fully prescribed investigation when the need for access to SCI is so urgent that the benefits would far outweigh the security risk. Requests for interim access are based on compelling need (see para*d*(l)(c), below). Requests for exceptions must clearly state the compelling need and describe how denial of access will affect the ability of the organization to accomplish its mission.**

d. Director of Central Intelligence Directive 1/14 requirements. **The DCID 1/14, paragraph 5b, requires that both the subject and members of their immediate family or cohabitant be U.S. citizens. Immediate family members, cohabitant, and persons to whom the subject is bound by affection or obligation should neither be subject to physical, mental, or other forms of duress by a foreign power, or advocate the use of force or violence to overthrow the Government of the United States by unconstitutional means.**

e. Foreign affiliation. **Individuals who are not U.S. citizens or who claim both U.S. and foreign citizenship are not eligible for SCI access. In addition, established criteria normally will not be waived if—**

(1) **Subject is a U.S. citizen but has resided in a country listed in appendix H for a significant period and/or has close foreign ties with relatives or associates residing in such a country. Whether or not such association is extensive or a risk to security depends on the nature and degree of contact and the potential for adverse influence or duress.**

(2) **Although a naturalized U.S. citizen, subject was born in a country listed in appendix H and has had extensive travel that was not a result of directed Federal service or has lived in or near the native country after obtaining U.S. citizenship.**

f. Family members with foreign affiliation. **A nominee who has parents, brothers, sisters, or children who are not U.S. citizens is not eligible for SCI unless CCF grants a waiver. The DCID 1/14 criteria may be waived in the absence of a compelling need, provided there is no evidence of anti-American feeling, and the family members were—**

(1) **Born in a country not listed in appendix H and live in the United States or in a country not listed in appendix H.**

(2) **Born in a country listed in appendix H but have not lived under a Communist regime, have no close ties with anyone living in a country listed in appendix H, and live in the United States.**

g. Spouse with foreign affiliation. **A nominee who is currently married to a foreign national is normally not eligible for SCI access. The prenomination interview required by paragraph 2–13 should reveal the affiliation and will normally preclude further processing of the SBI paperwork to DIS. This is particularly true when the nominee is identified by the losing command as requiring SCI access for a projected assignment. The losing command cannot determine the existence of a compelling need at the gaining command. When this situation arises, the losing command will immediately notify TAPA and suspend SCI processing pending notification by TAPA.**

(1) **The DCID 1/14 criteria may be waived if the commander (05 or above) certifies a compelling need exists and the following factors apply:**

(a) **Spouse was born in a country other than those listed in appendix H.**

(b) **There is no evidence of anti-American feeling demonstrated by spouse.**

(c) **A statement is submitted to CCF indicating that spouse intends to become a U.S. citizen, when eligible.**

(2) **The DCID 1/14 criteria may be waived for a non-U.S. citizen spouse from a country listed in appendix H provided the spouse has not lived for any significant period under a terrorist or Communist regime, has no close ties in such countries, and the supported command shows a compelling need for the nominee to have SCI access (see para*d*(l)(c), above). There must be no evidence that the spouse has anti-American feelings. A statement must have been submitted indicating intent to apply for U.S. citizenship as soon as eligible.**

(3) **Established criteria normally may not be waived if the following factors apply:**

(a) **Spouse was born in a country listed in appendix H and has resided under a terrorist or communist regime with interests adverse to those of the United States for a significant period and/or maintains close ties with anyone in a country listed in appendix H. The fact that the spouse has obtained U.S. citizenship does not alter the circumstances.**

(b) **Spouse is eligible for U.S. citizenship, but has not tried to apply within 12 months of eligibility.**

(4) **The circumstances described above that apply to foreign-born spouses apply equally to subjects who share living quarters or cohabitate with foreign nationals.**

(5) **Nominees for whom a foreign national spouse waiver is granted under paragraph 3–29*g* may not be transferred in status, recertified to a gaining command, or extended in their present assignment without prior authorization from CCF.**

h. Waiver of foreign connections. **Requests for waiver of foreign connections for personnel in career management field (CMF) 33 or 98 need not be accompanied by a compelling need statement. Possession of CMF 33 or 98 is considered a compelling need because of the extreme shortage of personnel in these CMFs. However, all**

other requirements of *i*, below, apply. If CCF grants a waiver, these individuals may retain their SCI access eligibility upon transfer outside the foreign spouse's country of origin, may extend their foreign duty tour within the spouse's country of origin up to 4 years, and may be reassigned to spouse's country of origin provided spouse has applied for U.S. citizenship within 12 months of becoming eligible. Individuals in CMF 33 and 98 may be recertified to the gaining command for SCI access without prior authorization from CCF provided the spouse has applied for U.S. citizenship within 12 months of becoming eligible.

i. Marriage to a foreign national. **The following measures apply to individuals indoctrinated for SCI access who plan to marry a non-U.S. citizen:**

(1) **An individual who declares an intent to marry a foreign national will immediately receive a command interview. Results of the interview stating whether or not a waiver will be requested will be forwarded to CCF and will cover the following information:**

(a) **Full name, date and place of birth, occupation, and citizenship of the prospective spouse and their family members.**

(b) **Whether or not the prospective spouse has had any connections with a hostile intelligence service or has any friends, relatives, or contacts residing in a country listed in appendix H.**

(c) **If the prospective spouse or a family member was born in what is now a country listed in appendix H, the dates, method, and circumstances of their departure from that country and the nature and extent of all ties remaining in that country will be fully determined.**

(d) **Whether or not the prospective spouse or any family member has expressed any unusual interest in the subject's assignments and/or duty position.**

(e) **Acknowledgment that the person understands the obligation to report any situation of potential subversion and espionage directed against the Army (SAEDA) and deliberate security violations interest under provisions of AR 381–12.**

(2) **If the command interview is favorable and the subject does not request a waiver or no compelling need for continuing access exists, the subject may remain indoctrinated until the marriage. At that time, the subject will be debriefed.**

(3) **If the subject wants to request a waiver and a compelling need exists, the request will be submitted through command channels to CCF. To permit continuous uninterrupted access, allow at least 6 months to process the waiver request and conduct the premarital investigation. The process involves the following actions:**

(a) **The command must certify that a compelling need exists and that a waiver is essential to the command's mission (or provide a statement that the person is in CMF 33 or 98) and furnish results of the command interview conducted under provisions of paragraph*i*(l), above.**

(b) **The person submitting the waiver request must furnish the following:**

1. **A statement that he or she understands that should the waiver be granted, he or she cannot be reassigned to the spouse's country of origin in a position requiring SCI access until the spouse has obtained U.S. citizenship, cannot be reassigned to a position requiring SCI access when a compelling need does not exist, and cannot request extension of a foreign service tour and retain SCI access unless exceptional circumstances involving operational deficiencies exist. (See para*h*, above, for exception for CMF 33 and 98.)**

2. **A current DD Form 398–2, or its dual-language equivalent, completed by the prospective spouse.**

3. **A statement by the prospective spouse indicating an intention to become a U.S. citizen when eligible.**

4. **If the person is assigned to an overseas command, the command endorsement of the waiver request will include a copy of the investigation completed on the spouse in accordance with AR 608–61 and paragraph 4, AR 600–240 (reference (ww)). These premarital investigations will essentially be at least equal to a foreign-country NAC, which includes investigative checks of national and local security and law enforcement agencies as well as other appropriate civil authorities in the place where the prospective spouse has resided since age 16 (Central Intelligence Agency (CIA) check will be requested by CCF, if required).**

5. **If the person is assigned to a continental United States (CONUS) command, CCF will use the DD Form 398–2 submitted with the waiver request to obtain appropriate CIA, Immigration and Naturalization Service (INS), and FBI checks on the prospective spouse. This will be the only investigation required unless adverse information is found during the processing and/or investigation.**

(c) **The person need not be debriefed from SCI access upon marriage to a foreign national if the requirements of this paragraph are met. If the command interview, review of the premarital investigation of the spouse, or review of DD Form 398–2 reveals information indicating a potential hostage situation, a SAEDA attempt, or possible connections with a hostile intelligence service, access will be suspended pending final determination by CCF and action under AR 381–12, if appropriate.**

(4) **If a person marries a foreign national without complying with the provisions outlined in paragraphs*i*(3)(a) and (b), above, he or she is ineligible for continued SCI access and will be debriefed. The SSO will tell CCF why the individual has been debriefed.**

(5) **When the spouse obtains U.S. citizenship, proof of citizenship must be presented to the supporting SSO. The SSO will immediately certify the following information to the CCF:**

(a) **Spouse's full identifying data.**

(b) **Date and place of entry of spouse into the United States.**

(c) **Naturalization certificate number.**

(d) **Date, court, and place of naturalization.**

(e) **Complete personal identifying data of the indoctrinated person.**

j. ***Close and continuous contact.*** **A person who establishes a close and continuous contact with a foreign national will have their SCI access suspended if there is reason to believe that the foreign national is involved with hostile intelligence, has connections in a country listed in appendix H, or is working for a foreign government in some capacity that may present a security threat. In the absence of those conditions, suspension may not be appropriate. The person should be counseled on their security responsibilities and given a SAEDA briefing. A report of the command's action will be sent to the CCF.**

k. ***Other conditions.*** **The CCF will be promptly notified if any of the following conditions become known or a matter of record:**

(1) **Adverse information reported or developed concerning the person or spouse.**

(2) **Spouse's refusal to apply, procrastination, or any other action that delays obtaining a U.S. citizenship.**

(3) **Spouse has or is suspected of having committed, on behalf of a foreign power, any act that is contrary to the best interest of the United States. The details of the situation will be immediately reported to the CCF and will include the person's degree of access to any compartment operation or project. No further action will be taken pending receipt of instructions from the CCF unless the security of SCI is endangered.**

l. ***Status of waiver.*** **CCF correspondence approving a waiver will advise whether or not the individual may be recertified to the gaining command for SCI access upon completion of current assignment without prior authorization from the CCF. The losing SSO's message to the gaining SSO will clearly state that the subject is married to a foreign national and whether or not CCF instructions allow a transfer in status.**

3–31. Retired general officer sensitive compartmented information access determinations

a. **A retired general officer (GO) may participate in activities requiring one-time SCI access under the provisions of AR 380–28 under the following conditions:**

(1) **The GO has a favorably completed SBI that meets the standards of DCID 1/14 at the time the investigation was completed.**

(2) **The GO is officially representing the U.S. Government at the request of an authorized U.S. Government agency. Such access is not authorized when the GO is representing a U.S. Government contractor, consulting firm, independent business, or the retired GO.**

(3) **No disqualifying information is available that would preclude granting SCI access.**

b. **An active duty GO whose SBI exceeds the 5-year-expiration period and who states an intention to retire within 6 months will not be required to have an SBI PR. However, such a GO will be encouraged to submit a request for an SBI PR because it would be advantageous to the Army and the GO to maintain current SCI eligibility.**

3–32. Single Integrated Operation Plan–Extra Sensitive Information

The investigative requirement for access to Single Integrated Operation Plan–Extra Sensitive Information (SIOP–ESI) is an SBI, including a NAC on the spouse and the individual's immediate family who are 18 years of age or over and who are U.S. citizens other than by birth or who are resident aliens.

3–33. Presidential support activities

a. DODD 5210.55 prescribes the policies and procedures for the nomination, screening, selection, and continued evaluation of DOD **and DA** military and civilian personnel and contractor employees assigned to or utilized in Presidential support activities. The type of investigation of individuals assigned to Presidential support activities varies according to whether the person investigated qualifies for Category One or Category Two as indicated below:

(1) *Category One.*

(a) Personnel assigned on a permanent or full-time basis to duties in direct support of the President (including the office staff of the Director, White House Military Office, and all individuals under his control):

1. Presidential aircrew and associated maintenance and security personnel.

2. Personnel assigned to the White House communications activities and the Presidential retreat.

3. White House transportation personnel.

4. Presidential mess attendants and medical personnel.

5. Other individuals filling administrative positions at the White House.

(b) Personnel assigned on a temporary or part-time basis to duties supporting the President:

1. Military social aides.

2. Selected security, transportation, flightline safety, and baggage personnel.

3. Others with similar duties.

(c) Personnel assigned to the Office of the Military Aide to the Vice President.

(2) *Category Two.*

(a) Personnel assigned to honor guards, ceremonial units, and military bands who perform at Presidential functions and facilities.

(b) Employees of contractors who provide services or contractors employees who require unescorted access to Presidential support areas, activities, or equipment, including maintenance of the Presidential retreat, communications, and aircraft.

(c) Individuals in designated units requiring a lesser degree of access to the President or Presidential support activities.

b. Personnel nominated for Category One duties must have been the subject of an SBI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are U. S. citizens other than by birth or who are resident aliens. The SBI must have been completed within the 12 months preceding selection for Presidential support duties. If such an individual marries subsequent to the completion of the SBI, the required spouse check shall be made at that time.

c. Personnel nominated for Category Two duties must have been the subject of a BI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are U.S. citizens other than by birth or who are resident aliens. The BI must have been completed within the 12 months preceding selection for Presidential support duties. It should be noted that duties (separate and distinct from their Presidential support responsibilities) of some Category Two personnel may make it necessary for them to have special access clearances which require an SBI.

d. The U.S. citizenship of foreign-born immediate family members of all Presidential support nominees must be verified by investigation.

e. A limited number of Category One personnel having especially sensitive duties have been designated by the Director, White House Military Office as"Category A." These personnel shall be investigated under special scoping in accordance with the requirements of reference (jj).

3–34. Nuclear weapon personnel reliability program

a. DODD 5210.42 **(AR 50–5)** (reference (s)) sets forth the standards of individual reliability required for personnel performing duties associated with nuclear weapons and nuclear components. The investigative requirement for personnel performing such duties is:

(1) *Critical position: Background investigation.* In the event that it becomes necessary to consider an individual for a critical position and the required BI has not been completed, interim certification may be made under carefully controlled conditions as set forth below.

(a) The individual has had a favorable DNACI or NAC (or ENTNAC) within the past 5 years without a break in **active** service or employment in excess of 1 year.

(b) The BI has been requested.

(c) All other requirements of the Personnel Reliability Program (PRP) screening process have been fulfilled.

(d) The individual is identified to supervisory personnel as being certified on an interim basis.

(e) The individual is not used in a two-man team with another such individual.

(f) Justification of the need for interim certification is documented by the certifying official.

(g) Should the BI not be completed within 150 days from the date of the request, the certifying official shall query the Component clearance authority **(by forwarding DA Form 5247–R to CDR, CCF (PCCF–M)),** who shall ascertain from DIS the status of the investigation. On the basis of such information, the certifying official shall determine whether to continue or to withdraw the interim certification.

(2) *Controlled position: Department of Defense National Agency check with written inquiries/national agency check with inquiries* .

(a) An ENTNAC completed for the purpose of first-term enlistment or induction into the Armed Forces does not satisfy this requirement.

(b) Interim certification is authorized for an individual who has not had a DNACI/NACI completed within the past 5 years, subject to the following conditions:

1. The individual has had a favorable ENTNAC/NAC, or higher investigation, that is more than 5 years old and has not had a break in service or employment in excess of 1 year.

2. A DNACI/NACI has been requested at the time of interim certification.

3. All other requirements of the PRP screening process have been fulfilled.

4. Should the DNACI/NACI not be completed within 90 days from the date of the request, the procedures set forth in paragraph *a*(l)(g), above, for ascertaining the delay of the investigation in the case of a critical position shall apply.

(3) Additional requirements apply.

(a) The investigation upon which certification is based must have been completed within the last 5 years from the

date of initial assignment to a PRP position and there must not have been a break in active service or employment in excess of 1 year between completion of the investigation and initial assignment.

(b) In those cases in which the investigation was completed more than 5 years prior to initial assignment or in which there has been a break in service or employment in excess of 1 year subsequent to completion of the investigation, a reinvestigation is required.

(c) **Periodic reinvestigation is required every 5 years for individuals assigned to critical nuclear weapon positions. PR is not required subsequent to initial assignment to PRP for controlled nuclear weapon positions so long as the individual remains in PRP.**

(d) A medical evaluation of the individual as set forth in DODD 5210.42 **(AR 50–5)** (reference (s)).

(e) Review of the individual's personnel file and other official records and information locally available concerning behavior or conduct which is relevant to PRP standards.

(f) A personal interview with the individual for the purpose of informing him of the significance of the assignment, reliability standards, the need for reliable performance, and of ascertaining his attitude with respect to the PRP.

(g) Service in the Army, Navy and Air Force Reserve does not constitute active service for PRP purposes.

b. **The Commander, CCF, will make security clearance determinations for nuclear duty positions under AR 50–5. The CCF will forward cases that contain potentially disqualifying information to the unit commander for PRP determination if the subject of the investigation is in a critical nuclear duty position. Where potentially disqualifying information exists, CCF will annotate part III of DA Form 873 (Certificate of Clearance and/or Security Determination) "Dossier review required for critical nuclear duty." If potentially disqualifying information does not exist, CCF will annotate the DA Form 873 "PRP/Surety Considered." If the certifying authority waives the potentially disqualifying information, he or she will annotate the individual's DA Form 3180 (Personnel Screening and Evaluation Record) in accordance with chapter 3, AR 50–5. In this event, the commander shall not annotate "PRP/Surety Considered" in part III of DA Form 873.**

3–35. Chemical Personnel Reliability Program

The CDR, CCF, will make security clearance determinations for chemical duty positions under AR 50–6 (reference (y)).

3–36. Automation security

The CDR, CCF, will make security clearance determinations for the Personnel Security and Screening Program. CCF will forward cases that contain potentially disqualifying information to the unit commander for Personnel Security and Screening Program determination if the subject of the investigation is in an ADP position. Where potentially disqualifying information exists, CCF will annotate part II of DA Form 873 "Dossier review required for critical nuclear duty." If potentially disqualifying information does not exist, CCF will annotate the DA Form 873"PRP/Surety Considered." (See para 3–614 and app K.) If the automation security officer waives the potentially disqualifying information, the commander will not annotate, "PRP/Surety Considered" in part III of DA Form 873.

3–37. Access to North Atlantic Treaty Organization classified information

a. Personnel assigned to NATO staff position requiring access to NATO COSMIC (TOP SECRET), SECRET or CONFIDENTIAL information shall have been the subject of a favorably adjudicated BI (10-year scope), DNACI/NACI, or NAC/ENTNAC, current within 5 years prior to the assignment, in accordance with USSAN Instruction 1–69 **(AR 380–15)** and paragraph 3–61, below.

b. Personnel *not* assigned to a NATO staff position, but requiring access to NATO COSMIC, SECRET or CONFIDENTIAL information in the normal course of their duties, must possess the equivalent final U.S. security clearance based upon the appropriate PSI (see app B) required by paragraphs 3–19 and 3–65 of this regulation.

3–38. Other special access programs

Special investigative requirements for special access programs not provided for in this paragraph may not be established without the written approval of the DUSD(P).

Section VI
Certain Positions Not Necessarily Requiring Access to Classified Information

3–39. General

DODD 5200.8 **(AR 190–16)** outlines the authority of military commanders under the Internal Security Act of 1950 to issue orders and regulations for the protection of property or places under their command. Essential to carrying out this responsibility is a commander's need to protect the command against the action of untrustworthy persons. Normally, the investigative requirements prescribed in this regulation should suffice to enable a commander to determine the trustworthiness of individuals whose duties require access to classified information or appointment to positions that are sensitive and do not involve such access. However, there are certain categories of positions or duties which, although

not requiring access to classified information, if performed by untrustworthy persons, could enable them to jeopardize the security of the command or otherwise endanger the national security. The investigative requirements for such positions or duties are detailed in this section.

3–40. Access to restricted areas, sensitive information, or equipment not involving access to classified information

a. Access to restricted areas, sensitive information or equipment **(such as critical COMSEC items)** by DOD military, civilian, or contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NAC (or ENTNAC) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NAC shall be conducted and favorably reviewed by the appropriate component agency or activity, **MACOM commander and staff agency heads authorized to request security investigations, or head of DA Staff agency** prior to permitting such access. DOD components, **MACOM commanders, and heads of DA Staff agencies** shall not request, and shall not direct or permit their contractors to request, security clearances to permit access to areas when access to classified information is not required in the normal course of duties or which should be precluded by appropriate security measures. In determining trustworthiness under this paragraph, the provisions of paragraph 2–4 and appendix I will be utilized.

b. In meeting the requirements of this paragraph, approval shall be obtained from one of the authorities designated in paragraph **F–1**, appendix F of this regulation, **or the DCSINT (DAMI–ClS)** for authority to request NACs on DOD military, civilian, or contractor employees. A justification shall accompany each request and shall detail the reasons why escorted access would not better serve the national security. Requests for investigative requirements beyond a NAC shall be forwarded to the DUSD(P) for approval.

c. The NAC requests shall (1) be forwarded to DIS in accordance with the provisions of paragraph **C–2**, appendix C, (2) contain a reference to this paragraph on the DD Form 398–2, and (3) list the authority in appendix F who approved the request.

d. Determinations to deny access under the provisions of this paragraph must not be exercised in an arbitrary, capricious, or discriminatory manner and shall be the responsibility of the military or installation commander as provided for in DODD 5200.8 **(AR 190–16)**.

3–41. Nonappropriated fund employees

a. Each nonappropriated fund employee who is employed in a position of trust as designated by an official authorized in paragraph **F–8**, appendix F, shall have been the subject of a NAC completed no longer than 12 months prior to employment or a prior PSI with no break in Federal service or employment greater than 12 months in accordance with DOD 1401.1–M **(AR 215–3)**. An individual who does not meet established suitability requirements may not be employed without prior approval of the authorizing official. Issuance of a CONFIDENTIAL or SECRET clearance will be based on a DNACI or NAC in accordance with paragraph 3–19.

b. **If a nonappropriated fund employee requires a security clearance, the commander of the host installation will request a personnel security clearance from CCF.**

3–42. Customs inspectors

DOD employees appointed as customs inspectors, under waivers approved in accordance with DOD 5030.49–R, shall have undergone a favorably adjudicated NAC completed within the past 5 years unless there has been a break in DOD employment greater than 1 year, in which case a current NAC is required.

3–43. Red Cross/united service organizations personnel

a. A favorably adjudicated NAC shall be accomplished on Red Cross or united service organizations personnel as a prerequisite for assignment with the Armed Forces overseas (DODD 5210.25 **(AR 380–49) Employees who are not U.S. citizens shall have been the subject of a BI, completed with favorable results, before being nominated for assignment with Army elements overseas.**

b. **A completed PSQ (DD Form 398 or DD Form 398–2) shall be forwarded to the Defense Industrial Security Clearance Office (DISCO), DIS, P.O. Box 2499, Columbus, OH 43216, for initiation of the BI or NAC in accordance with the provisions of DOD Directive 5220.6 (AR 380–49).**

c. **If a Red Cross or USO employee requires a personnel security clearance, the commander of the host installation will request the appropriate clearance from the CDR, CCF. The request for clearance will include a copy of the favorable employment determination by DISCO.**

3–44. Officials authorized to issue security clearances

Any person authorized to adjudicate personnel security clearances shall have been the subject of a favorably adjudicated BI.

3–45. Officials authorized to grant access to sensitive compartmented information

Any person authorized to adjudicate SCI access eligibility will have been the subject of a favorably completed SBI.

3–46. Personnel security clearance adjudication officials

Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorably adjudicated BI.

3–47. Persons requiring DOD building passes

Pursuant to DODD 5210.46, each person determined by the designated authorities of the components concerned as having an official need for access to DOD buildings in the National Capital Region shall be the subject of a favorably adjudicated NAC prior to issuance of a DOD building pass. Conduct of a BI for this purpose is prohibited unless approved in advance by ODUSD(P).

3–48. Foreign national employees overseas not requiring access to classified information

Foreign nationals employed by DOD organizations overseas, whose duties do not require access to classified information, shall be the subject of the following record checks, initiated by the appropriate military department investigative organization consistent with paragraph 2–19, prior to employment:

a. Host government law enforcement and security agency checks at the city, State (Province), and national level, whenever permissible by the laws of the host government;

b. DCII; and

c. FBI–Headquarters (HQ)/ID (where information exists regarding residence by the foreign national in the United States for 1 year or more since age 18).

3–49. Special agents and investigative support personnel

Special agents and those non-investigative personnel assigned to investigative agencies whose official duties require continuous access to complete investigative files and material require an SBI.

3–50. Persons requiring access to chemical agents

Personnel whose duties involve access to or security of chemical agents shall be screened initially for suitability and reliability and shall be evaluated on a continuing basis at the supervisory level to ensure that they continue to meet the high standards required. At a minimum, all such personnel shall have had a favorably adjudicated NAC completed within the last 5 years prior to assignment in accordance with the provisions of DODD 5210.65.**(AR 50–6)**.

3–51. Education and orientation personnel

Persons selected for duties in connection with programs involving the education and orientation of military personnel shall have been the subject of a favorably adjudicated NAC prior to such assignment. This does not include teachers/administrators associated with university extension courses conducted on military installations in the United States. Non-U.S. citizens from a country listed in appendix H shall be required to undergo a BI if they are employed in a position covered by this paragraph. **Investigations for military service or civilian employment with a DOD component satisfy the investigation requirement.**

3–52. Contract guards

Any person performing contract guard functions shall have been the subject of a favorably adjudicated NAC **by DISCO** prior to such assignment **to any security duties and in accordance with AR 190–56.**

3–53. Transportation of arms, ammunition and explosives

Any DOD military, civilian or contract employee (including commercial carrier) operating a vehicle or providing security to a vehicle transporting Category I, II, or CONFIDENTIAL arms, ammunition and explosives shall have been the subject of a favorably adjudicated NAC or ENTNAC. **Results of the completed NAC or ENTNAC shall be returned to CDR, Military Traffic Management Command (MTMC) (MT–SS), Room 403, 5611 Columbia Pike, Falls Church, VA 22041–5050, for adjudication.**

3–54. Personnel occupying information systems positions designated automated data processing–I, –II, and –III

DOD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with app K) and investigated as follows:

Table 3–1

ADP–I:	BI/SBI
ADP–II:	DNACI/NACI
ADP–III:	NAC/ENTNAC/NACI

3–55. Others

Requests for approval to conduct an investigation of other personnel not provided for in paragraphs 3–39 through 3–53, above, considered to fall within the general provisions of paragraph 3–38, above, shall be submitted, detailing the justification thereof, for approval **through the DCS, G–2 (DAMI–CIS)** to the DUSD(P). Approval of such requests shall be contingent upon an assurance that appropriate review procedures exist and that adverse determinations will be made at no lower than major command level.

Section VII
Reinvestigation

3–56. General

DOD policy prohibits unauthorized and unnecessary investigations. There are, however, certain situations and requirements that necessitate reinvestigation of an individual who has already been investigated under the provisions of this regulation. It is the policy to limit reinvestigation of individuals to the scope contained in paragraph **B–**5, appendix B, to meet overall security requirements. Reinvestigation, generally, is authorized only as follows:

a. To prove or disprove an allegation relating to the criteria set forth in paragraph 2–15 of this regulation with respect to an individual holding a security clearance or assigned to a position that requires a trustworthiness determination;

b. To meet the periodic reinvestigation requirements of this regulation with respect to those security programs enumerated below; and

c. Upon individual request, to assess the current eligibility of individuals who did not receive favorable adjudicative action after an initial investigation, if a potential clearance need exists and there are reasonable indications that the factors upon which the adverse determination was made no longer exists.

d. **Reinvestigation will not be requested if the subject is within 12 months of retirement.**

3–57. Allegations related to disqualification

Whenever questionable behavior patterns develop, derogatory information is discovered, or inconsistencies arise related to the disqualification criteria outlined in paragraph 2–15 that could have an adverse impact on an individual's security status, a SII, psychiatric, drug, or alcohol evaluation, as appropriate, may be requested to resolve all relevant issues in doubt. If it is essential that additional relevant personal data is required from the investigative subject and the subject fails to furnish the required data, the subject's existing security clearance or assignment to sensitive duties shall be terminated in accordance with paragraph 8–5 of this regulation.

3–58. Access to sensitive compartmented information

Each individual having current access to SCI shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph **B**–5, appendix B.

3–59. Critical-sensitive positions

Each DOD civilian employee occupying a critical-sensitive position shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph **B**–5, appendix B.

3–60. Critical military duties

All military personnel with a military occupational speciality (MOS) or specialty classification under PAM 611–21 that requires eligibility for SCI, regardless of access level, shall be the subject of a PR on a 5-year recurring basis as set forth in paragraph B–5, appendix B. So will military personnel with duties that fall under any of the following criteria:

a. **Access to TOP SECRET information.**

b. **Development or approval of plans, policies, or programs that affect the overall operations of the DOD or a Component.**

c. **Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.**

d. **Investigative and certain support duties, adjudication of personnel security clearances or access authorizations, or making personnel security determinations.**

e. **Fiduciary, public contact, or other duties demanding the highest degree of public trust.**

f. **Duties falling under special access programs (excluding controlled nuclear duty positions).**

g. **Category I ADP positions.**

h. **Any other position so designated by the SA or designee.**

3–61. Presidential support duties

Each individual assigned Presidential support duties shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph **B**–5, appendix B.

3–62. North Atlantic Treaty Organization staff

Each individual assigned to a NATO staff position requiring a COSMIC clearance shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph **B**–5, appendix B. Those assigned to a NATO staff position requiring a NATO SECRET clearance shall be the subject of a new NAC conducted on a 5-year recurring basis.

3–63. Extraordinarily sensitive duties

In extremely limited instances, extraordinary national security implications associated with certain SCI duties may require very special compartmentation and other special security measures. In such instances, a component of Senior Official of the Intelligence Community **or the DCS, G–2** may, with the approval of the DUSD(P), request PRs at intervals of less than 5 years as outlined in paragraph **B**–5, appendix B. Such requests shall include full justification and a recommendation as to the desired frequency. In reviewing such requests, the DUSD(P) shall give due consideration to:

a. The potential damage that might result from the individual's defection or abduction.

b. The availability and probable effectiveness of means other than reinvestigation to evaluate factors concerning the individual's suitability for continued SCI access.

3–64. Foreign nationals employed by DOD organizations overseas

Foreign nationals employed by DOD organizations overseas who have been granted a "limited access authorization" pursuant to paragraph 3–21 shall be the subject of a PR, as set forth in paragraph **B**–5, appendix B, conducted under the auspices of DIS by the appropriate military department or other U.S. Government investigative agency consistent with paragraph 2–19 and appendix J of this regulation.

3–65. Persons accessing very sensitive information classified SECRET

a. Heads of DOD Components shall submit a request to the DUSD(P) for approval to conduct periodic reinvestigations on persons holding SECRET clearances who are exposed to very sensitive SECRET information.

b. Generally, the DUSD(P) will only approve periodic reinvestigations of persons having access to SECRET information if the unauthorized disclosure of the information in question could reasonably be expected to:

(1) Jeopardize human life or safety.

(2) Result in the loss of unique or uniquely productive intelligence sources or methods vital to U.S. security.

(3) Compromise technologies, plans, or procedures vital to the strategic advantage of the United States.

c. Each individual accessing very sensitive SECRET information who has been designated by an authority listed in paragraph **F–1**, appendix F as requiring periodic reinvestigation, shall be the subject of a PR conducted on a 5-year recurring basis scoped as stated in paragraph **B–**5, appendix B.

3–66. Access to TOP SECRET information

Each individual having current access to TOP SECRET information shall be the subject of a PR conducted on a 5-year recurring basis scoped as outlined in paragraph **B–**5, appendix B.

3–67. Personnel occupying computer positions designated automated data processing–I

All DOD military, civilian, consultant, and contractor personnel occupying computer positions designated ADP–I shall be the subject of a PR conducted on a 5-year recurring basis as set forth in paragraph **B–**5, appendix B.

3–68. Critical nuclear duty positions

All DA military (including those with an MOS that requires eligibility for critical nuclear duties), civilian, and contractor personnel occupying critical nuclear duty positions in accordance with AR 50–5 shall be the subject of a PR conducted on a 5-year recurring basis as set forth in paragraph B–5, appendix B.

Section VIII
Authority to Waive Investigative Requirements

3–69. Authorized officials
Only an official designated in paragraph **F–**7, appendix F, is empowered to waive the investigative requirements for appointment to a sensitive position, assignment to sensitive duties or access to classified information pending completion of the investigation required by this chapter. Such waiver shall be based upon certification in writing by the designated official that such action is necessary to the accomplishment of a DOD mission. A minor investigative element that has not been met should not preclude favorable adjudication—nor should this require a waiver when all other information developed on an individual during the course of a prescribed investigation is favorable.

3–70. Combat operations, DA-directed mobilization
Under combat conditions, authorities listed in paragraph F–7, appendix F, may waive such provisions of this regulation as are operationally necessary and warranted by the circumstances. Under mobilization or similar conditions and mobilization exercises, prior approval to waive requirements of this regulation must be obtained from the DCS, G–2 (DAMI–CIS). This authority may be redelegated to commanders of subordinate elements to expedite security clearance actions. Such redelegation will not be made to echelons below that at which the military personnel records jacket (MPRJ) is maintained. Investigative prerequisites waived under the authority of this paragraph will be complied with as soon as the situation permits.

Chapter 4
Reciprocal Acceptance of Prior Investigations and Personnel Security Determinations

4–1. General
Previously conducted investigations and previously rendered personnel security determinations shall be accepted within DOD in accordance with the policy set forth below.

4–2. Prior investigations conducted by DOD investigative organizations
As long as there is no break in military service/civilian employment greater than 12 months, any previous personnel security investigation conducted by DOD investigative organizations that essentially is equivalent in scope to an investigation required by this regulation will be accepted without requesting additional investigation. There is no time limitation as to the acceptability of such investigations, subject to the provisions of paragraphs 2–12 and 4–3*b* of this regulation.

4–3. Prior personnel security determinations made by DOD authorities
a. Adjudicative determinations for appointment in sensitive positions, assignment to sensitive duties or access to classified information (including those pertaining to SCI) made by designated DOD authorities will be mutually and reciprocally accepted by all DOD Components without requiring additional investigation, unless there has been a break in the individual's military service/civilian employment of greater than 12 months or unless derogatory information that occurred subsequent to the last prior security determination becomes known. A check of the DCII should be conducted to accomplish this task.

b. Whenever a valid DOD security clearance or special access authorization (including one pertaining to SCI) is on record, Components shall not request DIS or other DOD investigative organizations to forward prior investigative files for review unless:

(1) Significant derogatory information or investigation completed subsequent to the date of last clearance or Special Access authorization is known to the requester; or

(2) The individual concerned is being considered for a higher level clearance (for example, SECRET or TOP SECRET) or the individual does not have a special access authorization and is being considered for one; or

(3) There has been a break in the individual's military service/civilian employment of greater than 12 months subsequent to the issuance of a prior clearance; or

(4) The most recent SCI access authorization of the individual concerned was based on a waiver.

c. Requests for prior investigative files authorized by this regulation shall be made in writing, shall cite the specific justification for the request (that is, upgrade of clearance, issue Special Access authorization, and so forth), and shall include the date, level, and issuing organization of the individual's current or most recent security clearance or special access authorization.

d. All requests for non-DOD investigative files, authorized under the criteria prescribed by paragraphs *a*, *b*(l), (2), (3), and (4) and *c*, above, shall be:

(1) Submitted on DD Form 398–2 to DIS;

(2) Annotated as a "single agency check" of whichever agency or agencies developed the investigative file or to obtain the check of a single national agency.

e. When further investigation is desired, in addition to an existing non-DOD investigative file, a DD Form 1879 will be submitted to DIS with the appropriate security forms attached. The submission of a Single Agency Check via DD Form 398–2 will be used to obtain an existing investigative file or check a single national agency.

f. Whenever a civilian or military member transfers from one DOD activity to another **(or from one Army organization to another),** the losing organization is responsible for advising the gaining organization of any pending action to suspend, deny, or revoke the individual's security clearance as well as any adverse information **(or disqualifying information, i.e., marriage to a foreign national)** that may exist in security, personnel, or other files. In such instances, the clearance shall not be reissued until the questionable information has been adjudicated.

4–4. Investigations conducted and clearances granted by other agencies of the Federal Government

a. Whenever a prior investigation or personnel security determination (including clearance for access to information classified under EO 12356 of another agency of the Federal Government meets the investigative scope and standards of this regulation, such investigation or clearance may be accepted for the investigative or clearance purposes of this regulation, provided that the employment with the Federal agency concerned has been continuous and there has been no break longer than 12 months since completion of the prior investigation, and further provided that inquiry with the agency discloses no reason why the clearance should not be accepted. If it is determined that the prior investigation does not meet the provisions of this paragraph, supplemental investigation shall be requested.

b. A NACI conducted by OPM **is of greater scope than a NAC or DNACI, and** shall be accepted and considered equivalent to a DNACI for the purposes of this regulation.

c. DOD policy on reciprocal acceptance of clearances with the Nuclear Regulatory Commission and the Department of Energy is set forth in DODD 5210.2 **(AR 380–5)**.

d. **When a DA organization must authorize access to classified information in its custody to a member of another service or agency who has not been cleared or who needs a higher degree of clearance, the parent service or agency will be asked to grant the clearance.**

e. **If it is not in the best interests of the national security to permit the person access to classified defense information in Army custody, or if the person is denied the required clearance, the commander will reassign the person to nonsensitive duties or, if appropriate, revoke the detail or assignment and advise the parent Service or agency of the reasons. The parent Service or agency is responsible for initiating security proceedings and denying or revoking a security clearance.**

f. **The CDR, CCF, is responsible for granting, revoking, or denying security clearances for Army personnel who are assigned or detailed to other Services, Defense Agencies, and the Unified and Specified Commands.**

Chapter 5
Requesting Personnel Security Investigations

5–1. General

Requests for PSIs shall be limited to those required to accomplish the Defense mission. Such requests shall be submitted only by the authorities designated in paragraph 5–2, below. These authorities shall be held responsible for determining if persons under their jurisdiction require a PSI. Proper planning must be effected to ensure that investigative requests are submitted sufficiently in advance to allow completion of the investigation before the time it is needed to grant the required clearance or otherwise make the necessary personnel security determination.

5–2. Authorized requesters

Requests for PSI shall be accepted only from the requesters designated below:

a. Military departments.

(1) *Army.*

(a) **CCF, Fort George G. Meade, MD 20755–5250.**

(b) **DCS, G–2.**

(c) All activity commanders **designated in paragraph F–7.**

(d) Chiefs of recruiting stations.

(e) **State adjutants general for the ARNG.**

(2) *Navy (including Marine Corps)*

(a) Central Adjudicative Facility.

(b) Commanders and commanding officers of organizations listed on the Standard Navy Distribution List.

(c) Chiefs of recruiting stations.

(3) *Air Force*

(a) Air Force Security Clearance Office.
(b) Assistant Chief of Staff for Intelligence.
(c) All activity commanders.
(d) Chiefs of recruiting stations.
b. Defense Agencies—Directors of Security and activity commanders.
c. Organization of the Joint Chiefs of Staff—Chief, Security Division.
d. Office of the Secretary of Defense—Director for Personnel and Security, WHS.
e. Commanders of the Unified and Specified Commands or their designees.
f. Such other requesters approved by the DUSD(P).

5–3. Criteria for requesting investigations

Authorized requesters shall use the tables set forth in appendix D to determine the type of investigation that shall be requested to meet the investigative requirement of the specific position or duty concerned.

5–4. Request procedures

To ensure efficient and effective completion of required investigations, all requests for PSIs shall be prepared and forwarded in accordance with appendix C and the investigative jurisdictional policies set forth in section IV, chapter 2 of this regulation.

5–5. Priority requests

To ensure that PSIs are conducted in an orderly and efficient manner, requests for priority for individual investigations or categories of investigations shall be kept to a minimum. DIS shall not assign priority to any PSI or categories of investigations without written approval of the DUSD(P).

5–6. Personal data provided by the subject of the investigation

a. To conduct the required investigation, it is necessary that the investigative agency be provided certain relevant data concerning the subject of the investigation. The Privacy Act of 1974 requires that, to the greatest extent practicable, personal information shall be obtained directly from the subject individual when the information may result in adverse determinations affecting an individual's rights, benefits, and privileges under Federal programs.

b. Accordingly, it is incumbent upon the subject of each PSI to provide the personal information required by this regulation. At a minimum, the individual shall complete the appropriate investigative forms, provide fingerprints of a quality acceptable to the FBI, and execute a signed release, as necessary, authorizing custodians of police, credit, education, employment, and medical and similar records, to provide relevant record information to the investigative agency. When the FBI returns a fingerprint card indicating that the quality of the fingerprints is not acceptable, an additional set of fingerprints will be obtained from the subject. In the event the FBI indicates that the additional fingerprints are also unacceptable, no further attempt to obtain more fingerprints need be made; this aspect of the investigation will then be processed on the basis of the name check of the FBI files. As an exception, a minimum of three attempts will be made (1) for all Presidential support cases, (2) for SCI access nominations if the requester so indicates, and (3) in those cases in which more than minor derogatory information exists. Each subject of a PSI conducted under the provisions of this regulation shall be furnished a Privacy Act Statement advising of (1) the authority for obtaining the personnel data, (2) the principal purpose(s) for obtaining it, (3) the routine uses, (4) whether disclosure is mandatory or voluntary, (5) the effect on the individual if it is not provided, and (6) that subsequent use of the data may be employed as part of an aperiodic review process to evaluate continued eligibility for access to classified information.

c. Failure to respond within the time limit prescribed by the requesting organization with the required security forms or refusal to provide or permit access to the relevant information required by this regulation shall result in termination of the individual's security clearance or assignment to sensitive duties utilizing the procedures of paragraph 8–6 or further administrative processing of the investigative request.

5–7. Requests for additional information or clarification

When questionable behavior, inconsistencies, or other derogatory information related to the criteria in paragraph 2–4 arise, CCF may request more information or clarification directly from the field commander or the subject (see para 3–56). Such requests include, but are not limited to the following:

a. **Results of command inquiries and investigations; copies of courts- martial proceedings; copies of administrative or disciplinary actions, written reprimands, Articles 15; results of local records file checks or of previous psychiatric or drug and alcohol evaluations; or letters of indebtedness received by the command.**

b. **DD Forms 398, fingerprint cards, and other forms or release statements required to conduct investigations; verification of citizenship of the subject and/or immediate family. Occasionally, to expedite the decisionmaking process, CCF will ask security managers to obtain specific information from the subject, such as current**

financial status, proof of payment of delinquent debts, or clarification of information listed on DD Form 398 or similar forms.

c. **Progress and final reports from Alcohol and Drug Abuse Prevention and Control Program officials on alcohol and drug rehabilitation treatment. Such reports will include history and extent of substance abuse, diagnosis, attitude toward treatment, results of treatment, and immediate and long-term prognosis. CCF will request a current alcohol or drug evaluation when incidents of alcohol or drug abuse are reported and the subject has not been referred for drug and/or alcohol treatment; more than 1 year has passed since treatment occurred, or it occurred during a previous assignment and results are not available; or there was an indication of substance abuse after completion of treatment. A physician or mental health clinician trained in the alcohol and drug rehabilitation field, who is employed by or under contract to the U.S. military or U.S. Government, will conduct the evaluation. The purpose of the evaluation is to assess the subject's ability to refrain from abuse and to obtain an opinion on the potential impact upon the subject's judgment and reliability in protecting classified information and material.**

d. **Information from medical records that indicates mental disorder or emotional instability or results of any psychiatric or mental health evaluation or treatment for a mental condition. When any information indicates a history of mental or nervous disorder or reported behavior appears to be abnormal, indicating impaired judgment, reliability, or maturity, CCF will request a mental health evaluation to determine whether or not any defect in judgment or reliability or any serious behavior disorder exists. A board- certified or board-eligible psychiatrist or licensed or certified clinical psychologist who is employed by or under contract to the U.S. military or U.S. Government will conduct mental health evaluations for security clearance purposes. The evaluation report should outline the methods used in the evaluation (for example, psychological testing and clinical interviews), include a narrative case history, assess the results of any psychological tests, and include a diagnosis under DSM III (see note) or state that no diagnosis exists. The report should include a prognosis and indicate what effect the diagnosed condition has on judgment, reliability, and stability, and describe any characteristics in a normal or stressful situation. If the individual's condition is under control through treatment or medication, the report should indicate what could happen if the individual did not comply with treatment and what likelihood exists of failure to comply. If appropriate, the report should indicate an estimated time or condition that could cause a favorable change.**

Note.

American Psychiatric Association: Diagnostic and Statistical Manual of Mental Disorders, Third Edition, Wash, DC: APA, 1980.

e. **It is imperative, in the interests of national security, that the commander and the subject of the case respond promptly to CCF's request for information. Failure to respond to requests for information required by CCF for personnel security clearance determinations within the prescribed time shall result in CCF directing suspension of the individual's access to classified information or termination of action to process request for security clearance. Continued failure to respond to CCF's request for information shall result in action to terminate the individual's security clearance utilizing the procedures of paragraph 8–6.**

5–8. Grounds for denial

If information developed by the command indicates the existence, current or past, of any mental or nervous disorder or emotional instability, a request for a PSI will not be submitted and interim clearance will not be granted. Clearance can be granted only if competent medical authority, as defined above, certifies that the disorder or instability has been overcome or will not cause a defect in the person's judgment or reliability.

5–9. Requesting National Agency Check and written inquiries from the Office of Personnel Management

A NACI will be submitted to OPM according to OPM instructions. Block H of the agency use block of Standard Form 86 will show the employing agency's security office identification (SOI) number where OPM will forward the results of the NACI. The Security Manager will coordinate with the appropriate civilian personnel office to determine eligibility for employment prior to requesting a security clearance determination from CCF.

a. **If the NACI is completely favorable, the Security Manager may attest to that fact in the "Remarks" block of DA Form 5247–R. If the NACI contains unfavorable information, a copy of the entire NACI will be submitted to the CCF with the request for security clearance.**

b. **If the NACI contains other than minor unfavorable information, an interim clearance is not authorized and DA Form 5247–R will indicate that a favorable employment determination was made.**

c. **If a clearance is not immediately required, the NACI results may be maintained by the Security Manager as long as the person is employed and may be transferred within the DOD.**

Chapter 6
Adjudication

6–1. General

a. The standard which must be met for clearance or assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

b. The principal objective of the DOD personnel security adjudicative function, consequently, is to ensure selection of persons for sensitive positions who meet this standard. The adjudication process involves the effort to assess the probability of future behavior which could have an effect adverse to the national security. Since few, if any, situations allow for positive, conclusive evidence of certain future conduct, it is an attempt to judge whether the circumstances of a particular case, taking into consideration prior experience with similar cases, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security. It is invariably a subjective determination, considering the past but necessarily anticipating the future. Rarely is proof of trustworthiness and reliability or untrustworthiness and unreliability beyond all reasonable doubt.

c. Establishing relevancy is one of the key objectives of the personnel security adjudicative process in evaluating investigative material. It involves neither the judgment of criminal guilt nor the determination of general suitability for a given position; rather, it is the assessment of a person's trustworthiness and fitness for a responsibility which could, if abused, have unacceptable consequences for the national security.

d. While equity demands optimal uniformity in evaluating individual cases, ensuring fair and consistent assessment of circumstances from one situation to the next, each case must be weighed on its own merits, taking into consideration all relevant facts, and prior experience in similar cases. All information of record, both favorable and unfavorable, must be considered and assessed in terms of accuracy, completeness, relevance, seriousness, and overall significance. In all adjudications the protection of the national security shall be the paramount determinant.

6–2. Central adjudication

a. To ensure uniform application of the requirement of this regulation and to ensure that DOD personnel security determinations are effected consistent with existing statutes and Executive orders, the head of each military department and Defense Agency shall establish a single central adjudication facility for their component. **The CCF, Fort George G. Meade, MD, has been designated as the single central adjudication facility for the DA.** The function of each facility **or the CCF** shall be limited to evaluating PSIs and making personnel security determinations. The chief of each central adjudication facility **or CDR, CCF,** shall have the authority to act on behalf of the head of the component **or the SA** with respect to personnel security determinations. All information relevant to determining whether a person meets the appropriate personnel security standard prescribed by this regulation shall be reviewed and evaluated by personnel security specialists specifically designated by the head of the component concerned, or designee, **or by the SA or the DCS, G–2.**

b. In view of the significance each adjudicative decision can have on a person's career and to ensure the maximum degree of fairness and equity in such actions, a minimum level of review shall be required for all clearance/access determinations related to the following categories of investigations:

(1) *Background investigation/special background investigation/periodic investigation/entrance national agency check/special investigative inquiry.*

(a) Favorable: Completely favorable investigations shall be reviewed and approved by an adjudicative official in the civilian grade of GS–7/9 or the military rank of O–3.

(b) Unfavorable: Investigations that are not completely favorable shall undergo at least two levels of review by adjudicative officials, the second of which must be at the civilian grade of GS–11/12 or the military rank of O–4. When an unfavorable administrative action is contemplated under paragraph 8–201, the letter of intent (LOI) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS–13/14 or the military rank of O–5. A final notification of unfavorable administrative action, subsequent to the issuance of the LOI, must be approved and signed at the civilian grade of GS–14/15 or the military rank of O–6.

(2) *National agency check with inquiries/Department of Defense National Agency check with written inquiries/ national agency check/entrance national agency check.*

(a) Favorable. A completely favorable investigation may be finally adjudicated after one level of review provided that the decisionmaking authority is at the civilian grade of GS–5/7 or the military rank of O–2.

(b) Unfavorable. Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS–7/9 or the military rank of O–3. When an unfavorable administrative action is contemplated under paragraph 8–6, the letter of intent to deny/revoke must be signed by an adjudicative official at the civilian grade of GS–11/12 or the military rank of O–4. A final notification of unfavorable administrative action subsequent to the issuance of the LOI must be signed by an adjudicative official at the civilian grade of GS–13 or the military rank of O–5 or above.

c. Exceptions to the above policy may only be granted by the Deputy Under Secretary of Defense for Policy.

6–3. Evaluation of personnel security information

a. The criteria and adjudicative policy to be used in applying the principles at paragraph 6–1, above, are set forth in paragraph 2–4 and appendix I of this regulation. The ultimate consideration in making a favorable personnel security determination is whether such determination is clearly consistent with the interests of national security and shall be an overall common sense evaluation based on all available information. Such a determination shall include consideration of the following factors:

(1) The nature and seriousness of the conduct;
(2) The circumstances surrounding the conduct;
(3) The frequency and recency of the conduct;
(4) The age of the individual;
(5) The voluntariness of participation; and
(6) The absence or presence of rehabilitation.

b. Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in appendix I. Adjudication policy for access to SCI is contained in DCID 1/14.

6–4. Adjudicative record

a. Each clearance/access determination, whether favorable or unfavorable, shall be entered **by the CDR, CCF,** into the Defense Central Security Index (DCSI), a sub-element of the DCII. (Operational details regarding implementation of the DCSI shall be implemented in a forthcoming change to this regulation.)

b. The rationale underlying each unfavorable administrative action shall be reduced to writing and is subject to the provisions of DODD 5400.7**(AR 25–55)** and DODD 5400.11 **(AR 340–21)**.

6–5. Reporting results of security or suitability determinations for civilian employees

The CCF will forward a copy of the initial BI or SBI of civilian employees, conducted by DIS, to the Security Manager of the employing command after making a security clearance determination. This will allow the employing command to determine employment eligibility and notify OPM. Employing activities will forward OFI Form 79A to report security or suitability determinations based on results of BI/SBI to: OPM–FIPC (OFI 79A), Boyers, PA 16018–0618, within 30 days after final determination.

Chapter 7
Issuing Clearance and Granting Access

7–1. General

a. The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the individual case with respect to the subject's suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of paragraph 8–6.

b. Only the authorities designated in paragraph **F–1**, appendix F, are authorized to grant, deny or revoke personnel security clearances or special access authorizations (other than SCI). Any commander or head of an organization, **to include CCF,** may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in paragraph 8–3 of this regulation are complied with.

c. All commanders and heads of DOD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this regulation.

7–2. Issuing clearance

a. Authorities designated in paragraph **F–1**, appendix F, shall record the issuance, denial or revocation of a personnel security clearance in the DSCI (see para 6–4, above). A record of the clearance issued shall also be recorded in an individual's personnel/security file or official personnel folder, as appropriate. **The CDR, CCF, will forward DA Form 873 to the command security manager for inclusion in the OPF or in the MPRJ in accordance with AR**

640–10. The DA Form 873 will not be removed except to make a copy, correct an administrative error, when a more recent clearance certificate is issued by CCF, to suspend access, or to comply with a direction of CCF.

b. A personnel security clearance remains valid until (1) the individual is separated from the Armed Forces, (2) separated from DOD civilian employment, (3) has no further official relationship with DOD **or other Federal agencies,** (4) official action has been taken to deny, revoke or suspend the clearance or access, or (5) regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of their duties. If an individual resumes the original status of (1), (2), (3), or (5) above, no single break in the individual's relationship with DOD exists greater than 12 months, and/or the need for regular access to classified information at or below the previous level recurs, the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

c. Personnel security clearances of DOD military personnel shall be granted, denied, or revoked only by the designated authority of the parent military department. Issuance, reissuance, denial, or revocation of a personnel security clearance by any DOD component concerning personnel who have been determined to be eligible for clearance by another component is expressly prohibited. Investigations conducted on Army, Navy, and Air Force personnel by DIS will be returned only to the parent service of the subject for adjudication regardless of the source of the original request. The adjudicative authority will be responsible for expeditiously transmitting the results of the clearance determination. As an exception, the employing DOD component may issue an interim clearance to personnel under their administrative jurisdiction pending a final eligibility determination by the individual's parent component. Whenever an employing DOD component issues an interim clearance to an individual from another component, written notice of the action shall be provided to the parent component.

d. When a Defense Agency, to include OJCS, initiates an SBI (or PR) for access to SCI on a military member, DIS will return the completed investigation to the appropriate Military Department adjudicative authority in accordance with paragraph *c*, above, for issuance (or reissuance) of the TOP SECRET clearance. Following the issuance of the security clearance, the military adjudicative authority will forward the investigative file to the Defense Agency identified in the "Return Results To" block of the DD Form 1879. The receiving agency will then forward the completed SBI on to DIA for the SCI adjudication in accordance with DCID 1/14.

e. The interim clearance **will be recorded on DA Form 873 and** shall be recorded in the DCSI by the parent DOD Component **in accordance with paragraph 6–103** in the same manner as a final clearance. **If a final clearance has not been received within 150 days, commanders will submit DA Form 5247–R (Request for Security Determination) to CDR, CCF (PCCF–M), as a tracer action and extend the interim period for an additional 180 days. If the DCII reveals existence of unevaluated derogatory information, CCF will advise requester that interim clearance is not authorized.**

f. **Requests for investigation for security clearances (DD Form 1879 and DD Form 398–2) forwarded to DIS do not require submission of DA Form 5247–R to CCF. DIS will forward the completed investigation to CCF, who will make a clearance determination and inform the requester. If a clearance determination is not received in 150 days, the requester may trace the action by forwarding DA Form 5247–R to CCF. Commands should forward DA Form 5247–R on newly arrived personnel in their command if the personnel file or the individual indicates that an investigation was initiated at the former command. This will allow CCF to forward the clearance determination to the current commander.**

g. **CCF will forward DA Form 873 to the command whose unit identification code (UIC) appears on the DA Form 5247–R, DD Form 1879, or DD Form 398–2, if the UIC is documented in CCF'S data base. The UIC is used by CCF to add the requester's mailing address to the DA Form 873. Action to add, delete, or correct a UIC or associated address should be forwarded to Commander, CCF (PCCF–S). Commands may also request that a higher command, "THRU" UIC, be associated with any of their subordinate command UICs. This will allow CCF to forward the DA Form 873 addressed through the higher headquarters to the subordinate commander.**

7–3. Granting access

a. Access to classified information shall be granted to persons whose official duties require such access, and who have the appropriate personnel security clearance. **CCF normally grants the highest level of clearance authorized by the personnel security investigation on record.** Access determinations (other than for special access programs) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

b. In the absence of derogatory information on the individual concerned, DOD commanders and organizational managers shall accept a personnel security clearance determination, issued by any DOD authority authorized by this regulation to issue personnel security clearances, as the basis for granting access, when access is required, without requesting additional investigation or investigative files. **For Army-affiliated personnel, this determination is documented by a DA Form 873 in the personnel file. A DA Form 873, as well as clearance certificates issued by other DOD Components, will be honored provided—**

(1) **There has been no break in Federal service exceeding 12 months since the investigation date; and**

(2) **A check of local records discloses no unfavorable information.**

c. The access level of cleared individuals will also be entered into the DCSI **by the CDR, CCF,** along with clearance eligibility status, as systems are developed and adopted which make such actions feasible.

d. **Once the CDR, CCF, has granted a person's security clearance, special access for NATO, SIOP–ESI, or other programs will be granted by the commander responsible for their control under appropriate regulations. The Commander, CCF, will make all eligibility determinations for SCI access.**

e. **DA Form 5247–R, with a copy of the clearance documentation, will be forwarded to CDR, CCF (PCCF–M), when accepting an Army clearance granted prior to CCF's assumption of clearance authority or by another DOD Component or Federal agency. In these cases, access to classified information need not be delayed pending receipt of a DA Form 873. Access may be granted and continued provided local file checks are favorable. Forwarding is not necessary if DA Form 873 is annotated, "Project Top Feed Completed."**

7–4. Administrative withdrawal

As set forth in paragraph 7–2*b*, above, the personnel security clearance and access eligibility must be withdrawn when the events described therein occur. When regular access to a prescribed level of classified information is no longer required in the normal course of an individual's duties, the previously authorized access eligibility level must be administratively downgraded or withdrawn, as appropriate. **Access based on an investigation completed over 5 years ago will be limited to no higher than SECRET unless a request for periodic reinvestigation was forwarded to DIS prior to the 5-year anniversary date of the previous investigation.**

Chapter 8
Unfavorable Administrative Actions

Section I
Requirements

8–1. General

For purposes of this regulation, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined in the terms section, and any unfavorable personnel security determination, as defined in the terms section. This chapter is intended only to provide guidance for the internal operation of the DOD and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

8–2. Referral for action

a. Whenever derogatory information relating to the criteria and policy set forth in paragraph 2–4 and appendix I of this regulation is developed or otherwise becomes available to any DOD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The CDR or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall ensure that the parent component of the individual concerned is informed promptly concerning (1) the derogatory information developed and (2) any actions taken or anticipated with respect thereto **by forwarding DA Form 5248–R (Report of Unfavorable Information for Security Determination) to the CDR, CCF (PCCF–M).** However, referral of derogatory information to the commander or security officer shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with paragraph 8–6, below, if such action is warranted and supportable by the criteria and policy contained in paragraph 2–4 and appendix I. No unfavorable administrative action as defined in the terms section may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in paragraph 8–6, below, or, in the case of SCI, Annex B, DCID 1/14.

b. The Director, DIS, shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other than through DOD command or industrial organization channels. Such access shall include utilization of the DOD Inspector General "hotline" to receive such reports for appropriate followup by DIS. DOD components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DOD components will augment the system when and where necessary. Heads of DOD components will be notified immediately to take action, if appropriate.

(1) **When the commander learns of credible derogatory information on a member of their command that falls within the scope of paragraph 2–4, the commander will immediately forward DA Form 5248–R to the CDR, CCF.**

(2) **DA Form 5248–R will be submitted in a timely manner. At a minimum, initial reports will indicate the details of the credible derogatory information and actions being taken by the commander or appropriate**

authorities (for example, conducting an inquiry or investigation) to resolve the incident. Followup reports will be submitted at 90-day intervals if the commander has not taken final action or, for example, the subject is still pending action by civil court. At the conclusion of the command action, a final report will be forwarded to CCF indicating the action taken by the commander. The final report must contain results of any local inquiry, investigation, or board action and recommendation of the command concerning restoration or revocation of the person's security clearance, if appropriate.

(3) **Commanders will not delay any contemplated personnel action while awaiting final action by CCF. The personnel action should proceed, with CCF being informed of the final action by submission of DA Form 5248–R through established channels.**

(4) **If the personnel file does not indicate the existence of a security clearance, commanders must still report information that falls within the scope of paragraph 2–4, since the person might later require a clearance. Only a final report is required on personnel who do not have a security clearance.**

(5) **The SSOs are charged with protecting SCI. If an SSO learns of any derogatory information falling within the scope of paragraph 2–4 concerning any person under the SSO's security cognizance, the SSO will immediately inform the commander. The failure of a commander to forward a DA Form 5248–R to CCF, when derogatory information has been developed on SCI indoctrinated individuals, should be brought to the attention of the individual's security manager and the senior intelligence officer.**

8–3. Suspension

The commander or head of the organization shall determine whether, on the basis of all the facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subject's security status unchanged or to take interim action to suspend subject's access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), if information exists which raises serious questions as to the individual's ability or intent to protect classified information, until a final determination is made by the appropriate authority designated in appendix F. Every effort shall be made to resolve a suspension action as expeditiously as possible.

a. **When a commander learns of significant derogatory information falling within the scope of paragraph 2–4, in addition to the reporting requirements of 8–2*a*, above, the commander must decide whether or not to suspend the individual's access to classified information. The commander may wish to suspend access on an "informal" basis while gathering information to determine whether or not formal suspension is warranted. After gathering the required data, the commander may decide to restore access. If the CDR does not suspend access, CCF will review all available information and, if warranted, advise the commander to suspend access.**

b. **If the commander decides on formal suspension of access, DA Form 873 will be removed from individual's personnel file and attached to DA Form 5248–R reporting the suspension to CCF. Once this is done, the commander may not restore access until a final favorable determination by the CDR, CCF, unless ALL the following criteria are met. These following procedures apply to both collateral and SCI access:**

(1) **If the commander determines that the person has been cleared of all charges and that the alleged offense or disqualifying information has been disproved or found groundless, and the commander is completely convinced that no element of risk remains, the commander may restore interim access in the name of the CDR, CCF. The commander will notify CCF of this action. Access will not normally be restored in cases where factors such as dismissal of charges, acquittal because of legal technicalities, plea bargaining, or absence of a speedy trial are involved. These factors cannot be construed as a clearing of all charges.**

(2) **When the commander is considering suspending or has suspended a person's access because of a suspected or actual psychological problem, the commander may elect to retain the person in status or reinstate access if the following conditions are met:**

(a) **A current medical evaluation indicates the condition was a one-time occurrence.**

(b) **The condition has no lasting effects that would affect the person's judgment.**

(c) **There is no requirement for further medical consultation relating to the condition.**

(d) **The examining physician recommends the person be returned to full duty status.**

(e) **The person exhibits no unacceptable behavior after the favorable medical evaluation.**

(f) **The commander firmly believes the person does not pose a risk to the security of classified information.**

(3) **If the commander has any doubts concerning the person's current acceptability for access, even though the above provisions have been met, the case will be referred to CCF. Only the CDR, CCF, may reinstate access in cases where the person attempted suicide.**

c. **The commander will ensure that the SSO is expeditiously notified of any information within the scope of paragraph 2–200 if the person is indoctrinated for SCI. This notification is especially critical if the commander suspends access.**

d. **A commander who suspends access to classified information will ensure that the suspension is documented**

in the Field Determined Personnel Security Status data field of the Standard Installation/Division Personnel System personnel file.

8–4. Final unfavorable administrative actions

The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in appendix F, except that the authority to terminate the employment of a civilian employee of a military DOD Agency is vested solely in the head of the DOD component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DOD components, on the basis of criteria listed in paragraphs 2–4, *a* through *f*, shall be coordinated with the DUSD(P) prior to final action by the head of the DOD component. DOD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this regulation if removal or separation can be effected under OPM regulations or administrative (nonsecurity) regulations of the military departments. However, actions contemplated in this regard shall in no way affect or limit the responsibility of the central adjudication facility to continue to process the individual for denial or revocation of a security clearance, or access to classified information on or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this regulation.

Section II
Procedures

8–5. General

No final personnel security determination shall be made on a member of the Armed Forces, an employee of the DOD, a consultant to the DOD, or any other person affiliated with the DOD without granting the individual concerned the procedural benefits set forth in 8–6, below, when such determination results in an unfavorable administrative action (see para 8–1). As an exception, Red Cross/united service organizations employees shall be afforded the procedures prescribed by DODD 5210.25 **(AR 380–49)**.

8–6. Unfavorable administrative action procedures

Except as provided for below, no unfavorable administrative action shall be taken under the authority of this regulation unless the person concerned has been given:

a. A written statement of the reasons why the unfavorable administrative action is being taken. The statement shall be as comprehensive and detailed as the protection of sources afforded confidentiality under the provisions of the Privacy Act of 1974 (5 USC 552a) and national security permit. Prior to issuing a statement of reasons to a civilian employee for suspension or removal action, the issuing authority must comply with the provisions of Federal Personnel Manual, chapter 732, subchapter 1, paragraph 1–6b. The signature authority must be as provided for in paragraphs 6–101*b*(1)(b) and 6–101*b* (2)(b).

(1) **The CDR, CCF, is the DA authority for denial and/or revocation of security clearances and/or SCI access eligibility. The CDR, CCF, may delegate this authority to those individuals outlined in paragraph 6–2*b***.

(2) **When CCF receives credible derogatory information and denial or revocation of a security clearance and/or SCI access eligibility is considered appropriate, CCF will forward a letter of intent through the command security manager to the individual. This LOI will outline the derogatory information and explain the proposed action. It will offer the person a chance to reply in writing with an explanation, rebuttal, or mitigation for the incidents.**

(3) **The LOI will direct suspension of access to classified information. If the LOI addresses SCI access only, access to collateral information may continue.**

(4) **If the person needs access to classified information in order to prepare a response to the LOI, CCF may authorize limited access for that specific purpose.**

(5) **When a commander receives an LOI concerning a person who is no longer assigned to the command, one of the following actions will be taken:**

(a) **If the person is transferred, endorse the LOI to the gaining command and forward an information copy of the endorsement to CCF (PCCF–M).**

(b) **If the person has been released from active duty and has a Reserve obligation, forward the LOI to the U.S. Army Reserve Personnel Center (DARP–SPI), St. Louis, MO 63132–5200. Forward an information copy of the endorsement to CCF (PCCF–M).**

(c) **If the person has been discharged from military service with no Reserve obligation, endorse the LOI to CCF (PCCF–M), attaching a copy of the discharge orders.**

(6) **The CDR, CCF, may waive the due process requirements of this chapter when a person is incarcerated by military or civilian authorities on conviction of a criminal offense, or when a person is dropped from the rolls as a deserter. In such instances, the commander will take the following actions immediately:**

(a) **Withdraw the DA Form 873 from the person's MPRJ or OPF and stamp or print across the face,**

"Revoked by authority of CDR, CCF—deserted (date)" or "Revoked by authority of Commander, CCF—incarcerated as a result of civil conviction or court-martial (date)," as appropriate for military and civilian personnel. Forward the DA Form 873 and DA Form 5248 explaining the circumstances to the CDR, CCF (PCCF–M).

(b) **If the MPRJ or OPF does not contain a DA Form 873, forward DA Form 5248–R, explaining the circumstances, to the Commander, CCF (PCCF–M).**

b. An opportunity to reply in writing to such authority as the head of the component concerned may designate.

(1) **The commander will ensure that the person acknowledges receipt of the LOI by signing and dating the form letter enclosed with the LOI. The person will indicate their intention of submitting a rebuttal. The form letter will be forwarded immediately to CCF.**

(2) **The commander will ensure that the person is counseled as to the seriousness of CCF's contemplated action and will offer advice and assistance needed in forming a reply. The person can obtain legal counsel or other assistance at his or her own expense and may request a copy of the investigative files under the provisions of the Privacy Act. Privacy requests must be forwarded to the Chief, Freedom of Information/Privacy Office, U.S. Army Intelligence and Security Command (IACSF–FI), Fort George G. Meade, MD 20755–5995. If other than Army investigative records repository files exist, the Freedom of Information (FOI)/Privacy Office will refer the request to the appropriate repository. The individual must provide full name (including aliases), SSN, and date and place of birth. The person's signature must be notarized by a commissioned officer. If the person requires an extension of the 60-day suspension, the command security manager should forward a request, with justification, to the CDR, CCF (PCCF–M). An expected completion date will be provided.**

(3) **The person's response must address each issue raised in CCF's LOI. Any written documentation may be forwarded. Letters of recommendation from supervisory personnel may be attached to the response.**

(4) **The person will forward the response to CCF through the representative of the CDR who provided the LOI. The LOI must be endorsed by at least one CDR. The CDR should recommend whether the person's clearance should be denied, revoked, or restored. The CDR should provide a rationale, addressing the issues outlined in the LOI. Responses to LOIs that do not include the CDR's recommendation will be returned with a request for comments.**

c. A written response to any submission under paragraph *b*, stating the final reasons therefore, which shall be as specific as privacy and national security considerations permit. The signature authority must be as provided for in paragraphs 6–2*b*(1)(b) and 6–2*b*(2)(b). Such response shall be as prompt as individual circumstances permit, not to exceed 60 days from the date of receipt of the appeal submitted under paragraph *b*, above, provided no additional investigative action is necessary. If a final response cannot be completed within the timeframe allowed, the subject must be notified in writing of this fact, the reasons therefore, and the date a final response is expected, which shall not, in any case, exceed a total of 90 days from the date of receipt of the appeal under paragraph *b*.

(1) **The CCF's decision is considered final. This decision will be forwarded through the command security office to the individual.**

(2) **In accordance with AR 600–37, CCF must provide unfavorable information developed during the PSI to both the DA Suitability Evaluation Board (DASEB) and the appropriate TAPA, Army Reserve Personnel Center, or Guard Personnel Center personnel management office on all senior enlisted (E–6 and above), commissioned, or warrant officer personnel. Specifically included is any information that results in denial or revocation of a security clearance. A copy of CCF's LOI, the person's response, and CCF's final letter will be forwarded. The regulation does not exclude providing other significant unfavorable information that does not in itself result in an adverse decision. The DASEB determines which information is retained in a person's official military personnel file (OMPF). The fact that the information is being forwarded to the DASEB or personnel management office will be documented in CCF's final letter of determination.**

d. **No final unfavorable personnel security clearance or access determination shall be made on an individual without granting them an opportunity to appeal to a higher level of authority as set forth in DOD 5200.02-R when such determination results in unfavorable administrative action.** CCF's final letter of determination will state that if the person intends to appeal in writing directly to the Army's Personnel Security Appeals Board (PSAB) or request a personal appearance to the Defense Office of Hearings and Appeals (DOHA). The DOHA will review the facts of the case and make a recommendation to the PSAB. If, upon review of the in person or written appeal, a determination by PSAB is considered the final security clearance eligibility determination, no further appeal is authorized. All requests for appeal must be returned within 60 days from receipt of the letter.

8–7. Requests for reconsideration

a. **If during the 60 days following receipt of CCF's final letter of determination the subject has additional information in rebuttal or mitigation, he or she should submit it to the CDR, CCF, rather than submitting an appeal to HQDA (DAMI–CIS). DAMI–CIS will forward such information to the CCF Commander. If the CCF review again results in denial or revocation, the person may then appeal to HQDA.**

b. **If after a final determination by the CDR, CCF, or by HQDA (DAMI–CIS), the person files an appeal,**

CCF will accept no requests for reconsideration based solely on the passage of time as a mitigating factor for at least 1 year from the date of the final letter of determination or the DA appeal decision, whichever was later.

c. **Any request for reconsideration submitted to the CDR, CCF, in accordance with the provisions of paragraphs *a* and *b*, above, must outline the reasons for loss of clearance and provide a rationale for favorable action by CCF. The request for reconsideration must be endorsed by the person's CDR. The CDR should be familiar with the information available to CCF and with CCF's rationale for denial or revocation. The CDR should state why the clearance and/or SCI access should be restored. If the person is not able to provide the CDR with a copy of CCF's original action, the commander should request a copy of the Army Investigative Records Repository dossier through their authorized file requester, normally the installation directorate of security (DSEC)/security manager at separate brigade, division, corps, and major command levels.**

8–8. Involuntary separation of military members and DA civilian personnel

As soon as involuntary separation is considered for military members or DA civilian personnel who have had access to SCI, Special Access programs, or other sensitive programs, the local CDR will send the information listed below to HQDA (DAMI–CIS), Washington, DC 20310–1051. Elimination action will not be completed until DAMI–CIS acknowledges receipt of this information.

a. **Individual's name, grade, and SSN.**

b. **Date and place of birth.**

c. **Marital status.**

d. **Length of service.**

e. **Reason(s) for proposed involuntary discharge or dismissal.**

f. **Type of discharge or dismissal contemplated.**

g. **Level of access to classified information. Classified details should not be submitted.**

8–9. Exceptions to policy

a. Notwithstanding paragraph 8–6, above, or any other provision of this regulation, nothing in this regulation shall be deemed to limit or affect the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national security so requires, pursuant to 5 USC 7532. Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph 8–6, above, are not appropriate. Such determination shall be conclusive.

b. **Notification of adverse action need not be given to—**

(1) **Military personnel who have been dropped from the rolls of their organization for absence without authority.**

(2) **Persons who have been convicted of a criminal offense by a civilian court or court-martial and are incarcerated.**

Section III
Reinstatement of Civilian Employees

8–10. General

Any person whose civilian employment in the DOD is terminated under the provisions of this regulation shall not be reinstated or restored to duty or reemployed in the DOD unless the Secretary of Defense, or the head of a DOD component, finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of national security. Such a finding shall be made a part of the personnel security record.

8–11. Reinstatement benefits

A DOD civilian employee whose employment has been suspended or terminated under the provisions of this regulation and who is reinstated or restored to duty under the provisions of 5 USC 3571 is entitled to benefits as provided for by PL 89–380.

Chapter 9
Continuing Security Responsibilities

Section I
Evaluating Continued Security Eligibility

9–1. General
A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood of the individual preserving the national security. Obviously it is not possible at a given point to establish with certainty that any human being will remain trustworthy. Accordingly, the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, there is the clear need to ensure that, after the personnel security determination is reached, the individual's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the individual's supervisor and, to a large degree, the individual himself. Therefore, the heads of DOD components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should ensure close coordination between security authorities and personnel, medical, legal, and supervisory personnel to ensure that all pertinent information available within a command is considered in the personnel security process.

9–2. Management responsibility
a. Commanders and heads of organizations shall ensure that personnel assigned to sensitive duties (or other duties requiring a trustworthiness determination under the provisions of this regulation) are initially indoctrinated and periodically instructed thereafter on the national security implication of their duties and on their individual responsibilities.

b. The heads of all DOD components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect to such areas as financial, medical or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long-term, job-related security problems.

9–3. Supervisory responsibility
Security programs shall be established to ensure that supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern. Specific instructions should be disseminated **by security managers** concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect the interests of national security as well as to provide any necessary help to the individual concerned to correct any personal problem which may have a bearing upon the individual's continued eligibility for access.

a. In conjunction with **the submission of BIs and SBIs stated in chapter 2, section II, and appendix B, paragraphs B–3 and B–4; and with** the submission of PRs stated in section VII, chapter 3, and paragraph **B–**5, appendix B; supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's **initial or** continued eligibility for access to classified information is omitted.

b. If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's **initial or** continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package. "I am aware of no information of the type contained in DOD 5200. 2–R, appendix E **(AR 380–67)** relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information."

c. If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated, and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package: "I am aware of information of the type contained in DOD 5200.2–R, appendix E **(AR 380–67)**, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on their ability to safeguard classified information and have reported all relevant details to the appropriate security official(s)."

d. In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with paragraphs 9–3 *b* and *c*, above, as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their component guidance.

e. **If the statement in paragraph 9–3*c*, above applies, the supervisor must ensure that all relevant information is reported to the local command security official responsible for processing the investigative paperwork.**

f. **If the information seems to warrant adverse action, the command security official will immediately refer it to the CDR, CCF (PCCF–M), using DA Form 5248–R. The CCF will process the cases in accordance with established procedures.**

g. **If the local command security official determines that the information is minor and does not warrant an adverse action, the PSI request should be forwarded to DIS. A summary of the derogatory information will be part of the investigative request packet. DIS will initiate the investigation and expand as appropriate. DIS will forward results of the investigation to CCF for adjudication.**

h. **It is important that immediate supervisors take an objective approach to the requirements in paragraphs*b* and *c*, above, to ensure equity to both the subject of the investigation and national security.**

9–4. Individual responsibility

a. Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.

b. Moreover, individuals having access to classified information must report promptly to their security office:

(1) Any form of contact, intentional or otherwise, with a citizen of a designated country, (see app H) unless occurring as a function of one's official duties.

(2) Attempts by representatives or citizens of designated countries to cultivate friendships or to place one under obligation.

(3) Attempts by representatives or citizens of foreign countries to:

(a) Cultivate a friendship to the extent of placing one under obligation that they would not normally be able to reciprocate, or by offering money payments or bribery to obtain information of actual or potential intelligence value.

(b) Obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact.

(c) Coerce by blackmail, by threats against or promises of assistance to relatives living under foreign control, especially those living in a designated country.

(4) All personal foreign travel in advance.

(5) Any information of the type referred to in paragraph 2–4 or appendix I.

9–5. Coworker responsibility

Coworkers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

Section II
Security Education

9–6. General

The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DOD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DOD personnel security program. Accordingly, heads of DOD components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information, or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

9–7. Initial briefing

a. All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this regulation shall be given an initial security briefing. **A record of this briefing will be maintained in the security office.** The briefing shall be in accordance with the requirements of paragraph 10–3, DOD 5200.1–R **(AR 380–5)** and consist of the following elements:

(1) The specific security requirements of their particular job.

(2) The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts **(AR 381–12).**

(3) The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.

(4) The penalties that may be imposed for security violations.

b. If an individual declines to execute SF Form 189, "Classified Information Nondisclosure Agreement," the DOD

component shall initiate action to deny or revoke the security clearance of such person in accordance with paragraph 8–6, above.

9–8. Refresher briefing

Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in paragraph 10–2, DOD 5200.1–R **(AR 380–5)** shall be tailored to fit the needs of experienced personnel.

9–9. Foreign travel briefing

a. DOD components will establish appropriate internal procedures requiring all personnel possessing a DOD security clearance to report to their security office all personal foreign travel in advance of the travel being performed. When travel patterns, or the failure to report such travel, indicate the need for investigation, the matter will be referred to the appropriate counterintelligence investigative agency.

b. Personnel having access to classified information shall be given a foreign travel briefing by a counterintelligence agent, security specialist, security manager, or other qualified individual, as a defensive measure prior to travel to a designated country (see app H) in order to alert them to their possible exploitation by hostile intelligence services. These personnel will also be debriefed upon their return. The briefings will be administered under the following conditions:

(1) Travel to or through designated country for any purpose.

(2) Attendance at international, scientific, technical, engineering, or other professional meetings in the United States or in any country outside the United States when it can be anticipated that representative(s) of designated countries will participate or be in attendance.

c. Individuals who travel frequently, or attend or host meetings of foreign visitors as described in paragraph *b*2, above, need not be briefed for each occasion, but shall be provided a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

d. Records on such employees **of all personal foreign travel** will be maintained for 5 years **and may be in manual or automated form. Foreign travel records will be forwarded to the gaining command upon transfer of the individual. The losing command will retain a copy of the foreign travel record on file for 1 year after the individual's departure. Record of individuals who retire, separate, or terminate employment will be retained at the losing command until the expiration of the 5-year period. Data to be recorded are listed below:**

(1) **Name.**

(2) **SSN.**

(3) **Organization.**

(4) **Date security office was notified of proposed travel.**

(5) **Country or countries to be visited and inclusive dates.**

(6) **Date of foreign travel briefing (if travel meets criteria in para *b*, above) and name of person conducting briefing.**

(7) **Date of foreign travel debriefing (in accordance with para *b*, above) and name of person conducting debriefing.**

(8) **Purpose of visit.**

9–10. Termination briefing

a. Upon termination of employment, administrative withdrawal of security clearance, **revocation of security clearance,** or contemplated absence from duty or employment for 60 days or more, DOD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. **DA Form 2962 (Security Termination Statement and Debriefing Certificate) will be used for this purpose. Paragraph 10–5, AR 380–5 applies.** This statement shall include the following;

(1) An acknowledgement that the individual has read the appropriate provisions of the Espionage Act and other criminal statutes and DOD regulations applicable to the safeguarding of classified information to which the individual has had access, and understands the implications thereof;

(2) A declaration that the individual no longer has any documents or material containing classified information in their possession;

(3) An acknowledgement that the individual will not communicate or transit classified information to any unauthorized person or agency; and

(4) An acknowledgement that the individual will report without delay to the FBI or the DOD component concerned any attempt by any unauthorized person to solicit classified information.

b. When an individual refuses to execute a security termination statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal to sign a security termination statement shall be reported to the Director, DIS, who shall ensure that it is recorded in the DCII.

c. The security termination statement shall be retained by the DOD component that authorized the individual access to classified information for the period specified in the component's records retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

d. In addition to the provisions of paragraphs *a*, *b*, and *c*, above, DOD components shall establish a central authority to be responsible for ensuring that security termination statements are executed by senior personnel (general officers, flag officers, and senior executive service (SES)s). Failure on the part of such personnel to execute a security termination statement shall be reported immediately to the DUSD(P). **Senior civilian employees, SESs and above, will execute the DA Form 2962 at the employing activity at time of separation. The General Officer Management Office, ODCS, G–1, is the control office authorized to execute a DA Form 2962 for each separating general officer.**

Chapter 10
Safeguarding Personnel Security Investigative Records

10–1. General

In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is DOD policy that such personal information shall be handled with the highest degree of discretion. Access to such information shall be afforded only for the purpose cited herein and to persons whose official duties require such information. Personnel security investigative reports may be used only for the purposes of determining eligibility of DOD military and civilian personnel, contractor employees, and other persons affiliated with the DOD, for access to classified information, assignment or retention in sensitive duties or other specifically designated duties requiring such investigation, or for law enforcement and counterintelligence investigations. Other uses are subject to the specific written authorization of the DUSD(P).

10–2. Responsibilities

DOD authorities responsible for administering the DOD personnel security program and all DOD personnel authorized access to personnel security reports and records shall ensure that the use of such information is limited to that authorized by this regulation and that such reports and records are safeguarded as prescribed herein. The heads of DOD components and the DUSD(P) for the Office of the Secretary of Defense shall establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records as required by paragraphs 10–3 and 10–4, below.

10–3. Access restrictions

Access to personnel security investigative reports and personnel security clearance determination information shall be authorized only in accordance with DODD 5400.7 **(AR 25–55)** and DODD 5400.11 **(AR 340–21)** and with the following:

a. DOD personnel security investigative reports shall be released outside of the DOD only with the specific approval of the investigative agency having authority over the control and disposition of the reports.

b. Within DOD, access to personnel security investigative reports shall be limited to those designated DOD officials who require access in connection with specifically assigned personnel security duties, or other activities specifically identified under the provisions of paragraph 10–1. **Under no circumstances will foreign national employees of the DA be permitted access to investigative files concerning U.S. military, U.S. civilian, or foreign national employees, unless such employees shall themselves have been the subject of a favorable counterintelligence scoped BI.**

c. Access by subjects of personnel security investigative reports shall be afforded in accordance with DODD 5400. 11 **(AR 340–21)**.

d. Access to personnel security clearance determination information shall be made available, other than provided for in paragraph *c*, above, through security channels, only to DOD or other officials of the Federal Government who have an official need for such information.

10–4. Safeguarding procedures

Personnel security investigative reports and personnel security determination information **(to include NACI)** shall be safeguarded as follows:

a. Authorized requesters shall control and maintain accountability of all reports of investigation received.

b. Reproduction, in whole or in part, of personnel security investigative reports by requesters shall be restricted to the minimum number of copies required for the performance of assigned duties.

c. Personnel security investigative reports shall be stored in a vault, safe, or steel file cabinet having at least a lock bar and an approved three-position dial-type combination padlock or in a similarly protected area/container.

d. Reports of DOD PSIs shall be sealed in double envelopes or covers when transmitted by mail or when carried by persons not authorized access to such information. The inner cover shall bear a notation substantially as follows: "TO

BE OPENED ONLY BY OFFICIALS DESIGNATED TO RECEIVE REPORTS OF PERSONNEL SECURITY INVESTIGATION."

e. An individual's status with respect to a personnel security clearance or a special access authorization is to be protected as provided for in paragraph VI.C.6., DODD 5400.7 **(AR 25–55)**.

10–5. Records disposition

a. Personnel security investigative reports, to include OPM NACIs may be retained by DOD recipient organizations, **if the head of the component deems it necessary to fulfill the requirements of paragraph 9–1 of this regulation**, only for the period necessary to complete the purpose for which they were originally requested. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization. All copies of such reports shall be destroyed within 90 days after completion of the required personnel security determination. Destruction shall be accomplished in the same manner as for classified information in accordance with paragraph 9–2, DOD 5200.1–R **(AR 380–5)**.

b. DOD record repositories authorized to file personnel security investigative reports shall destroy PSI reports of a favorable or of a minor derogatory nature 15 years after the date of the last action. That is, after the completion date of the investigation or the date on which the record was last released to an authorized user—whichever is later. Personnel security investigative reports resulting in an unfavorable administrative personnel action or court-martial or other investigations of a significant nature due to information contained in the investigation shall be destroyed 25 years after the date of the last action. Files in this latter category that are determined to be of possible historical value and those of widespread public or congressional interest may be offered to the National Archives after 15 years. **AR 381–45 applies.**

c. Personnel security investigative reports on persons who are considered for affiliation with DOD will be destroyed after 1 year if the affiliation is not completed.

10–6. Foreign source information

Information that is classified by a foreign government is exempt from public disclosure under the Freedom of Information and Privacy Acts. Further, information provided by foreign governments requesting an express promise of confidentiality shall be released only in a manner that will not identify or allow unauthorized persons to identify the foreign agency concerned.

Chapter 11
Program Management

11–1. General

To ensure uniform implementation of the DOD personnel security program throughout the department, program responsibility shall be centralized at the DOD component level.

11–2. Responsibilities

a. The DUSD(P) shall have primary responsibility for providing guidance, oversight, development and approval for policy and procedures governing personnel security program matters within the department:

(1) Provide program management through issuance of policy and operating guidance.

(2) Provide staff assistance to the DOD components and Defense Agencies in resolving day-to-day security policy and operating problems.

(3) Conduct inspections of the DOD Components for implementation and compliance with DOD security policy and operating procedures.

(4) Provide policy, oversight, and guidance to the component adjudication functions.

(5) Approve, coordinate and oversee all DOD personnel security research initiatives and activities.

b. The General Counsel shall ensure that the program is administered in a manner consistent with the laws; all proceedings are promptly initiated and expeditiously completed; and that the rights of individuals involved are protected, consistent with the interests of national security. The General Counsel shall also ensure that all relevant decisions of the courts and legislative initiatives of the Congress are obtained on a continuing basis and that analysis of the foregoing is accomplished and disseminated to DOD personnel security program management authorities.

c. The heads of the components shall ensure that—

(1) The DOD personnel security program is administered within their area of responsibility in a manner consistent with this regulation.

(2) A single authority within the office of the head of the DOD component is assigned responsibility for administering the program within the component.

(3) Information and recommendations are provided the DUSD(P) and the General Counsel at their request concerning any aspect of the program.

d. **The Deputy Assistant Secretary of the Army for Civilian Personnel, Nonappropriated Funds, and Security Policy will ensure the implementation of DODD 5200.2 and DOD 5200.2–R. The DASA (SAMR–PSP) will conduct oversight to include approving and disapproving of security-related policy and will provide guidance, as needed, on Army personnel security policy in its broadest dimensions.**

e. **The DCS, G–2 is responsible for formulating policy governing —**

(1) **Army personnel security.**

(2) **Submitting PSI requests.**

(3) **Adjudicating personnel security.**

(4) **Continually assessing the suitability of individuals for access to classified information.**

f. **The DCS , G–1 is responsible for—**

(1) **Accessing personnel for the total force.**

(2) **Determining personnel classification and standards.**

(3) **Adjudicating centralized personnel security.**

(4) **Formulating personnel management policy and procedures in compliance with existing security standards and criteria.**

(5) **Developing automation architecture for integrating the Total Army Information Systems.**

(6) **Using designation criteria to determine the number of civilian positions designated as sensitive. Records of sensitive and nonsensitive positions will be maintained by the servicing civilian personnel office. Those individuals authorized to designate sensitive positions will inform the servicing civilian personnel office of any change in position sensitivity.**

g. **The CDR, CCF, is responsible for the centralized adjudication, granting, revocation, and denial of personnel security clearances and SCI access eligibility determinations. The CDR, CCF, is authorized to suspend or direct the suspension of access to classified information.**

h. **The CDRs, Army Staff heads, and supervisors are responsible for implementing the personnel security provisions of this regulation. Personnel security functions are normally delegated to the installation DSEC/ security manager/G2, who will—**

(1) **Initiate requests for PSIs.**

(2) **Suspend an individual's access to classified information.**

(3) **Request security clearances.**

(4) **Grant interim security clearances.**

(5) **Report any adverse information.**

(6) **Assist personnel in completing applicable investigative forms.**

(7) **Conduct oversight visits of subordinate units at least once every 2 years.**

11–3. Reporting requirements

a. Personnel security program management data will be developed and submitted by **1 November** each year for the preceding fiscal year in a report to the DUSD(P) **DCS, G–2 (DAMI–CIS), Washington, DC 20310–1051.** The information required below is essential for basic personnel security program management and in responding to requests from the Secretary of Defense and Congress. The report will cover the preceding fiscal year, broken out by clearance category, according to officer, enlisted, civilian or contractor status.

b. **The CDR, CCF, will report the following:**

(1) Number of TOP SECRET, SECRET, and CONFIDENTIAL clearances issued;

(2) Number of TOP SECRET, SECRET, and CONFIDENTIAL clearances denied;

(3) Number of TOP SECRET, SECRET, and CONFIDENTIAL clearances revoked;

(4) Number of SCI access determinations issued;

(5) Number of SCI access determinations denied;

(6) Number of SCI access determinations revoked;

(7) Number of actions which resulted in nonappointment or nonselection to a sensitive position;

(8) Number of personnel adjudicating personnel security cases on a full- or part- time basis;

(9) Number of man-years expended in adjudicating personnel security cases.

c. **MACOM commanders and heads of Army Staff agencies will consolidate reports submitted by their subordinate units and field operating agencies pertaining to the following data:**

(1) Total number of personnel holding a clearance for TOP SECRET, SECRET, CONFIDENTIAL, and sensitive compartmented information as of the end of the fiscal year.

(2) Total number of personnel authorized access to TOP SECRET, SECRET, CONFIDENTIAL, and sensitive compartmented information as of the end of the fiscal year.

(3) Number of TOP SECRET billets established (see para 3–4).

(4) Number of civilian positions designated sensitive, by designation criteria.

(5) The number of limited access authorizations in effect (in accordance with para 3–21).

d. This reporting requirement has been assigned report control symbol DD–POL(A)1749.

11–4. Inspections

The heads of DOD components shall ensure that personnel security program matters are included in their administrative inspection programs.

11–5. Performance measures

a. Commander's and/or organization head.

(1) Provide the document that establishes or identifies command's security organization and demonstrates the security manager as having direct and ready access to the commanding officer.

(2) Provide evidence of formal security management training.

(3) Provide the documentation that identifies the security manager by name to all command personnel.

(4) Provide examples of security management functions that demonstrate overall management of the program.

(5) How many persons are assigned duties and responsibilities to support the command's security program, what are their duties, and how do they report to the security manager?

(6) Provide a copy of the most current written command security procedures.

(7) Explain any security services provided by the command including inspection, evaluation, education, or assist visits.

(8) Provide the format or requirements for the annual refresher briefings.

(9) Provide the command's security termination statement procedures.

(10) **What security procedures are in place to ensure only those with validated need are submitted for a limited access authorization?**

(11) What protocols are in place to limit investigative and security clearance requests to only those individuals who need such in performance of their duties or functions?

b. Security officers and/or managers.

(1) Annual volume of security clearances submitted.

(2) Provide number of submissions rejected by the Personnel Security Investigation Center of Excellence based on existence of a prior valid investigation that meets requirements.

(3) Does the security manager verify security clearance of persons authorized access to classified info?

Appendix A
References

Section I
Required Publications
This section contains no entries.

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read it to understand this regulation. DOD publications are available at http://www.dtic.mil/whs/directives/corres/pub1.html. United States Codes are available at http://www.gpoaccess.gov/uscode/

AR 11–2
Managers' Internal Control Program

AR 25–30
The Army Publishing Program

AR 25–55
Release of Information and Records from Army Files

AR 50–5
Nuclear Surety

AR 50–6
Chemical Surety

AR 190–16
Physical Security

AR 190–56
The Army Civilian Police and Security Guard Program

AR 215–3
Nonappropriated Funds Personnel Policy

AR 340–21
The Army Privacy Program

AR 380–5
Department of the Army Information Security Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives (U)

AR 380–28
Department of the Army Special Security System

AR 380–49
Industrial Program

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities

AR 381–12
Threat Awareness and Reporting Program

AR 381–20
The Army Counterintelligence Program (S)

AR 381–45
Investigative Records Repository

AR 600–8–2
Suspension of Favorable Personnel Actions (FLAGS)

AR 600–37
Unfavorable Information

AR 600–8–104
Military Personnel Information Management/Records

AR 608–10
Child Development Services

AR 614–200
Enlisted Assignments and Utilization Management

DA Pam 611–21
Military Occupational Classification and Structure

Director of Central Intelligence Directive: DCID No 1/14
Minimum Personnel Security Standards and Practices Governing Access to Sensitive Compartmented Information

DIS 20–1–M
Manual for Personnel Security Investigations

DOD 1401.1–M
Personnel Policy Manual for Nonappropriated Fund Instrumentalities

DOD 5030.49–R
Customs Inspection

DOD 5200.1–R
Information Security Program Regulation

DOD 5200.2–R
DOD Personnel Security Program

DOD 5220.22–R
Industrial Security Regulation

DOD 7000.14–R, Volume 13
Financial Management Regulation, Volume 13, Nonappropriated Funds Policy and Procedures

DODD 5100.3
Support of the Headquarters of Unified Specified, and Subordinate Joint Commands

DODD 5100.23
Administrative Arrangements for the National Security Agency

DODD 5100.55
United States Security Authority for North Atlantic Treaty Organization Affairs

DODD 5105.42
The Defense Investigative Service

DODD 5142.1
Assistant Secretary of Defense (Legislative Affairs)

DODD 5200.8
Security of Military Installations and Resources

DODD 5210.2
Access to and Dissemination of Restricted Data

DODD 5210.25
Assignment of American National Red Cross and United Service Organizations

DODD 5210.42
Nuclear Weapon Personnel Reliability Program

DODD 5210.45
Personnel Security in the National Security Agency

DODD 5210.46
Department of Defense Building Security for the National Capital Region

DODD 5210.48
DOD Polygraph Program

DODD 5210.55
Selection of DOD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities

DODD 5210.65
Chemical Agency Security Program

DODD 5220.22
Industrial Security Regulation

DODD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations

DODD 5400.7
DOD Freedom of Information Act Program

DODD 5400.11
Department of Defense Privacy Program

EO 9835
Prescribing Procedures for the Administration of an Employee Loyalty Program in the Executive Branch of the Government

EO 10450
Security Requirements for Government Employment

EO 11935
Citizenship Requirements for Federal Employment

EO 12333
United States Intelligence Activities

EO 12356
National Security Information

PL 86–36
National Security Agency–Officer and Employees

PL 88–290
National Security Agency–Personnel Security Procedures

PL 89–380
Unauthorized publication or use of communications

PL 96–456
Classified Information Procedures Act of 1980

UCMJ, Art. 15
Nonjudicial Punishment (Available at http://www.au.af.mil/au/awc/awcgate/ucmj.htm.)

Atomic Energy Act of 1954
Atomic Energy

Privacy Act of 1974
Antiterrorism

5 CFR 213.306
Accepted service

5 USC 552a
Records maintained on individuals

5 USC 3571
Reinstatement or restoration; individuals suspended or removed for national security

5 USC 7532
Suspension and removal

10 USC
Armed Forces

FPM letter 732
Military Personnel Information Management/Records

OMB Circular A–130
Management of Federal Resources (Available at http://www.whitehouse.gov/omb/circulars_a130.)

RCS DD–POL(A)1749
No information

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
The following forms are available on the APD Web site http:// www.apd.army.mil.

DA Form 11–2
Internal Control Evaluation Certification

DA Form 477 (obsolete)
Requisition for Enlisted Personnel

DA Form 872
Requisition for Individual Officer Personnel

DA Form 873 (obsolete)
Certificate Clearance and/or Security Determination

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 2962
Security Termination Statement

DA Form 5247–R (obsolete)
Request for Security Determination (LRA)

DA Form 5248–R
Report of Unfavorable Information for Security Determination (LRA)

DD Form 398 (obsolete)
Personnel Security Questionnaire

DD Form 398–2 (obsolete)
DOD National Agency Questionnaire (NAQ)

DD Form 1879 (obsolete)
DOD Request for Personnel Security Investigation

DD Form 2221 (obsolete)
DOD Authority for Release of Information and Records

FD 258
Applicant Fingerprint Card

FS–240
Report of Birth Abroad of a Citizen of the United States of America

FS–545
Certification of Birth

SF Form 85
Questionnaire for Non-Sensitive Positions

SF Form 87
Fingerprint Chart

SF 171 (superseded by OF 612)
Application for Federal Employment

Appendix B
Investigative Scope

This appendix prescribes the scope of the various types of PSIs.

B–1. National Agency Check

At a minimum, the first three of the described agencies (DCII, FBI/HQ, and FBI/ID) below shall be included in each complete NAC; however, a NAC may also include a check of any or all of the other described agencies, if appropriate.

a. The DCII records consist of an alphabetical index of personal names and impersonal titles that appear as subjects or incidentals in investigative documents held by the criminal, counterintelligence, fraud, and personnel security investigative activities of the three military departments, DIS, DCIS, and the National Security Agency. DCCI records will be checked on all subjects of DOD investigations.

b. The FBI/HQ has on file copies of investigations conducted by the FBI. The FBI/HQ check, included in every NAC, consists of a review of files for information of a security nature and that developed during applicant-type investigations.

c. An FBI/ID check, included in every NAC (but not ENTNAC), is based upon a technical fingerprint search that consists of a classification of the subject's fingerprints and comparison with fingerprint cards submitted by law enforcement activities. If the fingerprint card is not classifiable, a "name check only" of these files is automatically conducted.

d. The files of OPM contain the results of investigations conducted by OPM under EOs 9835 and 10450, those requested by the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE) and those requested since August 1952 to serve as a basis for "Q" clearances. Prior to that date, "Q" clearance investigations were conducted by the FBI. A "Q" clearance is granted to individuals who require access to DOE information. In order to receive a "Q" clearance, a full field BI must be completed on the individual requiring access in accordance with the Atomic Energy Act of 1954. Also on file are the results of investigations on the operation of the Merit System, violations of the Veterans Preference Act, appeals of various types, fraud and collusion in civil service examinations and related matters, data on all Federal employment, and an index of all BIs on civilian employees or applicants completed by agencies of the executive branch of the U.S Government. The OPM files may also contain information relative to U.S. citizens who are, or who were, employed by a United Nations organization or other public international organization such as the Organization of American States. OPM records are checked on all persons who are, or who have been, civilian employees of the U.S. Government; or U.S. citizens who are, or who have been, employed by a United Nations organization or other public international organization; and on those who have been granted security clearances by the NRC or DOE.

e. The files of Immigration and Naturalization Service (INS) contain (or show where filed) naturalization certificates, certificates of derivative citizenship, all military certificates of naturalization, repatriation files, petitions for naturalization and declaration of intention, visitors' visas, and records of aliens (including government officials and representatives of international organizations) admitted temporarily into the United States INS records are checked when the subject is—

(1) An alien in the United States, or

(2) A naturalized citizen whose naturalization has not been verified, or

(3) An immigrant alien, or

(4) A U.S. citizen who receives derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

f. The State Department maintains the following records:

(1) Security division files contain information pertinent to matters of security, violations of security, personnel investigations pertinent to that agency, and correspondence files from 1950 to date. These files are checked on all former State Department employees.

(2) Passport division shall be checked if subject indicates U.S. citizenship due to birth in a foreign country of American parents. This is a check of State Department Embassy files to determine if subject's birth was registered at the U.S. Embassy in the country where he was born. Verification of this registration is verification of citizenship.

g. The files of CIA contain information on present and former employees, including members of the Office of Strategic Services (OSS), applicants for employment, foreign nationals, including immigrant aliens in the United States, and U.S. citizens traveling outside the United States after July 1, 1946. These files shall be checked under the following guidelines.

Table B–1
Criteria for Central Intelligence Agency checks

Investigation: NAC, DNACI, or ENTNAC **Criteria for CIA checks:** Residence anywhere outside of the United States for a year or more since age 18 except under the auspices of the United States Government; and travel, education, residence, or employment since age 18 in any designated country (app H).
Investigation: BI **Criteria for CIA checks:** Same as NAC, DNACI, and ENTNAC requirements plus travel, residence, employment, and education outside the United States for more than a continuous 3-month period during the past 5 years, or since age 18, except when under the auspices of the Government.
Investigation: SBI **Criteria for CIA checks:** Same as BI requirements except the period of the investigation will cover the past 15 years, or since age 18. Also when subject's employment, education, or residence has occurred overseas for a period of more than 1 year under the auspices of the U.S. Government, such checks will be made.

h. Military personnel record center files are maintained by separate departments of the Armed Forces, General Services Administration and the reserve records centers. They consist of the master personnel records of retired, separated, reserve, and active duty members of the Armed Force. These records shall be checked when the requester provides required identifying data indicating service during the last 15 years.

i. The files of Treasury Department agencies (Secret Service, Internal Revenue Service, and Bureau of Customs)

will be checked only when available information indicates that an agency of the Treasury Department may be reasonably expected to have pertinent information.

j. The files of other agencies such as the National Guard Bureau, the DISCO, and so forth, will be checked when pertinent to the purpose for which the investigation is being conducted.

B–2. DOD National Agency Check and written inquiries

a. Scope. The time period covered by the DNACI is limited to the most recent 5 years, or since the 18th birthday, whichever is shorter, provided that the investigation covers at least the last 2 full years of the subject's life, although it may be extended to the period necessary to resolve any questionable or derogatory information. No investigation will be conducted prior to an individual's 16th birthday. All DNACI investigation information will be entered on the DD Form 398–2 and FD–Form 258 and forwarded to the Defense Investigative Service**C–4**, app C).

b. Components of a DOD National Agency Check and written inquiries.

(1) *NAC.* This is the same as described in paragraph **B–**1, above.

(2) *Credit.*

(a) A credit bureau check will be conducted to cover the 50 States, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, at all locations where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months (cumulative) during the past 5 years.

(b) When information developed reflects unfavorably upon a person's current credit reputation or financial responsibility, the investigation will be expanded as necessary.

(3) *Employment.*

(a) Non-Federal employment.

1. Verify, via written inquiry, all employment within the period of investigation with a duration of 6 months or more. Current employment will be checked regardless of duration.

2. If all previous employments have been less than 6 months long, the most recent employment, in addition to the current, will be checked in all cases.

3. Seasonal holiday, part-time and temporary employment need not be checked unless subparagraph 2, above, applies.

(b) Federal employment. All Federal employment (to include military assignments) within the period of investigation will be verified by the requester through locally available records, and a statement reflecting that such checks have been favorably accomplished will be contained in the investigative request. Those that cannot be verified in this fashion will be accomplished via written inquiry by DIS (within the 50 United States, Puerto Rico, Guam, and the Virgin Islands).

B–3. Background investigation

The period of investigation for the BI is 5 years and applies to military, civilian, and contractor personnel.

a. National agency check. See paragraph **B–**1, above.

b. Local agency checks. Same as paragraph **B–**4*j*, below, except period of coverage is 5 years.

c. Credit checks. Same as paragraph **B–**4*i*, below.

d. Subject interview. This is the principal component of a BI. In some instances an issue will arise after the primary SI and a secondary interview will be conducted. Interviews in the latter category are normally "issue" interviews that will be reported in the standard BI narrative format.

e. Employment records. Employment records will be checked at all places where employment references are interviewed with the exception of current Federal employment when the requester indicates that such employment has been verified with favorable results.

f. Employment reference coverage. A minimum of *three references, either supervisors or coworkers,* who have knowledge of the SUBJECT's activities in the work environment will be interviewed. At least one employment reference at the current place of employment will always be interviewed with the exception of an individual attending military basic training, or other military training schools lasting less than 90 days. However, if the SUBJECT has only been at the current employment for less than 6 months, it will be necessary to go not only to their current employment (for example, for one employment reference) but also to the preceding employment of at least 6 months for additional employment references. If the SUBJECT has not had prior employment of at least 6 months, interview(s) will be conducted at the most recent short-term employment in addition to the current employment.

g. Developed and listed character references. A minimum of three developed character references (DCRs) whose combined association with the subject covers the entire period of investigation will be interviewed. If coverage cannot be obtained through the DCRs, a listed character reference (LCR) will be contacted to obtain coverage.

h. Unfavorable information. Unfavorable information developed in the field will be expanded.

B–4. Special background investigation

a. Components of an special background investigation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is the shorter period, provided that the investigation covers at least the last 2 full

years of the subject's life. No investigation will be conducted for the period prior to an individual's 16th birthday. Emphasis shall be placed on peer coverage whenever interviews are held with personal sources in making education, employment, and reference (including developed) contacts.

b. National agency check. In addition to conducting a NAC on the subject of the investigation, the following additional requirements apply:

(1) A DCII, FBI/ID name check only and FBI/HQ check shall be conducted on subject's current spouse or cohabitant. In addition, such other national agency checks as deemed appropriate based on information on the subject's statement of personal history or PSQ shall be conducted.

(2) A check of FBI/HQ files on members of subject's immediate family who are aliens in the United States or immigrant aliens who are 18 years of age or older shall be conducted. As used throughout the regulation, members of subject's immediate family include the following:

(a) Current spouse.

(b) Adult children, 18 years of age or older, by birth, adoption, or marriage.

(c) Natural, adopted, foster, or stepparents.

(d) Guardians.

(e) Brothers and sisters either by birth, adoption, or remarriage of either parent.

(3) The files of CIA shall be reviewed on alien members of subject's immediate family who are 18 years of age or older, regardless of whether or not these persons reside in the United States.

(4) The INS files on members of subject's immediate family 18 years of age or older shall be reviewed when they are:

(a) Aliens in the United States, or

(b) Naturalized U.S. citizens whose naturalization has not been verified in a prior investigation, or

(c) Immigrant aliens, or

(d) U.S. citizens born in a foreign country of American parent(s) or U.S. citizens who received derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

c. Birth. Verify subject's date and place of birth (DPOB) through education, employment and/or other records. Verify through Bureau of Vital Statistics (BVS) records if not otherwise verified under paragraph *d,* below, or if a variance is developed.

d. Citizenship. Subject's citizenship status must be verified in all cases. U.S. citizens who are subjects of investigation will be required to produce documentation that will confirm their citizenship. Normally, such documentation should be presented to the DOD Component concerned prior to the initiation of the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that the designated authority in the DOD Component will be provided with the documentation prior to the issuance of a clearance. DIS will not check the BVS for native-born U.S. citizens except as indicated in paragraph *c,* above. In the case of foreign-born U.S. citizens, DIS will check INS records. The citizenship status of all foreign-born members of subject's immediate family shall be verified. Additionally, when the investigation indicates that a member of subject's immediate family has not obtained U.S. citizenship after having been eligible for a considerable period of time, an attempt should be made to determine the reason. The documents listed below are acceptable for proof of U.S. citizenship for personnel security determination purposes:

(1) A birth certificate must be presented if the individual was born in the United States. To be acceptable, the certificate must show that the birth record was filed shortly after birth and must be certified with the registrar's signature and the raised, impressed, or multicolored seal of their office except for States or jurisdictions which, as a matter of policy, do not issue certificates with a raised or impressed seal. Uncertified copies of birth certificates are not acceptable.

(a) A delayed birth certificate (a record filed more than 1 year after the date of birth) is acceptable provided that it shows that the report of birth was supported by acceptable secondary evidence of birth as described in paragraph (b), below.

(b) If such primary evidence is not obtainable, a notice from the registrar stating that no birth record exists should be submitted. The notice shall be accompanied by the best combination of secondary evidence obtainable. Such evidence may include a baptismal certificate, a certificate of circumcision, a hospital birth record, affidavits of persons having personal knowledge of the facts of the birth, or other documentary evidence such as early census, school, or family Bible records, newspaper files and insurance papers. Secondary evidence should have been created as close to the time of birth as possible.

(c) All documents submitted as evidence of birth in the United States shall be original or certified documents. Uncertified copies are not acceptable.

(2) A certificate of naturalization shall be submitted if the individual claims citizenship by naturalization.

(3) A certificate of citizenship issued by the INS shall be submitted if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

(4) A Report of Birth Abroad of A Citizen of The United States of America (Form FS–240), a Certification of Birth (Form FS–545 or DS–1350), or a Certificate of Citizenship is acceptable if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

(5) A passport or one in which the individual was included will be accepted as proof of citizenship.

e. Education.

(1) Verify graduation or attendance at institutions of higher learning in the United States within the last 15 years, if such attendance was not verified during a prior investigation.

(2) Attempts will be made to review records at overseas educational institutions when the subject resided overseas in excess of 1 year.

(3) Verify attendance or graduation at the last secondary school attended within the past 10 years if there was no attendance at an institution of higher learning within the period of investigation.

(4) Verification of attendance at military academies is only required when the subject failed to graduate.

f. Employment.

(1) *Non-Federal employment.* Verify all employment within the period of investigation to include seasonal, holiday, Christmas, part-time, and temporary employment. Interview one supervisor and one coworker at subject's current place of employment as well as at each prior place of employment during the past 10 years of 6 months or longer. The interview requirement for supervisors and coworkers does not apply to seasonal, holiday, Christmas, part-time, and temporary employment (4 months or less) unless there are unfavorable issues to resolve or the letter of inquiry provides insufficient information.

(2) *Federal employment.* All Federal employment will be verified within the period of investigation to include Christmas, seasonal temporary, summer hire, part-time, and holiday employment. Do not verify Federal employment through review of records if already verified by the requester. If Federal employment has not been verified by the requester, then subject's personnel file at their current place of employment will be reviewed. All previous Federal employment will be verified during this review. In the case of former Federal employees, records shall be examined at the Federal Records Center in St. Louis, Mo. Interview one supervisor and one coworker at all places of employment during the past 10 years if so employed for 6 months or more.

(3) *Military employment.* Military service for the last 15 years shall be verified. The subject's duty station, for the purpose of interview coverage, is considered as a place of employment. One supervisor and one coworker shall be interviewed at subject's current duty station if subject has been stationed there for 6 months or more; additionally, a supervisor and a coworker at subject's prior duty stations where assigned for 6 months or more during the past 10 years shall be interviewed.

(4) *Unemployment.* Subject's activities during all periods of unemployment in excess of 30 consecutive days, within the period of investigation, that are not otherwise accounted for shall be verified.

(5) When an individual has resided outside the United States continuously for over 1 year, attempts will be made to confirm overseas employments as well as conduct required interviews of a supervisor and coworker.

g. References. Three developed character references who have sufficient knowledge of subject to comment on their background, suitability, and loyalty shall be interviewed personally. Efforts shall be made to interview developed references whose combined association with subject covers the full period of the investigation with particular emphasis on the last 5 years. Employment, education, and neighborhood references, in addition to the required ones, may be used as developed references provided that they have personal knowledge concerning the individual's character, discretion, and loyalty. Listed character references will be interviewed only when developed references are not available or when it is necessary to identify and locate additional developed character references or when it is necessary to verify subject's activities (e.g., unemployment).

h. Neighborhood investigation. Conduct a neighborhood investigation to verify each of subject's residences in the United States of a period of 6 months or more on a cumulative basis, during the past 5 years or during the period of investigation, whichever is shorter. During each neighborhood investigation, interview two neighbors who can verify subject's period of residence in that area and who were sufficiently acquainted to comment on subject's suitability for a position of trust. Neighborhood investigations will be expanded beyond this 5-year period only when there is unfavorable information to resolve in the investigation.

i. Credit. Conduct credit bureau check in the 50 States, the District of Columbia, Puerto Rico, and overseas (where APO/FPO addresses are provided) at all places where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months or more, on a cumulative basis, during the last 7 years or during the period of the investigation, whichever is shorter. When coverage by a credit bureau is not available, credit references located in that area will be interviewed. Financial responsibility, including unexplained affluence, will be stressed in all reference interviews.

j. Local agency checks. LACs, including State central criminal history record repositories, will be conducted on subject at all places of residence to include duty stations and/or home ports, in the 50 States, the District of Columbia, and Puerto Rico, where residence occurred during the past 15 years or during the period of investigation, whichever is shorter. If subject's place of employment and/or education is serviced by a different law enforcement agency than that servicing the area of residence, LACs shall be conducted also in these areas.

k. Foreign travel. If subject has been employed or educated or has traveled or resided outside of the United States for more than 90 days during the period of investigation, except under the auspices of the U.S. Government, additional record checks during the NAC shall be made in accordance with paragraph **B–**1*f* of this appendix. In addition, the following requirements apply:

(1) *Foreign travel not under the auspices of the U.S. Government.* When employment, education, or residence has occurred overseas for more than 90 days during the past 15 years or since age 18, which was not under the auspices of the U.S. Government, a check of records will be made at the Passport Office of the Department of State, the CIA, and other appropriate agencies. Efforts shall be made to develop sources, generally in the United States, who knew the individual overseas to cover significant employment, education, or residence and to determine whether any lasting foreign contacts or connections were established during this period. If the individual has worked or lived outside of the United States continuously for over 1 year, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

(2) *Foreign travel under the auspices of the U.S. Government.* When employment, education, or residence has occurred overseas for a period of more than 1 year, under the auspices of the U.S. Government, a record check will be made at the Passport Office of the Department of State, the CIA, and other appropriate agencies. Efforts shall be made to develop sources (generally in the United States) who knew the individual overseas to cover significant employment, education, or residence and to determine whether any lasting foreign contacts or connections were established during this period. Additionally, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the United States Government in the foreign country in which the individual resided.

l. Foreign connections. All foreign connections (friends, relatives, and/or business connections) of subject and immediate family in the United States or abroad, except where such association was the direct result of subject's official duties with the U.S. Government, shall be ascertained. Investigation shall be directed toward determining the significance of foreign connections on the part of subject and the immediate family, particularly where the association is or has been with persons whose origin was within a country whose national interests are inimical to those of the United States. When subject or their spouse have close relatives residing in a Communist-controlled country, or subject has resided, visited, or traveled in such a country, not under U.S. Government auspices, the provisions of paragraph 2–308*c* of this regulation apply.

m. Organizations. Efforts will be made during reference interviews and record reviews to determine if subject and/or the immediate family has, or formerly had, membership in, affiliation with, sympathetic association towards, or participated in any foreign or domestic organization, association, movement, group, or combination of persons of the type described in paragraphs 2–4*a* through *d* of this regulation.

n. Divorce. Divorces, annulments, and legal separations of subject shall be verified only when there is reason to believe that the grounds for the action could reflect on subject's suitability for a position of trust.

o. Military service. All military service and types of discharge during the last 15 years shall be verified.

p. Medical records. Medical records shall not be reviewed unless:

(1) The requester indicates that subject's medical records were unavailable for review prior to submitting the request for investigation, or

(2) The requester indicates that unfavorable information is contained in subject's medical records, or

(3) The subject lists one or more of the following on the statement of personal history or PSQ:

(a) A history of mental or nervous disorders.

(b) That subject is now or has been addicted to the use of habit-forming drugs such as narcotics or barbiturates or is now or has been a chronic user to excess of alcoholic beverages.

q. Updating a previous investigation to SBI standards. If a previous investigation does not substantially meet the minimum standards of an SBI or if it is more than 5 years old, a current investigation is required but may be limited to that necessary to bring the individual's file up to date in accordance with the investigative requirements of an SBI. Should new information be developed during the current investigation that bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

B–5. Periodic reinvestigation

a. Each DOD military, civilian, consultant, and contractor employee (to include foreign nationals holding a limited access authorization) occupying a critical-sensitive position, possessing a TOP SECRET clearance, or occupying a special access program position **or whose MOS requires access to TOP SECRET and/or SCI**, shall be the subject of a PR initiated **not later than** 5 years from the date of completion of the last investigation. The PR shall cover the period of the last 5 years.

(1) **If there has been a break in the individual's military service, DA civilian employment, or contractor employment (for contractor employees who require access to SCI) of more than 12 months, a PR is not acceptable. A BI or SBI, as appropriate, is required.**

(2) **If the previous investigation (BI, SBI, or PR) is more than 6 years old, a PR is not acceptable. A BI or SBI, as appropriate, is required to cover the period since the last investigation.**

b. Minimum investigative requirements. A PR shall include the following minimum scope.

(1) *National agency check.* A valid NAC on the subject will be conducted in all cases. Additionally, for positions requiring SCI access, checks of DCII, FBI/HQ, FBI/ID name check only, and other agencies deemed appropriate will be conducted on the subject's current spouse or cohabitant, if not previously conducted. Additionally, NACs will be conducted on immediate family members, 18 years of age or older, who are aliens and/or immigrant aliens, if not previously accomplished.

(2) *Credit.* Credit bureau checks covering all places where the subject resided for 6 months or more, on a cumulative basis, during the period of investigation, in the 50 States, District of Columbia, Puerto Rico, and overseas (where APO/FPO addresses are provided) will be conducted.

(3) *Subject interview.* The interview should cover the entire period of time since the last investigation, not just the last 5-year period. Significant information disclosed during the interview, which has been satisfactorily covered during a previous investigation, need not be explored again unless additional relevant information warrants further coverage. An SI is not required if one of the following conditions exist:

(a) The subject is aboard a deployed ship or in some remote area that would cause the interview to be excessively delayed.

(b) The subject is in an overseas location serviced by the State Department or the FBI.

(4) *Employment.* Current employment will be verified. Military and Federal service records will not routinely be checked, if previously checked by the requester when PR was originally submitted. Also, employment records will be checked wherever employment interviews are conducted. Records need be checked only when they are locally available, unless unfavorable information has been detected.

(5) *Employment references.* Two supervisors or coworkers at the most recent place of employment or duty station of 6 months **will be interviewed**; if the current employment is less than 6 months, employment reference interviews will be conducted at the next prior place of employment **of** at least a 6-month duration.

(6) *Developed character references.* Two developed character references who are knowledgeable of the subject will be interviewed. The developed character references who were previously interviewed will only be reinterviewed when other developed references are not available.

(7) *Local agency checks.* The DIS will conduct local agency checks on the subject at all places of residence, employment, and education during the period of investigation, regardless of duration, including overseas locations.

(8) *Select scoping.* When the facts of the case warrant, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

Appendix C
Request Procedures

C–1. General

To conserve investigative resources and to ensure that PSIs are limited to those essential to current operations and are clearly authorized by DOD policies, organizations requesting investigations must ensure that continuing command attention is given to the investigative request process.

In this connection, it is particularly important that the provision of EO 12356 requiring strict limitations on the dissemination of official information and material be closely adhered to and that investigations requested for issuing clearances are limited to those instances in which an individual has a clear need for access to classified information. Similarly, investigations required to determine eligibility for appointment or retention in DOD, in either a civilian or military capacity, must not be requested in frequency or scope exceeding that provided for in this regulation.

In view of the foregoing, the following guidelines have been developed to simplify and facilitate the investigative request process:

a. Limit requests for investigation to those that are essential to current operations and clearly authorized by DOD policies and attempt to utilize individuals who, under the provisions of this regulation, have already met the security standard;

b. Ensure that military personnel on whom investigative requests are initiated will have sufficient time remaining in service after completion of the investigation to warrant conducting it;

c. Ensure that request forms and prescribed documentation are properly executed in accordance with instructions;

d. Dispatch the request directly to the DIS Personnel Investigations Center;

e. Promptly notify the DIS Personnel Investigations Center **through CCF (PCCF–M)** if the investigation is no longer needed (notify OPM if a NACI is no longer needed; and

f. Limit access through strict need to know, thereby requiring fewer investigations.

In summary, close observance of the above-cited guidelines will allow the DIS to operate more efficiently and permit more effective, timely, and responsive service in accomplishing investigations.

C–2. National agency check

When a NAC is requested, an original only of the DD Form 398–2 (National Agency Check Request) and a completed FD 258 (Applicant Fingerprint Card) are required. If the request is for an ENTNAC, an original only of the DD Form 398–2 and a completed DD Form 2280 (Armed Forces Fingerprint Card) are required. Those forms should be sent directly to: Personnel Investigation Center, Defense Investigative Service, P.O. Box 1083, Baltimore, MD 21203.

C–3. National agency check and written inquiries

When a NACI is requested, an original and one copy of the SF **86 (Questionnaire for Sensitive Positions),** an Of 612 (Optional Application for Federal Employment), and an SF 87 (U.S. Civil Service Commission Fingerprint Chart) shall be sent directly to: Office of Personnel Management, Bureau of Personnel Investigations, NACI Center, Boyers, PA 16018. The notation "ALL REFERENCES" shall be stamped immediately above the title at the top of the Standard Form 85.

C–4. DOD National Agency Check and written inquiries

a. When a DNACI is requested, one copy of DD Form 1879, an original and two copies of the DD Form 398–2 (National Agency Check Request), two copies of FD 258 (Fingerprint Card), and an original of DD Form 2221 (Authority for Release of Information and Records) shall be sent directly to: Personnel Investigations Center, Defense Investigative Service, P.O. Box 1083, Baltimore, MD 21203.

b. The DD Form 398–2 must be completed to cover the most recent 5-year period. All information, to include items relative to residences and employment, must be complete and accurate to avoid delays in processing.

C–5. Special background investigation/background investigation

a. When requesting a BI or SBI, one copy of DD Form 1879 (Request for Personnel Security Investigation), an original and four copies of DD Form 398 (Statement of Personnel History), two copies of FD 258, and an original of DD Form 2221 (Authority for Release of Information and Records) shall be sent directly to: Personnel Investigations Center, Defense Investigative Service, P.O. Box 454, Baltimore, MD 21203.

b. For the BI and SBI, the DD Form 398 must be completed to cover the most recent 5- and 15-year period, respectively, or since the 18th birthday, whichever is shorter.

c. **When requesting an SBI, DD Form 398–2 must be submitted for the spouse or cohabitant. A DD Form 398–2 must also be submitted for immediate family members over 18 years of age who are not U.S. citizens.**

C–6. Periodic reinvestigation

a. The PRs shall be requested only in such cases as are authorized by paragraph 2–12 of this regulation.

(1) For a PR requested in accordance with paragraph 2–12, the DD Form 1879 must be accompanied by the following documents:

(a) Original and four copies of DD Form 398.

(b) Two copies of FD–258.

(c) Original copy of DD Form 2221.

(2) In processing PRs, previous investigative reports will not be requested by the requesting organization, unless significant derogatory or adverse information, postdating the most recent favorable adjudication, is developed during the course of reviewing other locally available records. In the latter instance, requests for previous investigative reports may only be made if it is determined by the requesting organization that the derogatory information is so significant that a review of previous investigative reports is necessary for current adjudicative determinations.

b. No abbreviated version of DD Form 398 may be submitted in connection with a PR.

c. **The DD Form 398 completed for a BI PR will cover the most recent 5-year period and for an SBI PR it will be completed to cover the period from the date of the most recent SBI or SBI PR to present date.**

d. The PR request shall be sent to the address in paragraph**C–**5*a*, above.

C–7. Additional investigation to resolve derogatory or adverse information

a. Requests for additional investigation required to resolve derogatory or adverse information shall be submitted by DD Form 1879 (Request for Personnel Security Investigation) to: Defense Investigative Service, P.O. Box 454, Baltimore, MD 21203. Such requests shall set forth the basis for the additional investigation and describe the specific matter to be substantiated or disproved.

b. The request should be accompanied by an original and four copies of the DD Form 398, when appropriate, two copies of FD–258 and an original copy of DD Form 2221, unless such documentation was submitted within the last 12

months to DIS as part of a NAC or other PSI. If pertinent, the results of a recently completed NAC, NACI, or other related investigative reports available should also accompany the request.

C–8. Obtaining results of prior investigations

Requesters requiring verification of a specified type of PSI, and/or requiring copies of prior investigations conducted by the DIS shall submit requests by letter or message to: Defense Investigative Service Investigative Files Division, P. O. Box 1211, Baltimore, MD 21203. Message address: DIS personnel investigation center (PIC) Baltimore, MD/ / D0640. The request will include subject's name, grade, SSN, date and place of birth, and DIS case control number if known.

C–9. Requesting postadjudication cases

a. Requests pertaining to issues arising after adjudication of an investigation (post-adjudication cases) shall be addressed to DIS on a DD Form 1879 accompanied by a DD Form 398, when appropriate.

b. All requests for initial investigations will be submitted to PIC regardless of their urgency. If, however, there is an urgent need for a postadjudication investigation, or the mailing of a request to PIC for initiation of a postadjudication case would prejudice timely pursuit of investigative action, the DD Form 1879 may be directed for initiation, in CONUS, to the nearest DIS field office, and in overseas locations, to the military investigative service element supporting the requester (app J). The field element (either DIS or the military investigative agency) will subsequently forward either the DD Form 1879 or completed investigation to PIC.

c. A fully executed DD Form 1879 and appropriate supporting documents may not be immediately available. Further, a case that is based on sensitive security issues may be compromised by a request that the subject submit a DD Form 398. A brief explanation should appear on the DD Form 1879 which does not include complete supporting documentation.

C–10. Requests involving contractor employees

To preclude duplicative investigative requests and double handling of contractor employee cases involving access to classified information, all requests for investigation of contractor personnel must be submitted, using authorized industrial security clearance forms, for processing through the Defense Industrial Security Clearance Office, except for programs in which specific approval has been obtained from the Deputy Under Secretary of Defense for Policy to utilize other procedures.

C–11. Responsibility for proper documentation of requests

The official signing the request for investigation shall be responsible for ensuring that all documentation is completed in accordance with these instructions.

C–12. Requests involving Red Cross and United Services Organization employees

a. **The Red Cross and USO will prepare the request for NAC on prospective employees. DD Form 398–2 and FD Form 258 will be forwarded to the Defense Industrial Security Clearance Office (DISCO) for processing.**

b. **The DISCO will make a determination as to the acceptability of the prospective employee. If the determination is favorable, the Red Cross or USO will be notified. All unfavorable determinations will be forwarded to the Director for Industrial Security Clearance Review Office of the Defense General Counsel for action. The applicant, Red Cross or USO, and the host commander will be advised of the final determination.**

c. **If derogatory information is received on a Red Cross or USO employee, the host command or Red Cross or USO will forward the information for review to: Defense Industrial Security Clearance Office (DISCO–A), P.O. Box 2499, Columbus, OH 43216–5006.**

d. **The DISCO will initiate any investigation necessary to resolve derogatory information.**

e. **If a Red Cross or USO employee requires a security clearance, the host commander will forward the request together with a copy of the DISCO acceptability determination to the CDR, CCF, for action. All security clearances will be granted by the CDR, CCF, for Red Cross and/or USO employees on Army installations.**

Appendix D
Tables for requesting investigations

See table D-1 for a guide on requesting background investigations.

Table D–1
Guide for requesting background investigations

A	B	C
If the individual is a	and duties require	then a BI is required before
U.S. national military member, civilian, consultant, or contractor employee	TOP SECRET clearance	granting final clearance
U.S. national civilian employee	assignment to a “critical-sensitive” position	assignment to the position
U.S. national military member, civilian, or contractor employee	occupying a “critical” position in the Nuclear Weapon PRP	occupying a “critical” DOD position
U.S. national military member or civilian employee	granting or denying clearances	performing clearance functions
U.S. national military member or civilian employee	membership on security screening, hearing, or review board	appointment to the board
immigrant alien	limited access to SECRET or CONFIDENTIAL information	issuing limited access authorization (see note)
non-U.S. national employee, excluding immigrant alien,	limited access to SECRET or CONFIDENTIAL information	issuing limited access authorization
non-U.S. national nominee for military education and orientation program (from a country listed at app H)	education and orientation of military personnel	performing duties
U.S. national military member or DOD civilian or contractor employee	assignment to a category two Presidential support position	assignment
U.S. national military member or DOD civilian or contractor employee assigned to NATO	access to NATO COSMIC information	access may be granted

Notes:
BI will cover a 10-year scope.

Table D–2
Guide for requesting special background investigations

A	B	C
	then a SBI is required	
If the individual is a	and duties require	before
U.S. national military member or DOD civilian, consultant, or contractor employee	access to SCI	granting access
	assignment to a category one Presidential support position	assignment
	access to SIOP-ESI	granting access
	assignment to the National Security Agency	assignment
	access to other special access programs approved under paragraph 3–37	granting access
	assignment to personnel security, counterintelligence, or criminal investigative or direct investigative support duties	assignment

Table D–3
Guide for requesting periodic reinvestigations

A	B	C
If the individual is a	and duties require	then a PR is required
U.S. national military member or DOD civilian, consultant, or contractor employee	access to SCI	5 years from date of last SBI/BI or SBI PR
	TOP SECRET clearance 5 years from date of last SBI/BI or PR	
	access to NATO COSMIC	5 years from date of last SBI/BI or PR
	assignment to Presidential support activities	5 years from date of last SBI/BI or PR
U.S. national civilian employee	assignment to a “critical-sensitive” position	5 years from last SBI/BI or PR
non-U.S. national employee	current limited access authorization to SECRET or CONFIDENTIAL information	5 years from last SBI/BI or PR
U.S. national military member	assignment to duties defined in paragraph 3–59 or requiring TS or SCI eligibility in accordance with DA Pam 611–21.	5 years from last SBI/BI or PR

Table D–4
Guide for requesting DOD National Agency Check with written inquiries or national agency check and inquiries

A	B	C
If the individual is a	and duties require	then a DNACI/NACI is required
U.S. national military member or contractor employee	SECRET clearance	before granting clearance (see note 1)
	Interim SECRET clearance	automatically (see note 2)
U.S. national civilian employee or consultant	SECRET clearance	before granting clearance
	Interim SECRET clearance	automatically (see note 3)
	Appointment to “noncritical-sensitive” position	before appointment
U.S. national military member or DOD civilian or contractor employee	occupying a “controlled” position in the Nuclear Weapon PRR	before assignment
applicant for appointment as a commisioned officer	commission in the Armed Forces	before appointment (after appointment for health professionals, chaplains, and attorneys, under conditions authorized by para 3–15 of this regulation)
Naval Academy Midshipman, Military Academy Cadet, or Air Force Academy Cadet	enrollment	to be initiated 90 days after entry
Reserve Officer Training Corps (ROTC) Cadet or Midshipman	entry to advanced course or college scholarship program	to be initiated 90 days after entry

Notes:

[1] First-term enlistees shall require an ENTNAC.

[2] Provided DD Form 398–2 is favorably reviewed, local records check favorably accomplished, and DNACI initiated.

[3] Provided an authority designated in appendix F finds delay in such appointment would be harmful to national security; favorably review of DD Form 389–2; NACI initiated; and favorable local records check accomplished.

Table D–5
Guide for requesting National Agency Checks

A	B	C
If the individual is a	and duties require	then a NAC is required
first-term enlistee	retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT 3 work days after entry (see note 1)
prior service member reentering military service after break in Federal employment exceeding 1 year	retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT 3 work days after reentry
nominee for military education and orientation program	education and orientation of military personnel	before performing duties (see note 2)
U.S. national military or DOD civilian or contractor employee	access to restricted areas, sensitive information, or equipment as defined in paragraph 3–39	before authorizing entry
nonappropriated fund instrumentality (NAFI) civilian employee	appointment as NAFI custodian	before appointment
	accountability for nonappropriated funds	before completion of probationary period
	fiscal responsibility as determined by NAFI custodian	before completion of probationary period
	other “positions of trust”	before appointment
Persons requiring access to chemical agents	access to or security of chemical agents	before assignment
U.S. national, civilian employee nominee for customs inspection duties	waiver under provisions of paragraph 3–41	before appointment (see note 3)
Red Cross/USO personnel	assignment with the Armed Forces overseas	before assignment (see note 4 for foreign national personnel)
U.S. national	a DOD building pass	prior to issuance
Foreign national employed overseas	no access to classified information	prior to employment (see note 4)

Notes:

[1] Request ENTNAC only.

[2] Except when personnel whose country of origin is listed at appendix H, a BI will be required (see para 3–50).

[3] A NAC not over 5 years old suffices unless there has been a break in employment over 12 months. Then a current NAC is required.

[4] In such cases, the NAC shall consist of: (a) host government law enforcement and security agency record checks at the city, State (Province), and national level, and (b) DCII.

Appendix E
Reporting of Nonderogatory Cases

Rescinded.

Appendix F
Personnel Security Determination Authorities

F–1. Officials authorized to grant, deny, or revoke personnel security clearances (TOP SECRET, SECRET, and CONFIDENTIAL):

a. Secretary of Defense and/or designee.
b. Secretary of the Army and/or designee.
c. Secretary of the Navy and/or designee.
d. Secretary of the Air Force and/or designee.
e. Chairman, Joint Chiefs of Staff, and/or designee.
f. Directors of the Defense Agencies and/or designee.
g. Commanders of the Unified and Specified Commands and/or designee.

h. **DCS, G–2 and/or designee.**
i. Commander, CCF, and/or designee.

F–2. Officials authorized to grant limited access authorizations:

a. Secretaries of the Military Departments and/or designees.
b. Director, Washington Headquarters Services, for OSD and/or designee.
c. Chairman, JCS, and/or designee.
d. Directors of the Defense Agencies and/or designees.
e. Commanders, Unified and Specified Commands, and/or designees.
f. **Heads of HQDA Staff agencies.**
g. **Commanders of MACOMs.**
h. Commander, CCF.

F–3. Officials authorized to grant access to sensitive compartmented investigation

a. Director, NSA—for NSA.
b. Director, DIA—for OSD, OJCS, and Defense Agencies.
c. Senior Officers of the Intelligence Community of the Army (DCS, G–2), Navy, and Air Force—for their respective Military Departments, or their single designee.
d. **Commander, CCF.**

F–4. Officials authorized to certify personnel under their jurisdiction for access to restricted data (to include critical nuclear weapon design information)

See enclosure to DODD 5210.2 **(AR 380–5)**.

F–5. Officials authorized to approve personnel for assignment to Presidential support activities

a. The Executive Secretary to the Secretary.
b. Deputy Secretary of Defense or designee.

F–6. Officials authorized to grant access to SIOP–ESI

a. Director of Strategic Target Planning.
b. Director, Joint Staff, OJCS.
c. Chief of Staff, U.S. Army.
d. Chief of Naval Operations.
e. Chief of Staff, U.S. Air Force.
f. Commandant of the Marine Corps.
g. Commanders of Unified and Specified Commands.
h. The authority to grant access delegated above may be further delegated in writing by the above officials to the appropriate subordinates.

F–7. Officials authorized to designate sensitive positions

a. Heads of DOD Components or their designees for critical-sensitive positions.
(1) **Under Secretary of the Army.**
(2) **Assistant secretaries of the Army.**
(3) **Deputy assistant secretaries of the Army.**
(4) **Chief of Staff.**
(5) **Heads of HQDA Staff agencies.**
(6) **Commanders of MACOMs. Note: These officials may redelegate this authority to subordinate commanders as deemed necessary.**
b. Organizational commanders for noncritical-sensitive positions.

F–8. Nonappropriated Fund positions of trust

Officials authorized to designate Nonappropriated Fund positions of trust: Heads of DOD Components and/or their designees.
a. **Under Secretary of the Army.**
b. **Assistant secretaries of the Army.**
c. **Deputy assistant secretaries of the Army.**
d. **Chief of Staff.**
e. **Heads of HQDA Staff agencies.**

f. **Commanders of MACOMs.**
g. **Organizational commanders.**

Appendix G
Guidelines for Conducting Prenomination Personal Interviews
Deleted.

Appendix H
List of Designated Countries
Deleted.

Appendix I
Adjudicative Guidelines for Determining Eligibility for Access to Collateral Classified Information and Sensitive Compartmented Information and Controlled Access Program Information

I–1. Introduction
a. The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by Government departments and agencies in all final clearance determinations. Government departments and agencies may also choose to apply these guidelines to analogous situations regarding persons being considered for access to other types of protected information.

b. Decisions regarding eligibility for access to classified information take into account factors that could cause a conflict of interest and place a person in the position of having to choose between his or her commitment to the United States, including the commitment to protect classified information, and any other compelling loyalty. Access decisions also take into account a person's reliability, trustworthiness, and ability to protect classified information. No coercive policing could replace the self-discipline and integrity of the person entrusted with the nation's SECRETs as the most effective means of protecting them. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount.

I–2. Adjudicative Process
a. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole-person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(1) The nature, extent, and seriousness of the conduct.
(2) The circumstances surrounding the conduct, to include knowledgeable participation.
(3) The frequency and recency of the conduct.
(4) The individual's age and maturity at the time of the conduct.
(5) The extent to which participation is voluntary.
(6) The presence or absence of rehabilitation and other permanent behavioral changes.
(7) The motivation for the conduct.
(8) The potential for pressure, coercion, exploitation, or duress.
(9) The likelihood of continuation or remain.

b. Final determinations for Army personnel remains the responsibility of the CCF or Army PSAB, as appropriate. The Command may provide supporting documentation for CCF or Army PSAB consideration. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of national security.

c. The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. The ultimate determination of whether the granting or continuing of eligibility for security

clearance eligibility is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.

(1) Guideline A: Allegiance to the United States.
(2) Guideline B: Foreign Influence.
(3) Guideline C: Foreign Preference.
(4) Guideline D: Sexual Behavior.
(5) Guideline E: Personal Conduct.
(6) Guideline F: Financial Considerations.
(7) Guideline G: Alcohol Consumption.
(8) Guideline H: Drug Involvement.
(9) Guideline I: Psychological Conditions.
(10) Guideline J: Criminal Conduct.
(11) Guideline K: Handling Protected Information.
(12) Guideline L: Outside Activities.
(13) Guideline M: Use of Information Technology Systems.

d. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole-person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

e. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(1) Voluntarily reported the information.
(2) Was truthful and complete in responding to questions.
(3) Sought assistance and followed professional guidance, where appropriate.
(4) Resolved or appears likely to favorably resolve the security concern.
(5) Has demonstrated positive changes in behavior and employment.
(6) Should have his or her access temporarily suspended pending final adjudication of the information.

f. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance eligibility, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

I–3. Guideline A: Allegiance to the United States

a. The concern. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States of America.

(2) Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(3) Association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:

(a) Overthrow or influence the Government or any State or local government.
(b) Prevent Federal, State, or local government personnel from performing their official duties.
(c) Gain retribution for perceived wrongs caused by the Federal, State, or local government.
(d) Prevent others from exercising their rights under the Constitution or laws of the United States or of any State.

c. Conditions that could mitigate security concerns include:

(1) The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these.

(2) The individual's involvement was only with the lawful or humanitarian aspects of such an organization.

(3) Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest.

(4) The involvement or association with such activities occurred under such unusual circumstances, or so much times has elapsed, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or loyalty.

I–4. Guideline B: Foreign Influence

a. Concern. Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;

(2) Connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information;

(3) Counterintelligence information, that may be classified, indicates that the individual's access to protected information may involve unacceptable risk to national security;

(4) Sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion;

(5) A substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could subject the individual to heightened risk of foreign influence or exploitation;

(6) Failure to report, when required, association with a foreign national;

(7) Unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service;

(8) Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or coercion;

(9) Conduct, especially while traveling outside the United States, which may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

c. Conditions that could mitigate security concerns include:

(1) The nature of the relationships with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization, or government and the interests of the United States.

(2) There is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the United States, that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest.

(3) Contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation.

(4) The foreign contacts and activities are on U.S. Government business or are approved by the cognizant security authority.

(5) The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons, groups, or organizations from a foreign country.

(6) The value or routine nature of the foreign business, financial, or property interests is such that it is unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

I–5. Guideline C: Foreign Preference

a. Concern. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Exercise of any right, privilege, or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes but is not limited to:

(a) Possession of a current foreign passport.

(b) Military service or a willingness to bear arms for a foreign country.

(c) Accepting educational, medical, retirement, social welfare, or other such benefits from a foreign country.

(d) Residence in a foreign country to meet citizenship requirements.

(e) Using foreign citizenship to protect financial or business interests in another country.

(f) Seeking or holding political office in a foreign country.

(g) Voting in a foreign election.

(2) Action to acquire or obtain recognition of a foreign citizenship by an American citizen;

(3) Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of a foreign person, group, organization, or government in conflict with the national security interest;

(4) Any statement or action that shows allegiance to a country other than the United States: for example, declaration of intent to renounce U.S. citizenship; renunciation of U.S. citizenship.

c. Conditions that could mitigate security concerns include:

(1) Dual citizenship is based solely on parents' citizenship or birth in a foreign country.

(2) The individual has expressed a willingness to renounce dual citizenship.

(3) Exercise of the rights, privileges, or obligations of foreign citizenship occurred before the individual became a U.S. citizen or when the individual was a minor.

(4) Use of a foreign passport is approved by the cognizant security authority.

(5) The passport has been destroyed, surrendered to the cognizant security authority, or otherwise invalidated.

(6) The vote in a foreign election was encouraged by the U.S. Government.

I–6. Guideline D: Sexual Behavior

a. The concern. Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information. No adverse inference concerning the standards in the Guideline may be raised solely on the basis of the sexual orientation of the individual.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Sexual behavior of a criminal nature, whether or not the individual has been prosecuted.

(2) A pattern of compulsive, self-destructive, or high-risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder.

(3) Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress.

(4) Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

c. Conditions that could mitigate security concerns include:

(1) The behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature.

(2) The sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment.

(3) The behavior no longer serves as a basis for coercion, exploitation, or duress.

(4) The sexual behavior is strictly private, consensual, and discreet.

I–7. Guideline E: Personal Conduct

a. The concern. Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance eligibility process or any other failure to cooperate with the security clearance eligibility process. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(1) Refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation.

(2) Refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security clearance or trustworthiness determination.

b. Conditions that could raise a security concern and may be disqualifying also include:

(1) Deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(2) Deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official Government representative;

(3) Credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;

(4) Credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply

with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(a) Untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other Government protected information.

(b) Disruptive, violent, or other inappropriate behavior in the workplace.

(c) A pattern of dishonesty or rule violations.

(d) Evidence of significant misuse of Government or other employer's time or resources.

(5) Personal conduct or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

(6) Violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

(7) Association with persons involved in criminal activity.

c. Conditions that could mitigate security concerns include:

(1) The individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts.

(2) The refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance eligibility process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully.

(3) The offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

(4) The individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

(5) The individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

(6) The information was unsubstantiated or from a source of questionable reliability.

(7) Association with persons involved in criminal activities has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

I–8. Guideline F: Financial Considerations

a. The concern. Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Inability or unwillingness to satisfy debts.

(2) Indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.

(3) A history of not meeting financial obligations.

(4) Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust.

(5) Consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis.

(6) Financial problems that are linked to drug abuse, alcoholism, gambling problems, or other issues of security concern.

(7) Failure to file annual Federal, state, or local income tax returns as required or the fraudulent filing of the same.

(8) Unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by subject's known legal sources of income.

(9) Compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, "chasing losses" (that is, increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay gambling debts, family conflict, or other problems caused by gambling.

c. Conditions that could mitigate security concerns include:

(1) The behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment.

(2) The conditions that resulted in the financial problem were largely beyond the person's control (for example, loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation), and the individual acted responsibly under the circumstances.

(3) The person has received or is receiving counseling for the problem and/or there are clear indications that the problem is being resolved or is under control.

(4) The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

(5) The individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue.

(6) The affluence resulted from a legal source of income.

I–9. Guideline G: Alcohol consumption

a. The concern. Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent.

(2) Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent.

(3) Habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed as an alcohol abuser or alcohol dependent.

(4) Diagnosis by a duly qualified medical professional (for example, physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence.

(5) Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

(6) Relapse after diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program.

(7) Failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

c. Conditions that could mitigate security concerns include:

(1) So much time has passed, or the behavior was so infrequent, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment.

(2) The individual acknowledges his or her alcoholism or issues of alcohol abuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence (if alcohol dependent) or responsible use (if an alcohol abuser).

(3) The individual is a current employee who is participating in a counseling or treatment program, has no history of previous treatment and relapse, and is making satisfactory progress.

(4) The individual has successfully completed inpatient or outpatient counseling or rehabilitation along with any required aftercare, has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations, such as participation in meetings of Alcoholics Anonymous or a similar organization and has received a favorable prognosis by a duly qualified medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

I–10. Guideline H: Drug Involvement

a. The concern. Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.

(1) Drugs are defined as mood and behavior altering substances, and include:

(a) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (for example, marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(b) Inhalants and other similar substances.

(2) Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Any drug abuse (see above definition).

(2) Testing positive for illegal drug use.

(3) Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia.

(4) Diagnosis by a duly qualified medical professional (for example, physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence.

(5) Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program.

(6) Failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional.

(7) Any illegal drug use after being granted security clearance eligibility.

(8) Expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

c. Conditions that could mitigate security concerns include:

(1) The behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment.

(2) A demonstrated intent not to abuse any drugs in the future, such as:

(a) Dissociation from drug-using associates and contacts.

(b) Changing or avoiding the environment where drugs were used.

(c) An appropriate period of abstinence.

(d) A signed statement of intent with automatic revocation of clearance for any violation.

(3) Abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed, and abuse has since ended.

(4) Satisfactory completion of a prescribed drug treatment program, including but not limited to rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a duly qualified medical professional.

I–11. Guideline I: Psychological Conditions

a. The concern. Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional (for example, clinical psychologist or psychiatrist) employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the standards in this guideline may be raised solely on the basis of seeking mental health counseling.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Behavior that casts doubt on an individual's judgment, reliability, or trustworthiness that is not covered under any other guideline, including but not limited to emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior.

(2) An opinion by a duly qualified mental health professional that the individual has a condition not covered under any other guideline that may impair judgment, reliability, or trustworthiness.

(3) The individual has failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition (for example, failure to take prescribed medication).

c. Conditions that could mitigate security concerns include:

(1) The identified condition is readily controllable with treatment, and the individual has demonstrated ongoing and consistent compliance with the treatment plan.

(2) The individual has voluntarily entered a counseling or treatment program for a condition that is amenable to treatment, and the individual is currently receiving counseling or treatment with a favorable prognosis by a duly qualified mental health professional.

(3) Recent opinion by a duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government that an individual's previous condition is under control or in remission, and has a low probability of recurrence or exacerbation.

(4) The past emotional instability was a temporary condition (for example, one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual no longer shows indications of emotional instability.

(5) There is no indication of a current problem.

I–12. Guideline J: Criminal Conduct

a. The concern. Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules, and regulations.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) A single serious crime or multiple lesser offenses.

(2) Discharge or dismissal from the Armed Forces under dishonorable conditions.

(3) Allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted, or convicted.

(4) Individual is currently on parole or probation.

(5) Violation of parole or probation, or failure to complete a court-mandated rehabilitation program.

c. Conditions that could mitigate security concerns include:

(1) So much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

(2) The person was pressured or coerced into committing the act and those pressures are no longer present in the person's life.

(3) Evidence that the person did not commit the offense.

(4) There is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement.

I–13. Guideline K: Handling Protected Information

a. The concern. Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences.

(2) Collecting or storing classified or other protected information in any unauthorized location.

(3) Loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, game board, handheld, "palm" or pocket device or other adjunct equipment.

(4) Inappropriate efforts to obtain or view classified or other protected information outside one's need to know.

(5) Copying classified or other protected information in a manner designed to conceal or remove classification or other document control markings.

(6) Viewing or downloading information from a secure system when the information is beyond the individual's need to know.

(7) Any failure to comply with rules for the protection of classified or other sensitive information.

(8) Negligence or lax security habits that persist despite counseling by management.

(9) Failure to comply with rules or regulations that results in damage to the National Security, regardless of whether it was deliberate or negligent.

c. Conditions that could mitigate security concerns include:

(1) So much time has elapsed since the behavior, or it happened so infrequently or under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment.

(2) The individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

(3) The security violations were due to improper or inadequate training.

I–14. Guideline L: Outside Activities

a. The concern. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Any employment or service, whether compensated or volunteer, with:

(a) The government of a foreign country.

(b) Any foreign national, organization, or other entity.

(c) A representative of any foreign interest.

(d) Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology;

(2) Failure to report or fully disclose an outside activity when this is required.

c. Conditions that could mitigate security concerns include:

(1) Evaluation of the outside employment or activity by the appropriate security or counterintelligence office indicates that it does not pose a conflict with an individual's security responsibilities or with the national security interests of the United States.

(2) The individual terminates the employment or discontinued the activity upon being notified that it was in conflict with their security responsibilities.

I–15. Guideline M: Use of Information Technology Systems

a. Concern. Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information technology systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

b. Conditions that could raise a security concern and may be disqualifying include:

(1) Illegal or unauthorized entry into any information technology system or component thereof.

(2) Illegal or unauthorized modification, destruction, manipulation, or denial of access to information, software, firmware, or hardware in an information technology system.

(3) Use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system.

(4) Downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system.

(5) Unauthorized use of a Government or other information technology system.

(6) Introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines, or regulations.

(7) Negligence or lax security habits in handling information technology that persist despite counseling by management.

(8) Any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

c. Conditions that could mitigate security concerns include:

(1) So much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

(2) The misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available.

(3) The conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

Appendix J
Overseas Investigations

J–1. Purpose

The purpose of this appendix is to establish, within the framework of this regulation, DODD 5105.42 and DIS 20–1–M, standardized procedures for the military investigative agencies to follow when they perform administrative and investigative functions on behalf of DIS at overseas locations.

J–2. Type investigation

This regulation describes in detail background investigations (BIs) which are conducted for limited access authorizations and those special investigative inquiries conducted for postadjudicative purposes. Hereafter they are referred to as LAA and postadjudicative cases and are briefly described in paragraphs *a* and *b*, below:

a. Limited access authorization. A level of access to classified defense information that may be granted to a non-U.S. citizen under certain conditions, one of which is that a BI must have been completed with satisfactory results. Paragraph 3–403 further describes LAA cases.

b. Postadjudication investigation. A PSI predicated on new, adverse, or questionable security, suitability or hostage information that arises and requires the application of investigation procedures subsequent to adjudicative action on a DOD-affiliated person's eligibility for continued access to classified information, assignment to or retention in sensitive duties or other designated duties requiring such investigation. While these cases are normally predicated on the surfacing of unfavorable information subsequent to favorable adjudication, they may also be opened when favorable information is offered to counter a previous unfavorable adjudication. Paragraph 2–17*c* further describes these cases.

J–3. General

a. As a rule, investigative activity in most PSIs occurs in the United States even when the subject is at an overseas location. Therefore, the submission of requests for investigation to the PIC at Baltimore is a required procedure as it ensures uniform application of DOD PSI policy and the efficient dispatch and coordination of leads.

b. When the purpose of the investigation is for an LAA or postadjudication on a subject overseas, much, if not all of the leads are at an overseas location. While these cases also may be submitted directly to PIC for action, there is an inherent delay in the mailing of the request, the exchange of leads and reports with PIC, and transmittal of the reports back to the requester. To avoid this delay, the military investigative agencies, when acting for DIS overseas in accordance with DODD 5105.42 may, with their headquarters approval, accept these requests for investigations, initiate them and disseminate the results from the same level as they open, close, and disseminate their own cases. Usually this will greatly improve response time to the requester.

c. Under the procedures in paragraph *b*, above, DIS will not often be in a position to directly exercise its responsibility for control and direction until the case or lead is in progress or even completed; therefore, adherence to the policy stated in referenced documents, and as modified herein, is mandatory. When the policy of the military investigative agency is at variance with the above, the matter will be referred to the respective headquarters for resolution.

d. Since DIS is ultimately responsible for the personnel security product, it must be kept informed of all such matters referred to in this appendix. For instance, when the investigative agency overseas receives a DD Form 1879 (Request for Personnel Security Investigation), which sets forth an issue outside DIS jurisdiction, it will reject the request, inform the requester of the reason and furnish an information copy of the DD Form 1879 and rejection letter to PIC. When the issue/jurisdiction is unclear to the investigative agency, the DD Form 1879 and the perceived jurisdictional question should be promptly forwarded to DIS for action and, if appropriate, to the Component's headquarters for information. Questions on the interpretation of DIS or DOD policy and directives pertaining to individual PSI cases can usually be resolved through direct communications with PIC.

e. DODD 5105.42, establishes the supporting relationship of the military investigative agencies to DIS in overseas areas, and DIS provides these agencies with copies of relevant policy and interpretive guidance. For these reasons, the investigative agency vice the requester, is responsible for evaluating the request, processing it, collecting and evaluating the results within their jurisdiction for sufficiency, and forwarding the completed product to the appropriate activity.

f. The magnitude of operations at PIC requires that methods of handling LAA and postadjudicative cases be consistent to the maximum extent possible. For this reason, the procedures for LAA cases are nearly identical to those for postadjudicative cases. Briefly, the main exceptions are:

(1) The notification to PIC that a postadjudication case has been opened will be by message, since an issue is present at the outset, whereas notification of an LAA case should normally be by mail.

(2) The scope of the LAA investigation is 10 years or since the person's 18th birthday, whichever is shortest, whereas the leads in a postadjudication case are limited to resolving the issue.

J–4. Jurisdiction

a. As set forth in DODD 5105.42, DIS is responsible for conducting all DOD PSIs in the 50 States, District of Columbia, and Puerto Rico, and will request the military departments to accomplish investigative requirements elsewhere. The military investigative agencies in overseas locations routinely respond to personnel security investigative leads for DIS.

b. The DIS jurisdiction also includes investigation of subversive affiliations, suitability information, and hostage situations when such inquiries are required for personnel security purposes; however, jurisdiction will rest with the military investigative agencies, FBI and/or civil authorities as appropriate when the alleged subversion or suitability issue represents a violation of law or, in the case of a hostage situation, there is an indication that the person concerned is actually being pressured, coerced, or influenced by interests inimical to the United States, or that hostile intelligence is taking action specifically directed against that person. Specific policy guidance on the applicability of these procedures and the jurisdictional considerations are stated in chapter II, section 4.

J–5. Case opening

a. A request for investigation must be submitted by using DD Form 1879 and accompanied by supporting documentation unless such documentation is not immediately available, or the obtaining of documentation would compromise a sensitive investigation. Upon receipt of the request, the military investigative component will identify the issue(s), scope the leads, and ensure that the proposed action is that which is authorized for DIS as delineated in this regulation, DODD 5105.42, and DIS 20–1–M.

b. Upon such determination, the component will prepare an ALS which fully identifies the subject and the scope of the case, and specifies precisely the leads which each investigative component (including DIS/PIC when appropriate) is to conduct.

c. Case-opening procedures described above are identical for LAA and postadjudication cases except with respect to notification of case opening to PIC:

(1) *Postadjudication cases.* These cases, because they involve an issue, are potentially sensitive and must be examined as early as possible by PIC for conformity to the latest DOD policy. Accordingly, the initial notification to PIC of case openings will always be by message. The message will contain at a minimum:

(a) Full identification of the subject;

(b) A narrative describing the allegation/facts in sufficient detail to support opening of the case; and

(c) A brief listing of the leads that are planned. The DD Form 1879 and supporting documents, along with the agency's ALS, should be subsequently mailed to PIC.

(2) *Limited access authorization cases.* The notification to PIC of case opening will normally be accomplished by mailing the DD Form 1879, DD Form 398 (Personal History Statement), a copy of the ALS, and any other supporting documents to PIC. Message notification to PIC in LAA cases will only be required if there is a security or suitability issue apparent in the DD Form 1879 or supporting documents.

d. Beyond initial actions necessary to test allegation for investigative merit and jurisdiction, no further investigative action should commence until the notification of case opening to PIC has been dispatched.

e. The PIC will promptly respond to the notification of case opening by mail or message specifying any qualifying remarks along with a summary of previously existing data. PIC will also provide a DIS case control number (CCN). This number must be used by all Components on all case-related paperwork/reports.
(The investigating agency may assign its unique service CCN for interim internal control; however, the case will be processed, referenced, and entered into the DCII by the DIS case control number.) The first five digits of the DIS CCN will be the Julian date of the case opening when received at DIS.

J–6. Case processing

a. The expected completion time for leads in LAA cases is 50 calendar days and for postadjudication cases, 30 days, as computed from the date of receipt of the request. If conditions preclude completion in this time period, a pending report of the results to date, along with an estimated date of completion will be submitted to PIC.

b. Copies of all ALSs will be furnished to PIC. In addition, PIC will be promptly notified of any significant change in the scope of the case, or the development of an investigative issue.

c. The procedures for implementing the Privacy Act in PSI cases are set in DIS 20–1–M. Any other restrictions on the release of information imposed by an overseas source or by regulations of the country where the inquiry takes place will be clearly stated in the report.

d. The report format for these cases will be that used by the military investigative agency.

e. Investigative action outside the jurisdictional area of an investigative Component office may be directed elsewhere by ALS as needed in accordance with that agency's procedures and within the following geographical considerations:

(1) Leads will be sent to PIC if the investigative action is in the United States, District of Columbia, Puerto Rico, American Samoa, The Bahamas, the U.S. Virgin Islands, and the following islands in the Pacific: Wake, Midway, Kwajalin, Johnston, Carolines, Marshalls, and Eniwetok.

(2) Leads to areas not listed above may be dispatched to other units of the investigative agency or even to another military agency's field units if there is an agreement or memorandum of understanding that provides for such action. For case accountability purposes, copies of such "lateral" leads must be sent to the PIC.

(3) Leads that cannot be dispatched as described in paragraph (2), above, and those that must be sent to a non-DOD investigative agency should be sent to PIC for disposition.

f. The DIS 20–1–M calls for obtaining PIC approval before conducting a subject interview on a postadjudicative investigation. To avoid the delay that compliance with this procedure would create, a military investigative component may conduct the interview provided:

(1) All other investigative leads have been completed and reviewed.

(2) The CCN has been received, signifying DIS concurrence with the appropriateness of the investigation.

(3) Contrary instructions have not been received from the PIC.

(4) The interview is limited to the resolution of the relevant issues disclosed by the investigation.

g. Notwithstanding the provisions of paragraphs *f*(1) through (4), above, if time is of the essence due to imminent transfer of the subject, a subject interview may be conducted at the discretion of the investigative agency.

J–7. Case responsibility limited access authorization and PA

Paragraph **J**–3, above, describes the advantages of timely handling which accrue when the military investigative Components act for DIS overseas. These actions for DIS may, however, be limited by the component's staffing and resource limitations, especially since some cases require more administration and management than others. Postadjudication case leads, for instance, will normally be within the geographical jurisdiction of the component that accepted the request for investigation; therefore, relatively little case management is required. In contrast, LAA cases may require leads worldwide, and, therefore, create more complex case management and administration, especially in the tracking, monitoring and reviewing of leads outside the component's geographical area. Accordingly, an investigative component will accept the case from the requester, but only assign itself the appropriate leads within its own geographical jurisdiction and send the balance to PIC for appropriate disposition in accordance with the following:

a. The investigative agency will accept the request for investigation (thereby saving time otherwise lost in mailing to PIC) but limit its involvement in case management by extracting only those leads it will conduct or manage locally.

b. The agency should then prepare an ALS that shows clearly what leads it will cover and send PIC a copy of this

ALS, along with the request for investigation and any other appropriate documentation. It must be clear in the ALS that PIC is to act on all those leads that the unit has not assigned to itself.

c. PIC, as case manager, will assume responsibility for the complete investigative package and, upon receipt of the last lead, will send the results to the appropriate activity.

d. The agency that accepted the case and assigned itself leads may send a copy of its report to the activity in the "Results to" block at the same time it sends the originals to PIC. If so, the letter of transmittal must inform the recipient that these reports are only a portion of the investigation, and that the balance will be forthcoming from PIC. Similarly, PIC must be informed of which investigative reports were disseminated. (This is normally done by sending PIC a copy of the letter of transmittal.)

J–8. Scope

a. Limited access authorization. The scope of investigation is 10 years or from age 18, whichever is the shortest period.

b. Postadjudication cases. There is no standard scope. The inquiries conducted will be limited to those necessary to resolve the issue(s).

J–9. Case closing: limited access authorization and PA

a. Whether the investigative component or PIC closes out an investigation, there are three key elements to consider:

(1) The investigative results must be reviewed for quality and conformance to policy.

(2) The results must be sent to the activity listed in the "Results to" block of the DD Form 1879.

(3) PIC must be informed whether or not any dissemination was made by the investigative agency and, if so, what reports were furnished.

b. Investigative results may also be sent to a requester or higher level activity that makes a statement of need for the results. In such instances, a copy of the letter requesting the results and the corresponding letter of transmittal must be sent to PIC for retention.

c. When an investigative agency disseminates reports for PIC, it may use the transmittal documents, letters, or cover sheets it customarily uses for its own cases.

d. The material that is to be provided to PIC will consist of: The originals of all reports, and all other case documentation such as original statements, confidential source sheets, interview logs, requests for investigation, letters of transmittal to adjudicators/requesters, or communications with the requester, such as those that modify the scope of the investigation.

e. For DIS to fulfill its responsibilities under DOD 5220.22–R **(AR 380–49)** and the Privacy Act of 1974, all inquiries conducted in its behalf must be set forth in a Report of Investigation for the permanent file, whether the case is completed, terminated early, or referred to another agency.

J–10. Referral

A case may require premature closing at any time after receipt of the DD Form 1879 by the investigative Component if the information accompanying the request, or that which is later developed, is outside DIS jurisdiction. For example, alleged violations of law, a counterintelligence matter, or actual coercion/influence in a hostage situation (see para**J–**4*b* above) must be referred to the appropriate agency, and DIS involvement terminated. The requester will be informed by letter or endorsement to the DD Form 1879 of the information developed that, due to jurisdictional consideration, the case was referred to (fill in appropriate address) and that the DIS case is closed. The agency to which referral was made and PIC will be furnished with the results of all investigations conducted under DIS auspices. DIS, however, has an interest in the referral agency's actions and no information should be solicited from that agency.

Appendix K
ADP Position Categories and Criteria for Designating Positions

OMB Circular A–71 (and Transmittal Memo #1), July 1978, OMB Circular A–130, December 12, 1985 , and FPM Letter 732, November 14, 1978 contain the criteria for designating positions under the existing categories used in the personnel security program for Federal civilian employees as well as the criteria for designating ADP and ADP-related positions. This policy is outlined below:

K–1. Automated data processing position categories

a. Critical-sensitive positions (ADP–I positions).. Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

b. Noncritical-sensitive positions (ADP–II positions.) Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP–I category to ensure the integrity of the system.

c. Nonsensitive positions (ADP–III positions.) All other positions involved in computer activities.

In establishing the categories of positions, other factors may enter into the determination, permitting placement in higher or lower categories based on the agency's judgment as to the unique characteristics of the system or the safeguards protecting the system.

K–2. Criteria for designating positions

Three categories have been established for designating computer and computer-related positions—ADP–I, ADP–II, and ADP– III. Specific criteria for assigning positions to one of these categories are as follows:

a. ADP–I.

(1) Responsibility for the development and administration of agency computer security programs, including direction and control of risk analysis and/or threat assessment.

(2) Significant involvement in life-critical or mission-critical systems.

(3) Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.

(4) Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the ADP–I category to ensure the integrity of the system.

(5) Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

(6) Other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

b. ADP–II. Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP–I category, includes, but is not limited to:

(1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

(2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year. Other positions are designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP–I positions.

c. ADP–III. All other positions involved in Federal computer activities.

Appendix L
Defense Security Briefing Provided U.S. Government Employees Traveling to Communist-Controlled Countries

L–1. Introduction

All U.S. Government employees, regardless of position or assignment, are likely to be of interest to intelligence services of communist-controlled countries. Hostile intelligence networks make it their business to learn the identities of Americans, and frequently try to target them for intelligence approaches when they travel abroad. The approach may be direct or indirect, highly sophisticated or crudely obvious. In any case, U.S. personnel traveling to communist-controlled countries should be constantly alert to the problems that can befall them. The purpose of this briefing is to make employees aware of pitfalls associated with such travel, and to advise them on defensive measures against hostile intelligence exploitation.

L–2. Before departure

a. **The Bureau of Consular Affairs, U.S. Department of State, frequently publishes advisory material on current travel conditions in communist-controlled countries. This material should be available through your agency, and you should carefully review any such information covering a country you will be visiting. It is especially important that you are aware of the items that you may or may not take into a country.**

b. **Visa applications are routinely scrutinized by intelligence services of communist-controlled countries. To avoid difficulties in this area, it is important that you complete the forms truthfully and accurately. It is especially important that you name any relatives that you intend to visit in the host country.**

c. **When obtaining visas, ask the appropriate consular officer how much foreign currency (United States and other) and what valuables you may take into and out of the communist country or countries to be visited. Make**

sure you have enough money for the trip, and strictly follow the approved itinerary. You may not import local currency into a country you will be visiting.

d. **If you are a naturalized American citizen of East European origin, please note that there have been instances in which an East European country has not recognized the U.S. citizenship of former nationals and has taken the position that such persons retain their original nationality and are therefore subject to treatment as citizens of that country upon reentry into its jurisdiction. If this situation applies to you, consult first with the U.S. Department of State for advice and clarification of your status.**

e. **You may wish to carry with you gifts for friends or relatives. Such gifts should be neither controversial nor prohibited. Do not bring pornography, narcotics, or political material. Communist pornography laws are more strict than those in the United States, and you should avoid taking with you magazines or other materials that might be considered pornographic. Any patent medicines or prescription drugs should be clearly for your own use and in quantities reasonable enough to convince authorities that they are for your personal consumption.**

f. **Do not carry with you, on behalf of a third party, any letters, messages, or packages for private individuals in Communist countries. You may be deemed guilty of circumventing normal channels of communication, or you may be regarded as a courier for illegal or subversive purposes.**

g. **Carry only essential forms of identification. Leave Government badges, building passes, and so forth, at home. Write down your passport number and keep it separate from your passport. Do the same with the address and telephone number of the American Embassy.**

h. **DO NOT TAKE THIS DOCUMENT WITH YOU| Study, think about, and remember its warnings during your visit, but leave the document at home.**

L–3. Upon arrival

a. **Rules governing declaration of valuables and currency and those relating to transactions are strictly enforced. Make an accurate declaration at entry of all money and valuables, including travelers checks. Some countries give the traveler a copy of the declaration, which must be surrendered upon leaving. It is important to keep receipts of all money changes, as these are frequently requested upon departure. Undeclared sums of U.S. or other currency are most likely to cause difficulty with authorities and may be confiscated upon departure.**

b. **You will generally be permitted to take in such items as cameras, transistor radios, and so forth. It is wise to declare such items as you enter, however, to preclude possible explanations, customs charges, or confiscations when you leave. Baggage inspections may be extremely thorough or only perfunctory. On occasion, your baggage may not even be opened at entry.**

c. **As soon as possible after arrival, you should contact the American Embassy or consulate, either by telephone or in person, and provide your local address and the probable length of your visit.**

d. **It is unwise for you to drive in a communist country. Try to use public transportation or hire a driver, as local traffic regulations may be confusing. There have been incidents when traffic accidents were deliberately provoked to incriminate or embarrass a visitor.**

L–4. Activities while in communist countries

a. **Assume that your hotel room is equipped with devices to overhear or record your conversations. There may be devices installed through which you can be physically observed, even while your room is in darkness. In addition to the usual microphones, telephone tapes, miniature recording devices, and so forth, intelligence operatives today use infrared cameras, infrared "snooper-scopes" and optical lenses, closed-circuit TV, and other highly advanced equipment. Do not search for such devices, and do not make an issue of it if you should by chance find one. The presence of such equipment may not necessarily concern you. A device may or may not be monitored during your visit, or it may be monitored only on a "spot check" basis. Do not try to neutralize such a device by running tap water, playing your radio, and so forth. Some modern devices are so sophisticated that they cannot be neutralized. Efforts to combat such penetration will only make the intelligence service more suspicious of you. The best defense against such devices is to keep your conversations light and uninformative. IMPORTANT: Should you discover any device of the above kind, take no overt action against it. Continue your normal conversation, giving no indication of your discovery, and report your findings to the American Embassy or consulate or to your security officer upon your return.**

b. **Beyond your hotel room, you should assume that conversations in vehicles (including Embassy vehicles), train compartments, restaurants, conference rooms, and other public places may be monitored. Miniature microphones with transmitters or recorders can easily be secreted on the person of an individual in your group. It is even technically possible to record your conversations in open, outdoor areas; however, those areas are normally more secure than indoor locations.**

c. **Avoid unnecessary discussions of your job, your workplace, and other official matters. Also avoid discussing other U.S. employees' habits, character, or other matters that reveal weaknesses or idiosyncrasies.**

d. **Assume that your personal luggage will be searched at some time in your hotel room. If you discover evidence of this, do not make a big issue of it. You should, however, report positive evidence of such activity to**

the American Embassy and to your security officer upon your return. It is just as well not to bother locking your luggage since most locks will be readily picked. Locked luggage will only increase the curiosity of the intelligence agent and the lock may be broken. Never leave unattended luggage containing valuable papers or documents you do not wish anyone else to read. If you surprise someone searching your possessions, don't take any violent or physical action, but report the incident to local and U.S. authorities.

e. **You may receive a "wrong number" or otherwise mysterious telephone call in the hotel room at any hour. Do not let this unduly upset you. It may be a crude but effective method of determining whether you are in your room, or it may be only a result of poor telephone service.**

f. **Do not rely on hotel employees for protection service. Assume that they, as well as restaurant employees, are in the employ of the intelligence services. Be particularly circumspect in your relations with guides, interpreters, and Communist travel agency personnel, since these people are invariably used by intelligence agencies.**

g. **You may be under physical surveillance when you travel, whether on foot or in a vehicle. Or you may suspect you are being observed when actually you are not. In either event, the best tactic is to ignore it. Communist intelligence agents at various times observe visitors on a spot check basis for no apparent reason. On the other hand, they may be collecting detailed data concerning your activities in preparation for a more direct intelligence approach. Do not attempt to lose surveillance agents. If you are actually being followed for intelligence objectives, you will be covered by a team of several agents, and your evasion attempts will make them more suspicious.**

h. **You will be permitted to take photographs with your personal camera, but be careful not to photograph restricted areas. You should not take photographs from aircraft, or of military and police installations and personnel, industrial structures, harbors, rail and airport facilities, and border areas. Communist officials also resent your photographing items that put them in a bad light, such as slum areas, public drunks, scenes of civil disorder, or public disturbances. If you do take such photographs, your film may be confiscated.**

i. **Be particularly circumspect in approaches from persons offering social companionship, especially of a sexual nature. Many of these persons are"plants" from communist intelligence agencies and will attempt to entice you into a compromising situation, which they can use to blackmail you to force your cooperation in intelligence activities. Under no circumstances should you seek or accept this kind of companionship in a communist country. The intelligence services will capitalize immediately on any indication of immoral or indiscreet behavior of American travelers. Even when failing to detect a vulnerability, communist agents have attempted to entrap innocent travelers. For this reason, you should maintain the highest level of personal behavior at all times, avoid long walks at night alone, and endeavor always to be in the company of someone you can trust. Be especially careful not to drink too heavily so as not to weaken your defense or lose your self-control.**

j. **Do not accept from anyone (including friends, relatives, or professional contacts) letters, photographs, packages, or any other material to be smuggled out of the country or carried in your effects when you depart. Be firm in your denials in these matters, since such requests may be acts of intelligence agents seeking to entrap you.**

k. **Bear in mind that there are many political, cultural, and legal differences between the United States and Communist countries. Actions that are innocent or, at worst, carry wrist-slapping penalties in the United States, are often considered serious offenses against the law in communist-dominated societies. Persons violating the law, even unknowingly, run the risk of arrest or expulsion. Do not, for instance, take "souvenirs" from hotels or institutions, however insignificant in value they may appear.**

l. **Do not engage in any private currency transactions with individual citizens. Do not try to sell or trade any personal item, including clothing, which you have brought into the country, or purchase bargains from street peddlers or questionable vendors. Do not engage in black-market activities. Many communist countries have laws governing exportation of artwork and historic relics. Be familiar with these laws if you intend to purchase such items, and make these purchases only at official establishments.**

m. **Should you be detained or arrested for any reason by police or other officials of these countries, be cooperative, but insist politely and repeatedly, if necessary, that the American Embassy or consulate be notified promptly. Do not make any statements or sign any documents that you do not fully understand until you have had an opportunity to confer with an Embassy representative. You may possibly be accused of having some connection with an American intelligence service or of having accepted an assignment from such service to be carried out in the host country. You should make no admission that you had any dealings, under any circumstances, with any U.S. intelligence agency.**

n. **Mail you receive or send in a communist country is subject to censorship. In any correspondence before, during, or after your visit, make no reference to classified information nor reveal information of possible value to a hostile intelligence service. Be careful in writing to or about relatives or friends in these countries, since they may become targets for investigation or exploitation.**

o. **There have been several incidents in communist countries wherein speech-inducing drugs, medicines, and**

so forth, have been used to aid in interrogation. In nonemergency situations, make every effort to avoid communist hospitals or medical facilities without first notifying the American Embassy or consulate.

p. **Report immediately any attempt to pressure or compromise you, or any action that might lead to such pressure or compromise, to the American Embassy security officer in the country being visited. Report to your security manager immediately if you have unusual subsequent contacts with nationals of a communist country.**

L–5. Conclusion

This briefing covers many, but not necessarily all, pitfalls that an American traveler may encounter. New espionage techniques and tactics are constantly being developed, and you should always be alert for them. Although the techniques employed by communist countries' intelligence services may seem farfetched or taken from spy novels, they are in fact used in day-to-day activities and operations. American travelers must recognize that these techniques; however distasteful, are part of the communist system and be prepared to counter them. The pitfalls outlined above reflect possibilities, not probabilities, however. You probably will not have any problems if you respect local laws and customs, act honestly in your dealings, and behave discreetly. You can expect friendly treatment from most of the citizens you meet, and you will find that they are very interested in all aspects of American life. You can therefore serve as a valuable goodwill ambassador for the United States while you are traveling in communist countries. Be open to this experience, have a good trip, and come home safely.

Appendix M
Internal Control Evaluation

M–1. Function

The function covered by this evaluation is the Army Personnel Security Program.

M–2. Purpose

The purpose of this evaluation is to assist commanders and organizations in evaluating key internal controls outlined below. It is not intended to address all internal control elements.

M–3. Instructions

Answers must be based upon the actual testing of key internal controls (for example, document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and the corrective action indicated in the supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

M–4. Test questions

a. Are Security Managers appointed in writing?

b. Is personal identifiable information protected in accordance with AR 340-21?

c. Has a Joint Personnel Adjudication System Account been established for Security Managers, email addresses current, and security management office owning/servicing relationships in the JPAS reviewed/updated annually?

d. Are classified reports stored in accordance with AR 380-381 and AR 380-5?

e. When transported, are reports of personnel security information sealed in double envelopes when transmitted by mail or when carried by persons and the package labeled "TO BE OPENED ONLY BY OFFICIALS DESIGNATED TO RECEIVE REPORTS OF PERSONNEL SECURITY INVESTIGATION" noted on the package?

f. Is the DCS, G-2 monitoring, evaluating, and reporting on the administration of the Army Personnel Security Program?

g. Did the commander establish written local security policies and procedures?

h. Has the commander established a self inspection security program for his or her headquarters and subordinate programs?

i. Does the security manager advise, update, and communicate with the commander to ensure matters related to security clearance actions are presented for a final decision?

j. Do security managers promptly and appropriately report security incidents, violations, and compromises, related to classified and sensitive information, as directed by AR 380-5 to the commander?

k. Does the security manager adhered to deadlines and provide consultation to personnel who receive a letter of intent or statement of reason on the seriousness of the action; provide support to such persons to ensure due process is afforded?

l. Are personnel submitted for periodic reviews in a timely manner?

m. Are security managers trained?

n. Have supervisors ensured that subordinate personnel are trained in, understand, and follow requirements of this regulation, local command policy, and procedures concerning the Personnel Security Program?

o. Has the commander established annual security training for personnel having continued access to classified information?

p. Has the commander ensured personnel security investigations are initiated through the Personnel Security Investigation Center of Excellence as authorized?

q. Has the commander ensured prior to indoctrination, conduct initial security briefings, educating personnel on their security responsibilities?

r. Has the commander ensured supervisors are familiar with special responsibilities in matters pertaining to indicators that may signal matters of personnel security concern and reinforce the requirements for self, supervisor, and command reporting of security incidents via the JPAS?

s. Has the commander ensured personnel holding a security clearance report all foreign travel to the security office?

t. Has the commander immediately documented in writing any unfavorable incidents and made the recommendation on the DA Form 5248–R and subsequently submitted an incident report via the JPAS to the DOD Consolidated Adjudication Facility?

M–5. Supersession

Not applicable.

M–6. Comments

To make this evaluation a more useful tool for internal controls, submit comments to DCS, G-2, 1000 Army Pentagon, Washington, DC 20310-1000.

Glossary

Section I
Abbreviations

ADP
automated data processing

ALS
action lead sheet

ARNG
Army National Guard

BI
background investigation

BVS
Bureau of Vital Statistics

CAP
centralized assignment procedure

CCF
U.S. Army Central Clearance Facility

CIA
Central Intelligence Agency

CMF
career management field

DA
Department of the Army

DASEB
Department of the Army Suitability Evaluation Board

DCII
defense central investigations index

DCID
Defense Criminal Investigative Service

DCS, G–1
Deputy Chief of Staff , G–1

DCS, G–2
Deputy Chief of Staff, G–2

DDPSS
department-determined personnel security status

DIS
Defense Investigative Service

DISCO
Defense Industrial Security Clearance Office

DNACI
DOD National Agency Check and written inquiries

DOE
Department of Energy

DOHA
Defense Office of Hearings and Appeals

DPOB
date and place of birth

DUSD(P)
Deputy Under Secretary of Defense for Policy

ENTNAC
Entrance National Agency Check

FBI
Federal Bureau of Investigation

HQDA
Headquarters, Department of the Army

INS
Immigration and Naturalization Service

IRR
Individual Ready Reserve

LAA
limited access authorization

LAC
local agency check

LCR
listed character reference

LOI
letter of intent

MACOM
major Army command

MOS
military occupational specialty

MPRJ
Military Personnel Records Jacket

MTOE
modification table of organization and equipment

NAC
National Agency Check

NACI
National Agency Check and written inquiries

NAFI
nonappropriated fund instrumentality

NATO
North Atlantic Treaty Organization

NRC
Nuclear Regulatory Commission

NSA
National Security Agency

ODCS, G–1
Officer of the Deputy Chief of Staff, G–1

OJCS
Office of the Joint Chiefs of Staff

OMPF
official military personnel file

OPF
official personnel folder

OPM
Office of Personnel Management

OSS
Office of Strategic Services

PIC
personnel investigation center

PR
periodic reinvestigation

PRP
Personnel Reliability Program

PSAB
Personnel Security Appeals Board

PSI
personnel security investigation

PSQ
personal security questionnaire

ROTC
Reserve Officer Training Corps

SA
Secretary of the Army

SBI
special background investigation

SCI
sensitive compartmented information

SIDPERS
Standard Installation/Division Personnel

SII
special investigative inquiry

SIOP–ESI
Single Integrated Operation Plan–Extra Sensitive Information

SSN
social security number

SSO
special security officer

TAPA
Total Army Personnel Agency

UCMJ
uniform code of military justice

USO
United Services Organization

WHLO, OCSA
White House Liaison Office, Office of the Chief of Staff, Army

Section II
Terms

Access
The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.

Adverse action
A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

Applicant
A person not currently employed by the DA or serving in the Armed Forces, or a person being considered for employment for a sensitive position.

Background investigation
A PSI consisting of both record reviews and interviews with sources of information as prescribed in paragraph B–3, appendix B, this regulation, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

Classified information
Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order 12356 (reference (j)).

Close and continuous relationship
Persons to whom subject is bound by affection or obligation. May include sharing living quarters with an individual even though no intimate relationship exists.

Close foreign ties
Recurring contact, either personal or by correspondence, with foreign nationals residing in a foreign country.

Compelling need
ccess to Sensitive Compartmented information (SCI) is urgently required by an individual to prevent failure or serious impairment of missions or operations that are in the best interest of national security.

Competent medical authority
A board–eligible or board–certified psychiatrist or clinical psychologist employed by or under contract to the U.S. military or U.S. Government.

Defense Central Index of Investigation
An alphabetical index of personal names and impersonal titles that appear as subjects of incidents in investigative documents held by the criminal, counterintelligence, fraud, and personnel security investigative activities of the Defense Investigative Service (DIS), the Defense Criminal Investigative Service (DCIS), and the NSA. DCII records will be checked on all subjects of DOD investigations.

Defense Central Security Index
An automated subsystem of the Defense Central Index of Investigations (DCII) designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all DOD Components for military, civilian, and contractor personnel. The DCSI will serve as the central DOD repository of security–related actions in order to assist DOD security officials in making sound clearance and access determinations. The DCSI shall also serve to provide accurate and reliable statistical data for senior DOD officials, Congressional committees, the General Accounting Office and other authorized Federal requesters.

Denial of security clearance
The refusal to grant a security clearance or to grant a higher level of clearance to a person who possesses a clearance of a lower degree.

Department–determined personnel security status
Information that constitutes a possible basis for taking an adverse or unfavorable personnel security action.

a. Adverse loyalty information (see paras 2–4 a–f, k , and app E, para 3).

b. Adverse suitability information (see paras 2–200 g through j and 2–4 through q and app E, paras 1, 2, 4, 5, and 6).

DOD component
Includes the Office of the Secretary of Defense; the military departments; Organization of the Joint Chiefs of Staff; Directors of Defense Agencies and the United and Specified Commands.

Entrance national agency check
A PSI scoped and conducted in the same manner as a national agency check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

Federal service
Federal service consists of active duty in the military services, Federal civilian employment, membership in the ARNG or U.S. Army Reserve (includes Troop Program Units, Individual Mobilization Augmentee (IMA), and Individual Ready Reserve), membership in the ROTC Scholarship Program, Federal contractor employment with access to classified information under the Industrial Security Program, or a combination thereof, without a break exceeding 12 months.

Head of DOD component
The Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; and the Commanders of Unified and Specified Commands; and the Directors of Defense Agencies.

Immediate family
Includes subject's spouse, parents, brothers, sisters, and children.

Immigrant alien
Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

Interim security clearance
A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

Limited access authorization
Authorization for access to CONFIDENTIAL or SECRET information granted to non–U.S. citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (see app J).

Local records check
A review of local personnel, post military police, medical records, and other security records, as appropriate.

Major Army command (MACOM)
A command directly subordinate to, established by authority of, and specifically designated by HQDA. Army component of Unified and Specified Commands are MACOMs.

Minor derogatory information
Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

National Agency Check
A PSI consisting of a records review of certain national agencies as prescribed in paragraph 1, appendix B, this regulation, including a technical fingerprint search of the files of the FBI.

National Agency Check and written inquiries
A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

DOD National Agency Check and written inquiries
A personnel security investigation conducted by the DIS for access to SECRET information consisting of a NAC, a credit bureau check, and written inquiries to current and former employers (see para B–2, app B), covering a 5–year scope.

National of the United States
A citizen of the United States or a person who, though not a citizen, owes permanent allegiance to the United States. The provisions of this regulation are equally applicable to U.S. citizens and U.S. nationals.

National security
National security means the national defense and foreign relations of the United States.

Need to know
A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official U.S. Government program. Knowledge of, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

Periodic reinvestigation
An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation on persons occupying positions referred to in paragraphs 3–55 through 3–67. The scope will consist of a personal interview, NAC, LACs, credit bureau checks, employment records, employment references and developed character references and will normally not exceed the most recent 5–year period.

Personnel security
The application of standards and criteria to determine whether or not an individual is eligible for access to classified information, qualified for assignment to or retention in sensitive duties, and suitable for acceptance and retention in the total Army consistent with national security interests.

Personnel security investigation
Any investigation required for the purpose of determining the eligibility of DOD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DOD, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see para 2–18) conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to

determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

Polygraph examination
A voluntary examination by qualified examiners using polygraph equipment approved by the DA. (AR 195–6 applies).

Revocation of security clearance
The cancellation of a person's eligibility for access to classified information.

Scope
The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

Security clearance
A determination that a person is eligible under the standards of this regulation for access to classified information.

Senior officer of the Intelligence Community
The DOD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service; Director, Defense Intelligence Agency; DCS, G–2, U.S. Army; Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

Sensitive compartmented information
Classified information concerning or derived from intelligence sources, methods, or analytical processes that must be handled exclusively within formal access control systems established by the DCI. DCID Directive (DCID) 1/14 contains the minimum personnel security standards and procedures governing eligibility for access to SCI.

Sensitive position
Any position so designated within the DOD, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical–sensitive, noncritical–sensitive, or non-sensitive as described in paragraph 3.

Significant derogatory information
Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

Special access program
Any program imposing "need–to–know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, OR TOP SECRET information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of persons determined to have a need to know.

Special background investigation
A PSI consisting of all of the components of a BI plus certain additional investigative requirements as prescribed in paragraph B–4, appendix B, this regulation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

Special investigative inquiry
A supplemental PSI of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination under the provisions of this regulation.

Special geographic area
The assignment location of a person. It is determined by the Commanding General, U.S. Army Human Resources Command with the DCS, G–2.

Service
Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a DOD contractor or as a consultant involving access under the DOD Industrial Security Program. Continuity of service is maintained with change from one status to another

as long as there is no single break in service greater than 12 months. Service for nuclear and chemical surety positions is defined in AR 50–5 and AR 50–6 and in this regulation.

Suspension of access
The temporary withdrawal of a person's eligibility for access to classified information. Access is suspended when information becomes known that casts doubt on whether continued access is consistent with national security interests.

Unfavorable administrative action
Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this regulation.

Unfavorable personnel security determination
A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a special access authorization (including access to SCI); retention, non-appointment to or non-selection for appointment to a sensitive position; retention, non-appointment to or non-selection for any other position requiring a trustworthiness determination under this regulation; reassignment to a position of lesser sensitivity or to a non-sensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

United States citizen
a. Native born. A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Marina Islands; U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is a citizen of the United States).
b. Naturalized. A person born outside of the United States who has completed naturalization procedures and has been given U.S. citizenship by duly constituted authority.
c. Derivative birth. A person born outside the United States who acquires U.S. citizenship at birth because one or both of their parents are U.S. citizens at the time of the person's birth.
d. Derivative naturalization. A person who acquires U.S. citizenship after birth through naturalization of one or both parents.

Section III
Special Abbreviations and Terms
There are no special terms.

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-501

27 JANUARY 2005

Incorporating Through Change 2, 29 November 2012

Security

PERSONNEL SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ USAF/XOFI

Certified by: HQ USAF/XOF (Brig Gen James M. Shamess)

Supersedes: AFI31-501, 1 August 2000

Pages: 127

This instruction implements Air Force Policy Directive (AFPD) 315, *Personnel Security Program Policy*. It provides guidance for personnel security investigations and clearance needs. **Use this instruction with** Department of Defense (DOD) Regulation 5200.2-R, *DOD Personnel Security Program*, January 1987, and Executive Order 12968 "Access to Classified Information."

SUMMARY OF CHANGES

This interim change implements new guideline at **Paragraph 3.16 for processing requests for access by retired general officers of civilian equivalents. A margin bar (|) indicates newly revised material.**

Chapter 1

GENERAL PROVISIONS

1.1. Purpose.

1.1.1. **Use this instruction with the DOD Regulation 5200. 2-R and AFPD 31-5** to implement the personnel security program. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Executive Orders 9397, 9838, 10450, 11652, and 12968; and 5 United States Code (U.S.C.) 7513, 7532, 7533; 10 U.S.C. 8013. Privacy Act system of records notices F031 497IG A, SCI Personnel Records; F031 497IG B Special Security Case Files; F031 11 SPS A, Presidential Support Files; F031 11 SPS B, Personnel Security Clearance and Investigation Records; F031 AF SP N, Special Security Files;.F031 SAFPA A, Requests for Access to Classified Information by Historical Researchers; F036 497 IG B, For Cause Discharge Program apply.

1.1.2. Submit waivers to DOD Regulation 5200.2-R and AFPD 315 through command Information Security Program Manager (ISPM) channels to HQ USAF/XOFI, 1340 Air Force Pentagon, Washington DC 203301340.

1.2. Applicability. This AFI applies to DOD civilian employees, active duty military, the Air National Guard and Air Force Reserves.

1.3. Definitions. See **Attachment 1** for additional definitions. For purposes of this AFI the term "Commander" means: Commanders or equivalent and staff agency chiefs.

1.4. Records Management. Maintain and dispose of all records created as a result of prescribed processes in accordance with AFMAN 37-139, Records Disposition Schedule.

Chapter 2

POLICIES

2.1. Clearance and Sensitive Position Standard. The personnel security standard that must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interest of national security.

2.2. Military Service Standard. See AFPD 36-29, *Military Standards* and AFPD 36-20, *Accession of Air Force Military Personnel.* It provides policies to ensure the Air Force employs the right quantity and quality of people in the Air Force.

2.3. Criteria for Application of Security Standards. The criteria for determining eligibility for a security clearance are listed in DOD 5200.2-R, para 2-200. Commanders apply the criteria for security standards when granting access to classified information.

2.4. Types and Scope of Personnel Security Investigations. The scope of each type of personnel security investigation is listed in DoD 5200.2-R, Appendix B. See **Attachment 2** for procedures on requesting personnel security investigations (PSI). See **Attachment 3** for guidance on the types of required personnel security investigations and appropriate questionnaire forms and or Electronic Personnel Security Questionnaire (EPSQ) Software.

2.4.1. General. The investigations listed in DoD Regulation 5200.2R and this instruction are the only PSIs authorized. The Secretary of the Air Force and/or the Under Secretary of Defense, Intelligence must approve raising or lowering the scope of the authorized investigation.

2.4.2. Entrance National Agency Check (ENTNAC). ENTNACS were replaced by the NACLC on 1 Oct 99 for military accessions.

2.4.3. National Agency Check (NAC). NACs are primarily used for positions of trust.

2.4.4. National Agency Check Plus Written Inquiries and Credit Check (NACIC). NACICs are conducted by OPM and are required on all civilian employees entering government employment and assigned to nonsensitive positions.

2.4.5. Access National Agency Check with Written Inquiries and Credit Check (ANACI). ANACIs are conducted by OPM and are required for civilian employees' initial Secret security clearance or assignment to noncritical sensitive positions.

2.4.6. National Agency Check, Local Agency Checks and Credit Check (NACLC). NACLCs are required for military access to Secret information.

2.4.7. Single Scope Background Investigation (SSBI). SSBIs are required for access to TOP SECRET, Sensitive Compartmented Information (SCI), special sensitive positions and for critical sensitive positions.

2.4.8. Periodic Reinvestigation (PR). PRs are investigations conducted at prescribed intervals for the purpose of updating a previously completed background investigation.

2.4.9. Special Investigative Inquiry (SII). SIIs are used to prove or disprove allegations or new information concerning the security standards that arise after a person has been granted a security clearance.

2.5. Authorized Personnel Security Investigation Provider. The Office of Personnel Management (OPM) is the DoD Authorized Personnel Security Investigation Provider.

2.6. Allegations of Criminal Activity. Commanders refer possible criminal conduct to the supporting Air Force Office of Special Investigations (AFOSI) detachment.

2.7. Overseas Personnel Security Investigations. AFOSI personnel conduct the overseas portion of personnel security investigations, augmented by Army, Navy, and State Department counterparts.

2.8. Limitations and Restrictions. A break in service of over 24 months invalidates an individual's personnel security clearance eligibility.

Chapter 3

SECURITY CLEARANCE

3.1. Authority to Designate Sensitive Positions. Commanders with position designation authority determine the security sensitivity of civilian positions. Each civilian employee is subject to an investigation depending on the sensitivity of the position to be occupied, except for reappointment when the break in employment is less than 24 months.

3.2. Nonsensitive Positions.

3.2.1. The servicing civilian personnel flight (CPF) processes the initial request for NACIC's to OPM for civilians occupying nonsensitive positions, not requiring access to classified information. OPM forwards the investigation to the CAF. Suitability determinations for civilian government employment are made accordingly:

3.2.2. The CAF forwards the completed investigation, OPM "Certificate of Investigation" and the OPM INV Form 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations to the base servicing CPF.

3.2.3. The CPF:

3.2.3.1. Determines if the individual is deemed suitable for employment IAW 5 CFR 731.201-202. Coordination and or consultation with the supervisor and or commander may be made.

3.2.3.2. If employee is determined suitable, CPF signs off on the OPM Certificate of Investigation and the form is filed in the individual's Official Personnel Folder (OPF) IAW AFI 36.114, *Guide to Personnel Recordkeeping*.

3.2.3.3. If applicant is determined unsuitable, CPF fills out the OPM INV Form 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations and coordinates with the employee's supervisor and or commander. CPF forwards the OPM INV Form 79A to OPM.

3.3. Reassignment to a Noncritical Sensitive Position. If a civilian employee is subsequently selected for a position requiring access to classified information and unescorted entry into restricted areas (noncritical sensitive), security managers process the completed SF 86, **Questionnaire for National Security Positions**, to security forces authorized requesters.

3.3.1. Security Forces Authorized Requesters:

3.3.1.1. Submit the SF 86 to OPM for an "Access NACI". The address is: OPM-FIPC PO Box 618, 1137 Branchton Road, Boyers, PA, 16018. OPM does not have the EPSQ, therefore requests must be sent in hard copy. Use the EPSQ at the unit, validate the EPSQ, and print the SF 86 for mailing. Contact the servicing CPF for any questions concerning Part 1 of the SF 86 or the OPM Agency Use Information Sheet. A fingerprint card is not required as the individual has already been the subject of a NACI or NACIC.

3.4. Reassignment to a Critical Sensitive Position. If, in the future, the individual is selected for a critical sensitive position, security managers process the request for investigation to the

security forces authorized requester who will submit an SF 86 requesting a SSBI in accordance with **Attachment 2**.

3.5. PRs for Critical Sensitive and Noncritical Sensitive Positions. The periodic reinvestigation requirements apply to civilian employees in noncritical sensitive positions that require access to classified information. The reinvestigation requirements apply to civilian employees in critical sensitive positions whether or not they have access to classified information. See **Attachment 3**.

3.6. Pre-employment Waivers.

3.6.1. Sensitive Positions. Commanders must ensure procedures for pre-appointment to sensitive positions preclude an uncleared person from having access to classified information.

3.6.2. Noncritical Sensitive and Critical Sensitive Positions (3-204). The commander or staff agency chief (or designee) with position sensitivity determination authority prepares a waiver of preemployment investigation requirements when such action is necessary and in the national interest. See **Attachment 6** for sample waiver memorandum. The memorandum is filed in the individual's OPF IAW AFI 36-114, *Guide to Personnel Recordkeeping*.

3.7. Mobilization of DOD Civilian Retirees. MAJCOM commanders can waive the investigative requirements for the mobilization of selected re-employed annuitants for temporary appointment when the break in employment is greater than 24 months.

3.8. Military Appointment, Enlistment, and Induction. Personnel appointed, enlisted, or inducted to the active or reserve forces of the Air Force must have a favorable personnel security investigation. See **Attachment 3**.

3.8.1. Clearance requirements for officer training school selectees are outlined in Air Force Instruction (AFI)362005, *Appointment in Commissioned Grades and Designation and Assignment in Professional Categories*.

3.9. Mobilization of Military Retirees. MAJCOM commanders can waive the requirement for a full NACLC for the mobilization of military retirees upon reentry to active duty after a break of more than 24 months.

3.10. Security Clearance Authority. The 497 Intelligence Group/INS, Directorate of Security and Communications Management, the Air Force Central Adjudication Facility, is the designated authority to grant, suspend, deny, or revoke personnel security clearances and SCI access (see **Chapter 11**).

3.10.1. The CAF issues security clearance eligibility to the highest level authorized based on the type of investigation conducted. Unit commanders grant clearance access based on the level of the position occupied by the individual. The access level required should be annotated on the request for investigation.

3.10.2. The SAF Special Access Program (SAP) Central Adjudication Office, Wright-Patterson AFB Ohio is the designated authority to grant, suspend, deny, revoke, or limit SAF access. (See AFI 16-701, *Special Access Programs*).

3.10.3. Commanders control security clearances within their activity. See **para 7.1.2**.

3.10.4. See **Chapter 7** for granting of access to classified information.

3.11. Interim Security Clearances. Commanders may grant interim security clearances for access to Top Secret and Secret information when the requirements of DoD 5200.2-R, paragraph 3.401 have been met. Use of local information and the following requirements provide Commanders with the necessary tools to exercise their authority to grant interim security clearances. Also see **Attachment 25**, **Table A25.1** for guidance on the authority level to grant interim security clearance/access to specific programs.

3.11.1. Interim Top Secret security clearances:

3.11.1.1. Favorable ENTNAC, NAC, NACI, NACIC, NACLC, or ANACI completed.

3.11.1.2. Consult the Joint Personnel Adjudication System (JPAS) to determine the existence of a favorable ENTNAC, NAC, NACI, NACIC, NACLC, or ANACI. The investigation is acceptable if there is no break in service over two years.

3.11.1.3. Favorable review of personnel security questionnaire.

3.11.1.4. Favorable review of local personnel records, base and or security force records, medical records, and other security records, as appropriate.

3.11.1.5. SSBI package has been submitted by an Authorized Requester to the investigative agency provider.

3.11.2. Commanders can grant interim Top Secret security clearance if the above provisions have been met.

3.11.2.1. Favorable review of EPSQ or SF 86.

3.11.2.2. Favorable review of local personnel records, base/security force records, medical records, and other security records as appropriate.

3.11.2.3. Confirmation of a previous secret security clearance for newly hired civilian employees who have held a secret security clearance as a former military member (without a break in service of 24 months) or who hold a secret security clearance either as an Air Reserve Technician or as a traditional reservist.

3.11.2.4. Confirmed receipt of NACLC request at DSS by DSS EPSQ Receipt System. Confirmed receipt of ANACI request at OPM through the supporting CPF.

3.11.3. If there is no record of a completed investigation (NAC portion) in JPAS, contact Air Force Central Adjudication Facility (AFCAF) Customer Support through JPAS to determine if there is a favorable NAC. (Note Optional: Authorized requesters can request "Advanced NAC Results" from OPM on the OPM Agency Use Sheet.)

3.11.4. Interim Secret security clearances:

3.11.4.1. Favorable review of personnel security questionnaire.

3.11.4.2. Favorable review of local personnel records, base and or security forces records, medical records, and other security records, as appropriate.

3.11.4.3. NACLC or ANACI has been submitted by an Authorized Requester to an investigative agency provider.

3.11.5. Interim security clearances must be documented in JPAS or in writing if JPAS is unavailable, until the final security clearance eligibility is granted by the AFCAF.

3.11.6. For Civilians:

3.11.6.1. Consult JPAS on a newly hired civilian for a previous security clearance/personnel security investigation to determine if a previous security clearance was held as a former military member (without a break in service of two years) or if a security clearance as either an Air Reserve Technician or as a traditional reservist was held.

3.11.6.2. Pending completion of ANACIs or SSBIs, as appropriate, civilians may occupy non-critical sensitive or critical sensitive positions. Commanders prepare a waiver of pre-employment investigation requirements when such action is necessary and in the national interest. Interim security clearance may not be granted until after the commander signs the waiver memorandum.

3.11.7. JPAS is the source for determining investigative status on pending investigations. Also see **para 7.9**.

3.12. Access to Classified Information by Non-US Citizens.

3.12.1. Initial Limited Access Authorization (LAA). The MAJCOM/SF approves the request for a personnel security investigation for the purpose of LAA. Approvals are returned to the requester and an information copy is provided to the CAF. Authorized requesters initiate the personnel security action and submit a SSBI to DSS. A favorable SSBI is a prerequisite for LAA. The CAF will adjudicate the SSBI, issue the LAA authorization to MAJCOM/SF, and enter the information in the Adjudication Management System (AMS). MAJCOM/SF forwards the authorization to the requester. The requester grants the LAA. Requirements governing nondisclosure agreement form and a security termination statement apply to LAAs.

3.12.2. Annual Certification. MAJCOM/SF provides an annual report to the CAF by 1 Nov of each year certifying the continued need for the command's LAAs. The CAF provides a consolidated report to HQ USAF/XOFI by 25 Nov each year. HQ USAF/XOFI approves the report and forwards to OASD (C3I) by 1 Dec of each year.

3.13. Access by Persons Outside the Executive Branch. Refer to AFI 31401, *Information Security Program Management*, for granting access to persons outside the Executive Branch.

3.13.1. Authorized requesters submit the appropriate investigation according to **Attachment 2** based on the level of access required.

3.13.1.1. Annotate the request, "Request for investigation is required IAW DOD 5200.1-R, paragraph 6-201, Access to Person Outside the Executive Branch."

3.13.1.2. The CAF does the adjudication and enters the results in the AMS.

3.14. Access by Different Categories of Individuals.

3.14.1. Voluntary Emeritus Corps and Intergovernmental Personnel Act (IPA).

3.14.1.1. There is an affiliation with the Government by virtue of the signing of an agreement. As a general rule, these individuals will not have access to classified information. In certain instances, the commander may approve access to classified information.

3.14.1.2. Access will be justified and must provide a specific benefit or gain to the Government.

3.14.1.3. The access will be commensurate with the level the person held prior to retirement/separation or the level currently held by IPA personnel under the National Industrial Security Program. Offices should accept and maintain visit authorization requests submitted by the sponsoring cleared facility as evidence of an IPA participant's current clearance.

3.14.1.4. Access will be kept to the absolute minimum for the work being performed and limited to a specific time period.

3.14.1.5. The agreement between the individual and the organization will include a security clause.

3.14.1.6. The individual will sign an SF 312, **Classified Information Nondisclosure Agreement (NdA)** and be briefed or re-briefed on security requirements (individuals need not sign another SF 312 if verification can be made that an NdA was previously signed).

3.14.1.7. Physical custody of classified information is not authorized.

3.14.1.8. The CAF will certify the individual's security clearance. If a break in service exceeds 24 months, the requesting organization must initiate a request for the appropriate investigation.

3.14.1.9. The CAF will provide an AF Form 2584, **Record of Personnel Security Investigation and Clearance** to the requesting organization if required due to lack of automation capabilities.

3.14.2. Consultants. A consultant, paid or unpaid, will only require access to classified information at an Air Force activity or in connection with authorized visits and is not required to be cleared under the National Industrial Security Program. The consultant is considered to be an Air Force employee and will be issued a clearance, adjudicated by the CAF, in accordance with this AFI.

3.14.3. Individual Ready Reserve (IRR). The IRR is a manpower pool of pre-trained individuals who have already served in active component units or in the Selected Reserve and have some part of their Military Service Obligation remaining. Refer to DOD 1215.15-H, *Reserve Components of the U.S. Armed Forces*.

3.14.3.1. As a general rule, these individuals will not have access to classified information. In certain instances, the commander may approve access to classified information.

3.14.3.2. Access will be justified and must provide a specific benefit to the Air Force.

3.14.3.3. Access will be commensurate with the level the person held prior to transfer to the IRR, kept to the absolute minimum for the work being performed, and limited to a specific time.

3.14.3.4. An agreement between the individual and the organization is required and will include a security clause.

3.14.3.5. The individual will sign an SF 312, **NdA**, and be briefed or re-briefed on security requirements (individuals need not sign another SF 312 if verification can be made that one was previously signed).

3.15. One Time Access. A general court martial convening authority or equivalent Senior Executive Service member, MAJCOM commander, wing commander, or civilian equivalent may approve access to classified information at a higher level than authorized by the existing security clearance during contingencies, or when an urgent operational or contractual exigency exists. This authority can be used when the conditions of DOD 5200.2-R, para 3-406 are met. This does not apply to SCI access (see **para 3.18** below), COMSEC, NATO, or foreign government information. The approving authority's authorization for the access is maintained on file with the servicing security manager and or servicing security activity until the access is no longer needed.

3.16. Granting Access to Retired General Officers or Civilian Equivalents and Former Presidential Appointees

3.16.1. The Secretary of the Air Force (SecAF), Chief of Staff of the Air Force (CSAF) or Commanders of Air Force Major Commands (MAJCOM/CCs) or Headquarters Air Force two letter Directors may request that SAF/AA approve sponsorship for a retired general officer, Senior Executive Service (SES) member or former Presidential appointees to support a specific Air Force Program or mission where the authorized holder has verified the individual requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. SAF/AA, based upon information provided by the requesting official, will determine on a case by case basis, whether a nominee has a particular skill or expertise that would benefit the Air Force, clearly consistent, or compelling with the interests of national security, and there is a compelling need justifying sponsorship. Nominee must have in-scope investigation and be on appointment as an unpaid consultant with the Air Force. Any such request is subject to the following conditions and limitations.

3.16.1.1. Nominees with in-scope background investigations may be granted eligibility for one year or the completion of the mission/program whichever is less. Eligibility may be extended for additional periods provided there is a request specifying a continuing compelling need and the background investigation remains current.

3.16.1.2. Investigative requirements for nominees with out of scope investigations may be waived; however, access for such individuals will not exceed a period of 90 days. Access may be extended for additional periods of 90 days at the discretion of the approving authority upon a demonstration of continuing compelling need for access by the nominating official.

3.16.1.3. The decision to fund investigations to allow continued access will be made on a case by case basis depending on a demonstrated compelling need.

3.16.1.4. Level of access shall not exceed that held at the time of retirement or government separation.

3.16.1.5. SCI or SAP access will not be granted under this authority. Requests for SCI/SAP access must be processed thru AF/A2RS (SCI) and SAF/AAZ (SAP) after clearance eligibility is granted by SAF/AA.

3.16.1.6. Classified materials may not be removed from a Government installation or other area approved for storage of classified information.

3.16.1.7. Individuals employed by government contractors will abide by all ethical terms and agreements as put forth in the unpaid consultant package. Failure to do so will result in removal from the program and discontinued access under this program.

3.16.1.8. Blanket access based on a retiree's or former Presidential appointee's grade or past assignments is prohibited.

3.16.2. Nominating officials must send request to SAF/AAZ through MAJCOM/FOA/DRU Information Protection Office. SAF/AAZ will process request and forward to SAF/AA for approval. The request must include the following information:

3.16.2.1. The nominee's name, grade/rank, SSAN, telephone number, personal e-mail address, and last position held while on active duty, as a General Officer, SES, or Presidential appointee.

3.16.2.2. The justification must identify the particular program or mission, organization or personnel that will be supported.

3.16.2.3. The level of classification to which access is requested.

3.16.2.4. Individuals accepted for access/eligibility into the program will not be afforded any competitive advantage through material released to him/her.

3.16.3. SAF/AA will determine on a case by case basis whether: (a) nominated individuals have a particular skill or knowledge that would benefit a specific Air Force program, and (b) there is a compelling need justifying access. If eligibility is approved, SAF/AAZ will provide a memorandum to the appropriate agency(s) and ensure the necessary systems (JPAS) are updated.

3.16.4. Former Secretaries of the Air Force, retired Chief of Staffs of the Air Force, or other former Air Force Presidential Appointees may be approved for access to classified information upon a determination by SAF/AA that access by the individual is necessary for the purpose of accomplishing a national security objective and consistent with current administration guidance (see DoD 5200.1-R, C6.2.2.7). Investigative requirements may be waived upon a determination by SAF/AA that the individual is trustworthy and that the individual can and will safeguard information from unauthorized disclosure. Any such access must be reviewed and validated by SAF/AA at the beginning of each calendar year. Access will not be approved for individuals who are employees of government contractors unless they meet all ethical requirements and provisions and are on appointment as an unpaid consultant with the Air Force.

3.17. Processing Requests for Access by Historical Researchers. Refer to AFI 31-401 for guidance in granting of access to researchers.

3.17.1. Authorized requesters request a NAC according to **Attachment 2**. Identify the request as "Special Category Historical Researcher" in remarks.

3.17.2. The CAF will forward the completed investigation to the Air Force Historian.

3.17.3. The United States Air Force History Support Office (AFHSO/HO), 200 McChord, Box 94, Bolling AFB DC 20332, will make the access determination.

3.18. Sensitive Compartmented Information. The Director of Intelligence Surveillance and Reconnaissance (HQ USAF/XOI), 1480 Air Force Pentagon, Washington DC 20330-1480, controls access to SCI within the Air Force. Routine prescreening for SCI access is no longer required. Refer to AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (SCI).* for specific guidance on conducting SCI prescreening interviews, requesting investigations, granting access, and waiver information.

3.18.1. The 319th Training Squadron (319 TRS/TPCSS), 1550 Wurtsmith Street, Suite 7, Lackland AFB TX 78236-5242, conducts interviews pertaining to individuals identified for SCI positions during basic military training. They also conduct interviews of individuals requiring Top Secret for Air Force specialty code retention and critical personnel reliability program certification.

3.18.2. A single agency check (SAC) is required on the following categories of individuals associated with the subject of an SSBI (a) spouse or cohabitant, (b) immediate family members, 18 years old or older, who were born outside the United States. If marriage or cohabitation occurs after completion of the SSBI, submit Spouse SAC via EPSQ to DSS. Keep one copy for the authorized requester's suspense file.

3.19. Single Integrated Operational Plan-Extremely Sensitive Information. See AFI 10-1102, *Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).*

3.20. Presidential Support Activities. The following guidance supplements DOD Directive 5210.55, Department of Defense PSP and DOD Instruction 5210.87, Selection of DOD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs). The PSP includes personnel assigned duties involving regular or frequent contact with or access to the President or Presidential facilities, communications activities, or modes of transportation.

3.20.1. The Office of the Administrative Assistant, Director for Security and Investigative Programs (SAF/AAZ) is the single office designated to develop policy and represent the Air Force on matters covered by the DOD Presidential Support Directive and Instruction.

3.20.2. HQ USAF/XOFI implements policy for the PSP.

3.20.3. The CAF:

3.20.3.1. Manages adjudicative functions as required by the PSP.

3.20.3.2. Accomplishes requisite cover letters and coordination with support units on behalf of SAF/AAZ.

3.20.3.3. Forwards nomination packages, regardless of adjudicative outcome to SAF/AAZ.

3.20.3.4. Submits the "Information Requirements" report on a quarterly basis to SAF/AAZ for approval and forwards approved report to the Executive Secretary. Copies of the approved report are provided to HQ USAF/XOFI, the servicing security activity, and contracting officers for distribution.

3.20.3.5. Maintains historical files.

3.20.4. SAF/AAZ advises commanders or company representatives when nominees have been selected or nonselected by SAF/AAZ or the Executive Secretary. SAF/AAZ enters selection status information in the AMS.

3.20.5. Appeals. Any DOD civilian or contractor employee not selected for, or removed from, presidential support duties shall be afforded an opportunity to appeal this decision as provided in DODD 5210.55 and DODI 5210.87. The governing directives do not provide appeal rights for military members, however, when exceptional mitigating circumstances exist, or derogatory information is reported in error, SAF/AAZ will reconsider non-selection decisions. Reconsideration of military non-selections requires unit commander approval and involvement.

3.20.6. The servicing security activity of the nominating unit:

3.20.6.1. Processes the appropriate investigation to DSS or OPM. See **Attachment 2**.

3.20.6.1.1. Completes DD Form 1879 for an SSBI by typing "YANKEE WHITE" in capital letters in the remarks section. Checks the "Presidential Support" block and indicates the level of clearance required for the position. Includes the title of the authorized presidential support position and the unit or organization to which the individual will be assigned.

3.20.6.1.2. Completes the SF 86 for a NACLC by typing "YANKEE WHITE" in capital letters in the remarks section. Type "Presidential Support" and indicate the level of clearance required for the position. Include the title of the authorized presidential support position and the unit or organization to which the individual will be assigned.

3.20.6.2. Prepares the "servicing security activity" nomination memorandum for the CAF outlined in **Attachment 9**.

3.20.6.3. Forwards the nomination memorandum to the CAF for further processing.

3.20.6.4. Notifies the servicing medical facility that must mark and monitor the individual's medical records, upon notification by the Commander that the member has been approved for presidential support duties. See **Attachment 10**.

3.20.6.5. Notifies the servicing medical facility when individuals are no longer assigned presidential support duties.

3.20.6.6. Notifies the CAF presidential support representative telephonically within 24 hours when an individual's access has been temporarily suspended or removed and note if publicity is anticipated. The temporary suspension or removal should also be input into the CAVS which will provide the information to the CAF electronically. Provides written follow-up to include a summary of all available information within 2 working days. If applicable a full report of investigation of the allegations and commander's recommendation for removal or reinstatement shall be forwarded to the CAF within 50 days. Provide a status report within 30 working days. Temporary suspension in which the issues are unresolved by the applicant within 90 days shall become a permanent removal. Notifies the CAF within five working days, when this occurs. Notifies the CAF when individual's (1) are permanently removed from presidential support duties, (2) separate or (3) retire. The CAF notifies SAF/AAZ immediately in all cases.

3.20.6.7. Completes and forwards to DSS the FD Form 258, **FBI Fingerprint Card**.

3.20.6.8. Forwards requests for transfer or designation of additional presidential support positions to the CAF for coordination. The CAF will attach the current unit billet structure and forward it to SAF/AA for approval.

3.20.6.9. Processes individuals for periodic reinvestigations.

3.20.7. Servicing Medical Authority:

3.20.7.1. Ensures the medical records of members approved for presidential support duties are identified, evaluated and monitored while assigned to presidential support.

3.20.7.2. Identifies the medical records using AF Form 745, **Sensitive Duties Program Record Identifier** (see AFI 41-210, *Patient Administration Functions*).

3.20.7.3. Immediately notifies the individual's commander or designated representative and the servicing security activity when a significant effect on the individual's suitability to perform presidential support duties is expected as a result of medical, dental, or mental health treatment or medication, and if drug or alcohol abuse is suspected.

3.20.7.4. Provides a summary of pertinent health records to individual's commander or designated representative at their request. The actual record will be provided only if specifically requested for clarification purposes or other compelling need. Mental health clinic records may, if necessary, be reviewed in their entirety by the individual's commander or reviewing official, provided a privileged mental health provider is present to help interpret psychological testing data and other technical information which may be contained in the record. The information contained in the record is protected under the Privacy Act and is not to be discussed or released except as indicated in this paragraph.

3.20.8. Commander and or Supervisory Indoctrination Program. Commanders and or supervisors will become knowledgeable of DOD 55210.55 and requirements of this AFI prior to evaluating and recommending individuals for presidential support positions.

3.20.9. Continuing Evaluation. Commanders and supervisors continually evaluate the trustworthiness of personnel serving in presidential support duties to ensure they meet the standards. Take necessary action when adverse information becomes known to access the validity of the information. If appropriate, initiate action for suspension and or removal. Follow SIF procedures as outlined in **Chapter 8** when unfavorable information surfaces on an individual already in the PSP program.

3.20.10. Investigative Requirements. Persons nominated for presidential support duties must have an SSBI or NACLC current within 36 months of assignment to presidential support duties. The DD Form 1879/SF 86 will be annotated to reflect if the investigation is for initial assignment into the program.

3.21. Nuclear Weapons Personnel Reliability Program. Refer to AFI 36-2104, *Nuclear Weapons Personnel Reliability Program (PRP)* for PRP certification and investigative guidance. A new personnel security investigation (PSI) or periodic reinvestigation is required when there is a break in personnel reliability program certification of more than five years, or for new PRP assignments when the security investigation date is over five years. A new PSI is also required any time a break in service of more than 24 months occurs between completion of the security investigation and PRP certification dates.

3.22. Access to North Atlantic Treaty Organization Classified Information. U.S. military personnel, civilians, and contractors shall be permitted temporary access to COSMIC Top Secret information based on a final U.S. Secret clearance and issuance of an interim Top Secret clearance, pending completion of an SSBI and issuance of a final Top Secret clearance. The temporary access will be valid until completion of the investigation and adjudication of the final clearance. However, the agency granting the access will rescind it if adjudicatively significant information is identified during the course of the investigation. The same procedures apply to personnel not assigned to a NATO staff position, but requiring access to NATO COSMIC Top Secret, Secret or Confidential information. The granting agency records NATO access in the CAVS. Refer to AFI 31-406, ***Applying NATO Protection Standards***.

3.23. Special Access Program. Certain programs require additional investigative and or safeguarding requirements. Refer to AFI 16-701, *The US Air Force Special Access Programs*.

3.24. Processing Requests for Access to Restricted Areas, Sensitive Information or Equipment Not Involving Access to Classified Information. Access for unescorted entry may be granted based on the following investigative requirements. Refer to **Attachment 3**, **Table A3.6**.

3.24.1. DOD and OPM civilians require a National Agency Check with Written Inquiries and Credit Check (NACIC).

3.24.2. Air Reserve forces personnel with a current Entrance National Agency Check (ENTNAC) or NAC may have unescorted entry to restricted areas while in civilian status, pending completion of the required NACIC.

3.24.3. Department of Energy employees require an "L" (Secret) clearance.

3.24.4. Federal employees require a NAC.

3.24.5. United States active duty, retired, or separated military members with an Honorable Discharge and no break in service greater than 24 months, may use a previously completed ENTNAC or NACLC.

3.24.6. Contractor employees require a NAC. Contractors operating as visitor groups only (contract performance exceeding 90 consecutive days), have the following option. Commanders may grant individuals access to restricted areas subject to: (1) the contractor completing the SF 85P and it is submitted to OPM for a NAC; (2) a check of the Defense Clearance and Investigations Index reveals no relevant, significant information which might preclude unescorted access; and (3) a check of appropriate local records.

3.24.7. Commanders may waive on a case by case basis, the investigative requirements for unescorted entry to restricted areas containing PL2 and or 3 resources pending completion of a favorable NAC, or NACIC after favorable review of the completed personnel security questionnaire for the investigation. Decisions to deny or withdraw must be fully supported by the documented facts. Individuals must be informed of the adverse information about them (unless precluded by security considerations) and given the opportunity to appear before the commander. This allows the individual to refute or to mitigate the information. Forward appeals of denials or withdrawals to the MAJCOM commander or designee.

3.24.8. Interim access to restricted areas may be granted to military, civilians, and contractors. Use the same procedures for interim access as established for interim AIS (**para 3.27**).

3.24.9. For Foreign National military members and host military members assigned to USAF activities, entry authorization is based on government-to-government agreements, treaties, and unified command directives. A SSBI is required for restricted areas containing PL1 or 2 resources, and a local agency check for restricted areas containing PL3 resources.

3.24.10. Unit commanders through the installation commander, request NACs on contractor employees requiring unescorted entry to restricted areas. The CAF adjudicates the completed NAC and enters the results in the appropriate database. Installation commanders approve all denials or withdrawals of unescorted entry for contractor employees.

3.25. Nonappropriated Fund Employees. Human Resources Office (HRO) managers (**Attachment 4**) designate positions of trust. AFPD 34-3, *Nonappropriated Funds Personnel Management and Administration* and AFI 34-301, *Nonappropriated Fund Personnel Management and Administration* establish policies for the management of the AF Nonappropriated Fund Personnel Program. HRO managers make suitability determinations according to the suitability criteria outlined in 5 CFR 731.201-202. The determination will be filed in the individual's personnel file.

3.26. Special Agents and Investigative Support Personnel. See **Attachment 3**. Non-investigative personnel whose official duties require direct investigative support include administrative processing and or handling of the investigative reports on a continuous basis. The CAF adjudicates the investigation and enters the data in the DCII and AMS.

3.27. Personnel Occupying Information Systems Positions Designated Auto mated Information Systems, AIS-I, AIS-II, and AIS-III (formerly ADP positions). Refer to DOD 5200.2-R, appendix K for ADP definitions.

3.27.1. See **Attachment 3** for AIS I, II, and III investigation requirements. See **paragraph 3.11** for interim security clearance requirements.

3.27.2. The CAF provides the results of the investigations for AIS I, II, and III purposes to the authorized requester for the commander's suitability determination according to the suitability criteria outlined in 5 CFR 731.201-202. The CAF does not review the investigation for security clearance purposes.

3.27.3. Commanders may recommend to the Designated Approving Authority (DAA) that interim AIS access be granted. Commanders may waive, on a case by case basis, the investigative requirements for access to AIS pending completion of a favorable ENTNAC, NAC, NACIC, ANACI, or SSBI, after favorable review of the completed personnel security questionnaire for the investigation. Commanders confirm that the following actions have been accomplished prior to access:

3.27.3.1. Mandatory information assurance training has been given and documentation by a supervisor accompanies the request.

3.27.3.2. Systems Administrators have implemented measures to limit access to the information required to conduct assigned duties.

3.27.3.3. Commanders and or supervisors have ensured increased monitoring of the individual having AIS access.

3.27.3.4. For military members: after verification from the unit security manager that the required investigation has been initiated and the preliminary suitability determination has been made.

3.27.3.5. For AF Appropriated and NAF Civilians (over 180 day appointment or an aggregate of 180 days has been reached):

3.27.3.5.1. CPF/HRO returns to the commander, a favorable suitability determination based on the results of the completed OF 306, Declaration for Federal Employment, and the SF 85, Questionnaire for Non Sensitive Positions, or 85P.

3.27.3.5.2. Unit security managers initiate a local files check (LFC).

3.27.3.5.3. Security Forces verify that the appropriate investigation has been initiated and no adverse information was revealed in the completed LFC.

3.27.3.6. For AF Appropriated and NAF Seasonal or Summer Hire Employee (under 180 day appointment):

3.27.3.6.1. CPF/HRO returns to the commander, a favorable suitability determination based on the results of the completed OF 306.

3.27.3.6.2. Unit security managers initiate a LFC.

3.27.3.6.3. Security Forces verify that no adverse information was revealed in the completed LFC.

3.27.3.7. For Contractors:

3.27.3.7.1. Unit security managers initiate the LFC.

3.27.3.7.2. Security Forces verify that the appropriate investigation has been initiated and no adverse information was revealed in the completed LFC.

3.28. Periodic Reinvestigations (PR). PRs are required every 5 years for Top Secret and 10 years for Secret. Authorized requesters submit requests for reinvestigations to the DoD Authorized Investigation Provider as outlined in **A2.2.2.1**. See AFI 31-406, Applying North Atlantic Treaty Organization (NATO) Protection Standards, for submission of PRs for NATO investigations.

3.29. Explosive Ordnance Disposal (EOD). Although such personnel normally only require a Secret clearance, an SSBI is initially required due to training and assignments involving nuclear weapons. Persons occupying an EOD position shall undergo a Secret PR on a five year recurring basis.

Chapter 4

RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

4.1. Prior Federal Civilian Investigations. Investigations previously conducted on civilian employees are suitable and accepted for granting immediate access to classified information.

4.1.1. Civilian Personnel Flight:

4.1.1.1. Verifies prior federal employment in a sensitive position was continuous with no single break longer than 24 months.

4.1.1.2. Confirms the individual is employed in a sensitive position with the Air Force and that clearance eligibility is valid.

4.1.1.3. Confirms with the CAF that a valid investigation is on file. The CAF updates the DCII and AMS.

4.1.1.4. Forwards verification of the investigation to the subject's commander.

4.1.2. Unit commander:

4.1.2.1. Grants access when actions are completed.

4.1.2.2. Destroys all copies of the documentation when SK shows the security clearance data.

Chapter 5

REQUESTING PERSONNEL SECURITY INVESTIGATIONS

5.1. General.

5.1.1. Security Managers provide personnel security support to active duty military, civilian, and guard and reserve members assigned or attached to the active duty organization.

5.1.1.1. Submit completed personnel security questionnaires to supporting authorized requester. See **Attachment 3** for additional guidance.

5.2. Authorized Requesters.

5.2.1. MAJCOM, field operating agency (FOA), or direct reporting unit (DRU) staffs designate authorized requesters to initiate PSIs for their organization. As a general rule, the number of authorized requesters will be kept to the minimum number required to meet mission requirements. See **Attachment 2** for request procedures.

5.2.2. Authorized requesters provide the AFCAF with the name, telephone number, and office symbol of individual(s) who may obtain security clearance and or investigative data on individuals within their organization and provide copy to respective MAJCOM. See **para 6.1** for AFCAF address.

5.2.3. Authorized requesters may query the JCAVS or call the CAF Customer Support Section at DSN 754-1242/43 to determine investigative and/or adjudicative status.

5.2.4. Authorized requesters approve and submit personnel security questionnaires to the DoD Authorized Personnel Investigation Provider according to **Attachment 2**.

5.2.5. Advise HQ USAF/XOFI when authorized requesters are disestablished.

5.3. Criteria for Requesting Investigations. See **Attachment 3** for the type of investigation to request.

5.4. Request Procedures. See **Attachment 2** for the request procedures.

5.5. Priority Requests. The following sensitive programs are authorized priority processing service by OPM:

5.5.1. PRP. In cases where a PRP "C" coded case warrants "Priority" service by OPM, the authorized requester must coordinate the request through channels to AF/XOS-FI. Each authorized requester will maintain a fiscal year (FY) Excel spreadsheet listing for this purpose. The spreadsheet will include all previously coordinated FY priority PSIs and all new requirements the authorized requester is coordinating under this authority. When coordinating new priority cases, forward the entire FY spreadsheet to **afxofi.workflow@pentagon.af.mil.** AF/XOS-FI will return to the authorized requester for monitoring the completion of the investigation.

5.5.2. SCI. When the NACLC adjudication date is less than 12 months (DCID 6/4, Annex A, para 5), the servicing Authorized Requester will provide the servicing SSO a copy of the completed SF 86 for each SSBI request with an SCI access requirement. This will be done at the same time the request for SSBI/SCI is forwarded to OPM. Security Managers/SSOs/Authorized Requesters will expedite the processing of the SSBI off the

installation to OPM and request priority level of service. On the *OPM Agency Use Sheet annotate 30A in Block A.* Also see AFMAN 14-304.

5.6. Personal Data Provided by the Subject of the Investigation.

5.6.1. The Air Force goal for processing personnel security investigation requests at base level is 14 duty days. However, commands that have extensive deployments and TDY requirements may establish their own internal management controls and or timelines for the processing of investigation requests.

5.6.2. The subject of the investigation will provide the required documentation to the security manager to verify birth and education information. See **Attachment 2** for details.

5.6.3. Individual Mobilization Augmentee (IMA): Upon accession, IMAs complete the PSI during the first three days of the individual duty training (IDT) period or not later than 90 days at the unit of assignment or attachment and turn-in to the servicing security manager and or gaining active duty security manager.

5.6.4. See **Chapter 8** for actions when individuals refuse to provide the required information for a personnel security investigation.

5.6.5. DSS and OPM are the DOD repository of personnel security investigative files. To obtain a personal copy of an investigation, forward a notarized request that includes: name, SSAN, date of birth, and place of birth to: DSS, ATTN: Privacy Act Office, PO Box 46060, Baltimore, MD 212406060 or OPM, ATTN: FOIA, PO Box 618, 1137 Branchton Rd, Boyers, PA 16018-0618. The request should refer to the Privacy Act and include a valid return address. All signatures must be notarized. Military personnel may use a commissioned officer in lieu of a notary public to attest to the signature. Identify the SSN and rank of the officer. Also refer to AFI 33-332, *Air Force Privacy Act Program*.

5.7. Dual Citizenship. A security concern could exist when a military member, DoD civilian, contractor, or consultant is submitted for a personnel security investigation and they are a dual citizen and/or possess/use a foreign passport.

5.7.1. Dual Citizenship. Dual citizenship in and of itself is not an automatic disqualifier for security clearance eligibility. However, possession of dual citizenship and particularly the **exercise** of dual citizenship is a condition that raises a security concern and may be a disqualifying factor in a security clearance eligibility determination. There are factors that could mitigate the maintenance of dual citizenship, as outlined in DoD 5200.2-R, App I, Foreign Preference. An individual's expressed willingness to renounce dual citizenship is one of the conditions that *could* mitigate security concerns.

5.7.2. Possession or Use of a Foreign Passport. Possession and/or use of a foreign passport in preference to a US passport raises doubt as to whether the person's allegiance to the US is paramount and could also facilitate foreign travel unverifiable by the US. The security clearance will be denied or revoked, unless the applicant surrenders the foreign passport or obtains official approval for its use from SAF/AA. Requests for approval are forwarded through respective Information Security Program Manager (ISPM) channels to HQ USAF/XOS-FI for processing to SAF/AA. Justification must include what benefit the AF will gain from a person holding a foreign passport. AFCAF will annotate approvals in the remarks field of the JPAS.

5.7.3. Surrendering the Passport. Individuals who indicate they possess a foreign passport in item 15 of the Electronic Personnel Security Questionnaire or item 17d on the Standard Form 86, "**Questionnaire for National Security Positions**," will be required to surrender the passport via one of the following methods:

5.7.3.1. Return the passport to the appropriate country embassy or consulate via certified receipt mail. A copy of the transmittal memo forwarding the passport and the return receipt will be forwarded to the AFCAF. See **para 6.1** for AFCAF address. If the name of adjudicator assigned to the case is known, include this in the ATTN line of the address.

5.7.3.2. Destroy the passport as witnessed by an AF security manager. Cut up the passport and place in a burn bag. The witnessing security manager will document the destruction of the passport in an explanatory memorandum, which will be forwarded to the AFCAF and a copy provided to the subject.

5.7.4. Security Clearance Eligibility. In order for individuals who hold foreign passport and dual citizenship to be considered for and/or be granted security clearance eligibility the following must be completed:

5.7.4.1. Provide a written statement expressing their willingness to renounce foreign citizenship claims in favor of a sole United States citizenship status. Actual renouncement is not required.

5.7.4.2. Return and or destroy the passport.

5.7.5. The renouncement statement and documentation of destruction of the passport must be provided to the AFCAF. The AFCAF reviews each case on its own merits to determine security clearance eligibility.

5.7.6. This same guidance will apply if the passport is identified after a security clearance determination is made.

Chapter 6

ADJUDICATION

6.1. Central Adjudication Authority. The Air Force Central Adjudication Facility (AFCAF) is the Central Adjudication Authority. Address is: AFCAF/PSA, 229 Brookely Ave, Bolling AFB 20032.

6.1.1. The policy and criteria set forth in DOD Regulation 5200.2-R, paragraph 2-200, 6-102 and Appendix I will be applied in making personnel security determinations for a security clearance or assignment to sensitive duties.

6.1.2. Unfavorable adjudication results in the denial/revocation of clearance eligibility (see **Chapter 8**).

6.1.3. The AFCAF will review all investigative products and make an eligibility determination.

6.1.4. AFCAF Customer Service will not release adverse information to inquiring customers on pending investigations, as it invokes privacy act concerns. Derogatory issues are often resolved through completion of the investigation and or adjudication of the case. Premature dissemination of unresolved and or un-adjudicated issues could result in discriminatory practices with respect to such areas as employments or assignments.

6.2. Adjudicative Record. Personnel security determinations are reflected in the JPAS. JPAS replaced Sentinel Key (SK) as used throughout AFI 31-501.

Chapter 7

ISSUING CLEARANCE AND GRANTING ACCESS

7.1. General

7.1.1. The AFCAF is the designated authority to grant, suspend, deny, or revoke personnel security clearances and SCI accesses (see **Chapter 11**).

7.1.2. Position Designations (7-100c). Commanders:

7.1.2.1. Determine the level of access necessary for each military and civilian position based on mission needs. Each position is coded with the appropriate security access requirement (SAR) and identified in the unit manning document (UMD), the Defense Civilian Personnel Data System (DCPDS), and SK. See **Attachment 3**, for SAR code definitions. If the SAR code requires a change, the unit commander submits an authorization change request to the servicing security activity.

7.1.2.2. Conduct a review annually to determine the accuracy of position coding, eliminate unnecessary access codings, and adjust SAR code appropriately.

7.1.2.3. Record findings in the UMD and SK.

7.1.2.4. Ensure only necessary investigations are requested to meet mission essential needs.

7.2. Investigative Requirements for Coding Positions.

Commanders will:

7.2.1. Determine the type of investigation required for mission purposes for each military and civilian position in the organization. Investigations are required for multiple purposes: to determine suitability and/or trustworthiness of individual for employment/assignment to positions of trust/access to certain programs; and for security clearance. Each position is coded with the appropriate position code reflecting the required investigation level in the unit manning document (UMD) and the Defense Civilian Personnel Data System (DCPDS). These will also be reflected in the Headquarters Air Force Manpower Data System (HAF-MDS).

7.2.1.1. Assign one of the five investigation types to each position:

7.2.1.1.1. Single Scope Background Investigation (SSBI).

7.2.1.1.2. National Agency Check, Local Agency Checks and Credit (NACLC).

7.2.1.1.3. Access National Agency Check and Inquiries (ANACI).

7.2.1.1.4. National Agency Check Plus Inquiries (NACI).

7.2.1.1.5. National Agency Check (NAC).

7.2.1.2. The definitions and corresponding codes are located in **Attachment 22**, **Table A22.1**.

7.2.1.3. Conduct annual review to determine the accuracy of position coding. The last AF-wide directed review was conducted in May 04. Reviews will be conducted each May. Retain results for review during self inspections, etc.

7.2.1.4. Ensure only necessary investigations are requested to meet mission essential needs.

7.2.1.5. See **Attachment 22** for additional guidance.

7.2.2. Mandatory Secret or Top Secret requirement may be required when every position in a specialty is not coded as requiring access to classified information if the functional community can validate security access requirements for the AFSC and provide justification that demonstrates mandatory qualification required for mission accomplishment, such as access to classified information or equipment.

7.3. Investigative Requirements for Air Force Specialty Codes (AFSCs). HQ USAF/XOS-FI approves requests for adding security clearances or investigations as AFSC prerequisites. Requests are staffed through ISPM channels. AFMAN 36-2105, Officer Classification and AFMAN 36-2108, Enlisted Classification will reflect an SSBI requirement for entry, award, and retention for the respective mandatory AFSCs. See **Attachment 22**; **Table A22.2**, **A22.3**.

7.3.1. Security clearance data can be verified by the CAVS, Permanent Change of Station Orders, or Temporary Duty Orders.

7.4. Investigative Requirements for Sensitive Programs. There are several sensitive programs that have been designated as a mandatory SSBI requirement, i.e., Presidential Support, Personnel Reliability Program, etc. See **Attachment 22**, **Table A22.4**.

7.4.1. AMS is the application used by the CAF and is restricted to CAF personnel only.

7.4.1.1. It is a centralized database enabling CAF personnel to post adjudication results; security clearance determinations; access eligibility; pending actions; status of due process actions, i.e. security information files; statistical reporting requirements; and other personnel security management functions.

7.4.1.2. Selected data fields from AMS will be available through CAVS to Air Force customers/users almost immediately after input by CAF personnel and within 24 hours of data input by other customers/users.

7.4.2. CAVS is the application used by MAJCOM/FOA/DRUs, ISPMs, SSOs, unit level security managers, and other individuals with personnel/physical security responsibilities. MAJCOM/FOA/DRUs will determine those organizations and individuals within their organizations who will be given CAVS access. Clearance data elements in the CAVS include the full date and type of investigation and the full date and status of security clearance. The information is invalid when any of these four data elements are incomplete.

7.4.2.1. Use the most current highest level eligibility recorded in the CAVS when more than one entry appears for an individual.

7.4.2.2. An individual may have multiple SAR codes recorded in the CAVS if the individual is in multiple positions (i.e. civilian, reserve, or air national guard). The level of access given to the individual should be based on the access necessary for the position. Commanders make the decision on the level of access required.

7.4.2.3. The term “DCID 6/4 (formerly DCID 1/14)” means the person has been the subject of a SSBI, has been granted a Top Secret security clearance, is eligible for SCI

access if required for mission essential purposes (depending on the currency of the investigation) and or may already have SCI access. See AFMAN 14-304.

7.4.2.4. The CAVS will provide the following information:

7.4.2.4.1. An individual's security clearance level and access.

7.4.2.4.2. Visit and suspension notifications.

7.4.2.4.3. SCI indoctrination, nondisclosure statement, and debriefing dates.

7.4.2.4.4. Establishment of a SIF.

7.4.2.5. Access to the CAVS is restricted to Air Force employees only. Contractors and others who are assigned to an ISPM or SSO office must have prior approval by the SK Program Management Office (497 IG/INSP (PMO)) for access.

7.4.2.6. There are 7 User Levels in the CAVS. These levels are defined as follows:

7.4.2.6.1. Level 1: CAF personnel and Systems Administrators.

7.4.2.6.2. Level 2: MAJCOM/FOA/DRU SCI security personnel.

7.4.2.6.3. Level 3: Base SCI security personnel.

7.4.2.6.4. Level 4: MAJCOM/FOA/DRU non-SCI security personnel.

7.4.2.6.5. Level 5: Base ISPM security personnel.

7.4.2.6.6. Level 6: Entry Controller.

7.4.2.6.7. Level 7: Unit Level Security Manager.

7.4.2.7. User Levels have the following CAVS read and write access:

7.4.2.7.1. User levels 2-7 have read access to all Air Force personnel.

7.4.2.7.2. User levels 2 and 4 may write to records within their MAJCOM/FOA/DRU PASCODE.

7.4.2.7.3. User levels 3 and 5 may write to records within their local PASCODE and to records of individuals assigned to another MAJCOM/FOA/DRU supported by levels 3 and 5.

7.4.2.7.4. User level 6, entry controller, has the ability to verify an individual's clearance eligibility and access in the CAVS. MAJCOM/FOA/DRU may have reports printed for entry controllers by base ISPM security personnel (user level 5) listing the clearance eligibility and access of expected visitors. Reports will only be valid for the date and time printed.

7.4.2.7.5. User level 7 has the ability to write non-SCI access (interim, secret, and top secret); nondisclosure dates; NATO access; and the indoctrination/debriefing dates. Level 7 is also authorized to view non-SCI access history and print reports associated with their write capabilities.

7.4.2.8. ISPMs determine the number of users and the access level for each user within their command. The system administrator will establish user accounts. SK allows

unlimited users on one computer, but each user must have an individual account. A user account must be restricted to the registered user only.

7.4.2.9. User Levels 1-3 must have a Top Secret clearance based on an SSBI or PR. User Levels 4-7 require a Secret clearance based on an ENTNAC, NAC, NACLC, NACI, NACIC, or ANACI.

7.4.3. The CAF will publish and keep current a SK training guide with instructions on the use of AMS and CAVS. The CAF will review/update the SK web page at least monthly, to provide additional guidance and references as needed.

7.4.4. Requests for changes to SK must be forwarded by the MAJCOM/FOA/DRU Security Forces or Special Security Office (SSO) to the SK Requirements Group through the 497 IG/INSP, 229 Brookley Ave, Bolling AFB DC, 20332-7040.

7.4.5. SK will be replaced with the Joint Personnel Adjudication System (JPAS) which will be the DOD personnel security automated system that contains investigative and security clearance data.

7.5. Investigative Requirements for Air Force Deployments, Operational or Contractual Exigencies. This policy does not apply to SCI. Positions identified for deployments will, as a minimum, be assigned a NACLC, requiring access to Secret information for the in-country threat briefing. SSBIs are not authorized for purposes of Top Secret eligibility "just in case of" deployment. In these situations, commanders grant interim Top Secret access for a period of up to 180 days. This can be renewed for extended deployment purposes and for redeployment. Interim Top Secret access is granted for the purpose of deployment based on the existing NACLC, and discontinued upon return to home station. SSBIs will not be required for this purpose. Persons must be US citizens and have not had a break in service for more than 24 months. Record of the interim TS is annotated in JPAS or in cases where it is not available, documented and maintained with security related documents. However, SSBI is authorized if a joint or theater deployment requires a final Top Secret security clearance and will not accept interims, i.e., JCS contingencies. These requirements need to be identified and positions coded IAW **para 7.2** of this instruction.

7.6. Approval Authorities for Additional/New/Upgrade of SSBIs. 3-Star/Civilian Equivalent authority is required to approve any additional/new/upgrade SSBIs before the servicing Manpower Office codes the positions on the UMD. Approval authorized can not be delegated. Approval authorities are as follows:

7.6.1. MAJCOMs: CV or NAF/CC

7.6.1.1. The authorized requester forwards a copy of the MFR to the individual's security manager.

7.6.1.2. The authorized requester and the unit keep the MFR until the CAVS shows a final security clearance.

7.6.2. FOAs: parent 2-Ltr or SAF/AA or AF/CVA if the parent 2-Ltr is not at the appropriate grade level.

7.6.3. DRUs: AF/CVA.

7.6.4. HQ USAF:

7.6.4.1. Air Staff: AF/CVA

7.6.4.2. Secretariate: SAF/AA

7.6.5. Commands will establish internal certifying procedures. The approval documentation will be retained by the Manpower Office for three years and is subject to compliance review by HQ AFIA or their designee. Approval will increase MAJCOM funds withhold for personnel security investigations through the FYDP.

7.7. Periodic Reinvestigations. Periodic Reinvestigations will be kept current for incumbents assigned against positions coded as requiring SSBI and NACLC/ANACI. Also see **para A2.7**.

7.8. Issuing Security Clearance Eligibility. AFCAF issues security clearance eligibility and enters the determination into JPAS.

7.9. The Joint Personnel Adjudication System (JPAS). JPAS is the Department of Defense (DoD) personnel security clearance and access database. It facilitates personnel security management for the DoD Central Adjudication Facilities (CAF), security managers, and offers both non-SCI and SCI functions. It interfaces with the investigative providers, the personnel systems within the Department thus eliminating manual transactions and expediting the flow of personnel security information to warfighters.

7.9.1. JPAS is the primary source for determining investigative data/status of investigations on individuals in the DoD. JPAS allows communication between the CAFs and its customers. All information in JPAS is unclassified, but must be protected according to the requirements for privacy/sensitive information and For Official Use Only (FOUO) in accordance with AFI 33-332, Air Force Privacy Act Program and DoDR 5400.7/AF Supplement, DoD Freedom of Information Act Program.

7.9.2. JPAS has two applications: The Joint Adjudication Management System (JAMS) and Joint Clearance and Access Verification System (JCAVS)

7.9.2.1. JAMS is for adjudicative personnel only and provides capabilities such as case management/distribution, adjudication decisions, adjudicative history and summary, due process, and future ability for each CAF to electronically access investigative reports from the investigative providers.

7.9.2.1.1. JAMS replaced the Adjudicative Management System (AMS), as used throughout this instruction.

7.9.2.2. JCAVS is for non-SCI and SCI security managers/officers and authorized requesters and provides capabilities such as access indoctrination/debriefing history, incident/issue file reporting, history and management of unit personnel security functions.

7.9.2.2.1. JCAVS replaced Clearance and Access Verification System (CAVS), as used throughout this instruction.

7.9.3. ISPMs determine the number of users and the access levels for each user. Clearance data elements in the JCAVS include the full date and type of investigation and the full date and status of security clearance. The information is invalid when any of these four data elements are incomplete.

7.9.3.1. Use the most current highest level eligibility recorded in the JCAVS when more than one entry appears for an individual.

7.9.3.2. The term "DCID 6/4 (formerly DCID 1/14)" means the person has been the subject of a SSBI, has been granted a Top Secret security clearance eligibility, is eligible for SCI access if required for mission essential purposes and may already have SCI access. See AFMAN 14-304.

7.9.4. The JCAVS will provide the following information:

7.9.4.1. An individual's security clearance eligibility level and access level.

7.9.4.2. Visit notification.

7.9.4.3. Suspension notification.

7.9.4.4. SCI indoctrination, nondisclosure statement, and debriefing dates.

7.9.4.5. Establishment of a SIF.

7.9.5. JCAVS User Levels are as follows:

7.9.5.1. Level 2 - SCI security personnel at unified command, DoD agency, military installation or major command/equivalent headquarters. Personnel Security Management (PSM) - Net is determined by the responsible SOIC or designee. (Read and Write Access - SSBI/DCID 6/4 with current SCI Access.)

7.9.5.2. Level 3 - SCI security personnel at echelons subordinate to Level 2 at a particular geographic location (installation, base, post, naval vessel). PSM - Net is determined by the responsible SOIC or designee. (Read and Write Access - SSBI/DCID 6/4 with current SCI Access.)

7.9.5.3. Level 4 - Non-SCI security personnel at unified command, DoD agency, military department or major command/equivalent headquarters. PSM - Net is determined by the responsible Security Officer or designee. (Read and Write Access - NACLAC/ANACI/Secret Eligibility.)

7.9.5.4. Level 5 - Non-SCI security personnel at echelons subordinate to Level 4 at geographic location (installation, base, post, naval vessel). PSM - Net is determined by the responsible Security Officer or designee. (Read and Write Access - NACLC/ANACI/Secret Eligibility.)

7.9.5.5. Level 6 - Unit Security Manager (additional duty) responsible for security functions as determined by responsible senior security official. (Read and Write Access - NACLC/ANACI/Secret Eligibility.)

7.9.5.6. Level 7 - Non-SCI Entry Control Personnel. Individuals who grant access to installations, buildings, etc. Varies according to organizations. (Read Access - NACLC/ANACI/Secret Eligibility.)

7.9.5.7. Level 8 - SCI Entry Control Personnel. Individuals who grant access to SCIF installations, buildings, etc. Varies according to organizations. (Read Access - SSBI/DCID 6/4 Eligibility.)

7.9.5.8. Level 10 - Visitor Management. Level 10 users will have the same view of the JCAVS Personnel Summary as a JCAVS Level 7 User. They will receive Visit Notification when their Security Management Office (SMO) is being notified of a visit.

A Level 10 User may **not** be an account manager to create or delete an account at any level. NACLC/ANACI/Secret Eligibility.

7.10. AF JPAS Users Guide. Contains detailed instructions on operating JPAS and becoming a new user. See the follow URL: **https://wwwmil.lackland.af.mil/afsf/Organization/AFXOF/XOF%20memo%2012%20Jul%2004%20AF%20JPAS%20Guide1.pdf**. JPAS web site is: **https://jpas.osd.mil**. Requests for changes to JPAS may be made on-line at **https://jpas.osd.mil**.

7.11. Granting Access. Commanders grant access to classified information when a mission essential need exists and only when all of the following prerequisites are met: (1) individual has the appropriate security clearance eligibility; (2) individual has signed an SF 312 (see AFI 31-401); and (3) individual has a need-to-know. Authorized base level users will record access in the JCAVS. See **Chapter 3** for other situations when access to classified information may be granted.

7.12. Obtaining Information from the AFCAF.

7.12.1. Authorized requesters may contact the AFCAF Customer Support Section through JPAS. In situations where no security clearance data is available at the unit, no information is available in the JCAVS, and the AFCAF has valid security clearance information on file, a record of the call will be used as evidence of valid clearance data pending update of the JCAVS. The authorized requester prepares a memorandum for record (MFR) showing: (1) name, grade, and organization of the individual calling the AFCAF; (2) name, grade, organization, and SSN of the subject; (3) name of person at the AFCAF providing clearance eligibility data, and (4) type and date of investigation and, if granted, level and date of security clearance eligibility. Also see **para 6.1**.

7.12.1.1. The authorized requester forwards a copy of the MFR to the individual's security manager.

7.12.1.2. The authorized requester and the security manager keep the MFR until JCAVS is updated to show the data addressed in the MFR.

Chapter 8

UNFAVORABLE ADMINISTRATIVE ACTIONS

8.1. Referral for Action.

8.1.1. Security Information File (SIF). A SIF is a collection of documents generated as a result of the discovery or development of unfavorable information which brings into question a person's continuing eligibility for a security clearance or access to SCI. It may be established by a commander, civilian equivalent, or by the CAF. The SIF serves as a repository for unfavorable or derogatory information that requires further review, evaluation, or investigation to resolve outstanding administrative or adjudicative concerns. Report administrative change of status information for individuals with SCI access according to AFMAN 14-304.

8.1.2. Reporting Government Charge Card Abuses and Misuse. Security Officials, AFOSI, or AF Government Charge Card program coordinators are required to immediately report Government Charge Card abuses and misuses to the appropriate commander. This information constitutes serious questions as to the individual's ability or intent to protect classified information or execute sensitive duties. The commander will make an immediate determination to either leave the individual's security status unchanged or suspend their access to classified information or assignment to sensitive duties until the appropriate authority makes a final determination regarding the individual's eligibility to retain a security clearance. In addition, commanders may take action in accordance with **Chapter 8**, to determine if a SIF should be established and/or the person's access to classified information should be suspended.

8.1.3. Implementation of Restrictions on the Granting or Renewal of Security Clearances as Mandated by the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 – Smith Amendment. **Attachment 24** outlines the instructions.

8.2. Suspension.

8.2.1. Commander:

8.2.1.1. Reviews unfavorable information on individuals under the commander's jurisdiction when reported or developed which would directly impact an individual's security clearance or SCI access, to include the following (see **Attachment 11** for sample memorandum):

8.2.1.1.1. Activities' tenant or geographically separated units.

8.2.1.1.2. TDY personnel.

8.2.1.2. Establishes a SIF when an individual's activity, conduct or behavior is inconsistent with the security criteria specified in DOD 5200.2-R, para 2-200 and Appendix I. See **Attachment 12** for sample request for SIF establishment to the servicing security activity.

8.2.1.3. Determines whether or not to establish a SIF on a case by case basis, normally within 20 days of receipt of unfavorable information (as soon as possible if SCI access is involved). This decision is made by considering the seriousness of the incident; the

individual's motivation; whether it was out of character for the individual; or whether the undesirable conduct or behavior is likely to continue. Coordination and consultation with the chief of the servicing security activity, SSO (for SCI access) or program security officer (for SAP access) and legal representatives is recommended. However, if the commander has sufficient reason to doubt the validity of unfavorable information the decision to establish a SIF and notification to the CAF may be extended up to 45 days. If the servicing security activity and the commander disagree on establishment of a SIF, elevate the issue to the installation commander for resolution. Once a SIF is formally established it must be processed accordingly and only the CAF has closure authority.

8.2.1.3.1. Examples of reasons to establish a SIF are outlined in para 2-200, DOD 5200.2-R and include the following:

8.2.1.3.1.1. Refusal to sign a required SF 312 or other nondisclosure agreement.

8.2.1.3.1.2. Refusal or intentional failure of an individual requiring an investigation or periodic reinvestigation to provide the personnel security questionnaire information or release statements for review of medical, financial, or employment records.

8.2.1.3.1.3. Refusal by an individual to be interviewed in connection with a personnel security investigation, regardless of whether the information is requested by the investigative agency or the CAF.

8.2.1.3.1.4. Incidents of theft, embezzlement, child or spouse abuse, unauthorized sale or use of firearms, explosives, or dangerous weapons, or misuse or improper disposition of government property or other unlawful activities.

8.2.1.3.1.5. Information leading to permanent decertification from PRP for other than physical reasons.

8.2.1.3.2. The following are some examples of reasons that may not warrant establishment of a SIF:

8.2.1.3.2.1. Minor traffic violations.

8.2.1.3.2.2. Minor one-time alcohol related incident.

8.2.1.3.2.3. Permanent decertification from PRP related to medical reasons of a physical nature.

8.2.1.3.2.4. Disciplinary issues; such as failure to repair; poor duty performance; failure to maintain weight standards; and any single isolated incident of poor judgment based on immaturity or extenuating circumstances which does not impact on the individual's ability to safeguard classified information.

8.2.1.3.2.5. Federal civilian employees occupying nonsensitive positions.

8.2.1.3.2.6. Incidents where a SIF has already been established by the CAF based on the same unfavorable information.

8.2.1.4. Determines whether or not to initiate suspension action for the individual's access to classified information upon establishment of a SIF. If the decision is to suspend the person's access to classified information the same decision automatically applies to

the SCI and SAP access. The access to classified information and SCI is considered one under the new DOD personnel security common adjudicative guidelines. Additionally, the commander determines suspension of unescorted entry to restricted areas if applicable. The determination to suspend should be based on a thorough review of the facts and an assessment of the risk to national security. For SCI access see AFMAN 14-304 and DOD S-5105.21-M-1, *Sensitive Compartmented Information Administrative Manual*.

8.2.1.5. Notifies the individual accordingly with information copy to the servicing security activity. See **Attachment 13** and **Attachment 14** for sample memorandums.

8.2.1.6. Requests AFOSI investigation, if criminal activity is involved.

8.2.1.7. Includes a recommendation whether to grant, reinstate, deny, or revoke the individual's security clearance and or SCI/SAP access and the rationale for the decision in the completed SIF. The documented facts must fully support the recommendation. Refer to DOD 5200.2-R, Appendix I, Adjudicative Guidelines.

8.2.1.8. Requests the CAF to *immediately* close a SIF favorably via priority message (through the MAJCOM or activity SSO for SCI) when special circumstances exist (i.e., individual was falsely accused or holds a special expertise that is essential for mission accomplishment). The commander provides the CAF with the SIF (if not already at the CAF) and full justification for favorable closure. The CAF will then make the security clearance determination or request additional information, if necessary.

8.2.1.9. Endorses requests by Chief of Servicing Security Activity (SF), SSO, and Program Security Officer (PSO) for evaluations and relevant documentation from on base activities when issues warrant such coordination.

8.2.2. Chief of Servicing Security Activity, SSO, and PSO:

8.2.2.1. Provides guidance to commanders on SIF establishment. SF is OPR for Top Secret and Secret security clearance SIFs; SSO is OPR for SCI access SIFs.

8.2.2.2. Establishes, processes, maintains, monitors SIFs for commanders. See **Attachment 15** for sample memorandum for notification to the commander of SIF establishment. See **Attachment 16** for sample SIF custodian checklist.

8.2.2.3. Provides initial notification to the CAF upon SIF establishment via message or CAVS within 10 days. Provide full name, SSAN, security clearance data, date SIF established, reason, and if access to classified information and SCI has been suspended or withdrawn. If the individual has or is being processed for SCI access, forward the notification to the CAF through the MAJCOM or activity SSO. Notify the CAF via memorandum when the individual will be permitted to continue access to classified information and SCI access. See **Attachment 17** for sample memorandum. Notify the CAF via memorandum when the individual's access is withdrawn. Process SIFs concerning SCI access according to AFMAN 14-304. If SCI access is involved, the SSO is responsible for managing the SIF in its entirety to include actions required for the security clearance. SF, SSO, and PSO exchange notification information and coordinate actions with each other. Additionally, notify the CAF when:

8.2.2.3.1. Unfavorable information results in a discharge, retirement, or separation. Forward a copy of the discharge or separation orders or a copy of the SF 50B3PT, Notification of Personnel Action, plus any additional unfavorable information used in these actions. If discharge is involved and the individual is or has been indoctrinated for SCI in the past three years, see AFMAN 14-304 for discharge for cause procedures.

8.2.2.3.2. An adverse discharge is overturned and the individual returns to active duty.

8.2.2.4. Notifies the Installation Commander when SIFs are established. See **Attachment 18** for sample memorandum.

8.2.2.5. Requests evaluations and relevant documentation from the following activities when the issue involved indicates coordination is appropriate (see **Attachment 19**):

8.2.2.5.1. Director of Personnel. For any Unfavorable Information Files (UIF), performance report summaries, suitability determinations, and personnel actions.

8.2.2.5.2. Security Forces. For any criminal activities or other pertinent data regarding the subject's police record, involvement in previous compromises or security incidents.

8.2.2.5.3. Judge Advocate. For any court proceedings or nonjudicial punishment if legally supportable by nature of individual's actions. For suitability determinations and legal advice, when needed.

8.2.2.5.4. Surgeon General. For any physical, mental, or emotional evaluation that may affect the subject's ability to protect classified information.

8.2.2.5.5. Mental Health Clinic. For any reports of involvement, previous or present, with alcohol or dangerous drugs which may indicate security weakness.

8.2.2.6. Forwards SIF to the gaining servicing security activity or SSO when an individual transfers to another assignment. See **Attachment 20** for sample memorandum.

8.2.2.7. Forwards completed SIF, with required documentation, to the CAF for closure within 120 days. See **Attachment 21** for sample memorandum. If SCI access is involved forward the SIF through the MAJCOM or activity SSO to the CAF. See AFMAN 14-304 and DOD S5105.21-M-1 for SCI guidance. Refer to DOD 5200.2-R, Chapter 8-102d regarding suspension cases over 180 days. Use first class mail in accordance with DODM 4525-8AFSUP1, *Official Mail Manual*.

8.2.2.8. Contacts the CAF for an extension if SIF cannot be closed in 120 days.

8.2.2.9. Ensures all supporting documentation is included prior to submitting to the CAF. The commander's recommendation and rationale for the final decision must also be included. The following are examples of the types of required documentation relevant to the issue:

8.2.2.9.1. PSIs conducted by DSS, OPM, or similar agencies.

8.2.2.9.2. AFOSI reports of investigation, civil, police, or child advocacy reports.

8.2.2.9.3. Security forces incident or complaint reports and SSO reports.

8.2.2.9.4. Summaries of facts to substantiate any unfavorable information not covered by one of the investigative sources above. Include a complete reference to the source of the information.

8.2.2.9.5. Summaries of UIF entries.

8.2.2.9.6. Medical or mental health evaluations which indicate impairment of the individual's judgment or reliability. The report of evaluation must contain a diagnosis, its effect on the individual's judgment or reliability and prognosis along with any additional instructions or restrictions on the use of the information by appropriate medical authority.

8.2.2.9.7. Summaries of actions by Mental Health Clinics, such as, when individual was enrolled in the program; why the person was enrolled; how the program personnel categorized the individual's situation; a diagnosis and Mental Health authorities recommendations regarding subject's ability to safeguard classified information.

8.2.2.9.8. Reports showing the date of successful completion of a rehabilitation program, progress in a rehabilitation program, or the date termed a rehabilitative failure.

8.2.2.9.9. Summaries or actual report of administrative or disciplinary actions to include records of counseling, letters of reprimand, Article 15, Uniform Code of Military Justice (UCMJ), or courts-martial orders, bankruptcy petitions, discharge orders, or copies of letters of indebtedness.

8.2.2.9.10. Orders or written notification advising the status and location of individuals placed in retraining, on appellate leave, or rehabilitation or confinement status.

8.2.2.9.11. Reports relating to the withdrawal of access, including special access programs, unescorted entry, or decertification from PRP.

8.2.2.10. Forwards to the CAF within 60 days all SIFs returned from the CAF as incomplete. Requests an extension in writing to the CAF if an incomplete SIF cannot be completed in 60 days. When the SIF was established by the CAF, return the original case file to the CAF.

8.2.2.11. Maintains a suspense copy until the CAF has made the final determination, then destroys the SIF. If the individual had SCI access, destroy six months after accountability of the person ceases or when no longer needed, whichever is longer.

8.2.3. Unit Security Manager:

8.2.3.1. Implements the personnel security program within the organization and provides support to the servicing security activity or SSO.

8.2.4. The CAF:

8.2.4.1. Adjudicates the information contained in the SIF and makes a final security clearance and or SCI access determination.

8.2.4.2. Requests a Special Investigative Inquiry from DSS or a Reimbursable Suitability Investigation from OPM when required in order to make an adjudicative decision.

8.2.4.3. Forwards the notification of eligibility decision to the commander (through the MAJCOM or activity SSO for SCI access) and updates the AMS and DCII with the eligibility determination.

8.2.4.4. Initiates and oversees due process procedures when security clearance eligibility and or access is denied, revoked, or suspended.

8.2.4.5. Returns incomplete SIFs to commanders, through the servicing security activity, with a request for: (1) the required documentation; (2) the commander's recommendation (3) an update on the individual's current situation; and or (4) actions taken, expected, or pending.

8.2.4.6. Establishes SIFs when unfavorable information is provided from other government agencies, court-martial orders, information summary reports from DSS, AFOSI reports of investigation, and notification of special access denial from various access granting authorities. Notifies the commander for further action, when necessary.

8.3. Air Force Office of Special Investigations. AFOSI conducts personnel security investigation leads in overseas areas for DSS. All Air Force commanders must report to AFOSI any alleged criminal activity falling under the security standards criteria. A table of offenses by case category that AFOSI investigates is available in AFI 71- 101, Volume I, *Criminal Investigations.*

8.4. Final Unfavorable Administrative Actions.

8.4.1. The CAF is the designated authority to make personnel security determinations that can result in an unfavorable administrative action. Commanders take actions for removal due to unsuitability IAW 5 CFR 731.201-202, Suitability for Government Employment, at the same time as actions are being taken for denial or revocation of a person's security clearance. The unfavorable administrative action on civilian personnel may not include any reference to security clearance issues until the results of the final security adjudication are available.

8.5. Procedures.

8.5.1. General. The CAF will make a final personnel security determination resulting in an unfavorable clearance action on an Air Force member, civilian employee, contractor (for SCI), or any other Air Force affiliated person when the individual concerned has been afforded due process procedures according to this AFI and DOD 5200.2-R. These same due process procedures are also applicable for suspension, denial, or revocation of access to SCI. There is no distinction between a security clearance and SCI access in the adjudication process. If a clearance is revoked or denied, SCI access is also revoked or denied. The CAF will notify individuals concerning unfavorable administrative actions using the instructions in this AFI and DOD 5200.2-R. Although SAP access is also revoked or denied when a clearance is revoked or denied, administrative recourse (appeal) procedures are separate and distinct. See AFI 16-702, *The Appeal Board (for Special Access Programs).*

8.5.2. The Air Force is not authorized to make any adverse security clearance determination on a civilian employee occupying a nonsensitive position. Since such positions do not

involve sensitive duties or access to classified information, the provisions of the personnel security program regarding security clearance eligibility do not apply.

8.5.3. Confinement. When it is determined that an applicant for a security clearance, or a person holding a clearance, has been convicted of a crime and sentenced to imprisonment for more than one year, the clearance of such person shall be denied or revoked with the following actions taken by the CAF:

8.5.3.1. Verification that the individual is presently imprisoned, serving a term of more than 12 months.

8.5.3.2. A Notice of Revocation or Denial of Security Clearance Eligibility forwarded through the Servicing Security Activity and SSO (for SCI) to the individual and the commander. The Notice is final and no rebuttal privileges or appeal rights are applicable.

8.5.3.3. The revocation or denial action is entered in DCII and AMS.

8.6. Unfavorable Administrative Action Procedures.

8.6.1. Denial Authority. The CAF provides individuals with written statements of reasons and other required documentation stating intent to deny or revoke their security clearances and SCI access using sample format in DOD 5200.2-R, App L and Atch 11.

8.6.2. Instructions. Individuals may appeal unfavorable administrative actions according to the instructions in this AFI, DOD 5200.2-R, Chapter 8, and Appendix L and M. Individuals send communications to the CAF and the local supporting Staff Judge Advocate (SJA) through their commanders.

8.6.3. Designated Point of Contact (POC). Unit commanders will designate a POC to serve as a liaison between the CAF and individuals under their jurisdiction when unfavorable administrative actions are being taken. POCs conduct the associated duties as outlined in DOD 5200.2-R, Appendix L-2. The CAF will send communications to the individual through the commander, SF, and SSO (for SCI). The supporting SJA will provide the Defense Office of Hearings and Appeals (DOHA) Administrative Judge (AJ) appropriate legal support, upon request.

8.6.4. Individual's Response to the CAF. Individuals must advise the CAF in writing of their intent to respond to the statements of reasons. This must be done within ten days of receipt of the statement of reasons. Individuals state whether they intend to submit statements or documents to refute, correct, or mitigate the intended actions. Within 60 days from the date of receipt of statements of reasons, individuals must provide the CAF with their written rebuttals.

8.6.5. Extensions. Extensions may only be granted by the CAF. A written request for an extension for up to 30 days can be submitted to the CAF through the POC and installation or unit commander.

8.6.6. CAF Review of Individual's Response to the Statement of Reasons. Upon receipt of the rebuttal, the CAF will determine whether a security clearance should be reinstated, revoked, or denied and a final response will be provided to the individual. This must be done within 60 days from the date of receipt of the individual's response. If a final response cannot be completed within 60 days, the individual must be notified in writing of this fact, the

reasons, and the date a final response is expected. AMS will be updated to reflect the CAF decision.

8.6.7. CAF Decision to Deny or Revoke. If the CAF decision is to deny or revoke a person's security clearance the reasons for the final action will be included in a Letter of Denial/Revocation to the individual. Individuals will be afforded an opportunity to appeal to a letter of denial/revocation through the Personnel Security Appeal Board (PSAB) by ***one*** of two methods as outlined in this section and DOD 5200.2-R: (1) appeal *without* a personal appearance; or (2) appeal *with* a personal appearance before an Administrative Judge (AJ) from DOHA. Individuals must elect either (1) or (2); individuals may not do both. The CAF will process appeal cases as outlined in DOD 5200.2-R, Appendix L and Atch 11.

8.6.7.1. Appeal Without a Personal Appearance. Individuals directly notify the PSAB of their intent to appeal without a personal appearance within 10 days of receipt of the letter of denial/revocation. Address requests to: President, Personnel Security Appeal Board, NAIC/IAN, 5113 Leesburg Pike, Falls Church, VA 22041-3230. Individuals send their appeals to the President of the PSAB within 40 days of receipt of the letter of denial/revocation.

8.6.7.2. Appeal With a Personal Appearance. Individuals include the name and telephone number of the supporting SJA when requesting a personal appearance from DOHA (see **Attachment 13**). The POC will provide this information to the individual. DOHA initially contacts the SJA for support with the appeal proceedings. Individuals advise DOHA in writing of their desire for a personal appearance within 10 days of receipt of the letters of denial/revocation. Copies of these advisement's are provided to the following: the POC, the supporting SJA, and the CAF. The SJA will coordinate with the DOHA AJ to assist in providing legal support, upon request and will advise on legal matters to the commander and the POC. The CAF will provide the individual's case file to DOHA within 10 days upon DOHA's request. A DOHA AJ will hear the individual's case and forward the file, transcripts, any documentation obtained from the individual, and a recommendation to sustain or overturn the letter of denial/revocation to the PSAB. The deadline for this is 30 days after the personal appearance. The AJ provides the CAF with a copy of the recommendation.

8.6.7.2.1. Within CONUS personal appearances will be conducted at the individual's duty station or at a nearby location for duty stations within the lower 48 states. For personnel assigned OCONUS, the appearances will be conducted at: (1) the individual's duty station or a nearby suitable location; or (2) at DOHA facilities located in the metropolitan area of Washington, DC, or Los Angeles, California. The Director, DOHA or designee determines the appearance location. Travel and TDY costs for the individual will be the responsibility of the employing organization.

8.6.8. Personnel Security Appeal Board (PSAB). The PSAB will review the individuals appeal package, along with DOHA recommendation (if applicable) and notify the individual through the CAF of the board's final decision. See **Attachment 5** for additional guidance on the PSAB.

8.7. Security Clearance Reinstatement. An individual's commander may request reinstatement of their security clearance 12 months after the effective date of revocation or denial or decision of the PSAB, whichever is later. Requests should be sent to the CAF with the

commander's recommendation for approval. The commander includes an explanation on how the individual's behavior has improved and the appropriate documentation corresponding to the reason(s) for the denial or revocation. The documentation required depends on the reason(s) involved, such as, evaluation for mental health issues, evaluation for drug or alcohol abuse; or current financial statement(s).

8.8. Special Access Programs. Administrative due process for special access programs is handled separately. See AFI 16-702, *The Appeal Board (for Special Access Programs).*

8.9. Obtaining Permission to Proceed in Courts-Martial, Administrative Discharges, and Civilian Removal Actions.

8.9.1. Unit commanders contemplating disciplinary or administrative action against military members or civilian employees that could lead to a discharge or removal must first obtain permission to proceed when personnel hold a special access. Do not take action on personnel who now hold or have held access within the periods specified below, to Single Integrated Operational Plan-Extremely Sensitive Information (SIOPESI), SCI, research and development (R&D) special access program, AFOSI special access program, or other special access program information until the appropriate special access program office approves. (Exceptions are for investigative and preliminary administrative procedures until the proposed action has been reviewed and approved by the functional activities having overall ownership for the affected information.) Commanders send a written request to the appropriate special access program functional office for permission to proceed with further processing as outlined below. Apply security classification according to message contents. The request must include:

8.9.1.1. The individual's name, SSAN, age, marital status, duty assignment, unit assignment, date of separation and length of service of the member.

8.9.1.2. The name of the official who authorized SCI or other special access. Include inclusive dates that the person was given access and the units involved.

8.9.1.3. The specific reason for the proposed "for cause" action. Include the maximum sentence and type of separation, or discharge, or dismissal allowable.

8.9.1.4. The type of separation, discharge, or dismissal contemplated in administrative cases, and the commander's recommended type of discharge certificate to be issued.

8.9.1.5. The type of court-martial, to include a description of offenses, with an outline of proposed charges and specifications; data as to any restraint; and any unusual circumstances which may affect the trial.

8.9.1.6. Comparable data for civilian employees.

8.9.1.7. Any other information bearing on the proposed action.

8.9.2. For SCI access contact the servicing MAJCOM or FOA Senior Intelligence Officer (SIO) for persons having current SCI access, and persons debriefed within the past three years, where damage assessment is considered *minimal.* Contact the servicing Special Security Office (SSO) to determine if the individual had SCI access. Commanders will continue to forward "Authority to Proceed" requests, where disclosure could result in *serious* damage, to SSO HQ USAF/INSD for AF Director of Intelligence, Surveillance and Reconnaissance (HQ USAF/XOI) approval. Send the request as a Defense Special Security

Communications System (DSSCS) message through the SSO to the MAJCOM or FOA SIO and to SSO HQ USAF/INSD. See AFMAN 14-304 for detailed instructions on how to prepare the DSSCS message.

8.9.3. For SIOP-ESI access. Refer to AFI 10-1102, Safeguarding the Single Integrated Operational Plan (SIOP).

8.9.4. For R&D access contact SAF/AQL for persons having current access to R&D special access programs and persons debriefed within the past year.

8.9.5. For persons who have had a duty assignment with AFOSI and have held an AFOSI special access contact HQ AFOSI/IVO. The personnel records will reflect AFOSI employment or assignment. Commanders contact the local AFOSI detachment commander or HQ AFOSI/IVO to determine if the person held an AFOSI special access.

8.9.6. For multiple accesses, commanders must obtain separate authorizations from each appropriate action agency listed above prior to proceeding.

8.9.7. Processing goals at all command levels must comply with the speedy trial requirement and the potentially more restrictive time requirements in civilian removal actions. Normally, the processing time period should be concluded within 15 days; measured from the date of initiation request, to the date of approval; or denial by the OPR. Voluntary separations of airmen, officers, and civilian resignations will not be handled under these procedures unless they are in lieu of adverse action. For voluntary separations that are in lieu of adverse action, do not allow the separation authority to approve the separation until the appropriate action office grants authority to proceed.

8.9.8. If a commander contemplates a general or special court-martial, processing of the case may proceed through preferral of charges and completion of the investigation required by Article 32, UCMJ together with collateral actions required under Article 32. Under no circumstances may the charges be referred to trial until the appropriate action office grants authority to proceed. Actions required by this paragraph do not apply to summary court-martials.

8.9.9. If a commander contemplates discharging an enlisted member, processing of a "notification" case or a board hearing entitlement may proceed through giving the member notice of the proposed discharge, obtaining the member's response, scheduling necessary appointments, and conducting those appointments. Under no circumstances may the discharge be "approved" by the separation authority until the appropriate action office grants authority to proceed. For board hearing cases, the processing may proceed through initiation of the case, obtaining the member’s response, scheduling necessary appointments, and conducting those appointments. Under no circumstances may the convening authority order the board to be convened to hear the case until the appropriate action office grants authority to proceed.

8.9.10. If a commander or staff agency chief contemplates discharging an officer, the show cause authority may not initiate the discharge, issue the show cause memorandum, or otherwise require officers to show cause for retention until the appropriate action office grants authority to proceed.

8.9.11. If a supervisor contemplates removal action against a civilian employee who holds special access, the supervisor must first coordinate with the servicing CPF. The commander of the unit to which the civilian is assigned will then forward a message to the appropriate Air Force OPR. Under no circumstances may a "notice of proposed removal" be issued until the Air Force OPR grants authority to proceed.

8.9.12. Periodic reporting by the unit commanders should advise the parent MAJCOM and decision authority of any changes to the proposed action every 90 days until the action has been completed. If the nature of the case changes significantly (for example, from discharge to court martial or from voluntary to involuntary discharge), the unit commander should notify the decision authority and seek further instruction. Unit commanders should transmit a final report when the adverse action has been completed. In the final report, include date and place of discharge. If a SIF has been established on the individual, the commander will notify the CAF of the discharge, and request closure of the SIF.

8.9.13. Decision authorities submit an annual report of completed cases showing the number of cases considered, number of approvals and disapprovals, and number pending as of the end of the fiscal year to SAF/AAZ, 1720 Air Force Pentagon, Washington DC 203301720. For SCI: Quarterly Reporting Requirement (Jan/Apr/Jul/Oct): MAJCOM and FOA SIOs will submit quarterly reports to 497 IG/INSD (SSO), 229 Brookley Ave, Bolling AFB DC 20332-7040. For case management and control purposes include in the reports (1) name, grade, SSAN, organization; (2) reason for action (drug abuse, minor disciplinary infraction, etc); (3) proposed action (type discharge or court martial); (4) date authority to proceed given by SIO; and (5) current disposition (indicate whether case is open or closed). If closed, show type and date of discharge.

Chapter 9

CONTINUING SECURITY RESPONSIBILITIES

9.1. Evaluating Continued Security Clearance.

9.1.1. Commanders and supervisors:

9.1.1.1. Continuously evaluate cleared personnel to ensure they continue to be trustworthy in accordance with the standards in DOD 5200.2-R, Chapter 2.

9.1.1.2. Determine the appropriate steps to take when information or actions occur that bring into question a person's compliance with the adjudication guidelines. See **Chapter 8** for unfavorable administrative actions.

9.2. Supervisory Responsibility. Supervisors do not review the security forms of anyone undergoing a periodic reinvestigation. Supervisory knowledge of any significant adverse information is to be independent of the information reflected on the security form.

9.3. Initial Briefings and Refresher Briefings. Commanders, supervisors, and or security managers provide initial and refresher briefings to individuals with security clearance eligibility to ensure they are knowledgeable to execute security responsibilities tailored to the specific job requirements. These briefings will emphasize the individual's responsibility to meet the standards and criteria for a security clearance as stated in DOD 5200.2-R.

9.4. Foreign Travel Briefing. Individuals possessing a security clearance will report to their security manager or supervisor contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities, when:

9.4.1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

9.4.2. Individuals are concerned that they may be the target of exploitation by a foreign entity.

9.5. Termination Briefing. Security Managers execute AF 2587, **Security Termination Statement** according to AFI 31-401.

Chapter 10

SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS

10.1. Responsibilities. The CAF will establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records under its jurisdiction as required by DOD 5200.2-R, Chapter 10.

10.2. Access Restrictions.

10.2.1. The CAF will approve release of completed reports of investigation to appropriate officials for mission essential needs, such as public trust determinations, suitability determinations and appeal decisions. These reports will be safeguarded according to DOD 5200.2-R, Chapter X and not released further without permission from the CAF. HQ AFOSI may request investigations from DSS.

10.2.2. See AFI 33-332, *Air Force Privacy Act Program* and DOD 5400.7-R/AF Supplement AFI 37-131, *Freedom of Information Act Program.*

10.3. Safeguarding Procedures. Officials authorized to receive completed investigation reports ensure the appropriate safeguarding measures are in place in accordance with DOD 5200.2-R, Chapter X.

Chapter 11

PROGRAM MANAGEMENT

11.1. Responsibilities.

11.1.1. Chief, Information Security Division, Air Force Chief of Security Forces (HQ USAF/XOFI), 1340 Air Force Pentagon, Washington DC 203301340, develops Air Force personnel security policy.

11.1.2. Director of Intelligence Surveillance and Reconnaissance (HQ USAF/XOI) is responsible for SCI policy. HQ USAF/XOI has designated:

11.1.2.1. The 497 IG/INS (CAF), 229 Brookley Avenue, Bolling AFB DC 20332-7040, to serve as the single authority to grant, suspend, deny, or revoke personnel security clearance eligibility's and SCI accesses, as well as the determinations of acceptability or non-acceptability for assignment or retention of personnel in sensitive positions.

11.1.2.2. Air Force Intelligence Security (HQ USAF/XOIIS) as the cognizant security authority (CSA) for the development and promulgation of the Air Force SCI security policy.

11.1.2.3. The Personnel Security Appeal Board as the appeal authority for personnel security clearances and SCI access (see **Attachment 5**).

11.1.3. The CAF is the single issuing authority for LAAs. The CAF is also the Office of Primary Responsibility (OPR) for the LAA, PSP, and SK.

11.1.4. ISPMs at MAJCOM and installation levels implement the personnel security program.

11.1.5. Commanders ensure:

11.1.5.1. Security managers are appointed to implement their personnel security programs.

11.1.5.2. Personnel security program oversight is included in self-inspections, unit inspections, program reviews and metrics.

11.1.5.3. Continuing evaluation of personnel with security clearances (see **Chapter 9**).

Chapter 12

DELETED

12.1. (DELETED)

RONALD E. KEYS, Lt General, USAF
DCS/Air & Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 10-1102, *Safeguarding Single Integrated Operational Plan (SIOP)*

AFI 16-701, *The US Air Force Special Access Programs*

AFI 16-702, *The Appeal Board (for Special Access Programs)*

AFI 31-401, *Information Security Program Management*

AFI 33-332, *Air Force Privacy Act Program*

AFI 34-301, *Nonappropriated Fund Personnel Management and Administration*

AFI 36-2005, *Appointment in Commissioned Grades and Designation and Assignment in Professional Categories Reserve of the Air Force and United States Air Force*

AFI 36-2104, *Nuclear Weapons Personnel Reliability Program*

AFI 41-210, *Patient Administration Functions*

AFI 71-101, Volume I, *Criminal Investigations*

AFH 31-502, *Personnel Security Program Policy*

AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (SCI)*

AFMAN 37-139, *Records Disposition Schedule*

AFPD 31-5, *Investigations, Clearances, and Program Requirements*

AFPD 34-3, *Nonappropriated Funds Personnel Management and Administration*

DCID 6/4, *"Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information"*

DODM 4525-8AFSUP1, *Official Mail Manual*

DOD S-51105.21-M-1, *Sensitive Compartmented Information Administrative Manual*

DOD Regulation 5200.2-R, *DoD Personnel Security Program*

DOD 5210.42, *Nuclear Weapons Personnel Reliability Program*

DOD 5210.55, *Department of Defense Presidential Support Program*

DOD 5210.87, *Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities*

DOD 5400.7-R/AF Supplement 37-131, *Freedom of Information Act Program*

Abbreviations and Acronyms

AF—Air Force

AFH—Air Force Handbook

AFI—Air Force Instruction

AFOSI— Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFR—Air Force Regulation

AFSC—Air Force Specialty Codes

AIS—Automated Information Systems

AMS—Adjudication Management System

ANACI—Access National Agency Check with Written Inquiries and Credit Check

ASCAS—Automated Security Clearance Approval System

BI—Background Investigation

CAF—Central Adjudication Facility

CAVS—Clearance and Access Verification System

CEIC—Catch'Em In CONUS

CONUS—Continental United States

CPF—Civilian Personnel Flight

DCII—Defense Clearance and Investigations Index

DCID—Director of Central Intelligence Directive

DCPDS—Defense Civilian Personnel Data System

DSS—Defense Security Service

DOD—Department of Defense

DRU—Direct Reporting Unit

ENTNAC—Entrance National Agency Check

EPSQ—Electronic Personnel Security Questionnaire

ESI—Extremely Sensitive Information

FBI—Federal Bureau of Investigations

FOA—Field Operating Agency

HQ USAF—Headquarters United States Air Force

IMA—Individual Mobilization Augmentee

ISPM—Information Security Program Manager

LAA—Limited Access Authorization

LFC—Local Files Check

MAJCOM—Major Command

MEPS—Military Entrance Processing Station

NAC—National Agency Check

NACIC—National Agency Check with Written Inquiries and Credit Check

NACLC—National Agency Check with Local Agency Check and Credit Check

NAFI—Nonappropriated Fund Instrumentalities

NAQ—National Agency Questionnaire

NATO—North Atlantic Treaty Organization

NdA—Nondisclosure Agreement

OPM—Office of Personnel Management

OPR—Office of Primary Responsibility

PCS—Permanent Change of Station

PCIII—Personnel Concept III

PDS—Personnel Data System

PR—Periodic Reinvestigation

PRP—Personnel Reliability Program

PSAB—Personnel Security Appeal Board

PSI—Personnel Security Investigation

PSO—Program Security Officer

PSP—Presidential Support Program

PSQ—Personnel Security Questionnaire

R&D—Research & Development

SAC—Single Agency Check

SAF—Secretary of the Air Force

SAP—Special Access Program

SAR—Security Access Requirement

SBI—Special Background Investigation

SCI—Sensitive Compartmented Information

SIF—Security Information File

SII—Special Investigative Inquiry

SIOP—Single Integrated Operational Plan

SIOP-ESI—Single Integrated Operational Plan -Extremely Sensitive Information

SK—SENTINEL KEY

SSN—Social Security Number

SSBI—Single Scope Background Investigation

SIF—Security Information File

TDY—Temporary Duty

UCMJ—Uniform Code of Military Justice

UIF—Unfavorable Information File

UMD—Unit Manpower Document

U.S.C.—United States Code

497 IG/INS—497th Intelligence Group/Directorate of Security and Communications Management

Terms

Authorized Requester—Organizations authorized to request Personnel Security Investigations (PSIs) from DSS or OPM. The servicing security forces activity usually requests PSIs from DSS. The CPF requests National Agency Check with Written Inquiries and Credit Check (NACICs) and Access National Agency Check with Written Inquiries and Credit Check (ANACIs) from OPM.

Authorized Requester Code Listing—A listing of organizations specifically designated by MAJCOM, FOA, or DRU to request PSIs.

Break In Service—Any break in active employment with a Federal agency or DOD contractor, including suspension or termination of service or temporary retirement, whether or not seniority or pay is affected. This does not include active duty military personnel attending civilian schools from which a service commitment remains. A 24-month continuous break in service requires completion of a new PSI prior to reissuance of a security clearance eligibility.

Catch'Em In CONUS—A DSS Program utilized to facilitate the completion of an SSBI or SSBI-PR on individuals who are within 180 days of departing for an overseas assignment. This program allows the DSS investigator to conduct the personal interview prior to PCS.

Central Adjudication Facility (CAF)—A single facility designated by the head of the DOD Component to evaluate PSIs and other relevant information and to render final personnel security determinations. The 497 IG/INS is the CAF for the Air Force.

Classified Information Nondisclosure Agreement, Standard Form 312—An individual must sign a Standard Form 312 before being given access to classified information.

Cohabitant—A person living in a spouse-like relationship with another person.

Continuing Evaluation—Procedures employed to ensure an individual remains eligible for access to classified information.

Critical Sensitive Position—Include positions involving any of the following: Access to Top Secret defense information; development or approval of war plans, plans or particulars of future or major special operations of war, or critical and extremely important items of war; investigative duties, the issuance of personnel security clearances, or duty on personnel security

appeal boards, computer and or computer-related positions designed AIS I, or other positions related to national security, regardless of duties that require the same degree of trust.

Defense Civilian Personnel Data System (DCPDS)—Method used to transmit civilian personnel data to or from an installation.

Defense Security Service (DSS)—The personnel security investigative agency for DOD to include the military departments, defense agencies and DOD contractors.

Escorted Entry—A situation where personnel are required to be escorted into a restricted area and kept under surveillance by authorized personnel while in the area.

Foreign National—Any person who is neither a citizen nor national of the United States nor an immigrant alien. Also referred to as a non-United States national.

Foreign Travel—Any travel outside the 50 United States and its territories.

Immediate Family—Includes: father, mother, brother, sister, spouse, cohabitant, son, daughter. The basis of the relationship is immaterial: included are stepparents, foster parents, brothers and sisters by adoption, half-brothers and half-sisters, foster brothers and sisters, adopted children, stepchildren, and foster children.

Indoctrination Briefing—A briefing of job related security responsibilities and requirements, intelligence collection techniques employed by foreign intelligence activities, and penalties that may be imposed for security violations.

Installation Records Check—An investigation conducted through the records of all installations of an individual's identified residences for the preceding 2 years before the date of the application. This record check shall include at a minimum, police (base and or military police, security office, or criminal investigators or local law enforcement) local files check, Drug and Alcohol Program, Family Housing, Medical Treatment Facility for Family Advocacy Program to include Service Central Registry records and mental health records, and any other record checks as appropriate, to the extent permitted by law.

Local Files Check (LFC)—A local check of the security forces, medical facility, personnel files, etc., designed to uncover the existence of unfavorable information concerning a person.

Nonappropriated Fund Instrumentalities (NAFI) Employee—Personnel hired by the DOD components, compensated from NAFI funds. This includes temporary employees, 18 years or older, who work with children.

Nonappropriated Fund Position of Trust (NAF)—An employee whose duties are fiduciary in nature and require a high degree of trust and integrity to ensure the safety of people, protection of money or property or who could directly and adversely affect the mission of the organization.

Noncritical—Sensitive Position-Includes positions that involve access to Secret or Confidential national security material or information; or duties that may directly or indirectly adversely affect the national security operations of the agency.

Personnel Data System (PDS)—Method used to transmit personnel data from or to an installation.

Personnel Reliability Program (PRP)—A program designed to ensure the highest possible standards of individual reliability in personnel performing duties associated with nuclear weapons systems and critical components.

Personnel Security—A criterion of security based upon standards that must be met for clearance or assignment to sensitive duties. The allegiance, reliability, trustworthiness and judgment of the individual being considered for such positions must be assessed to ensure that the placement of each individual in such a position is clearly consistent with the interests of national security.

Personnel Security Appeal Board—Designated representatives review appeals to denials or revocations of security clearances.

Presidential Support—Personnel assigned to duties involving regular or frequent contact with or access to the President or Presidential facilities, communication activities, or modes of transportation.

Program Security Officer—The government official who administers the security policies for the Special Access Program (SAP).

Restricted Area—A legally established military zone under Air Force jurisdiction into which persons may not enter without specific authorization.

Secret Clearance—The individual has been granted eligibility to information classified Secret or below.

Security Access Requirement—A code used to manage and control security clearances within the Air Force. It identifies the level of access required for day-to-day job performance. The security access requirement code is based upon the supervisors or commanders determination of level of access required for each position and the security clearance eligibility determined by the CAF for the incumbent.

Security Clearance—A determination that a person has met the standards of DOD and Air Force personnel security programs for eligibility to classified information.

Sensitive Compartmented Information (SCI)—Classified information concerning or derived from intelligence sources, methods, or analytical processes which must be processed exclusively within formal access control systems established by the Director of Central Intelligence.

SENTINEL KEY—The Air Force system of records for personnel security and access information. Replaces the ASCAS.

Service—Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in government service, or civilian employment with a DOD contractor involving access under the National Industrial Security Program. Continuity of service is maintained with change from one status to another provided no single break in service is greater than 24 months.

SCI Screening Interview—A representative from the SSO or a security manager will conduct an interview to assist in determining the acceptability of an individual for nomination and further processing for a position requiring access to SCI. This interview is conducted when there is no

current investigative information available to make an adjudicative determination of eligibility for immediate access to SCI.

Sensitive Position—Any civilian position designated within the Air Force wherein the occupant could cause by virtue of the nature of the position a materially adverse effect on national security. All federal civilian positions are designated either special sensitive, critical sensitive, noncritical sensitive, or nonsensitive.

Servicing Security Activity—The activity, designated by the commander, that supports the installation population and tenant units in all areas of personnel security program implementation.

Single Agency Check—A check of one or more designated agencies of a NAC.

Single Scope Background Investigation (SSBI)—A PSI covering 7 years of a person's history (10 years for employment, residence, and education). It is used to determine acceptability for a Top Secret security clearance, access to specific special access programs, or access to SCI.

Top Secret Clearance—The individual has been granted eligibility to Top Secret information or below.

Trustworthiness Determination—A determination made by commanders to protect DOD property and resources under their jurisdiction.

Unescorted Entry—Authority for an individual to enter and move about a restricted area without escort.

Unfavorable Information—Information that could justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

Unfavorable Personnel Security Determinations—A denial or revocation of a person’s security clearance; denial or revocation of access to classified information; denial or revocation of special access authorization (including SCI access); non-appointment to or non-selection for appointment to a sensitive position; non-appointment to or non-selection for any other position requiring a trustworthiness determination; reassignment to a position of lesser sensitivity or to a nonsensitive position; and non-acceptance for or discharge from the armed forces when any of the foregoing actions are based on derogatory information of personnel security significant.

Attachment 2

REQUEST PROCEDURES

A2.1. General

A2.1.1. Security managers:

A2.1.1.1. Process completed personnel security questionnaires for active duty, reserve military, National Guard, civilian and or contractor personnel to the unit's supporting authorized requester of investigations IAW with this AFI. See **Attachment 3** for required security forms, types of investigations to request and in what situations. An individual must have one year retainability for an investigation to be requested.

A2.1.1.2. Verify the most recent or most significant claimed attendance, degree or diploma at an educational institution. This is not required for Periodic Reinvestigations.

A2.1.1.3. Verify the date and place of birth through a check of appropriate documentation, e.g., a birth certificate, certificate of naturalization, passport, or Report of Birth Abroad of a Citizen of the United States of America. This is not required for Periodic Reinvestigations.

A2.1.1.4. Show the verification of birth and highest level of education on the SF 86/EPSQ software.

A2.1.2. The subject will provide the required documentation to the security manager.

A2.1.3. Air Force Reserves and IMAs. The Air Force Reserve Recruiting Service (AFRS/RS) processes reservist's initial personnel security investigation during accession to the supporting authorized requester.

A2.2. Authorized Requesters.

A2.2.1. Authorized Requestors for Accessions.

A2.2.1.1. HQ AFRS submits initial investigations (NACLC) for enlisted recruits through the Air Force Recruiting Information Support System (AFRISS).

A2.2.1.1.1. 319 TRS/DPAS:

A2.2.1.1.1.1. Verifies that the NACLC, submitted by AFRS, is open by checking JPAS and the OPM help desk, if necessary. When an open NACLC cannot be confirmed through either source, the 319 TRS/DPAS:

A2.2.1.1.1.1.1. Submits a new NACLC and file a copy of the submitted investigation in the member's Unit Personnel Record Group (UPRG).

A2.2.1.1.1.2. Submits SSBI investigation requests to OPM for all personnel training into a sensitive skill. A copy of the investigation request and receipt will be filed in the member's UPRG. On arrival at the student's technical training location, security managers will remove the investigation package and forward to the servicing security activity.

A2.2.1.1.1.3. Processes priority SSBI investigations for authorized AFSCs. HQ AETC/SFI, in conjunction with AF/XOS-FI, is the approval authority for priority

investigations for accessions.

A2.2.1.2. Officer accession sources submit initial investigations (NACLC) to OPM for recruits, normally within 30 days of their contract obligation to the Air Force.

A2.2.1.3. Officer accession sources submit SSBI investigation requests to OPM for personnel training into a sensitive skill.

A2.2.1.4. Losing authorized requesters and AFRS submit SSBI requests for prior service and non-prior service OTS selects prior to their departure.

A2.2.2. Authorized Requesters for Non-Accessions:

A2.2.2.1. Request personnel security investigations according to position coding requirements (see **para 7.2** and **Attachment 22**). See **Attachment 3**, for required security forms, types of investigations to request. Submit investigation requests to OPM.

A2.2.2.2. Use the EPSQ software as the primary source for the investigative request. Validate the EPSQ, and print a hard copy for mailing investigation requests to OPM. OPM does not have electronic transmission capability.

A2.2.2.2.1. For additional EPSQ guidance consult the DSS web site: **http://www.dss.mil**. Contact DSS Customer Service Center at 1-800-542-0237 or DSN 283-7731, if necessary.

A2.2.2.3. Request all types of investigations from OPM, as the DoD Authorized Investigation Provider. Use OPM Investigation Handbook, IS-15, Requesting OPM Personnel Investigations. It can be accessed via AF/XOS-FI web: **https://wwwmil.lackland.af.mil/afsf**/.

A2.2.2.4. Obtain Submitting Office Number (SON) from OPM. This four character SON identifies the office as authorized to request investigations from OPM.

A2.2.2.5. A complete package requesting an investigation includes the following: OPM Agency Use Sheet, applicable personnel security questionnaire, Fingerprint Card, if applicable, original signed "Authorization for Release of Information," and if applicable, the "Authorization for Release of Medical Information."

A2.2.2.6. OPM does not require the DD Form 1879.

A2.2.2.7. Complete OPM Agency Use Sheet – AF specifics:

A2.2.2.7.1. AF has two billing codes which are annotated in Block N.

A2.2.2.7.1.1. DoD-AFM. This is for investigation requests on military members.

A2.2.2.7.1.2. DoD-AF. This is for investigation requests other than military.

A2.2.2.7.1.2.1. Civilians (appropriated and nonappropriated).

A2.2.2.7.1.3. Child Care

A2.2.2.7.1.3.1. Contractor suitability/trustworthiness. (Not security clearances. AF does not request investigations for security clearances on contractors under the National Industrial Security Program.)

A2.2.2.7.2. Block L is always: AF 00.

A2.2.2.7.3. Block H. Annotate "J" to indicate Personnel Reliability Program (PRP) investigation.

A2.2.2.8. Mail requests as OPM does not have electronic transmission capability. See Table A2.2.2.8. for OPM addresses and type of investigation.

Table A2.1. Mailing Addresses for OPM.

OPM Address		**Investigation Description**
OPM-FIPC PO Box 700 ATTN: AF Liaison 1137 Branchton Rd Boyers, PA 16018		General correspondence and MEPS new accession releases and fingerprint cards that require the SF 86 to be printed via the AFRISS program (No actual PSI should be mailed to this address)
OPM-FIPC PO Box 49 ATTN: AF Liaison 1137 Branchton Rd Boyers, PA 16018		All Periodic Reinvestigations. 35-Day Cases All Presidential Support, PRP, Blowtorch Cases (initials & PRs)
OPM-FIPC PO Box 618 1137 Branchton Rd Boyers, PA 16018		All Initial Investigations

A2.2.2.9. Maintain a suspense copy of PSIs and all other information until the investigative data appears in the JCAVS.

A2.2.2.10. Check JPAS weekly to monitor the status of the investigation until it is closed. An SII inquiry, from the Person Summary screen, should be conducted to ascertain if the case was determined unacceptable. Should the investigation remain unopened for 30 days after it was submitted, and is not shown as unacceptable in SII, contact the OPM help desk at (724) 794-5228 to inquire as to its status. If the status cannot be ascertained, resubmit the investigation.

A2.2.2.11. Forward the suspense copy of the PSI to the gaining base authorized requester when a permanent change of station (PCS) occurs.

A2.2.3. Investigation Types.

A2.2.3.1. **National Agency Check with Local Agency Checks and Credit Check (NACLC).** SF 86 for individuals requiring access to Secret information and/or suitability. All military members require a NACLC.

A2.2.3.1.1. The SF 86 must cover the most recent seven-year period. The "Have you ever" questions cover the individual's entire lifetime.

A2.2.3.1.2. NACLCs will be requested for military personnel with no prior or current security clearance eligibility if and when access to Secret information is required.

A2.2.3.1.3. Existing ENTNAC or NAC investigations remain valid for individuals with prior or current Secret eligibility regardless of the age of the investigations there has been no break in service over 24 months. Periodic reinvestigation rules apply.

A2.2.3.2. **Single Scope Background Investigation (SSBI).** Authorized requesters submit SF 86.

A2.2.3.2.1. The questionnaire must be completed to cover the most recent seven-year period with 10 years coverage on the residence, education, and employment questions, or since the 18th birthday, but at least the last two years. "Have you ever" questions must cover the individual's entire lifetime. Use SF 86A, *Continuation Sheet for Questionnaires* for information for years 8 through 10.

A2.2.3.2.2. Provide both the alien and naturalization/citizenship number for each foreign-born relative and associate listed on the SF 86 that claims US citizenship. Other authorized means in proving U.S. citizenship for foreign-born relatives are the State Department form 240, Report of Birth Abroad of a Citizen of the U.S., or the number from either a current or previous U.S. passport.

A2.2.3.2.3. If selective service number is not known, the subject's SSAN will be accepted.

A2.2.3.2.4. A Single Agency Check (SAC) is required on the following individuals associated with the subject of an SSBI: (a) spouse or cohabitant, (b) immediate family members 18 years old or older who were born outside the United States. If marriage or cohabitation occurs after completion of the SSBI, transmit Spouse SAC to OPM, using EPSQ software. Keep a hard copy for suspense file.

A2.2.3.3. National Agency Check (NAC). Authorized requesters use SF 85P and an SF 87 or FD Form 258.

A2.2.3.4. National Agency Check Plus Written Inquiries and Credit Check (NACI). The CPF will submit SF 85 or SF 85P, as appropriate and SF 87 or FD Form 258.

A2.2.3.5. Access National Agency Check with Written Inquiries and Credit Check (ANACI). For civilians requiring access to classified information at the Secret level in order to perform mission duties or in noncritical sensitive positions, the CPF will submit SF 86 or FD Form 258 and an SF 87.

A2.3. IMAs. The authorized requester of the unit of assignment or attachment will submit periodic reinvestigations or confirm revalidation's of security clearances for IMAs.

A2.4. Catch'Em in Continental United States (CEIC) Program. Personnel requiring an SSBI or periodic reinvestigation and who are scheduled for a PCS move to an overseas location, including Shemya AFB, AK, fall within the CEIC program. Such individuals must complete the personnel security questionnaire within 180 days prior to departure. This allows the investigative agency time to conduct the personal interview before they PCS.

A2.5. Subject Interview. Individuals completing a personnel security questionnaire must specify any circumstances that would make them unavailable for a subject interview within 180 calendar days of the date the form is transmitted. Detailed information regarding the period in which the individual will be unavailable such as date, location, and duration should be provided

in the remarks section of the appropriate form. The investigative agency will try to conduct the subject interview prior to departure of the individual.

A2.6. Local Files Check. The unit security manager initiates and verifies completion of a LFC that includes a review of local personnel, medical facility, law enforcement, or other security records, as appropriate. Use AF Form 2583, **Request for Personnel Security Action**, to document an LFC. See **Attachment 23** for instructions on filling out AF Form 2583.

A2.6.1. Headquarters Air Education and Training Command/Recruiting Service (HQ AETC/RS), 550 D Street West, Suite 1, Randolph AFB TX 781504527 does not have to complete AF Form 2583 when personnel records are unavailable.

A2.6.2. The Reserve Recruiting Service (HQ AFRS/RS) or their authorized requesters do not have to complete AF Form 2583 for IMAs, IRRs, and traditional reservists when personnel records are unavailable.

A2.6.3. AF Form 2583 is not needed for civilian applicants for federal employment when local files are unavailable.

A2.6.4. Record briefings for access to special access program information on AF Form 2583 when the governing program directive does not prescribe other procedures.

A2.7. Periodic Reinvestigations (PR).

A2.7.1. Requests for PRs are submitted in the same manner as initial investigations. However, no fingerprint card or birth certification is required. No abbreviated version of SF 86/EPSQ may be submitted in connection with a PR. A person must have one-year retainability before a PR may be requested.

A2.7.2. An authorized requester should initiate a Secret PR at the **9.5** year mark from the date of the previous investigation or reinvestigation. Questionnaire must cover the most recent 10-year period or the period since the last investigation.

A2.7.3. An authorized requester should initiate a Top Secret PR at the **4.5** year mark from the date of the previous investigation or reinvestigation.

A2.7.4. For individuals in a NATO billet, submit the PR IAW AFI 31-406, Applying North Atlantic Treaty Organization (NATO) Protection Standards and **Table A3.5**, Rule 12 & 15.

A2.8. Air Force Liaison Office at the Operations Center-Baltimore. Address for the AFLNO is: Defense Security Service, ATTN: Air Force Liaison Office, 601 10TH street, Suite 135, Ft George Meade, MD 20755-5134.

A2.9. Air Force Liaison Office at OPM. Address for the AF Liaison at OPM is: OPM-FIPC, PO Box 700, ATTN: Air Force Liaison, 1137 Branchton Road, Boyers, PA 16018.

Attachment 3

TABLES FOR INVESTIGATIONS AND ASSIGNING SECURITY ACCESS REQUIREMENTS (SAR)

A3.1. Personnel Security Investigations. Use the following table for guidance on the types of required personnel security investigations and appropriate questionnaire forms and or EPSQ.

Table A3.1. Personnel Security Questionnaire Forms/Software for Investigations.

RULE	A Type of Investigation		B EPSQ Software or SF 86/85P/85	C FD Form 258 or SF 87 (Either Form)
1	NAC		SF 85P	1 signed original of SF 87/FD Form 258
2	NACLC including Secret/PRs and SAP/ PRs		SF 86	1 signed original of SF 87/FD Form 258 (except PRs)
3	NACIC		Original and 1 copy of SF 85/85P	1 signed original of SF 87/FD Form 258
4	ANACI		Original and 1 copy of SF 86	
5	SSBI including TS/PRs		SF 86	1 signed original of SF 87/FD Form 258 (except PRs)
6	Special Investigative Inquiry		Original and 2 copies of SF 86 (see notes 1& 2)	1 signed original if FBI/ID check desired

NOTES:

1. Send original and 1 copy to the AFCAF for forwarding to OPM. One copy is for the authorized requester's suspense file.

2. An original copy of the SF 86 (or EPSQ) should accompany the request, where appropriate, unless such documentation was submitted within the last 12 months to OPM as part of another PSI. The results of any other recently completed investigative reports should also be sent. Indicate the specific areas or issues requiring investigation with justification in Remarks.

A3.2. Requesting NAC/NACIC Investigations. Use the following table for guidance on NAC and NACIC investigations as a minimum requirement for positions having no access to classified information.

Table A3.2. Requesting NAC/NACIC Investigations.

RULE	A If the individual is a	B and duties require	C Then a NAC/NACIC is required
1	Person requiring unescorted entry (see note 1)	**unescorted entry into restricted areas, access to sensitive areas, or equipment**	NAC for military & contractor employee NACIC for DOD civilian Before entry or access (see notes 2 & 3)
2	Nonappropriated fund employee	employment in a position of trust	NAC before performing duties (see note 4)
3	Person requiring a DOD building pass	a DOD building pass	NAC before issuance
4	Foreign national employed overseas	no access to classified information	NAC before employment (see note 5)
5	Person requiring access to chemical agents	access to or security of chemical agents	NAC before assignment
6	Civilian nominee for military education and orientation program	education and orientation of military personnel	A NACIC before performing duties (process limited access authorization for non-United States citizens) (foreign educators are employed in noncritical sensitive positions)
7	Contract guard	performing guard functions	NAC prior to assignment
8	Person assigned to AIS II or III positions	Assignment to AIS II or III (formerly ADP) positions	NAC for military & contractor employee NACIC for DOD civilians

NOTES:

1. A NACLC is a prerequisite for military members upon entry. DOD civilians receive a NACIC as a prerequisite for federal employment. These investigations exceed the required investigations and can be used for unescorted entry.

2. Air Reserve forces personnel with a current ENTNAC or NAC on file may have unescorted entry to restricted areas while in civilian status, pending completion of the required NACIC.

3. Prior ENTNAC/NAC/NACI/NACIC investigations meet the requirements for prior military members who have been separated. Commanders may waive on a case by case basis, the investigative requirements for unescorted entry to restricted areas containing Protection Level (PL) 2 and or 3 resources pending completion of a favorable NACLC, NAC, or NACIC after favorable review of the completed personnel security questionnaire for the investigation.

4. Installation records checks on employees in child care services include a check of the state criminal history repository. The state criminal history repository checks are for suitability affecting the consolidated civilian personnel office and morale, welfare, and recreation programs. The sponsoring activity sends out and receives the state criminal history repository.

5. The NAC must consist of: (a) host-government law enforcement and security agency records check at the city, state, province, and national level, (b) DCII check, and (c) FBI check where information exists indicating residence by the foreign national in the United States for one year or more since the age 18.

A3.3. Requesting NACLC/ANACI Investigations. Use the following table for guidance on NACLC and ANACI investigations required for access to classified information.

Table A3.3. Requesting NACLC/ANACI Investigations.

RULE	**A** **If the individual is a**	**B** **and duties require**	**C** **Then a NACLC/ANACI is required**
1	United States military member	a Secret clearance	NACLC before granting final clearance
2	Prior military member reentering Air Force after a break in military service exceeding 24 months	retention in the Air Force to include Air Reserve forces	NACLC to be initiated no later than 3 workdays after reentry
3	Applicant for appointment as a commissioned officer	Commissioning as an officer, includes Air Reserve forces	NACLC before appointment (after appointment for health professionals, chaplains, and attorneys) (see note 1)
4	Air Force academy cadet, military academy cadet, or naval academy midshipman	Enrollment	NACLC to be initiated 90 days after entry

RULE	A **If the individual is a**	B **and duties require**	C **Then a NACLC/ANACI is required**
5	Reserve officer training candidate or midshipman	entry to advanced course of college scholarship program (see note 2)	NACLC to be initiated 90 days after entry
6	United States military member	customs inspector duty	NACLC before assignment
7	DOD military or contract employee	access to or security of chemical agents	NACLC before assignment
8	United States military member, civilian, or contract employee	assignment to North Atlantic Treaty Organization positions	NACLC for military and contractor employee, ANACI for civilian employee
9		secret special access programs	Before performing duties and at 5-year intervals thereafter while assigned
10		assignment to Category III PSP	
11		assignment to a controlled PRP position	NACLC for military and contractor employee, ANACI for civilian employee before PRP certification

NOTES:

1. The individual must agree in writing that if the results of the investigation are unfavorable, the individual will be subject to discharge. Under the exception, commissions in the reserve components other than the National Guard may be offered to immigrant alien health professionals, chaplains, and attorneys.

2. Reserve officer training candidate graduates who delay entry on active duty pending completion of further college study are not authorized a new NACLC once they have been commissioned. Request recertification when the officer comes on active duty.

A3.4. Guide for Requesting SSBIs. Use the following table for guidance on the minimum standards required for SSBIs.

Table A3.4. Guide for Requesting SSBIs.

RULE	A If the individual is a (an)	B and duties require	C then a favorably completed SSBI is required before
1	United States military member, civilian, or contractor employee	Top Secret clearance	granting final clearance
2		assignment to a "critical or special sensitive position"	assignment to position
3		assignment to a "critical" position in the personnel reliability program	PRP certification
4		AIS I (formerly ADP I) positions	assignment
5		assignment to a category I or II presidential support position	within 36 months prior to selection
6		access to North Atlantic Treaty Organization COSMIC Top Secret or COSMIC Top Secret ATOMAL	access may be granted
7		access to SCI or an approved special access program	granting access
8		access to SIOP-ESI	
9		Assignment to the National Security Agency	Assignment
10		Assignment to the Defense Courier Service	
11		Assignment to personnel security adjudicative functions, counterintelligence, or criminal investigative or direct investigative support duties	
12	immigrant alien	limited access to Secret or Confidential information	Issuing limited access authorization
13	non-United States national employee		
14		the education and orientation of military personnel	performing duties
15		Unescorted entry to PL 1 and 2 restricted areas	authorized entry

A3.5. Guide for Requesting Periodic Reinvestigations. Use the following table for guidance on the minimum standards for PRs.

Table A3.5. Guide For Requesting Periodic Reinvestigations.

RULE	A If the individual is a	B and duties require	C then request a periodic reinvestigation
1	United States military member, DOD civilian, or contractor employee	access to Top Secret	4.5 years from the date of the last SSBI or SSBI-PR
2		access to SCI	
3		assignment to presidential support	
4		assignment to an AIS I position	
5		access to SIOP-ESI	
6		assignment to AFOSI duties	
7		assignment to a critical personnel reliability program position	
8		access to Top Secret special access programs	
9	United States civilian employee	assignment to a special or critical sensitive position	
10	Non-United States national employee and immigrant alien	limited access authorization	
11		unescorted entry to PL 1 or 2 restricted areas	
12	United States military member, DOD civilian, or contractor employee	North Atlantic Treaty Organization COSMIC Top Secret or COSMIC Top Secret ATOMAL	4 years from the date of the last SSBI or SSBI/PR
13	United States military member, DOD civilian, or contractor employee	access to an approved Secret special access program	4.5 years from the date of the last investigation
14		Explosives Ordinance Disposal (EOD)	4.5 years from the date of the last SSBI/S-PR (note 1)
15		assigned to a North Atlantic Treaty Organization staff position	9 years from the date of the last investigation
16		access to Secret information and/or assignment to noncritical sensitive positions	9.5 years from the date of the last investigation

NOTE: 1. EOD assignment requires a Secret PR on a five year recurring basis.

A3.6. Guide for Requesting Investigations for Unescorted Entry to Restricted Areas. Use the following table for guidance for investigations required for the minimum investigative standards for unescorted entry to restricted areas.

Table A3.6. Guide for requesting investigations for Unescorted Entry to Restricted Areas.

RULE	A If the individual is a (an)	B and duties require	C Then the following favorably completed Investigation is required before entry
1	U.S. active duty military (includes immigrant aliens)	Unescorted entry into restricted areas, access to sensitive information areas, or equipment	NACLC
2	U.S. retired or separated military member with an Honorable Discharge and no break in service greater than 24 months.		NAC
3	DOD Civilian with no break in federal service greater than 24 months		NACIC (see note 1)
4	NAF employee		NAC
5	DOE employees with no break in service greater than 24 months		NACIC is equivalent to the Department of Energy "L" investigation
6	Federal employees		NAC or equivalent investigation certified by the non DOD agency
7	Contractor employees		NAC
8	Foreign nationals, Other non-US national		SSBI for PL 1 or 2 resources. Local Agency Check for PL 3.
9	Foreign National Military members and host nation military members assigned to USAF activities		Security assurance of favorable investigation based on government-to-government agreements, treaties, (NATO) agreements, for PL 1 & 2. For PL 3, verification of security clearance by foreign commander and authenticated by Security forces or designated representative; personnel foreign travel orders; and the restricted area badge or home-station equivalent controlled picture identification credential.
10	Foreign National Employees Overseas Employed by DOD organizations		Host government law enforcement and security agency checks at the city, state (province) and national level whenever permissible by the law of the host government, DCII, and FBI-HQ/ID (where information exists regarding residence in US for one year or more since age 18).

NOTES:

1. Verification of NACIC can be made by contacting the CPF.

A3.7. (DELETED)

Table A3.7. (DELETED)

Attachment 4

DOD SECURITY CLEARANCE AND OR SCI ACCESS DETERMINATION AUTHORITIES

A4.1. Officials Authorized to Grant, Deny, or Revoke Personnel Security Clearances (Top Secret, Secret). The 497th Intelligence Group/INS, Directorate of Security and Communications Management, the Air Force Central Adjudication Facility, is the designated authority to grant, suspend, deny, or revoke personnel security clearances and SCI access.

A4.2. Officials Authorized to Grant, Deny, or Revoke LAA. The CAF is the single authority to grant, deny, or revoke an individual's LAA.

A4.3. Officials Authorized to Certify Personnel Under Their Jurisdiction for Access to Critical Nuclear Weapon Design Information. Commanders and staff agency chiefs have the authority to grant CNWDI access. This authority is assigned to division chiefs and above at all levels of command. (Refer to AFI 31-401, *Information Security Program Management*).

A4.4. Official Authorized to Approve Personnel for Assignment to Presidential Support Activities. Commanders nominate individuals to the CAF for assignment to Presidential Support Activities. The CAF makes the final recommendation to the DOD Executive Secretary to the Secretary of Defense.

A4.5. Officials Authorized to Grant Access to SIOP-ESI. The Air Force has approved the Chief of Staff, Vice Chief of Staff, Assistant Vice Chief of Staff, and Deputy Chiefs of Staff for SIOP-ESI access and has designated them as SIOP-ESI access granting authorities. These officials may further delegate their access granting authority. (Refer to AFI 10-1102, *Safeguarding the Single Integrated Operational Plan*).

A4.6. Authority to Render Final Appeal Decisions. The Personnel Security Appeal Board is designated as the appeal authority for personnel security clearances and SCI access.

A4.7. Officials Authorized to Suspend Access to Classified Information.

A4.7.1. Security Clearances. Commanders have the authority to suspend access to classified information.

A4.7.2. SCI. Director of Intelligence Surveillance and Reconnaissance (HQ USAF/XOI) and Senior Intelligence Officers or their designees are the authorities to suspend access to SCI.

A4.8. Official's Authorized to Grant, Deny, Suspend, Revoke, or Limit SAP access. The Air Force CAO, Wright-Patterson AFB, OH is the authority to grant, deny, suspend, revoke, or limit SAP access eligibility.

A4.9. Officials Authorized to Issue Interim Clearances. Commanders have the authority to grant interim security clearances.

A4.10. Officials Authorized to Designate Nonappropriated Fund Positions of Trust. HRO managers designate these positions within their jurisdiction. See AFI, 34-301, *Nonappropriated Fund Personnel Management and Administration.*

Attachment 5

STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD

A5.1. Personnel Security Appeal Board.

A5.1.1. Responsibilities:

A5.1.1.1. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) has oversight of the Personnel Security Appeal Board (PSAB).

A5.1.1.2. The PSAB:

A5.1.1.2.1. The PSAB is the appeal authority for security clearances and SCI access (see **Chapter 11**). Determinations made to deny or revoke security clearances shall be made IAW DOD 5200.2-R, this AFI **Chapter 8**, and "BY AUTHORITY OF THE SECRETARY OF THE AIR FORCE."

A5.1.1.2.2. The PSAB is comprised of three members.

A5.1.1.2.3. The PSAB President will be an HQ USAF/XO representative and will serve as a permanent member. An attorney from HQ USAF/JA and a security official from HQ USAF/XOFI will be permanent members. A medical advisor from HQ USAF/SG will be available to the board at two-year intervals. The members will be briefed on and familiar with the personnel security clearance process.

A5.1.1.2.4. Minimum grade 0-5/GS-14. In cases where the appellant is at or above the grade of military 0-5 or GM/GS-14, at least one member of the board will be equivalent or senior in grade to the appellant.

A5.1.1.2.5. The President executes board responsibilities as outlined in DOD 5200.2-R, Appendix M and this AFI.

A5.1.1.2.6. The PSAB convenes upon receipt of appeal cases.

A5.1.1.2.7. The PSAB president notifies appellants, in writing, of the decision generally within 60 days of receipt of the appeal (with no personal appearance) or 30 days of receipt of the Administrative Judge's recommendation (with a personal appearance). The notice will include a statement that the PSAB decision is final and no other appeal rights are authorized. If SCI is involved, the notice will specify the status of the access to SCI, in addition to the security clearance. A copy of the board's final decision is forwarded to the CAF.

A5.1.1.3. The CAF:

A5.1.1.3.1. Provides operational support to SAF/AA and the PSAB.

A5.1.1.3.2. Forwards the appeal case file to the PSAB President and includes a case summary on all cases to assist the board members' review.

A5.1.1.3.3. Sends membership letters to designated functional representatives to serve on the board.

A5.1.1.3.4. Provides the Defense Office of Hearings and Appeals (DOHA) with the case files upon request.

A5.1.1.3.5. Updates the DCII and AMS.

A5.1.1.3.6. Maintains the redacted file for the PSAB. AFI 37-131 applies when requests for information are received.

A5.1.1.3.7. Provides SAF/AA with a report quarterly that tracks the decisions on appeal cases.

Attachment 6

SAMPLE WAIVER OF PRE-APPOINTMENT INVESTIGATIVE REQUIREMENTS

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR (Servicing Civilian Personnel Flight)

FROM: Unit of Assignment Full Address

SUBJECT: Waiver of Preappointment Investigative Requirements

In accordance with AFI 31-501, **paragraph 3.1**, I have waived the investigative requirements and give authority to fill a critical sensitive (or noncritical sensitive) position prior to completion of the personnel security investigation. (Name of individual, SSAN) has been selected for the position of (fill in), grade, and office symbol.

Appointment prior to completion of the investigation is necessary to accomplish (fill in) function in support of national security.

Temporary changes will be made in duties or work situation to preclude the person from access to classified material or information before completion of the required investigation.

Commander's Signature Block

Attachment 7

SAMPLE MEDICAL CERTIFICATION TO THE COMMANDER OF INDIVIDUAL FOR PRESIDENTIAL SUPPORT PROGRAM

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Commander of Individual Being Nominated)

FROM: Medical Officer Full Address

SUBJECT: Medical Certificate

(One of the following actions have been taken:)

This certifies a competent medical authority reviewed the medical records regarding (grade, full name, SSN of individual) and no physical or mental disorder is noted in the record that could adversely affect the individual's judgment or reliability. The medical authority who reviewed the records is (name) and may be contacted at (telephone number).

OR

This certifies a competent medical authority reviewed the medical records regarding (grade, full name, SSN of individual) and found the following potentially disqualifying information that could adversely affect the individual's judgment or reliability: (i.e., drug abuse, alcohol abuse, mental or emotional problems, etc). The medical authority who reviewed the records is (name) and may be contacted at (telephone number).

Medical Officer's Signature Block

NOTE: If a commander needs an interview with the medical authority to discuss the findings in order to base a nominating decision, the medical authority provides a statement of that interview to the commander. Any statements will be kept with the certificate.

Attachment 8

SAMPLE COMMANDER'S NOMINATION TO CHIEF, SERVICING SECURITY ACTIVITY FOR A PRESIDENTIAL SUPPORT POSITION

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR CHIEF, SERVICING SECURITY ACTIVITY

FROM: Commander Full Address

SUBJECT: Presidential Support Nomination for (Job Title) by (Full Name, Rank/Grade, SSAN)

The attached personnel security investigation package on (enter name, rank or civilian grade, SSAN), United States Air Force (or company name of contractor) has been completed in accordance with DOD Instruction 5210.55 and AFI 31-501. It is forwarded for further processing (Atchs 1 & 2).

(Enter name) is being nominated for (state initial or continued assignment) to (identify the specific presidential support activity) as a (identify the individual's specific duty assignment, i.e., aviation maintenance technician, security force, steward, rotor blade examiner, driver, etc).

These duties are identified as (Category One) or (Category Two) requiring a favorably completed Single Scope Background Investigation (SSBI) or (Category Three) requiring completion of a favorable National Agency Check, local agency check and credit check (NACLC).

I have personally reviewed the individual's records as follows and there is no derogatory information that would disqualify the nominee from selection:

(1) efficiency and or fitness reports file reflects the individual has demonstrated consistent high standards of performance;

(2) military personnel records or civilian official personnel folder, or contractor personnel records reveal no derogatory information; and

(3) local security files reveal no derogatory information.

I have on file the certificate from a competent medical authority that certifies no physical or mental disorder is noted that could adversely affect the individual's reliability or judgment. I have no knowledge of, and base law enforcement records do not reveal, any delinquency or criminal activities on the part of the nominee. No actions are pending to deny, revoke, or withdraw any security clearance or access.

(Enter name) is recommended for assignment to (enter unit/company and location) and duties (enter job title) for which nominated. (Justify the recommendation if derogatory information is in the records. Specifically identify all reasons for a recommendation that a contractor employee shall not be selected for the particular position in question).

Our POC is (name and telephone number)

Commander’s Signature Block

Attachments:

1. EPSQ Disk & 1 Signed Original
2. FBI Fingerprint Card

Attachment 9

SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, MEMORANDUM TO 497 IG/INS FOR PROCESSING OF PRESIDENTIAL SUPPORT PROGRAM NOMINEE

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR 497 IG/INS

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Request for Processing Presidential Support Program Nominee

The attached Commander's Nomination Memorandum on (enter name, rank or civilian grade, SSAN), United States Air Force (or company name of contractor) has been processed in accordance with DOD 5210.55 and AFI 31-501. It is forwarded for your further processing.

The commander (name and unit) has recommended (enter name, rank or civilian grade, SSAN) for assignment to (or continued assignment) (enter unit/company and location) and duties to an authorized Presidential Support position (enter job title).

The commander has certified the records of (enter name, rank or civilian grade, SSAN) reveal no disqualifying information.

The required investigation (NACLC or SSBI) was submitted to the Defense Security Service or the Office of Personnel Management on (date).

Our POC is (name, grade, telephone number).

Chief, Servicing Security Activity Signature Block

Attachment:

Commander's Nomination Memorandum (attachments withdrawn)

Attachment 10

SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, NOTIFICATION TO THE SERVICING MEDICAL FACILITY OF THE INDIVIDUAL APPROVED FOR PRESIDENTIAL SUPPORT DUTIES

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Servicing Medical Facility)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Assignment of Presidential Support Duties

The following individual has been approved for assignment to a Presidential Support position on (date).

(name, rank, grade, SSAN, unit, office symbol)

Request the individual's medical records be marked and monitored during this assignment in accordance with the instructions in AFI 31-501, *Personnel Security Program Management* and use of AF Form 745, Sensitive Duties Program Record Identifier. See AFI 41-210, *Patient Administration Functions.* Notify the individual's commander or designated representative and this office when a significant effect on the individual's suitability to perform Presidential Support duties is expected as a result of medical, dental, or mental health treatment or medication, and if drug or alcohol abuse is suspected.

We will notify you to terminate monitoring when the individual is no longer assigned to Presidential Support duties.

Our POC is (name, grade, and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment 11

SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, REQUEST FOR EVALUATION OF CONTINUED SECURITY CLEARANCE TO COMMANDER

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Unit Commander)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Evaluation of Continued Security Clearance

The attached unfavorable and or derogatory information has been developed concerning the above member of your organization. Please review this information and determine on the basis of the facts available, if it is in the interest of national security to establish a Security Information File (SIF) and whether or not to suspend access to classified information/unescorted entry to restricted areas while such information is resolved. Your review of the security standard criteria in AFI 31-501, **Chapter 8**, and DOD 5200.2-R, paragraph 2-200 will guide your decision.

Upon completion, please provide your decision and rationale for or against SIF establishment.

My POC, (name and telephone number) stands ready to assist you. Please respond NLT (date).

Chief, Servicing Security Activity Signature Block

Attachments(s):

1st Ind, (date)

TO: Unit HQ USAF/SFAI

I have reviewed the referred available unfavorable information concerning subject and do not believe the suspension of access to classified information and or unescorted entry is warranted. My rationale for this decision is (explain). Consequently, I've determined this case doesn't meet the purview of AFI 31-501 for SIF establishment. This individual's continued access and or entry is in the best interest of national security. Should additional unfavorable and or derogatory information become available, I will reevaluate my decision. I have or have not coordinated this decision with the JA.

OR

I have reviewed the referred unfavorable information concerning the subject. I have determined the derogatory and or unfavorable information concerning subject falls within the criteria of AFI 31-501, **Chapter 8**. A SIF has been established, please set up a folder and maintain a SIF as outlined in AFI 31- 501, **Chapter 8**.

I have or have not withdrawn (suspended) subject's access to classified information and or unescorted entry to restricted areas. Attached as applicable is the:

a. AF Form 2583, **Request for Personnel Security Action**. (This form is used to document Special Access, i.e., NATO, CNWDI, SIOP, etc.)

b. AF Form 2586, **Unescorted Entry Authorization Certificate**, stamped by Pass & Registration Section, reflecting restricted area badge was returned.

c. AF Form 2587, **Security Termination Statement**.

d. Notification of suspension of access.

My rationale for this decision is: Subject's current situation (conduct, incident, status, pending administrative or judicial action, etc.). Previous disciplinary problems/incidents and action taken, if any. Subject's duty performance. Any evaluations the subject has received. Any other pertinent information. Subject's retainability in the Air Force.

To assist in resolving this case I've taken the following actions: requested investigation, referred individual for evaluation, etc. We'll keep your office informed of any developments and or changes.

Our POC is (name and telephone number):

Commander's Signature Block

Attachment(s)

Attachment 12

SAMPLE REQUEST TO ESTABLISH A SECURITY INFORMATION FILE (SIF)

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR SFS/SFAI

FROM: Commander Full Address

SUBJECT: Request Establishment of Security Information File (SIF), re**: (Last Name, First, Middle, Rank, SSAN)**

Request a SIF be established on **(Individual)** and processed IAW AFI 31-501, *Personnel Security Program Management.*

I have become aware of the Subject's involvement in (specify situation). After review of DOD 5200.2-R, paragraph 2-200, Appendix I, and AFI 31-501, **Chapter 8**, it is determined that further evaluation is needed to determine the subject's eligibility to retain access to classified information/unescorted entry to restricted areas.

(One of the following actions have been taken:)

(SUBJECT) has been placed in a nonsensitive position and all access to classified information and or unescorted entry to restricted areas has been **withdrawn (suspended)** in accordance with AFI 31-501.

Or

(SUBJECT) will **continue** access to classified information/unescorted entry to restricted areas in accordance with AFI 31-501. **(ANY OF THE FOLLOWING AS PERTINENT).**

Please notify the 497 IG/INS (CAF) of the suspension (or continued access to classified information).

There is a Report of Investigation (ROI). Name of agency conducting the investigation. Date of ROI.

Subject has been referred to (when applicable):

Mental Health for an evaluation Date of referral.

Subject was given disciplinary action for this incident. Type of disciplinary action. (e.g., Article 15)

A Court-Martial is projected for this individual: **(Date)**

Subject was placed in appellate leave status: **(Date)**

The subject's present Date Eligible Retirement or Separation (DEROS) date is.

We **(do/do not)** intend to discharge the subject in accordance with AFI 36-3206, *Administrative Discharge Procedures for Commissioned Officers*, or AFI 36-3208, *Administrative Separation of Airmen.*

I will provide your office with status updates. Our POC is (name and telephone number).

Commander's Signature Block

Attachments:

1. Adverse Security Determination
2. AF Form 2583 (Only if special access is being withdrawn, not to include SCI)
3. AF Form 2586
4. AF Form 2587

Attachment 13

SAMPLE COMMANDER NOTIFICATION TO INDIVIDUAL OF SIF ESTABLISHMENT AND SUSPENSION OF ACCESS TO CLASSIFIED INFORMATION

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Individual Concerned)

FROM: Commander Full Address

SUBJECT: Notification of Suspension of Access

You are hereby notified that a security determination has been made to suspend your access to classified information/unescorted entry into restricted areas. This action is being taken because of your alleged (be as specific as protection of sources allows and national security permits.)

If you wish to provide a rebuttal reply to this determination, I must receive it no later than 72 hours (unit establishes time frame) after your receipt of this notification.

If you choose to reply, a written response to your submission will be made dealing with the points or questions you raise.

A Security Information File will be established. When all final actions in this case have been completed, I will evaluate the incident(s) and make a security recommendation. The 497 IG/INS (CAF) will make the final security determination concerning your reinstatement of clearance eligibility.

Our POC is (name and telephone number).

Commander’s Signature Block

cc:

Servicing Security Activity

1st Ind, (Individual Concerned)

TO: (Individual’s Commander or Staff Agency Chief)

Receipt acknowledge (Date)

I (do/do not) intend to submit a written reply within 72 hours. (Unit establishes time frame)

Individual’s Signature Block

cc:

Servicing Security Activity

Attachment 14

SAMPLE COMMANDER NOTIFICATION TO INDIVIDUAL OF SIF ESTABLISHMENT WITH CONTINUED ACCESS TO CLASSIFIED INFORMATION

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Individual Concerned)

FROM: Commander Full Address

SUBJECT: Notification of Decision to Establish a Security Information File with Individual Continuing Access to Classified Information

You are hereby notified that a security determination has been made to establish a Security Information File. This action is being taken because of your alleged (be as specific as protection of sources allows and national security permits.)

However, I have determined your current access to classified information may continue until further notice.

If you wish to provide a written rebuttal reply to this determination, I must receive it no later than 72 hours (unit establishes time frame) after your receipt of this notification.

If you choose to reply, a written response to your submission will be made dealing with the points or questions you raise.

When all final actions in this case have been completed, I will evaluate the incident(s) and make a security recommendation. The 497 IG/INS (CAF) will make the final security determination concerning your security clearance eligibility.

Our POC is (name and telephone number).

Commander's Signature Block

cc:

Servicing Security Activity

Attachment 15

SAMPLE CHIEF, SERVICING SECURITY ACTIVITY, NOTIFICATION TO COMMANDER OF SIF ESTABLISHMENT

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Commander of Subject)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Establishment of a Security Information File (SIF) RE: (Name of Subject)

A SIF has been established on subject individual within your organization IAW AFI 31-501, **Chapter 8**.

The following documents have been placed in the file:

a. A copy of your letter, dated (date) Subject: Establishment of a Security Information File.

b. A copy of the SIF establishment notification to 497 IG/INS (CAF).

c. A copy of my notification to the (Commander, Support Group), informing him/her of establishment of the file and the contents therein.

The file will be maintained by this office until all local actions are complete. The file will then be forwarded to the 497 IG/INS for a final security clearance determination.

We will request written opinions from base level staff agencies, such as legal, medical, mental health, security forces, and personnel on your behalf. If a Special Investigative Inquiry is necessary, we will request the CAF have DSS conduct one accordingly.

Please provide us with the following recommendation and or documentation for incorporation into the file:

a. Copies of any investigative reports (e.g., AFOSI, DSS, local security forces investigations, FBI, etc.) that will have a bearing on the final resolution of the case.

b. Summary of appropriate portions of subject's Unfavorable Information File (UIF), if any, that may have a bearing on the final adjudication of the case.

c. Correspondence and forms related to withdrawal, revocation, suspension of special access, or correspondence documenting a commander's recommendations relating to withdrawal or suspension of special access or clearance. If not already accomplished, the AF Form 2586, **Unescorted Entry Authorization Certificate**, must be submitted to show that the AF Form 1199A/B/C/, **Restricted Area Badge**, has been turned over to the Pass & Registration Section. In addition, an AF Form 2587, **Security Termination Statement**; and an AF Form 2583, **Special Access Certificate**; must be supplied for inclusion in the SIF.

Please advise this office of any changes and or status reports in order that we may keep the CAF informed of the actions taken. The first update is due to our office by (date) (determined by security activity) and at (number of days) day intervals until the case file is closed.

Once all required documentation is provided, we will provide you with the completed file for your review and final recommendation for closure. We will then forward it to the CAF for final adjudication.

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment 16

SAMPLE SIF CUSTODIAN CHECKLIST ITEMS

1. Identifying Data: NAME, RANK, SSAN, OFFICE SYMBOL

2. Establishment Date: DATE, BY (AUTHORITY), REASON, SOURCE: (If appropriate)

3. Review SENTINEL KEY Data: CLEARANCE/SAR CODE, INVESTIGATION TYPE, SPECIAL ACCESS

4. SIF request letter to Chief, Security Activity. (***NOTE:*** Discuss with Chief, Servicing Security Activity if establishment may compromise an ongoing investigation.)

5. Evaluation letter to unit commander based on unfavorable information developed within SF channels, e.g., DD Form 1569, AF 3545, OSI report, PRP suspension/decertification, etc.

6. Adverse action determination letter presented.

7. Moved to nonsensitive position, access to classified/unescorted entry to restricted areas suspended, peers/supervisors briefed.

8. SIF establishment notification to the 497 IG/INS (CAF).

9. Installation Commander notified of SIF establishment.

10. Relinquish AF Form 1199, **USAF Restricted Area Badge**, to Pass and Registration.

11. AF Form 2583, **Request for Personnel Security Action**, used as a special access certificate, withdrawn.

12. AF Form 2586, **Unescorted Entry Authorization Certificate**, annotated.

13. AF Form 2587, **Security Termination Statement**, completed.

14. Request appropriate Servicing Security Activity, AFOSI, or DSS investigation. (Ensure copies of all reports are provided to Servicing Security Activity for SIF inclusion.)

15. Direct and ensure subject receives assistance and counseling as necessary from such agencies as mental health, social actions, chaplains, etc.

16. Provide status reports, via CAVS or memorandum to the 497 IG/INS (CAF).

17. Judicial/administrative actions complete.

18. Obtain written opinions requested and received from appropriate staff agencies, e.g. DP, SF, JA, SG, etc.

19. Forward SIF to gaining installation Chief, Servicing Security Activity based on PCS orders. Information copy to the 497 IG/INS (CAF).

20. Completed file with any written suspension response from subject transmitted to the CAF.

21. Maintain all documentation necessary to complete the SIF.

Attachment 17

SAMPLE NOTIFICATION TO 497 IG/INS OF SIF ESTABLISHMENT WHEN INDIVIDUAL MAINTAINS ACCESS

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR 497 IG/INS (CAF)

229 Brookley Ave

Bolling AFB, DC 20332-7040

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Establishment of Security Information File (SIF), re: (name of subject)

The commander of (identify unit) has requested establishment of a SIF on (name and SSAN) due to (specify issue as outlined in the adjudication guidelines, DOD 5200.2-R). At this time the commander has authorized the individual to maintain current access to classified information, to include SCI access.

The SIF was established on (date).

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment 18

SAMPLE SIF ESTABLISHMENT NOTIFICATION TO INSTALLATION COMMANDER

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (Installation Commander)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Establishment of Security Information File (SIF)

The following information is provided to inform you of the establishment of a SIF:

a. Name:

b. Rank:

c. Organization:

d. Reason for SIF Establishment:

e. Date SIF was established by commander or staff agency chief:

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment 19

SAMPLE REQUEST FOR REVIEW AND WRITTEN OPINION

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR (DP, SF, JA, SG, as determined by the nature of the case)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Review and Written Opinion - Security Information File (SIF)

The Commander of (organization) has requested this office to establish a SIF on (individual and SSAN).

AFI 31-501, **Chapter 8**, request your review and written opinion concerning the attached SIF. Please review the file and provide your professional opinion and or recommendation concerning whether this individual should or should not retain a security clearance. This information is required to assist me and 497 IG/INS (CAF) in determining if this person's clearance is in the best interest of the Air Force and national security.

In addition, please review any other pertinent records available in your office and advise if there is any additional information that would warrant the continued denial of access to all classified information and unescorted entry to all restricted areas. A denial or revocation will cover classified at all levels.

Please return the entire package with a record of your review comments and recommendation not later than (10 working days).

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment:

SIF, RE: (Name of Subject)

cc:

Commander (organization)

Attachment 20

SAMPLE SIF TRANSFER MEMORANDUM TO GAINING SECURITY ACTIVITY

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR (Gaining Chief, Security Activity)

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Transfer of Security Information File (SIF), ref: (Name of Subject, Rank, SSAN)

The attached SIF is forwarded in accordance with AFI 31-501, **Chapter 8**.

The subject has received orders for Permanent Change of Station (PCS) to your installation, with a report date of (date).

A copy of this transmittal letter is being forwarded to the 497 IG/INS (CAF) for information.

Our POC is (name and telephone number).

Chief, Servicing Security Activity Signature Block

Attachment:

SIF

cc:

Commander (of subject)

497 IG/INS (CAF) w/o attachment

Attachment 21

SAMPLE RECOMMENDATION TO 497 IG/INS FOR SIF CLOSURE

DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR 497 IG/INSAF

FROM: Chief, Servicing Security Activity Full Address

SUBJECT: Recommendation for SIF Closure RE: (Name of Subject)

The attached SIF on (name and SSAN of subject) is forwarded for your final adjudication. All final actions in this case completed as outlined below:

a. Mental health evaluation:

b. Completed alcohol and/or drug rehabilitation program:

c. Received financial counseling from:

d. Administrative action taken:

e. Judicial action: (An opinion from staff judge advocate regarding factors used in determination of withdrawal or dismissal of charges when there is evidence the individual engaged in the misconduct. For example, positive urinalysis, but found not guilty through court-martial. Was the finding based on technicalities or evidence?)

f. Add any additional pertinent information.

This individual will be returned to duty and or cross trained/separated/placed in appellate leave status.

The individual's commander (name, organization, telephone number) recommendation for (favorable closure and or revocation of security clearance) is included in the SIF.

Our POC is (name and DSN telephone number).

Chief, Servicing Security Activity Signature Block

Attachment:

SIF (if applicable)

cc:

Commander (of subject)

Attachment 22

INSTRUCTIONS FOR IDENTIFYING PERSONNEL SECURITY INVESTIGATION REQUIREMENTS FOR AF POSITIONS.

A22.1. Guide for Identifying Investigative Requirements for Position Coding. Use the following table for guidance on identifying investigative requirements for each authorized manpower position. See **Chapter 7** for additional guidance on coding of investigations.

Table A22.1. Personnel Security Investigation Position Coding

Position Code	Investigation Type	Investigation Description
5	SSBI	The SSBI is the initial investigation for access to Top Secret (including Top Secret Special Access Programs (SAP), SCI, and for Critical Sensitive Positions.) In addition, the SSBI is required for Mandatory AFSCs or Program Mandates.
6	NACLC	The NACLC is the prescribed investigation for initial and continued access to Secret and Confidential information for DoD military and contractor personnel. It is also the reinvestigation requirement for federal employees at the same access levels. Also, all military or Mandatory Program Mandate.
7	ANACI	The ANACI is the investigative requirement for federal employees under Executive Order 10450, "Suitability for Government Hire," in non-critical sensitive positions that require access to classified information up to the Secret level. Access to Secret (civilian) or Mandatory Program Mandate.
8	NACI	The NACI is the baseline investigative requirement for entry into government service under Executive Order 10450 and for federal employees in nonsensitive positions that do not require access to classified information. All OPM NACIs conducted for DoD include a credit check (NACIC). Suitability Requirement (civilian).
9	NAC	The NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making personnel security determinations. A NAC is also an integral part of all initial and periodic reinvestigations and is the baseline for trustworthiness determinations. Trustworthiness Positions (Non Appropriated Fund/Contractor/Consultant).

A22.2. Mandatory SSBI Requirement List for Officer AFSCs. The following is the Officer Mandatory SSBI list. The appropriate position coding is reflected in the Headquarters Air Force Manpower Data System (HAF-MDS).

AFSC AFSC DESCRIPTION
10C Operations Commander
11B Bomber Pilot
11F Fighter Pilot

11G Generalist Pilot
11R Reconnaissance/Surveillance/Electronic Warfare Pilot
11S Special Operations Pilot
11T Tanker Pilot
12B Bomber Navigator
12F Fighter Navigator
12G Generalist Navigator
12R Reconnaissance/Surveillance/Electronic Warfare Navigator
12S Special Operations Navigator
12T Tanker Navigator
13B Air Battle Manager
13D Control And Recovery
13S Space And Missile Operations
14N Intelligence
15W Weather
16F Foreign Area
16G Air Force Operations Staff Officer
16R Planning And Programming
20C Logistics Commander
21M Munitions and Maintenance
21B Maintenance
33C Communications Commander
60C Program Director
65A Audit
71S Special Investigations
84H Historian
85G United States Air Force Honor Guard
86P Command And Control
88A Aide-De-Camp
90G General Officer
91W Wing Commander
92T0 Pilot Trainee
92T1 Navigator Trainee
97E Executive Officer Above Wing Level

A22.3. Mandatory SSBI Requirement List for Enlisted AFSCs. The appropriate position coding is reflected in the Headquarters Air Force Manpower Data System (HAF-MDS).

AFSC AFSC DESCRIPTION
1A0 In-Flight Refueling
1A3 Airborne Communications Systems
1A6 Flight Attendant
1A8 Airborne Cryptologic Linguist
1C3 Command Post
1N0 Intelligence Applications
1N1 Imagery Analysis
1N2 Signals Intelligence Production

1N3 Cryptologic Linguist
1N4 Signals Intelligence Analysis
1N5 Electronic Signals Intelligence Exploitation
1N6 Electronic System Security Assessment
2E2 Computer, Network, Switching And Cryptographic Systems
2MO Missile and Space Systems Maintenance (Excluding 2M0X3)
2W2 Nuclear Weapons
3C0 Communications - Computer Systems Operations
3C2 Communications - Computer Systems Control
3H0 Historian
3N2 Premier Band
7S0 Special Investigations
8E0 Research And Development Technician
8P0 Courier
8P1 Defense Attaché
9C0 Chief Master Sergeant of the Air Force
9S1 Technical Applications Specialist

A22.4. Mandatory SSBI Sensitive Program Requirements. The following table outlines mandatory SSBI requirements for selected positions/programs.

Table A22.2. Mandatory SSBI Sensitive Programs Requirements.

Positions/Programs
Top Secret Access
IT-I
Presidential Support Category 1 and 2 duties
Personnel Reliability Program Critical duties
Sensitive Compartmented Information required
Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) Access
Top Secret Special Access Program (SAP) Access Mandate
DoD or Agency External to AF Top Secret Access Mandate
Civilian Critical Sensitive Positions (which includes: access to TS; development or approval of war plans, future major or special operations of war; critical and extremely important of war; or other positions related to national security, regardless of duties, that requires the same degree of trust)
Initial assignment - Explosive Ordnance Disposal involving Nuclear Weapons positions
Defense Courier Service duties
Access to NATO COSMIC Top Secret
AFOSI investigative agents and investigative support staff, the issuance of personnel security clearances or access authorizations, rendering of personnel security determinations, or duty on personnel security boards

A22.5. Mandatory Positions/Programs Requiring Investigation (Other Than SSBIs). The following table outlines mandatory NACLC, ANACI, NACI, NAC investigation requirements for selected positions/programs.

Table A22.3. Mandatory Positions/Programs Requiring Investigations by Type (Other Than SSBIs).

Positions/Programs	**Investigation Type**				
	Military	**Civilian**		**Contractor Or Consultant**	**Volunteer/ Child Care Provider**
	NACLC	**ANACI**	**NACI**	**NAC**	**NAC**
Access to Secret Information	X	X			
Military Accessions	X				
Commissioned Officers	X				
Civilian Non-Critical Sensitive Positions		X			
Presidential Support Program Category 3	X	X			
Personnel Reliability Program Controlled Position	X	X			
Customs Inspectors	X	X			
Secret SAP Access Mandate	X	X			
Information Technology (IT)-II	X		X		
IT-III*	X		X	X	X
Access to NATO Secret/ Confidential	X	X			
Access to Chemical Agents	X	X			
Arms, Ammunition & Explosives (AA&E) Duties	X	X			
Deployment Purposes	X				
Suitability Requirement			X		X
Trustworthiness				X	
Federal Employment			X		

*IT-III for military only requires a NAC, however, all AF military receive a NACLC which is above a NAC.

Attachment 23

INSTRUCTIONS TO COMPLETE AF FORM 2583,REQUEST FOR PERSONNEL SECURITY ACTION

Table A23.1. Instructions to Complete AF Form 2583, Request for Personnel Security Action.

LINE	A	B	C
	To Complete		Enter
	Section	Item	
1	I	1	last, first, middle, and maiden name to agree with military or employment records; if not, explain in Section VII. If no middle name, or initial only, enter "NUN" or "IOU," respectively. Also, enter the maiden name for female personnel.
2		2	the unit designation. When the form pertains to non-DOD personnel, enter the unit designation of the sponsoring activity.
3		3	grade. Do not change this entry after the form is filed and a change in grade occurs.
4		4	social security number.
5		5	an "X" in only one block.
6		6	year, month, and day of birth, in that order. For example: 20000210
7		7	city, state, and country of place of birth.
8	II	8	an "X" in only one block.
9		9	an "X" in applicable blocks. Check only the highest level of clearance, access, or entry requirement. (See Note 1 for Limited Access Authorization requests.)
10	III	10	activities required to search their records for possible derogatory information from a personnel security standpoint. Medical and security police activities are usually the agencies required to take this action (see Notes 2 and 3).
11		11	unit of assignment. Also include the telephone number of the requester, to ensure that immediate contact can be made in the event questions should arise.
12		12	date when requester signs the form.
13		13	typed name, grade, and title of the unit commander or staff agency chief, or security manager when delegated this authority.
14		14	self-explanatory. The signature certifies actions in Note 4 have been complied with.
15	IV	15	self-explanatory (see Note 3).
16		16	date when the check is completed.
17		17	typed name and grade of base director of medical services (see Note 5).
18		18	self-explanatory.
19	V	19	see Notes 2 and 6.
20		20	date when the check is completed.
21		21	typed name and grade of the chief of servicing security activity, or designees, in the security clearance function or reports and analysis section.
22		22	self-explanatory.

23	VI	23	an "X" in applicable blocks. In spaces provided, also include the classification level the member requires access to. Except for sensitive compartmented information (SCI) and the PRP, use Section VII to add any other special access program not covered. SCI is not entered, because the MAJCOM or FOA SCI billet manager centrally manages personnel authorized this access. PRP is not entered, since separate forms are used to administer this program.
24		24	self-explanatory.
25		25	enter name, grade, and title of one-time access approving official.
26		26	self-explanatory.
27		27	date when access to special program information is granted.
28		28	typed name, grade, and title of special access program certifying official. Only officials authorized by the governing directive may certify this entry. Use Section VII to show coordination action when two or more special access programs are involved, and the same official grants all access.
29		29	self-explanatory.
30	VII	30	self-explanatory (see Note 7).

NOTES:

1. Send a request letter through channels to the approving authority when non-US nationals or immigrant alien personnel require limited access to Secret or Confidential defense information or unescorted entry to PL 1, 2, or 3 restricted areas.

2. Complete items 10 through 14 when an investigation or a security clearance is required. The LFC is not required when recording special access program authorizations, unless specified in the governing directive. This guidance also applies to sections IV and V.

3. If the individual records derogatory information in Section VII, promptly notify the requester and security information file custodians. This action determines if re-adjudication of the person's security clearance is necessary by the CAF. This guidance also applies to Section V.

4. Ensure the request process includes a review of SK for evidence of an UIF concerning the member. Also, review personnel records to determine if derogatory information exists from a personnel security standpoint. Check personnel records to confirm other data, such as employment or military service as listed on SF Form 86, when necessary. Persons designated to sign Item 14 of the form must take or confirm these actions. Enter results of these reviews in Section VII.

5. Note that this authority may be delegated to other medical staff personnel who may review medical records and form professional opinions based on the information being evaluated. If no medical records are on file (as for many civil service employees) annotate the form to that effect. The DD Form 1879 then shows no local medical records were checked and DSS agents check the records.

6. Review the records of the security clearance function and reports and analysis section. If a SIF exists, deny the requested personnel security action pending completion of adjudication actions. In these cases, also enter in Section VII that a SIF exists. Also, review the remarks section for any other derogatory information reported and evaluate the need to establish a SIF for further adjudication. Enter results of this evaluation in Section VII.

7. Annotate Section VII to reflect what document was used to verify citizenship status.

Attachment 24

SMITH AMENDMENT

A24.1. Implementation of the Section 1071 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, which amended Title 10, United States Code, to add a new section that precludes the initial granting or renewal of a security clearance by the DoD under four specific circumstances as outlined below.

A24.1.1. Provision (1) disqualifies persons with convictions in both State and Federal courts, including UCMJ offenses, with sentences imposed of more than one year, regardless of the amount of time actually served.

A24.1.2. Provision (2) does not change the substance of the existing adjudication guideline relative to current drug involvement. Anyone who is currently an unlawful user of, or addicted to, a controlled substance.

A24.1.3. Provision (3) does not change the substance of the adjudication guidelines for emotional, mental, or personality disorders. Anyone who is found to be mentally incompetent (incapable of safeguarding classified information) by a credentialed mental health professional approved by DoD.

A24.1.4. Provision (4) disqualifies persons who have been discharged or dismissed from the Armed Forces under dishonorable conditions.

A24.2. Secretary of the Air Force may authorize a waiver in meritorious cases under provisions (1) & (4). Waiver authority is not delegable.

A24.3. Provision (2) & (3) disqualifies a person for eligibility for a security clearance and may not be waived.

A24.4. Individuals that fall under the categories (1) through (4) will be afforded applicable due process and appeal opportunity IAW the DoD 5200.2-R, Personnel Security Program and this instruction.

A24.5. When AFCAF issues a final statement of reasons to deny or revoke a security clearance in cases where a waiver is allowed (provisions 1 and 4) the subject will be informed of the waiver provision, provided a copy of the statute and other information on how to respond. The subject must include in the response to the statement of reasons if they want to be considered for a waiver, if applicable.

A24.6. Decision process for determining whether a particular case warrents a meritorious waiver:

A24.6.1. The AFCAF is the first level nominating office and determines if the case warrants a meritorious waiver under the provisions of the statute. If approved, the case is forwarded with the proposed request for waiver and full justification to the Air Force Personnel Security Appeal Board (PSAB) for review.

A24.6.2. If the PSAB determines the case has meritorious justification, the case summary is returned to the AFCAF for forwarding to SAF/AA.

A24.6.2.1. SAF/AA may disapprove the waiver request or forward it to the SECAF with recommendation for approval. Both the SAF/AA and SECAF decisions are final.

A24.7. AFCAF will provide quarterly summaries to SAF/AA by the10th of each month following the end of each calendar quarter of all waivers submitted to SECAF. SAF/AA provides report to USD/I by the 15th.

A24.8. The statute policy applies to:

A24.8.1. All initial determinations to grant security clearance eligibility or access and determinations to continue clearance eligibility/accesses following a reinvestigation.

A24.8.2. Existing clearances eligibility or access which a previous or other investigation reveals a previous favorably resolved issue involving one or more of the four statutory provisions, regardless of the presence or absence of subsequent disqualifying issues;

A24.8.3. Previous and follow-on periodic reinvestigations and other investigations initiated for other reasons; such as:

A24.8.3.1. Security Information File, Special Investigation Inquiry, etc., and all pending cases in which a final decision had not been issued as of 7 Jun 01.

A24.9. The statue polices do not apply to:

A24.9.1. Conversions/transfers/reinstatements of current DoD security clearances, including transfers of clearances of employees within the DoD, clearances of employees who fall under the National Industrial Security Program, and transfers of clearances to the DoD of employees coming from other Federal agencies.

Attachment 25

TABLE FOR INTERIM SECURITY CLEARANCE/ACCESS AUTHORITY

A25.1. Authority to Grant Interim Security Clearance/Access. Use the following table for guidance on authority level to grant interim security clearance/access to specific programs. Items contained in Column E, 3a-d & 4 may be found at: **https://wwwmil.lackland.af.mil/afsf**/. Copy and paste into the browser. Once at the home page, click on "HQ USAF Security Forces," click "Information Security Division," scroll down to "Personnel Security Policy Updates." The references are listed under Personnel Security Policy Updates.

Table A25.1. Authority to Grant Interim Security Clearance/Access.

	A	B	C	D	E
RULE	**If the requirement is for**	**The investigation requirements are**	**The access level is**	**The authorization level is**	**As governed by**
1	**Interim Secret** (see note 1)	- Local files check - Favorable Review of SF 86 - NACLC/ANACI submitted	Secret	Unit Commander	AFI 31-501, Personnel Security Program Management
2	**Interim Top Secret** (see note 1)	- Local files check - Favorable review of SF 86 - SSBI submitted - Favorable NAC, ENTNAC, NACI, NACIC, NACLC, ANACI	Top Secret	Unit Commander	AFI 31-501, Personnel Security Program Management
3	**Interim PRP** (see note 1)				
	(a) Initial PRP Interim Certification for Controlled Position	- NACLC submitted - Favorable PRP interview	PRP Controlled Position	PRP Certifying Official	AF/XOFI Memo, 17 Dec 03, Extension of Temporary PRP Procedures
	(b) Initial PRP Interim Certification for Critical Position	- SSBI submitted - Favorable PRP interview	PRP Critical Position	PRP Certifying Official	AF/XOFI Memo, 17 Dec 03, Extension of Temporary PRP Procedures

	A	B	C	D	E
RULE	**If the requirement is for**	**The investigation requirements are**	**The access level is**	**The authorization level is**	**As governed by**
	(c) Formally Certified for Controlled Position When Investigation is Over 5 Years Old	- NACLC-PR submitted - Favorable PRP interview	PRP Controlled Position	PRP Certifying Official	AF/XOFI Memo, 29 Apr 04, Extension of the Relief to DoD 5210.42, Nuclear Weapons PRP, Para C31
	(d) Formally Certified for Critical Position When Investigation is Over 5 Years Old	- SSBI-PR submitted - Favorable PRP interview	PRP Critical Position	PRP Certifying Official	AF/XOFI Memo, 29 Apr 04, Extension of the Relief to DoD 5210.42, Nuclear Weapons PRP, Para C31
4	**Interim Crypto Access** for Access to Missile Entry Control System (see note 1)	- Interim Secret clearance granted	Secret for Crypto Equipment	Unit Commander	AF/AF AF/XOFI Memo, 18 Dec 03, Request Extension for Authorization for Interim Secret Clearance for COMSEC
5	**Interim SCI** (see note 1)	- Interim Top Secret clearance granted - Favorable SCI screening interview	SCI	Special Security Office obtains AFCAF approval then SSO conducts SCI indoctrination	AFMAN 14-304, The Security, Use and Dissemination of SCI

NOTE:

1. Rule 1 or 2 must be in place accordingly before application of rules 3-5.

Attachment 26

IC 2005-1 TO AFI 31-501, PERSONNEL SECURITY PROGRAM MANAGEMENT

27 JANUARY 2005

SUMMARY OF REVISIONS

This revision incorporates Interim Change IC 2005-1. This change **incorporates** previously published guidance concerning: personnel security investigation forms (**paragraph 2.4**); DoD authorized personnel security investigation provider (**paragraph 2.5**); interim security clearances (**paragraph 3.11**); requesting investigations (**paragraph5.2**; **Attachment 2**); requesting priority processing of investigations (**paragraph 5.5**); dual citizenship/possession or use of a foreign passport (**paragraph 5.7**); investigative requirements for coding positions on the Unit Manning Document (**paragraph 7.2**); mandatory SSBI requirement for certain AFSCs (**paragraph 7.3**); mandatory SSBI requirement for sensitive programs (**paragraph 7.4**); requirements for AF deployments (**paragraph 7.5**); approval process for new/upgrade SSBIs (**paragraph 7.6**); central repository for adjudicative/investigative data Joint Personnel Adjudication System (JPAS) (**paragraph 7.9**); reporting government charge card abuses and misuse (**paragraph 8.1.2**); restrictions on the granting or renewal of security clearances as mandated by the Floyd D Spence National Defense Authorization Act for FY 2001 – Smith Amendment **(Attachment 24)**. **Replaces:** the organization title 497th IG/INS with the Air Force Central Adjudication Facility (AFCAF) (**paragraph 7.1**); **Attachment 22** on DCII with new **Attachment 22** on instructions for identifying personnel security investigation requirements for positions. **Revises:** frequency of submission of PRs **(3.28)**, **A2.7**, & **Table A3.5**. **Clarifies:** definition of Commander **(paragraph 1.3)**. **Adds:** initial and PR requirements for Explosive Ordnance Disposal assignments **(3.29.) and Table A3.5;** address for AFCAF (**paragraph 6.1**)**;** position coding annual review to be conducted each May **(7.2.1.3);** option to use FD Form 258 in place of SF 87 for fingerprint form **(Table A3.1)**; OPM as the organization to send requests for investigation (paragraph **2.5. & A2.2.2.1**); mailing addresses for OPM (Table **A2.2.2.8**); address for AF Liaison Office at OPM (paragraph **A2.9**); Table for Personnel Security Investigation Position Coding (**Table A22.1**); Table for Mandatory SSBI Requirement List for Officer AFSCs (paragraph **A22.2**); Mandatory SSBI Requirement List for Enlisted AFSCs (paragraph **A22.3**); Mandatory SSBI Sensitive Program Requirements (Table **A22.4**); Mandatory Positions/Programs Requiring Investigations by Type (Other than SSBIs) (Table **A22.5**); Authority to Grant Interim Security Clearance/Access (**Table A25.1**). **Deletes:** use of PCS or TDY orders as verification of security clearance (paragraph **7.8.**); reference to Sentinel Key **(7.9)**; **Chapter 12** on DCII; DSS as organization to send investigation requests (**A2.2.2.1**); reference to security access requirement (SAR) (**paragraph 7.2**.)

1.3. Definitions. See **Attachment 1** for additional definitions. For purposes of this AFI the term "Commander" means: Commanders or equivalent and staff agency chiefs.

2.4. Types and Scope of Personnel Security Investigations. The scope of each type of personnel security investigation is listed in DoD 5200.2-R, Appendix B. See **Attachment 2** for procedures on requesting personnel security investigations (PSI). See **Attachment 3** for guidance on the types of required personnel security investigations and appropriate questionnaire forms and or Electronic Personnel Security Questionnaire (EPSQ) Software.

2.4.1**.** General. The investigations listed in DoD Regulation 5200.2-R and this instruction are the only PSIs authorized. The Secretary of the Air Force and/or the Under Secretary of Defense, Intelligence must approve raising or lowering the scope of the authorized investigation.

2.5 Authorized Personnel Security Investigation Provider. The Office of Personnel Management (OPM) is the DoD Authorized Personnel Security Investigation Provider.

2.7. Overseas Personnel Security Investigations. AFOSI personnel conduct the overseas portion of personnel security investigations, augmented by Army, Navy, and State Department counterparts.

3.11. Interim Security Clearances. Commanders may grant interim security clearances for access to Top Secret and Secret information when the requirements of DoD 5200.2-R, paragraph 3.401 have been met. Use of local information and the following requirements provide Commanders with the necessary tools to exercise their authority to grant interim security clearances. Also see **Attachment 25**, **Table A25.1** for guidance on the authority level to grant interim security clearance/access to specific programs.

3.11.1. Interim Top Secret security clearances**:**

3.11.1.1 Favorable ENTNAC, NAC, NACI, NACIC, NACLC, or ANACI completed.

3.11.1.2. Consult the Joint Personnel Adjudication System (JPAS) to determine the existence of a favorable ENTNAC, NAC, NACI, NACIC, NACLC, or ANACI. The investigation is acceptable if there is no break in service over two years.

3.11.1.3. Favorable review of personnel security questionnaire.

3.11.1.4. Favorable review of local personnel records, base and or security force records, medical records, and other security records, as appropriate.

3.11.1.5. SSBI package has been submitted by an Authorized Requester to the investigative agency provider.

3.11.2. Commanders can grant interim Top Secret security clearance if the above provisions have been met.

3.11.3. If there is no record of a completed investigation (NAC portion) in JPAS, contact Air Force Central Adjudication Facility (AFCAF) Customer Support through JPAS to determine if there is a favorable NAC. (Note Optional: Authorized requesters can request "Advanced NAC Results" from OPM on the OPM Agency Use Sheet.)

3.11.4. Interim Secret security clearances:

3.11.4.1. Favorable review of personnel security questionnaire.

3.11.4.2. Favorable review of local personnel records, base and or security forces records, medical records, and other security records, as appropriate.

3.11.4.3. NACLC or ANACI has been submitted by an Authorized Requester to an investigative agency provider.

3.11.5. Interim security clearances must be documented in JPAS or in writing if JPAS is unavailable, until the final security clearance eligibility is granted by the AFCAF.

3.11.6. For Civilians:

3.11.6.1. Consult JPAS on a newly hired civilian for a previous security clearance/personnel security investigation to determine if a previous security clearance was held as a former military member (without a break in service of two years) or if a security clearance as either an Air Reserve Technician or as a traditional reservist was held.

3.11.6.2. Pending completion of ANACIs or SSBIs, as appropriate, civilians may occupy non-critical sensitive or critical sensitive positions. Commanders prepare a waiver of pre-employment investigation requirements when such action is necessary and in the national interest. Interim security clearance may not be granted until after the commander signs the waiver memorandum.

3.11.7. JPAS is the source for determining investigative status on pending investigations. Also see **para 7.9**.

3.28. Periodic Reinvestigations (PR). PRs are required every 5 years for Top Secret and 10 years for Secret. Authorized requesters submit requests for reinvestigations to the DoD Authorized Investigation Provider as outlined in **A2.2.2.1**. See AFI 31-406, Applying North Atlantic Treaty Organization (NATO) Protection Standards, for submission of PRs for NATO investigations.

3.29. Explosive Ordnance Disposal (EOD). Although such personnel normally only require a Secret clearance, an SSBI is initially required due to training and assignments involving nuclear weapons. Persons occupying an EOD position shall undergo a Secret PR on a five year recurring basis.

5.2. Authorized Requesters.

5.2.1. MAJCOM, field operating agency (FOA), or direct reporting unit (DRU) staffs designate authorized requesters to initiate PSIs for their organization. As a general rule, the number of authorized requesters will be kept to the minimum number required to meet mission requirements. See **Attachment 2** for request procedures.

5.2.2. Authorized requesters provide the AFCAF with the name, telephone number, and office symbol of individual(s) who may obtain security clearance and or investigative data on individuals within their organization and provide copy to respective MAJCOM. See **para 6.1** for AFCAF address.

5.2.3. Authorized requesters may query the JCAVS or call the CAF Customer Support Section at DSN 754-1242/43 to determine investigative and/or adjudicative status.

5.2.4. Authorized requesters approve and submit personnel security questionnaires to the DoD Authorized Personnel Investigation Provider according to **Attachment 2**.

5.5. Priority Requests. The following sensitive programs are authorized priority processing service by OPM:

5.5.1. PRP. In cases where a PRP "C" coded case warrants "Priority" service by OPM, the authorized requester must coordinate the request through channels to AF/XOS-FI. Each authorized requester will maintain a fiscal year (FY) Excel spreadsheet listing for this purpose. The spreadsheet will include all previously coordinated FY priority PSIs and all new requirements the authorized requester is coordinating under this authority. When coordinating new priority cases, forward the entire FY spreadsheet to **afxofi.workflow@pentagon.af.mil**. AF/XOS-FI will return to the authorized requester for monitoring the completion of the investigation.

5.5.2. SCI. When the NACLC adjudication date is less than 12 months (DCID 6/4, Annex A, para 5), the servicing Authorized Requester will provide the servicing SSO a copy of the completed SF 86 for each SSBI request with an SCI access requirement. This will be done at the same time the request for SSBI/SCI is forwarded to OPM. Security Managers/SSOs/Authorized Requesters will expedite the processing of the SSBI off the installation to OPM and request priority level of service. On the *OPM Agency Use Sheet annotate 30A in Block A.* Also see AFMAN 14-304.

5.7. Dual Citizenship. A security concern could exist when a military member, DoD civilian, contractor, or consultant is submitted for a personnel security investigation and they are a dual citizen and/or possess/use a foreign passport.

5.7.1. Dual Citizenship. Dual citizenship in and of itself is not an automatic disqualifier for security clearance eligibility. However, possession of dual citizenship and particularly the **exercise** of dual citizenship is a condition that raises a security concern and may be a disqualifying factor in a security clearance eligibility determination. There are factors that could mitigate the maintenance of dual citizenship, as outlined in DoD 5200.2-R, App I, Foreign Preference. An individual's expressed willingness to renounce dual citizenship is one of the conditions that *could* mitigate security concerns.

5.7.2. Possession or Use of a Foreign Passport. Possession and/or use of a foreign passport in preference to a US passport raises doubt as to whether the person's allegiance to the US is paramount and could also facilitate foreign travel unverifiable by the US. The security clearance will be denied or revoked, unless the applicant surrenders the foreign passport or obtains official approval for its use from SAF/AA. Requests for approval are forwarded through respective Information Security Program Manager (ISPM) channels to HQ USAF/XOS-FI for processing to SAF/AA. Justification must include what benefit the AF will gain from a person holding a foreign passport. AFCAF will annotate approvals in the remarks field of the JPAS.

5.7.3. Surrendering the Passport. Individuals who indicate they possess a foreign passport in item 15 of the Electronic Personnel Security Questionnaire or item 17d on the Standard Form 86,

"**Questionnaire for National Security Positions**," will be required to surrender the passport via one of the following methods:

5.7.3.1. Return the passport to the appropriate country embassy or consulate via certified receipt mail. A copy of the transmittal memo forwarding the passport and the return receipt will be forwarded to the AFCAF. See **para 6.1** for AFCAF address. If the name of adjudicator assigned to the case is known, include this in the ATTN line of the address.

5.7.3.2. Destroy the passport as witnessed by an AF security manager. Cut up the passport and place in a burn bag. The witnessing security manager will document the destruction of the passport in an explanatory memorandum, which will be forwarded to the AFCAF and a copy provided to the subject.

5.7.4. Security Clearance Eligibility**.** In order for individuals who hold foreign passport and dual citizenship to be considered for and/or be granted security clearance eligibility the following must be completed:

5.7.4.1. Provide a written statement expressing their willingness to renounce foreign citizenship claims in favor of a sole United States citizenship status. Actual renouncement is not required.

5.7.4.2. Return and or destroy the passport.

5.7.5. The renouncement statement and documentation of destruction of the passport must be provided to the AFCAF. The AFCAF reviews each case on its own merits to determine security clearance eligibility.

5.7.6. This same guidance will apply if the passport is identified after a security clearance determination is made.

6.1. Central Adjudication Authority. The Air Force Central Adjudication Facility (AFCAF) is the Central Adjudication Authority. Address is: AFCAF/PSA, 229 Brookely Ave, Bolling AFB 20032.

6.1.1. The policy and criteria set forth in DOD Regulation 5200.2-R, paragraph 2-200, 6-102 and Appendix I will be applied in making personnel security determinations for a security clearance or assignment to sensitive duties.

6.1.2. Unfavorable adjudication results in the denial/revocation of clearance eligibility (see **Chapter 8**).

6.1.3. The AFCAF will review all investigative products and make an eligibility determination.

6.1.4. AFCAF Customer Service will not release adverse information to inquiring customers on pending investigations, as it invokes privacy act concerns. Derogatory issues are often resolved through completion of the investigation and or adjudication of the case. Premature dissemination of unresolved and or unadjudicated issues could result in discriminatory practices with respect to such areas as employments or assignments.

6.2. Adjudicative Record. Personnel security determinations are reflected in the JPAS. JPAS replaced Sentinel Key (SK) as used throughout AFI 31-501.

7.1. General

7.1.1. The AFCAF is the designated authority to grant, suspend, deny, or revoke personnel security clearances and SCI accesses (see **Chapter 11**).

7.2. Investigative Requirements for Coding Positions. Commanders will:

7.2.1. Determine the type of investigation required for mission purposes for each military and civilian position in the organization. Investigations are required for multiple purposes: to determine suitability and/or trustworthiness of individual for employment/assignment to positions of trust/access to certain programs; and for security clearance. Each position is coded with the appropriate position code reflecting the required investigation level in the unit manning document (UMD) and the Defense Civilian Personnel Data System (DCPDS). These will also be reflected in the Headquarters Air Force Manpower Data System (HAF-MDS).

7.2.1.1. Assign one of the five investigation types to each position:.

7.2.1. l.1. Single Scope Background Investigation (SSBI).

7.2.2.1.2. National Agency Check, Local Agency Checks and Credit (NACLC).

7.2.2.1.3. Access National Agency Check and Inquiries (ANACI).

7.2.2.1.4. National Agency Check Plus Inquiries (NACI).

7.2.2.1.5. National Agency Check (NAC).

7.2.1.2. The definitions and corresponding codes are located in **Attachment 22**, **Table A22.1**.

7.2.1.3. Conduct annual review to determine the accuracy of position coding. The last AF-wide directed review was conducted in May 04. Reviews will be conducted each May. Retain results for review during self inspections, etc.

7.2.1.4. Ensure only necessary investigations are requested to meet mission essential needs.

7.2.1.5. See **Attachment 22** for additional guidance.

7.3. Investigative Requirements for Air Force Specialty Codes (AFSCs). HQ USAF/XOS-FI approves requests for adding security clearances or investigations as AFSC prerequisites. Requests are staffed through ISPM channels. AFMAN 36-2105, Officer Classification and AFMAN 36-2108, Enlisted Classification will reflect an SSBI requirement for entry, award, and retention for the respective mandatory AFSCs. See **Attachment 22**; **Table A22.2.**, **A22.3**.

7.4. **Investigative Requirements for Sensitive Programs**. There are several sensitive programs that have been designated as a mandatory SSBI requirement, i.e., Presidential Support, Personnel Reliability Program, etc. See **Attachment 22**, **Table A22.4**.

7.5. Investigative Requirements for Air Force Deployments, Operational or Contractual Exigencies. This policy does not apply to SCI. Positions identified for deployments will, as a minimum, be assigned a NACLC, requiring access to Secret information for the in-country threat briefing. SSBIs are not authorized for purposes of Top Secret eligibility "just in case of" deployment. In these situations, commanders grant interim Top Secret access for a period of up

to 180 days. This can be renewed for extended deployment purposes and for redeployment. Interim Top Secret access is granted for the purpose of deployment based on the existing NACLC, and discontinued upon return to home station. SSBIs will not be required for this purpose. Persons must be US citizens and have not had a break in service for more than 24 months. Record of the interim TS is annotated in JPAS or in cases where it is not available, documented and maintained with security related documents. However, SSBI is authorized if a joint or theater deployment requires a final Top Secret security clearance and will not accept interims, i.e., JCS contingencies. These requirements need to be identified and positions coded IAW **para 7.2.** of this instruction.

7.6. Approval Authorities for Additional/New/Upgrade of SSBIs. 3-Star/Civilian Equivalent authority is required to approve any additional/new/upgrade SSBIs before the servicing Manpower Office codes the positions on the UMD. Approval authorized cannot be delegated. Approval authorities are as follows:

7.6.1. MAJCOMs: CV or NAF/CC

7.6.2. FOAs: parent 2-Ltr or SAF/AA or AF/CVA if the parent 2-Ltr is not at the appropriate grade level

7.6.3. DRUs: AF/CVA.

7.6.4. HQ USAF:

7.6.4.1. Air Staff: AF/CVA

7.6.4.2. Secretariate: SAF/AA.

7.6.5. Commands will establish internal certifying procedures. The approval documentation will be retained by the Manpower Office for three years and is subject to compliance review by HQ AFIA or their designee. Approval will increase MAJCOM funds withhold for personnel security investigations through the FYDP.

7.7. Periodic Reinvestigations. Periodic Reinvestigations will be kept current for incumbents assigned against positions coded as requiring SSBI and NACLC/ANACI. Also see **para A2.7**.

7.8. Issuing Security Clearance Eligibility. AFCAF issues security clearance eligibility and enters the determination into JPAS.

7.9. The Joint Personnel Adjudication System (JPAS). JPAS is the Department of Defense (DoD) personnel security clearance and access database. It facilitates personnel security management for the DoD Central Adjudication Facilities (CAF), security managers, and offers both non-SCI and SCI functions. It interfaces with the investigative providers, the personnel systems within the Department thus eliminating manual transactions and expediting the flow of personnel security information to warfighters.

7.9.1 JPAS is the primary source for determining investigative data/status of investigations on individuals in the DoD. JPAS allows communication between the CAFs and its customers. All information in JPAS is unclassified, but must be protected according to the requirements for privacy/sensitive information and For Official Use Only (FOUO) in accordance with AFI 33-332, Air Force Privacy Act Program and DoDR 5400.7/AF Supplement, DoD Freedom of Information Act Program.

7.9.2. JPAS has two applications: The Joint Adjudication Management System (JAMS) and Joint Clearance and Access Verification System (JCAVS)

7.9.2.1. JAMS is for adjudicative personnel only and provides capabilities such as case management/distribution, adjudication decisions, adjudicative history and summary, due process, and future ability for each CAF to electronically access investigative reports from the investigative providers.

7.9.2.1.1. JAMS replaced the Adjudicative Management System (AMS), as used throughout this instruction.

7.9.2.2. JCAVS is for non-SCI and SCI security managers/officers and authorized requesters and provides capabilities such as access indoctrination/debriefing history, incident/issue file reporting, history and management of unit personnel security functions.

7.9.2.2.1. JCAVS replaced Clearance and Access Verification System (CAVS), as used throughout this instruction.

7.9.3. ISPMs determine the number of users and the access levels for each user. Clearance data elements in the JCAVS include the full date and type of investigation and the full date and status of security clearance. The information is invalid when any of these four data elements are incomplete.

7.9.3.1. Use the most current highest level eligibility recorded in the JCAVS when more than one entry appears for an individual.

7.9.3.2. The term "DCID 6/4 (formerly DCID 1/14)" means the person has been the subject of a SSBI, has been granted a Top Secret security clearance eligibility, is eligible for SCI access if required for mission essential purposes and may already have SCI access. See AFMAN 14-304.

7.9.4. The JCAVS will provide the following information:

7.9.4.1. An individual's security clearance eligibility level and access level.

7.9.4.2. Visit notification.

7.9.4.3. Suspension notification.

7.9.4.4. SCI indoctrination, nondisclosure statement, and debriefing dates.

7.9.4.5. Establishment of a SIF.

7.9.6. JCAVS User Levels are as follows:

7.9.6.1. Level 2 - SCI security personnel at unified command, DoD agency, military installation or major command/equivalent headquarters. Personnel Security Management (PSM) - Net is determined by the responsible SOIC or designee. (Read and Write Access - SSBI/DCID 6/4 with current SCI Access.).

7.9.6.2. Level 3 - SCI security personnel at echelons subordinate to Level 2 at a particular geographic location (installation, base, post, naval vessel). PSM - Net is determined by the responsible SOIC or designee. (Read and Write Access - SSBI/DCID 6/4 with current SCI Access.)

7.9.6.3. Level 4 - Non-SCI security personnel at unified command, DoD agency, military department or major command/equivalent headquarters. PSM - Net is determined by the responsible Security Officer or designee. (Read and Write Access - NACLAC/ANACI/Secret Eligibility.)

7.9.6.4. Level 5 - Non-SCI security personnel at echelons subordinate to Level 4 at geographic location (installation, base, post, naval vessel). PSM - Net is determined by the responsible Security Officer or designee. (Read and Write Access - NACLC/ANACI/Secret Eligibility.)

7.9.6.5. Level 6 - Unit Security Manager (additional duty) responsible for security functions as determined by responsible senior security official. (Read and Write Access - NACLC/ANACI/Secret Eligibility.)

7.9.6.6. Level 7 - Non-SCI Entry Control Personnel. Individuals who grant access to installations, buildings, etc. Varies according to organizations. (Read Access - NACLC/ANACI/Secret Eligibility.)

7.9.6.7. Level 8 - SCI Entry Control Personnel. Individuals who grant access to SCIF installations, buildings, etc. Varies according to organizations. (Read Access - SSBI/DCID 6/4 Eligibility.)

7.9.6.8. Level 10 - Visitor Management. Level 10 users will have the same view of the JCAVS Personnel Summary as a JCAVS Level 7 User. They will receive Visit Notification when their Security Management Office (SMO) is being notified of a visit. A Level 10 User may **not** be an account manager to create or delete an account at any level. NACLC/ANACI/Secret Eligibility.

7.10. AF JPAS Users Guide. Contains detailed instructions on operating JPAS and becoming a new user. See the follow URL: **https://wwwmil.lackland.af.mil/afsf/Organization/AFXOF/XOF%20memo%2012%20Jul%2004%20AF%20JPAS%20Guide1.pdf** .

JPAS web site is: **https://jpas.osd.mil** Requests for changes to JPAS may be made on-line at **https://jpas.osd.mil**.

7.11. Granting Access. Commanders grant access to classified information when a mission essential need exists and only when all of the following prerequisites are met: (1) individual has the appropriate security clearance eligibility; (2) individual has signed an SF 312 (see AFI 31-401); and (3) individual has a need-to-know. Authorized base level users will record access in the JCAVS. See **Chapter 3** for other situations when access to classified information may be granted.

7.12. Obtaining Information from the AFCAF.

7.12.1. Authorized requesters may contact the AFCAF Customer Support Section through JPAS. In situations where no security clearance data is available at the unit, no information is available in the JCAVS, and the AFCAF has valid security clearance information on file, a record of the call will be used as evidence of valid clearance data pending update of the JCAVS. The authorized requester prepares a memorandum for record (MFR) showing: (1) name, grade, and organization of the individual calling the AFCAF; (2) name, grade, organization, and SSN of the subject; (3) name of person at the AFCAF providing clearance eligibility data, and (4) type and

date of investigation and, if granted, level and date of security clearance eligibility. Also see **para 6.1**.

7.12.1.1. The authorized requester forwards a copy of the MFR to the individual's security manager.

7.12.1.2. The authorized requester and the security manager keep the MFR until JCAVS is updated to show the data addressed in the MFR.

8.1.2. Reporting Government Charge Card Abuses and Misuse. Security Officials, AFOSI, or AF Government Charge Card program coordinators are required to immediately report Government Charge Card abuses and misuses to the appropriate commander. This information constitutes serious questions as to the individual's ability or intent to protect classified information or execute sensitive duties. The commander will make an immediate determination to either leave the individual's security status unchanged or suspend their access to classified information or assignment to sensitive duties until the appropriate authority makes a final determination regarding the individual's eligibility to retain a security clearance. In addition, commanders may take action in accordance with **Chapter 8**, to determine if a SIF should be established and/or the person's access to classified information should be suspended.

8.1.3. Implementation of Restrictions on the Granting or Renewal of Security Clearances as Mandated by the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 – Smith Amendment. **Attachment 24** outlines the instructions.

8.9.3. For SIOP-ESI access. Refer to AFI 10-1102, Safeguarding the Single Integrated Operational Plan (SIOP).

Chapter 12

DELETED

12.1. DELETED

Attachment 2

REQUEST PROCEDURES

A2.1. General

A2.1.1. Security managers:

A2.1.1.1. Process completed personnel security questionnaires for active duty, reserve military, National Guard, civilian and or contractor personnel to the unit's supporting authorized requester of investigations IAW with this AFI. See **Attachment 3** for required security forms, types of investigations to request and in what situations. An individual must have one year retainability for an investigation to be requested.

A2.1.1.2. Verify the most recent or most significant claimed attendance, degree or diploma at an educational institution. This is not required for Periodic Reinvestigations.

A2.1.1.3. Verify the date and place of birth through a check of appropriate documentation, e.g., a birth certificate, certificate of naturalization, passport, or Report of Birth Abroad of a Citizen of the United States of America. This is not required for Periodic Reinvestigations.

A2.1.1.4. Show the verification of birth and highest level of education on the SF 86/EPSQ software.

A2.1.2. The subject will provide the required documentation to the security manager.

A2.1.3. Air Force Reserves and IMAs. The Air Force Reserve Recruiting Service (AFRS/RS) processes reservist's initial personnel security investigation during accession to the supporting authorized requester.

A2.2. Authorized Requesters.

A2.2.1. Authorized Requestors for Accessions.

A2.2.1.1. HQ AFRS submits initial investigations (NACLC) for enlisted recruits through the Air Force Recruiting Information Support System (AFRISS).

A2.2.1.1.1. 319 TRS/DPAS:

A2.2.1.1.1.1. Verifies that the NACLC, submitted by AFRS, is open by checking JPAS and the OPM help desk, if necessary. When an open NACLC cannot be confirmed through either source, the 319 TRS/DPAS:

A2.2.1.1.1.1.1. Submits a new NACLC and file a copy of the submitted investigation in the member's Unit Personnel Record Group (UPRG).

A2.2.1.1.1.2. Submits SSBI investigation requests to OPM for all personnel training into a sensitive skill. A copy of the investigation request and receipt will be filed in the member's UPRG. On arrival at the student's technical training location, security managers will remove the investigation package and forward to the servicing security activity.

A2.2.1.1.1.3. Processes priority SSBI investigations for authorized AFSCs. HQ AETC/SFI, in conjunction with AF/XOS-FI, is the approval authority for priority investigations for accessions.

A2.2.1.2. Officer accession sources submit initial investigations (NACLC) to OPM for recruits, normally within 30 days of their contract obligation to the Air Force.

A2.2.1.3. Officer accession sources submit SSBI investigation requests to OPM for personnel training into a sensitive skill.

A2.2.1.4. Losing authorized requesters and AFRS submit SSBI requests for prior service and non-prior service OTS selects prior to their departure.

A2.2.2. Authorized Requesters for Non-Accessions:

A2.2.2.1. Request personnel security investigations according to position coding requirements (see **para 7.2.** and **Attachment 22**). See **Attachment 3**, for required security forms, types of investigations to request. Submit investigation requests to OPM.

A2.2.2.2. Use the EPSQ software as the primary source for the investigative request. Validate the EPSQ, and print a hard copy for mailing investigation requests to OPM. OPM does not have electronic transmission capability.

A2.2.2.2.1. For additional EPSQ guidance consult the DSS web site: **http://www.dss.mil**. Contact DSS Customer Service Center at 1-800-542-0237 or DSN 283-7731, if necessary.

A2.2.2.3. Request all types of investigations from OPM, as the DoD Authorized Investigation Provider. Use OPM Investigation Handbook, IS-15, Requesting OPM Personnel Investigations. It can be accessed via AF/XOS-FI web: **https://wwwmil.lackland.af.mil/afsf/.**

A2.2.2.4. Obtain Submitting Office Number (SON) from OPM. This four character SON identifies the office as authorized to request investigations from OPM.

A2.2.2.5. A complete package requesting an investigation includes the following: OPM Agency Use Sheet, applicable personnel security questionnaire, Fingerprint Card, if applicable, original signed "Authorization for Release of Information," and if applicable, the "Authorization for Release of Medical Information."

A2.2.2.6. OPM does not require the DD Form 1879.

A2.2.2.7. Complete OPM Agency Use Sheet – AF specifics:

A2.2.2.7.1. AF has two billing codes which are annotated in Block N.

A2.2.2.7.1.1. DoD-AFM. This is for investigation requests on military members.

A2.2.2.7.1.2. DoD-AF. This is for investigation requests other than military.

A2.2.2.7.1.2.1. Civilians (appropriated and nonappropriated).

A2.2.2.7.1.2.2. Child Care.

A2.2.2.7.1.2.3. Contractor suitability/trustworthiness. (Not security clearances. AF does not request investigations for security clearances on contractors under the National Industrial Security Program.)

A2.2.2.7.2. Block L is always: AF 00.

A2.2.2.7.3. Block H. Annotate "J" to indicate Personnel Reliability Program (PRP) investigation.

A2.2.2.8. Mail requests as OPM does not have electronic transmission capability. See **Table A2.2.2.8** for OPM addresses and type of investigation.

Table A2.1. Mailing Addresses for OPM.

OPM Address		Investigation Description
OPM-FIPC PO Box 700 ATTN: AF Liaison 1137 Branchton Rd Boyers, PA 16018		General correspondence and MEPS new accession releases and fingerprint cards that require the SF 86 to be printed via the AFRISS program (No actual PSI should be mailed to this address)
OPM-FIPC PO Box 49 ATTN: AF Liaison 1137 Branchton Rd Boyers, PA 16018		All Periodic Reinvestigations. 35-Day Cases All Presidential Support, PRP, Blowtorch Cases (initials & PRs)

OPM-FIPC PO Box 618 1137 Branchton Rd Boyers, PA 16018		All Initial Investigations

A2.2.2.9. Maintain a suspense copy of PSIs and all other information until the investigative data appears in the JCAVS.

A2.2.2.10. Check JPAS weekly to monitor the status of the investigation until it is closed. An SII inquiry, from the Person Summary screen, should be conducted to ascertain if the case was determined unacceptable. Should the investigation remain unopened for 30 days after it was submitted, and is not shown as unacceptable in SII, contact the OPM help desk at (724) 794-5228 to inquire as to its status. If the status cannot be ascertained, resubmit the investigation.

A2.2.2.11. Forward the suspense copy of the PSI to the gaining base authorized requester when a permanent change of station (PCS) occurs.

A2.2.3. Investigation Types.

A2.2.3.1. **National Agency Check with Local Agency Checks and Credit Check (NACLC).** SF 86 for individuals requiring access to Secret information and/or suitability. All military members require a NACLC.

A2.2.3.1.1. The SF 86 must cover the most recent seven-year period. The "Have you ever" questions cover the individual's entire lifetime.

A2.2.3.1.2. NACLCs will be requested for military personnel with no prior or current security clearance eligibility if and when access to Secret information is required.

A2.2.3.1.3. Existing ENTNAC or NAC investigations remain valid for individuals with prior or current Secret eligibility regardless of the age of the investigations there has been no break in service over 24 months. Periodic reinvestigation rules apply.

A2.2.3.2. **Single Scope Background Investigation (SSBI).** Authorized requesters submit SF 86.

A2.2.3.2.1. The questionnaire must be completed to cover the most recent seven-year period with 10 years coverage on the residence, education, and employment questions, or since the 18th birthday, but at least the last two years. "Have you ever" questions must cover the individual's entire lifetime. Use SF 86A, *Continuation Sheet for Questionnaires* for information for years 8 through 10.

A2.2.3.2.2. Provide both the alien and naturalization/citizenship number for each foreign-born relative and associate listed on the SF 86 that claims US citizenship. Other authorized means in proving U.S. citizenship for foreign-born relatives are the State Department form 240, Report of Birth Abroad of a Citizen of the U.S., or the number from either a current or previous U.S. passport.

A2.2.3.2.3. If selective service number is not known, the subject's SSAN will be accepted.

A2.2.3.2.4. A Single Agency Check (SAC) is required on the following individuals associated with the subject of an SSBI: (a) spouse or cohabitant, (b) immediate family members 18 years

old or older who were born outside the United States. If marriage or cohabitation occurs after completion of the SSBI, transmit Spouse SAC to OPM, using EPSQ software. Keep a hard copy for suspense file.

A2.2.3.3. National Agency Check (NAC). Authorized requesters use SF 85P and an SF 87 or FD Form 258.

A2.2.3.4. National Agency Check Plus Written Inquiries and Credit Check (NACI). The CPF will submit SF 85 or SF 85P, as appropriate and SF 87 or FD Form 258.

A2.2.3.5. Access National Agency Check with Written Inquiries and Credit Check (ANACI**).** For civilians requiring access to classified information at the Secret level in order to perform mission duties or in noncritical sensitive positions, the CPF will submit SF 86 or FD Form 258 and an SF 87.

A2.3. IMAs. The authorized requester of the unit of assignment or attachment will submit periodic reinvestigations or confirm revalidation's of security clearances for IMAs.

A2.4. Catch'Em in Continental United States (CEIC) Program. Personnel requiring an SSBI or periodic reinvestigation and who are scheduled for a PCS move to an overseas location, including Shemya AFB, AK, fall within the CEIC program. Such individuals must complete the personnel security questionnaire within 180 days prior to departure. This allows the investigative agency time to conduct the personal interview before they PCS.

A2.5. Subject Interview. Individuals completing a personnel security questionnaire must specify any circumstances that would make them unavailable for a subject interview within 180 calendar days of the date the form is transmitted. Detailed information regarding the period in which the individual will be unavailable such as date, location, and duration should be provided in the remarks section of the appropriate form. The investigative agency will try to conduct the subject interview prior to departure of the individual.

A2.6. Local Files Check. The unit security manager initiates and verifies completion of a LFC that includes a review of local personnel, medical facility, law enforcement, or other security records, as appropriate. Use AF Form 2583, **Request for Personnel Security Action**, to document an LFC. See **Attachment 23** for instructions on filling out AF Form 2583.

A2.6.1. Headquarters Air Education and Training Command/Recruiting Service (HQ AETC/RS), 550 D Street West, Suite 1, Randolph AFB TX 78150-4527 does not have to complete AF Form 2583 when personnel records are unavailable.

A2.6.2. The Reserve Recruiting Service (HQ AFRS/RS) or their authorized requesters do not have to complete AF Form 2583 for IMAs, IRRs, and traditional reservists when personnel records are unavailable.

A2.6.3. AF Form 2583 is not needed for civilian applicants for federal employment when local files are unavailable.

A2.6.4. Record briefings for access to special access program information on AF Form 2583 when the governing program directive does not prescribe other procedures.

A2.7. Periodic Reinvestigations (PR).

A2.7.1. Requests for PRs are submitted in the same manner as initial investigations. However, no fingerprint card or birth certification is required. No abbreviated version of SF 86/EPSQ may be submitted in connection with a PR. A person must have one-year retainability before a PR may be requested.

A2.7.2. An authorized requester should initiate a Secret PR at the **9.5** year mark from the date of the previous investigation or reinvestigation. Questionnaire must cover the most recent 10-year period or the period since the last investigation.

A2.7.3. An authorized requester should initiate a Top Secret PR at the **4.5** year mark from the date of the previous investigation or reinvestigation.

A2.7.4. For individuals in a NATO billet, submit the PR IAW AFI 31-406, Applying North Atlantic Treaty Organization (NATO) Protection Standards and **Table A3.5**, Rule 12 & 15.

A2.8. Air Force Liaison Office at the Operations Center-Baltimore. Address for the AFLNO is: Defense Security Service, ATTN: Air Force Liaison Office, 601 10TH street, Suite 135, Ft George Meade, MD 20755-5134.

A2.9. Air Force Liaison Office at OPM. Address for the AF Liaison at OPM is: OPM-FIPC, PO Box 700, ATTN: Air Force Liaison, 1137 Branchton Road, Boyers, PA 16018.

A3.1. Personnel Security Investigations. Use the following table for guidance on the types of required personnel security investigations and appropriate questionnaire forms and or EPSQ.

Table A3.1. Personnel Security Questionnaire Forms/Software for Investigations.

RULE	**A** **Type of Investigation**		**B** **EPSQ Software or SF 86/85P/85**	**C** **FD Form 258 or SF 87 (Either Form)**
1	NAC		SF 85P	1 signed original of SF 87/FD Form 258
2	NACLC including Secret/PRs and SAP/PRs		SF 86	1 signed original of SF 87/FD Form 258 (except PRs)
3	NACIC		Original and 1 copy of SF 85/85P	1 signed original of SF 87/FD Form 258
4	ANACI		Original and 1 copy of SF 86	
5	SSBI including TS/PRs		SF 86	1 signed original of SF 87/FD Form 258 (except PRs)
6	Special Investigative Inquiry		Original and 2 copies of SF 86 (see notes 1& 2)	1 signed original if FBI/ID check desired

RULE	A		B	C
	Type of Investigation		EPSQ Software or SF 86/85P/85	FD Form 258 or SF 87 (Either Form)

NOTES:

1. Send original and 1 copy to the AFCAF for forwarding to OPM. One copy is for the authorized requester's suspense file.

2. An original copy of the SF 86 (or EPSQ) should accompany the request, where appropriate, unless such documentation was submitted within the last 12 months to OPM as part of another PSI. The results of any other recently completed investigative reports should also be sent. Indicate the specific areas or issues requiring investigation with justification in Remarks.

A3.5. Guide for Requesting Periodic Reinvestigations. Use the following table for guidance on the minimum standards for PRs.

Table A3.5. Guide For Requesting Periodic Reinvestigations.

RULE	A	B	C
	If the individual is a	and duties require	then request a periodic reinvestigation
1	United States military member, DOD civilian, or contractor employee	access to Top Secret	4.5 years from the date of the last SSBI or SSBI-PR
2		access to SCI	
3		assignment to presidential support	
4		assignment to an AIS I position	
5		access to SIOP-ESI	
6		assignment to AFOSI duties	
7		assignment to a critical personnel reliability program position	
8		access to Top Secret special access programs	
9	United States civilian employee	assignment to a special or critical sensitive position	
10	Non-United States national employee and immigrant alien	limited access authorization	
11		unescorted entry to PL 1 or 2 restricted areas	

RULE	A If the individual is a	B and duties require	C then request a periodic reinvestigation
12	United States military member, DOD civilian, or contractor employee	North Atlantic Treaty Organization COSMIC Top Secret or COSMIC Top Secret ATOMAL	4 years from the date of the last SSBI or SSBI/PR
13	United States military member, DOD civilian, or contractor employee	access to an approved Secret special access program	4.5 years from the date of the last investigation
14		Explosives Ordinance Disposal (EOD)	4.5 years from the date of the last SSBI/S-PR (note 1)
15		assigned to a North Atlantic Treaty Organization staff position	9 years from the date of the last investigation
16		access to Secret information and/or assignment to noncritical sensitive positions	9.5 years from the date of the last investigation

Note 1. EOD assignment requires a Secret PR on a five year recurring basis.

A3.7. Deleted.

Table A3.7. DELETED

Attachment 22

INSTRUCTIONS FOR IDENTIFYING PERSONNEL SECURITY INVESTIGATION REQUIREMENTS FOR AF POSITIONS

A22.1. Guide for Identifying Investigative Requirements for Position Coding. Use the following table for guidance on identifying investigative requirements for each authorized manpower position. See **Chapter 7** for additional guidance on coding of investigations.

Table A22.1. Personnel Security Investigation Position Coding

Position Code	Investigation Type	Investigation Description

Position Code	Investigation Type	Investigation Description
5	SSBI	The SSBI is the initial investigation for access to Top Secret (including Top Secret Special Access Programs (SAP), SCI, and for Critical Sensitive Positions.) In addition, the SSBI is required for Mandatory AFSCs or Program Mandates.
6	NACLC	The NACLC is the prescribed investigation for initial and continued access to Secret and Confidential information for DoD military and contractor personnel. It is also the reinvestigation requirement for federal employees at the same access levels. Also, all military or Mandatory Program Mandate.
7	ANACI	The ANACI is the investigative requirement for federal employees under Executive Order 10450, "Suitability for Government Hire," in non-critical sensitive positions that require access to classified information up to the Secret level. Access to Secret (civilian) or Mandatory Program Mandate.
8	NACI	The NACI is the baseline investigative requirement for entry into government service under Executive Order 10450 and for federal employees in nonsensitive positions that do not require access to classified information. All OPM NACIs conducted for DoD include a credit check (NACIC). Suitability Requirement (civilian).
9	NAC	The NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making personnel security determinations. A NAC is also an integral part of all initial and periodic reinvestigations and is the baseline for trustworthiness determinations. Trustworthiness Positions (Non Appropriated Fund/Contractor/Consultant).

A22.2. Mandatory SSBI Requirement List for Officer AFSCs. The following is the Officer Mandatory SSBI list. The appropriate position coding is reflected in the Headquarters Air Force Manpower Data System (HAF-MDS).

AFSC AFSC DESCRIPTION

10C Operations Commander

11B Bomber Pilot

11F Fighter Pilot

11G Generalist Pilot

11R Reconnaissance/Surveillance/Electronic Warfare Pilot

11S Special Operations Pilot

11T Tanker Pilot

12B Bomber Navigator

12F Fighter Navigator

12G Generalist Navigator

12R Reconnaissance/Surveillance/Electronic Warfare Navigator

12S Special Operations Navigator

12T Tanker Navigator

13B Air Battle Manager

13D Control And Recovery

13S Space And Missile Operations

14N Intelligence

15W Weather

16F Foreign Area

16G Air Force Operations Staff Officer

16R Planning And Programming

20C Logistics Commander

21M Munitions and Maintenance

21B Maintenance

33C Communications Commander

60C Program Director

65A Audit

71S Special Investigations

84H Historian

85G United States Air Force Honor Guard

86P Command And Control

88A Aide-De-Camp

90G General Officer

91W Wing Commander

92T0 Pilot Trainee

92T1 Navigator Trainee

97E Executive Officer Above Wing Level

A22.3. Mandatory SSBI Requirement List for Enlisted AFSCs. The appropriate position coding is reflected in the Headquarters Air Force Manpower Data System (HAF-MDS).

AFSC AFSC DESCRIPTION

1A0 In-Flight Refueling

1A3 Airborne Communications Systems

1A6 Flight Attendant

1A8 Airborne Cryptologic Linguist

1C3 Command Post

1N0 Intelligence Applications

1N1 Imagery Analysis

1N2 Signals Intelligence Production

1N3 Cryptologic Linguist

1N4 Signals Intelligence Analysis

1N5 Electronic Signals Intelligence Exploitation

1N6 Electronic System Security Assessment

2E2 Computer, Network, Switching And Cryptographic Systems

2MO Missile and Space Systems Maintenance (Excluding 2M0X3)

2W2 Nuclear Weapons

3C0 Communications - Computer Systems Operations

3C2 Communications - Computer Systems Control

3H0 Historian

3N2 Premier Band

7S0 Special Investigations

8E0 Research And Development Technician

8P0 Courier

8P1 Defense Attaché

9C0 Chief Master Sergeant of the Air Force

9S1 Technical Applications Specialist

A22.4. Mandatory SSBI Sensitive Program Requirements. The following table outlines mandatory SSBI requirements for selected positions/programs.

Table A22.4. Mandatory SSBI Sensitive Programs Requirements.

Positions/Programs
Top Secret Access
IT-I
Presidential Support Category 1 and 2 duties
Personnel Reliability Program Critical duties
Sensitive Compartmented Information required

Positions/Programs
Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) Access
Top Secret Special Access Program (SAP) Access Mandate
DoD or Agency External to AF Top Secret Access Mandate
Civilian Critical Sensitive Positions (which includes: access to TS; development or approval of war plans, future major or special operations of war; critical and extremely important of war; or other positions related to national security, regardless of duties, that requires the same degree of trust)
Initial assignment - Explosive Ordnance Disposal involving Nuclear Weapons positions
Defense Courier Service duties
Access to NATO COSMIC Top Secret
AFOSI investigative agents and investigative support staff, the issuance of personnel security clearances or access authorizations, rendering of personnel security determinations, or duty on personnel security boards

A22.5. Mandatory Positions/Programs Requiring Investigation (Other Than SSBIs). The following table outlines mandatory NACLC, ANACI, NACI, NAC investigation requirements for selected positions/programs.

Table A22.5. Mandatory Positions/Programs Requiring Investigations by Type (Other Than SSBIs).

Positions/Programs	Investigation Type				
	Military	Civilian		Contractor Or Consultant	Volunteer/ Child Care Provider
	NACLC	ANACI	NACI	NAC	NAC
Access to Secret Information	X	X			
Military Accessions	X				
Commissioned Officers	X				
Civilian Non-Critical Sensitive Positions		X			
Presidential Support Program Category 3	X	X			
Personnel Reliability Program Controlled Position	X	X			
Customs Inspectors	X	X			
Secret SAP Access Mandate	X	X			
Information Technology (IT)-II	X		X		

Positions/Programs	**Investigation Type**				
	Military	**Civilian**		**Contractor Or Consultant**	**Volunteer/ Child Care Provider**
	NACLC	**ANACI**	**NACI**	**NAC**	**NAC**
IT-III*	X		X	X	X
Access to NATO Secret/Confidential	X	X			
Access to Chemical Agents	X	X			
Arms, Ammunition & Explosives (AA&E) Duties	X	X			
Deployment Purposes	X				
Suitability Requirement			X		X
Trustworthiness				X	
Federal Employment			X		

*IT-III for military only requires a NAC, however, all AF military receive a NACLC which is above a NAC.

Attachment 24

SMITH AMENDMENT

A24.1. Implementation of the Section 1071 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, which amended Title 10, United States Code, to add a new section that precludes the initial granting or renewal of a security clearance by the DoD under four specific circumstances as outlined below.

A24.1.1. Provision (1) disqualifies persons with convictions in both State and Federal courts, including UCMJ offenses, with sentences imposed of more than one year, regardless of the amount of time actually served.

A24.1.2. Provision (2) does not change the substance of the existing adjudication guideline relative to current drug involvement. Anyone who is currently an unlawful user of, or addicted to, a controlled substance.

A24.1.3. Provision (3) does not change the substance of the adjudication guidelines for emotional, mental, or personality disorders. Anyone who is found to be mentally incompetent (incapable of safeguarding classified information) by a credentialed mental health professional approved by DoD.

A24.1.4. Provision (4) disqualifies persons who have been discharged or dismissed from the Armed Forces under dishonorable conditions.

A24.2. Secretary of the Air Force may authorize a waiver in meritorious cases under provisions (1) & (4). Waiver authority is not delegable.

A24.3. Provision (2) & (3) disqualifies a person for eligibility for a security clearance and may not be waived.

A24.4. Individuals that fall under the categories (1) through (4) will be afforded applicable due process and appeal opportunity IAW the DoD 5200.2-R, Personnel Security Program and this instruction.

A24.5. When AFCAF issues a final statement of reasons to deny or revoke a security clearance in cases where a waiver is allowed (provisions 1 and 4) the subject will be informed of the waiver provision, provided a copy of the statute and other information on how to respond. The subject must include in the response to the statement of reasons if they want to be considered for a waiver, if applicable.

A24.6. Decision process for determining whether a particular case warrents a meritorious waiver:

A24.6.1. The AFCAF is the first level nominating office and determines if the case warrants a meritorious waiver under the provisions of the statute. If approved, the case is forwarded with the proposed request for waiver and full justification to the Air Force Personnel Security Appeal Board (PSAB) for review.

A24.6.2. If the PSAB determines the case has meritorious justification, the case summary is returned to the AFCAF for forwarding to SAF/AA.

A24.6.2.1. SAF/AA may disapprove the waiver request or forward it to the SECAF with recommendation for approval. Both the SAF/AA and SECAF decisions are final.

A24.7. AFCAF will provide quarterly summaries to SAF/AA by the10th of each month following the end of each calendar quarter of all waivers submitted to SECAF. SAF/AA provides report to USD/I by the 15$^{th.}$

A24.8. The statute policy applies to:

A24.8.1. All initial determinations to grant security clearance eligibility or access and determinations to continue clearance eligibility/accesses following a reinvestigation;

A24.8.2. Existing clearances eligibility or access which a previous or other investigation reveals a previous favorably resolved issue involving one or more of the four statutory provisions, regardless of the presence or absence of subsequent disqualifying issues;

A24.8.3. Previous and follow-on periodic reinvestigations and other investigations initiated for other reasons; such as:

A24.8.3.1. Security Information File, Special Investigation Inquiry, etc., and all pending cases in which a final decision had not been issued as of 7 Jun 01.

A24.9. The statue polices do not apply to:

A24.9.1. Conversions/transfers/reinstatements of current DoD security clearances, including transfers of clearances of employees within the DoD, clearances of employees who fall under the National Industrial Security Program, and transfers of clearances to the DoD of employees coming from other Federal agencies.

Attachment 25

TABLE FOR INTERIM SECURITY CLEARANCE/ACCESS AUTHORITY

A25.1. Authority to Grant Interim Security Clearance/Access. Use the following table for guidance on authority level to grant interim security clearance/access to specific programs. Items

contained in Column E, 3a-d & 4 may be found at: **https://wwwmil.lackland.af.mil/afsf/**. Copy and paste into the browser. Once at the home page, click on "HQ USAF Security Forces," click "Information Security Division," scroll down to "Personnel Security Policy Updates." The references are listed under Personnel Security Policy Updates.

Table A25.1. Authority to Grant Interim Security Clearance/Access.

	A	B	C	D	E
RULE	**If the requirement is for**	**The investigation requirements are**	**The access level is**	**The authorization level is**	**As governed by**
1	**Interim Secret** (see note 1)	- Local files check - Favorable Review of SF 86 - NACLC/ANACI submitted	Secret	Unit Commander	AFI 31-501, Personnel Security Program Management
2	**Interim Top Secret** (see note 1)	- Local files check - Favorable review of SF 86 - SSBI submitted - Favorable NAC, ENTNAC, NACI, NACIC, NACLC, ANACI	Top Secret	Unit Commander	AFI 31-501, Personnel Security Program Management
3	**Interim PRP** (see note 1)				
	(a) Initial PRP Interim Certification for Controlled Position	- NACLC submitted - Favorable PRP interview	PRP Controlled Position	PRP Certifying Official	AF/XOFI Memo, 17 Dec 03, Extension of Temporary PRP Procedures
	(b) Initial PRP Interim Certification for Critical Position	- SSBI submitted - Favorable PRP interview	PRP Critical Position	PRP Certifying Official	AF/XOFI Memo, 17 Dec 03, Extension of Temporary PRP Procedures
	(c) Formally Certified for Controlled Position When Investigation is Over 5 Years Old	- NACLC-PR submitted - Favorable PRP interview	PRP Controlled Position	PRP Certifying Official	AF/XOFI Memo, 29 Apr 04, Extension of the Relief to DoD 5210.42, Nuclear Weapons PRP, Para C31

	A	B	C	D	E
RULE	**If the requirement is for**	**The investigation requirements are**	**The access level is**	**The authorization level is**	**As governed by**
	(d) Formally Certified for Critical Position When Investigation is Over 5 Years Old	- SSBI-PR submitted - Favorable PRP interview	PRP Critical Position	PRP Certifying Official	AF/XOFI Memo, 29 Apr 04, Extension of the Relief to DoD 5210.42, Nuclear Weapons PRP, Para C31
4	**Interim Crypto Access** for Access to Missile Entry Control System (see note 1)	- Interim Secret clearance granted	Secret for Crypto Equipment	Unit Commander	AF/AF AF/XOFI Memo, 18 Dec 03, Request Extension for Authorization for Interim Secret Clearance for COMSEC
5	**Interim SCI** (see note 1)	- Interim Top Secret clearance granted - Favorable SCI screening interview	SCI	Special Security Office obtains AFCAF approval then SSO conducts SCI indoctrination	AFMAN 14-304, The Security, Use and Dissemination of SCI

NOTES:

1. Rule 1 or 2 must be in place accordingly before application of rules 3-5.

DEPARTMENT OF DEFENSE

PERSONNEL SECURITY PROGRAM

JANUARY 1987

ADMINISTRATIVE REISSUANCE INCORPORATING
THROUGH CHANGE 3, FEBRUARY 23, 1996

OFFICE OF THE DEPUTY UNDER SECRETARY OF DEFENSE
(POLICY)

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

POLICY

December 16, 1986

FOREWORD

This "Personnel Security Program Regulation" is reissued under the authority of DoD Directive 5200.2, "DoD Personnel Security Program," December 20, 1979. It contains expanded direction and procedures for implementing those references cited in Chapter 1 and in Appendix A of this Regulation that pertain to acceptance and retention of DoD military, civilian, consultant and contractor personnel and of granting such persons access to classified information or assignment to a sensitive position. It also implements such recommendations from the Defense Security Review Commission Report as pertains to personnel security and approved by the Secretary of Defense.

DoD 5200.2-R, "Department of Defense Personnel Security Program," December 1979, is hereby canceled as of December 31, 1986. The effective date of this Regulation is January 1, 1987.

The provisions of this Regulation apply to the Office of the Secretary of Defense (OSD) and activities supported administratively by OSD, the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies.

This Regulation is mandatory for use by all DoD Components. Heads of DoD Components may issue supplementary instructions when necessary to provide for internal administration of this Regulation within their respective components.

Forward communications, including recommended changes, regarding this Regulation and copies of supplemental instructions issued, through appropriate channels to: Deputy Under Secretary of Defense for Policy, Attention: Director Counterintelligence and Investigative Programs, Room 3C-267, The Pentagon, Washington, D.C. 20301-2200.

This Regulation is being published in Title 32, Code of Federal Regulations (CFR). DoD Components may obtain copies of this Regulation through their own publications channels. Federal Agencies and the public may obtain copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

Craig Alderman, Jr.
Deputy

TABLE OF CONTENTS

REFERENCES

(a) DoD 5200.2-R, "DoD Personnel Security Program," January 1987, authorized by DoD Directive 5200.2, May 6, 1992

(b) DoD 5220.22-R, "Industrial Security Regulation," authorized by DoD Directive 5220.22, December 8, 1980

(c) DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," February 2, 1992

(d) Reference Not Used

(e) Public Law 88-290, "National Security Agency - Personnel Security Procedures," March 26, 1964 (78 STAT. 168)

(f) Public Law 86-36, "National Security Agency Officers and Employees," May 29, 1959 (73 Stat. 63)

(g) Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953

(h) Executive Order 12333, "United States Intelligence Activities," December 4, 1981

(i) DoD Directive 5210.45, "Personnel Security in the National Security Agency," May 9,1964

(j) Executive Order 1295.8, "Classified National Security Information," April 17,1995

(k) Executive Order 11935, "Citizenship Requirements for Federal Employment," September 2, 1976

(l) Director of Central Intelligence Directive (DCID) No. 1/14, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," January 22, 1992

(m) Section 552a of title 5, United States Code

(n) DoD Directive 5100.23, "Administrative Arrangements for the National Security Agency, May 17, 1967

(o) Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979

(p) DoD Directive 5210.48, "DoD Polygraph Program," December 24, 1984

(q) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982

(r) DoD Directive 5210.55, "Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities," July 6, 1977

(s) DoD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program (PRP)," May 25, 1993

(t) DoD Directive 5200.8, "Security of Military Installations and Resources," April 25,1991

(u) DoD 1401.1-M, "Personnel Policy Manual for Nonappropriated Fund Instrumentalities," January 1981, authorized by DoD Instruction 1401.1, November 15, 1985

(v) DoD 5030.49-R, "Customs Inspection," May 1977, authorized by DoD Directive 5030.49, January 6, 1984

(w) DoD Instruction 5210.25, "Assignment of American National Red Cross and United Service Organizations, Inc., Employees to Duty with the Military Services," May 12, 1983

(x) DoD Directive 5210.46, "DoD Building Security for the National Capital Region," January 28, 1982

(y) DoD Directive 5210.65, "Chemical Agent Security Program," October 15, 1986

(z) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978

(aa) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988

(bb) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982

(cc) 5 CFR, Part 732, "National Security Positions," January 1, 1995

(dd) Section 3571 of title 5, United States Code

(ee) Section 3 of Public Law 89-380, "Back Pay Act of 1966," March 30, 1966 (80 Stat. 94)

(ff) Executive Order 9835, "Prescribing Procedures for the Administration of an Employee Loyalty Program in the Executive Branch of the Government," issued 1947 (superseded by Executive Order 10450)

(gg) Public Law 83-703, "Atomic Energy Actof 1954," as amended, August 30, 1954

(hh) DoD Directive 5105.42, "Defense Investigative Service," June 14, 1985

(ii) Defense Investigative Service 20-1-M, "Manual for Personnel Security Investigations," January 1993

(jj) Memorandum of Understanding between the Director, White House Military Office and the Special Assistant to the Secretary and Deputy Secretary of Defense, "White House Clearances," July 30, 1980

(kk) USSAN Instruction 1-69, April 21, 1982 (Enclosure 2 to DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs," April 21, 1982

(ll) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1982

(mm) DoD Directive 5100.3, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands," November 1, 1988

(nn) Public Law 96-456, "Classified Information Procedures Act," October 15, 1980 (94 Stat. 2025)

(oo) DoD Directive 5142.1, "Assistant Secretary of Defense (Legislative Affairs)," July 2, 1982

(pp) Section 7532 of title 5, United States Code

(qq) DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 4, 1989

(rr) National Security Directive 63, "Single Scope Background Investigations," October 21, 1991

DL1. DEFINITIONS

DL1.1.1. Access. The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified informaiton by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.

DL1.1.2. Adverse Action. A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

DL1.1.3. Background Investigation (BI). A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in paragraph AP1.1.1.3., Appendix 1, this Regulation, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

DL1.1.4. Classified Informaiton. Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order 12356 (reference (j)).

DL1.1.5. Defense Central Security Index (DCSI). An automated sub-system of the Defense Central Index of Investigations (DCII) designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all DoD Components for military, civilian, and contractor personnel. The DCSI will serve as the central DoD repository of security related actions in order to assist DoD security officials in making sound clearance and access determinations. The DCSI shall also serve to provide accurate and reliable statistical data for senior DoD officials, Congressional committees, the General Accounting Office and other authorized Federal requesters.

DL1.1.6. DoD Component. Includes the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, The DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

DL1.1.7. Entrance National Agency Check (ENTNAC). A personnel security

investigation scoped and conducted in the same manner as a National Agency Check (NAC) except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

DL1.1.8. Head of DoD Component. The Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; and the Commanders of the Combatant Commands; and the Directors of Defense Agencies.

DL1.1.9. Immigrant Alien. Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

DL1.1.10. Interim Security Clearance. A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

DL1.1.11. Limited Access Authorization. Authorization for access to Confidential or Secret information granted to non-United States citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (paragraph AP1.1.1.3., Appendix 1).

DL1.1.12. Minor Derogatory Information. Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

DL1.1.13. National Agency Check (NAC). A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph AP1.1.1.1., Appendix 1, this Regulation, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

DL1.1.14. National Agency Check Plus Written Inquiries (NACI). A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

DL1.1.15. DoD National Agency Check Plus Written Inquiries (DNACI). A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to SECRET information consisting of a NAC, credit bureau check, and written inquiries to current and former employers (see paragraph AP1.1.1.2., Appendix 1), covering a 5-year scope.

DL1.1.16. National Security. National security means the national defense and foreign relations of the United States.

DL1.1.17. Need-to-Know A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

DL1.1.18. Periodic Reinvestigation (PR). An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation on persons occupying positions referred to in paragraphs C3.7. through C3.7.10. The scope will consist of a personal interview, NAC, LACs, credit bureau checks, employment records, employment references and developed character references and will normally not exceed the most recent 5-year period.

DL1.1.19. Personnel Security Investigation (PSI). Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see paragraph C2.4.3.) conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

DL1.1.20. Scope The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

DL1.1.21. Security Clearance. A determination that a person is eligible under the

standards of this Regulation for access to classified information.

DL1.1.22. Senior Officer of the Intelligence Community (SOIC). The DoD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service; Director, Defense Intelligence Agency; Assistant Chief of Staff for Intelligence, U.S. Army; Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

DL1.1.23. Sensitive Position. Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical-sensitive, noncritical-sensitive, or nonsensitive as described in paragraph C3.1.1.

DL1.1.24. Significant Derogatory Information. Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

DL1.1.25. Special Access Program. Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of persons determined to have a need-to-know.

DL1.1.26. Special Background Investigation (SBI). A personnel security investigation consisting of all of the components of a BI plus certain additional investigative requirements as prescribed in paragraph AP1.1.1.4., Appendix 1, this Regulation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

DL1.1.27. Special Investigative Inquiry (SII). A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination under the provision of this Regulation.

DL1.1.28. Service. Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a DoD contractor or as a consultant involving access under the DoD Industrial Security Program. Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months.

DL1.1.29. Unfavorable Administrative Action. Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this Regulation.

DL1.1.30. Unfavorable Personnel Security Determination. A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to SCI); nonappointment to or nonselection for appointment to a sensitive position; nonappointment to or nonselection for any other position requiring a trustworthiness determination under this Regulation; reassignment to a position of lesser sensitivity or to a nonsensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

DL1.1.31. United States Citizen. (Native Born) - A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or the Republic of Panama (former Panama Canal Zone) (if the father or mother (or both) was or is, a citizen of the United States).

C1. CHAPTER 1

DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM GENERAL PROVISIONS

C1.1. PURPOSE AND APPLICABILITY

C1.1. Purpose

C1.1.1. To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense, and granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security.

C1.1.2. This Regulation:

C1.1.2.1. Establishes DoD personnel security policies and procedures;

C1.1.2.2. Sets forth the standards, critera, and guidelines upon which personnel security determinations shall be based;

C1.1.2.3. Prescribes the kinds and scopes of personnel security investigations required;

C1.1.2.4. Details the evaluation and adverse action procedures by which personnel security determinations shall be made; and

C1.1.2.5. Assigns overall program management responsibilities.

C1.2. Applicability

C1.2.1. This Regulation implements the Department of Defense Personnel Security Program and takes precedence over all other departmental issuances affecting that program.

C1.2.2. All provisions of this Regulation apply to DoD civilian personnel, members of the Armed Forces, excluding the Coast Guard in peacetime, contractor personnel and other personnel who are affiliated with the Department of Defense except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DoD 5220.22-R

(reference (b)) and in DoD Directive 5220.6 (reference (c)).

C1.2.3. The policies and procedures THAT govern the National Security Agency are prescribed by Public Laws 88-290 and 86-36, Executive Orders 10450 and 12333, DoD Directive 5210.45, Director of Central Intelligence Directive (DCID) 1/14 (references (e), (f), (g), (h), (i), and (l) respectively), and regulations of the National Security Agency.

C1.2.4. Under combat conditions or other military exigencies, an authority in paragraph AP6.1., Appendix 6, may waive such-provisions of this regulation as the circumstances warrant.

C2. CHAPTER 2

POLICIES

C2.1. STANDARDS FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES

C2.1.1. General. Only United States citizens shall be granted a personnel security clearance, assigned to sensitive duties, or granted access to classified information unless an authority designated in Appendix 6 has determined that, based on all available information, there are compelling reasons in furtherance of the Department of Defense mission, including, special expertise, to assign an individual who is not a citizen to sensitive duties or grant a Limited Access Authorization to classified information. Non-U.S. citizens may be employed in the competitive service in sensitive civilian positions only when specifically approved by the Office of Personnel Management, pursuant to E.O. 11935 (reference (k)). Exceptions to these requirements shall be permitted only for compelling national security reasons.

C2.1.2. Clearance and Sensitive Position Standard. The personnel security standard that must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

C2.1.3. Military Service Standard. The personnel security standard that must be applied in determining whether a person is suitable under national security criteria for appointment, enlistment, induction, or retention in the Armed Forces is that, based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States.

C2.2. CRITERIA FOR APPLICATION OF SECURITY STANDARDS

C2.2.1. Criteria for Application of Security Standards. The ultimate decision in applying either of the security standards set forth in paragraph C2.1.2. and C2.1.3., above, must be an overall common sense determination based upon all available facts. The criteria for determining eligibility for a clearance under the security standard shall include, but not be limited to the following:

C2.2.1.1. Commission of any act of sabotage, espionage, treason, terrorism,

anarchy, sedition, or attempts thereat or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

C2.2.1.2. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

C2.2.1.3. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

C2.2.1.4. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations), which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

C2.2.1.5. Unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by Statute, Executive Order or Regulation.

C2.2.1.6. Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner which serve or which could be expected to serve the interests of another government in reference to the interests of the United States.

C2.2.1.7. Disregard of public law, Statutes, Executive Orders or Regulations including violation of security regulations or practices.

C2.2.1.8. Criminal or dishonest conduct.

C2.2.1.9. Acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness.

C2.2.1.10. Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case.

C2.2.1.11. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be:

C2.2.1.11.1. The presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States; or

C2.2.1.11.2. Any other circumstances that could cause the applicant to be vulnerable.

C2.2.1.12. Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

C2.2.1.13. Habitual or episodic use of intoxicants to excess.

C2.2.1.14. Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug.

C2.2.1.15. Any knowing and willful falsification, cover up, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the Department of Defense or any other Federal Agency.

C2.2.1.16. Failing or refusing to answer or-to-authorize others to answer questions or provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment.

C2.2.1.17. Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society.

C2.3. TYPES AND SCOPE OF PERSONNEL SECURITY INVESTIGATIONS

C2.3.1. General. The types of personnel security investigations authorized below vary in scope of investigative effort required to meet the purpose of the particular investigation. No other types are authorized. The scope of a PSI may be neither raised nor lowered without the approval of the Deputy Under Secretary of Defense for Policy.

C2.3.2. National Agency Check (NAC) Essentially, a NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making a personnel security determination. An ENTNAC is a NAC (scope as outlined in paragraph AP1.1.1., Appendix 1) conducted on inductees and first-term enlistees, but lacking a technical fingerprint search. A NAC is also an integral part of each BI, SBI, and Periodic Reinvestigation (PR). Chapter 3 prescribes when a NAC is required.

C2.3.3. National Agency Check plus Written Inquiries. The Office of Personnel Management (OPM) conducts a NAC plus Written Inquiries (NACIs) on civilian employees for all Departments and Agencies of the Federal Government, pursuant to E.O. 10450 (reference (g)). NACIs are considered to meet the investigative requirements of this Regulation for a nonsensitive or noncritical sensitive position and/or up to a SECRET clearance and, in addition to the NAC, include coverage of law enforcement agencies, former employers and supervisors, references, and schools covering the last 5 years.

C2.3.4. DoD National Agency Check (DNCI) Plus Written Inquiries. DIS will conduct a DNACI, consisting of the scope contained in paragraph AP1.1.1.1.2., Appendix 1, for DoD military and contractor personnel for access to SECRET information. Chapter 3 prescribes when a DNACI is required.

C2.3.5. Background Investigation (BI). The BI is the principal type of investigation conducted when an individual requires TOP SECRET clearance or is to be assigned to a critical sensitive position. The BI normally covers a 5-year period and consists of a subject interview, NAC, LACs, credit checks, developed character references (3), employment records checks, employment references (3), and select scoping as required to resolve unfavorable or questionable information. (See paragraph AP1.1.1.1.3., Appendix 1). Chapter 3 prescribes when a BI is required.

C2.3.6. Special Background Investigation (SBI)

C2.3.6.1. An SBI is essentially a BI providing additional coverage both in

period of time as well as sources of information, scoped in accordance with the provisions of DCID 1/14 (reference (l)) but without the personal interview. While the kind of coverage provided for by the SBI determines eligibility for access to SCI, the Department of Defense has adopted this coverage for certain other Special Access programs. Chapter 3 prescribes when an SBI is required.

C2.3.6.2. The OPM, FBI, Central Intelligence Agency (CIA), Secret Service, and the Department of State conduct specially scoped BIs under the provisions of DCID 1/14. Any investigation conducted by one of the above-cited Agencies under DCID 1/14 standards is considered to meet the SBI investigative requirements of this Regulation.

C2.3.6.3. The detailed scope of an SBI is set forth in paragraph AP1.1.1.1.4., Appendix 1.

C2.3.7. Special Investigative Inquiry (SII)

C2.3.7.1. A Special Investigative Inquiry is a personnel security investigation conducted to prove or disprove allegations relating to the criteria outlined in paragraph C2.2.1. of this Regulation, except current criminal activities (see paragraph C2.4.3.4.), that have arisen concerning an individual upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a trustworthiness determination.

C2.3.7.2. Special Investigative Inquiries are scoped as necessary to address the specific matters requiring resolution in the case concerned and generally consist of record checks and/or interviews with potentially knowledgeable persons. An SII may include an interview with the subject of the investigation when necessary to resolve conflicting information and/or to provide an opportunity to refute or mitigate adverse information.

C2.3.7.3. In those cases when there is a disagreement between Defense Investigative Service (DIS) and the requester as to the appropriate scope of the investigation, the matter may be referred to the Deputy Under Secretary of Defense for Policy for resolution.

C2.3.8. Periodic Reinvestigation (PR). As referred to in paragraph C3.7.1. and other national directives, certain categories of duties, clearance, and access require the conduct of a PR every five years according to the scope outlined in paragraph AP1.1.1.1.5., Appendix 1. The PR scope applies to military, civilian, contractor, and foreign national personnel.

C2.3.9. Personal Interview. Investigative experience over the years has demonstrated that, given normal circumstances, the subject of a personnel security investigation is the best source of accurate and relevant information concerning the matters under consideration. Further, restrictions imposed by the Privacy Act of 1974 (reference (m)) dictate that Federal investigative agencies collect information to the greatest extent practicable directly from the subject when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. Accordingly, personal interviews are an integral part of the DoD personnel security program and shall be conducted in accordance with the requirements set forth in the following paragraphs of this section.

C2.3.9.1. BI/PR. A personal interview shall be conducted by a trained DIS agent as part of each BI and PR.

C2.3.9.2. Resolving Adverse Information. A personal interview of the subject shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations), when necessary, as part of each Special Investigative Inquiry, as well as during the course of initial or expanded investigations, to resolve or clarify any information which may impugn the subject's moral character, threaten the subject's future federal employment, raise the question of subject's security clearability, or be otherwise stigmatizing.

C2.3.9.3. Hostage Situation. A personal interview shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations) in those instances in which an individual has immediate family members or other persons bound by ties of affection or obligation who reside in a nation whose interests are inimical to the interests of the United States. (See paragraph C2.4.4.)

C2.3.9.4. Applicants/Potential Nominees for DoD Military or Civilian Positions Requiring Access to SCI or Other Positions Requiring SBI. A personal interview of the individual concerned shall be conducted, to the extent feasible, as part of the selection process for applicants/potential nominees for positions requiring access to SCI or completion of an SBI. The interview shall be conducted by a designee of the Component to which the applicant or potential nominee is assigned. Clerical personnel are not authorized to conduct these interviews. Such interviews shall be conducted utilizing-resources in the order of priority indicated below:

C2.3.9.4.1. Existing personnel security screening systems (e.g., Air Force

Assessment Screening Program, Naval Security Group Personnel Security Interview Program, U.S. Army Personnel Security Screening Program); or

C2.3.9.4.2. Commander of the nominating organization or such official as he or she has designated in writing (e.g., Deputy Commander, Executive Officer, Security Officer, Security Manager, S-2, Counterintelligence Specialist, Personnel Security Specialist, or Personnel Officer); or

C2.3.9.4.3. Agents of investigative agencies in direct support of the DoD Component concerned.

C2.3.9.5. Administrative Procedures

C2.3.9.5.1. The personal interview required by paragraph C2.3.9.4., above, shall be conducted in accordance with Appendix 6.

C2.3.9.5.2. For those investigations requested subsequent to the personal interview requirements of paragraph C2.3.9.4., above, the following procedures apply:

C2.3.9.5.2.1. The DD Form 1879 (Request for Personnel Security Investigation) shall be annotated under Item 20 (Remarks) with the statement, "Personal Interview Conducted by (cite the duty assignment of the designated official (e.g., Commander, Security Officer, Personnel Security Specialist, etc.))" in all cases in which an SBI is subsequently requested.

C2.3.9.5.2.2. Unfavorable information developed through the personal interview required by paragraph C2.3.9.4., above, will be detailed in a written report attached to the DD Form 1879 to include full identification of the interviewer. Failure to provide such information may result in conduct of an incomplete investigation by DIS.

C2.3.9.5.2.3. Whenever it is determined that it is not feasible to conduct the personal interview required by paragraph C2.3.9.4., above, prior to requesting the SBI, the DD Form 1879 shall be annotated under Item 20 citing the reason for not conducting the interview.

C2.3.10. Expanded Investigation. If adverse or questionable information relevant to a security determination is developed during the conduct of a personnel security investigation, regardless of type, the investigation shall be expanded, consistent with the restrictions in paragraph C2.5.5., to the extent necessary to substantiate or disprove the adverse or questionable information.

C2.4. AUTHORIZED PERSONNEL SECURITY INVESTIGATIVE AGENCIES

C2.4.1. Genera. The DIS provides a single centrally directed personnel security investigative service to conduct personnel security investigations within the 50 States, District of Columbia, and Commonwealth of Puerto Rico for DoD Components, except as provided for in DoD Directive 5100.23 (reference (n)). DIS will request the Military Departments or other appropriate Federal Agencies to accomplish DoD investigative requirements in other geographic areas beyond their jurisdiction. No other DoD Component shall conduct personnel security investigations unless specifically authorized by the Deputy Assistant Secretary of Defense (Intelligence and Security). In certain instances provided for below, the DIS shall refer an investigation to other investigative agencies.

C2.4.2. Subversive Affiliations

C2.4.2.1. General. In the context of DoD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. Specifically, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:

C2.4.2.1.1. Overthrowing the Government of the United States or the government of a State;

C2.4.2.1.2. Substantially impairing for the purpose of influencing U.S. Government policies or decisions:

C2.4.2.1.2.1. The functions of the Government of the United States, or

C2.4.2.1.2.2. The functions of the government of a State;

C2.4.2.1.2.3. Depriving persons of their civil rights under the Constitution or laws of the United States.

C2.4.2.2. Military Department/FBI Jurisdiction. Allegations of activities covered by criteria C2.2.1.1. through C2.2.1.6. of paragraph C2.2.1. of this Regulation are in the exclusive investigative domain of either the counterintelligence agencies of the Military Departments or the FBI, depending on the circumstances of the case and the provisions of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the FBI (reference (o)). Whenever

allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a personnel security investigation conducted by DIS, they shall be referred immediately to either the FBI or to a Military Department counterintelligence agency as appropriate.

C2.4.2.3. DIS Jurisdiction. Allegations of activities limited to those set forth in criterion C2.2.1.7. through C2.2.1.17. of paragraph C2.2.1. of this Regulation shall be investigated by DIS.

C2.4.3. Suitability Information

C2.4.3.1. General. Most derogatory information developed through personnel security investigations of DoD military or civilian personnel is so-called suitability information, that is, information pertaining to activities or situations covered by criteria C2.2.1.7. through C2.2.1.17. of paragraph C2.2.1. of this Regulation. Almost all unfavorable personnel security determinations made by DoD authorities are based on derogatory suitability information, although such information is often used as a basis for unfavorable administrative actions not of a security nature, such as action under the Uniform Code of Military Justice or removal from Federal employment under OPM regulations.

C2.4.3.2. Pre-Clearance Investigation. Derogatory suitability information, except that covered in C2.4.3.4., below, developed during the course of a personnel security investigation, prior to the issuance of an individual's personnel security clearance, shall be investigated by DIS to the extent necessary to confirm or refute its applicability to criteria C2.2.1.7. through C2.2.1.17. of paragraph C2.2.1.

C2.4.3.3. Postjudicative Investigation. Derogatory suitability allegations, except those covered by C2.4.3.4., below, arising subsequent to clearance requiring investigation to resolve and to determine the individual's eligibility for continued access to classified information, reinstatement of clearance/access, or retention in a sensitive position shall be referred to DIS to conduct a Special Investigative Inquiry. Reinvestigation of individuals for adjudicative reconsideration due to the passage of time or evidence of favorable behavior shall also be referred to DIS for investigation. In such cases, completion of the appropriate statement of personal history by the individual constitutes consent to be investigated. Individual consent or completion of a statement of personal history is not required when paragraph C3.7.2. applies. Post adjudication investigation of allegations of a suitability nature required to support other types of unfavorable personnel security determinations or disciplinary procedures independent of a personnel security determination shall be handled in accordance with applicable Component administrative regulations. These latter categories of allegations

lie outside the DoD personnel security program and are not a proper investigative function for departmental counterintelligence organizations, Component personnel security authorities, or DIS.

C2.4.3.4. Allegations of Criminal Activity. Allegations of possible criminal conduct arising during a personnel security investigation shall be referred to the appropriate Department of Defense criminal investigative agency, Military Department or civilian jurisdiction unless the limitations in paragraph C2.4.3.4.1. through C2.4.3.4.3., below, apply. Where the allegation concerns a potential violation of the Uniform Code of Military Justice, Military Department investigative agencies have primary investigative jurisdiction. The following limitations apply to referrals to all law enforcement agencies, both military and civilian.

C2.4.3.4.1. Allegations shall not be referred or reported to law enforcement agencies where agreements with the agency or in cases where there is no agreement, past experience indicates that the jurisdiction does not have a substantial interest in prosecution of the offense or in receiving reports of the offense either due to the type or offense involved or the circumstances under which it occurred.

C2.4.3.4.2. Allegations about private consensual sexual acts with adults shall not be referred or reported to law enforcement agencies or to Military Departments (other than consolidated adjudication facilities) for any purpose. That limitation does not apply to allegations that an individual attempted, solicited, or committed a criminal offense in the following circumstances:

C2.4.3.4.2.1. By using force, coercion, or intimidation.

C2.4.3.4.2.2. With a person under 17 years of age.

C2.4.3.4.2.3. Openly in public view.

C2.4.3.4.2.4. For compensation or with an offer of compensation to another individual.

C2.4.3.4.2.5. While on active duty in, or on duty in a Reserve component of, the Armed Forces of the United States, and

C2.4.3.4.2.5.1. Aboard a military vessel or aircraft; or

C2.4.3.4.2.5.2. With a subordinate in circumstances that violate customary military superior-subordinate relationships.

Exceptions to that limitation will be made only with the specific written authorization of the General Counsel of the Department of Defense, or his or her designee.

C2.4.3.4.3. Information about an individual's sexual orientation or statements by an individual that he or she is a homosexual or bisexual, or words to that effect, shall not be referred or reported to law enforcement agencies or to Military Departments (other than consolidated adjudication facilities) for any purpose. If investigative reports containing such information are referred to law enforcement agencies or Military Departments for other reasons, information subject to the limitations in this paragraph will be removed.

C2.4.4. Hostage Situations

C2.4.4.1. General. A hostage situation exists when a member of subjects immediate family or such other person to whom the individual is bound by obligation or affection resides in a country whose interests are inimical to the interests of the United States. The rationale underlying this category of investigation is based on the possibility that an individual in such a situation might be coerced, influenced, or pressured to act contrary to the interests of national security.

C2.4.4.2. DIS Jurisdiction. In the absence of evidence of any coercion, influence or pressure, hostage investigations are exclusively a personnel security matter, rather than counterintelligence, and all such investigations shall be conducted by DIS.

C2.4.4.3. Military Department and/or FBI Jurisdiction. Should indications be developed that hostile intelligence is taking any action specifically directed against the individual concerned, or should there exist any other evidence that the individual is actually being coerced, influenced, or pressured by an element inimical to the interests of national security, then the case becomes a counter intelligence matter (outside of investigative jurisdiction of DIS) to be referred to the appropriate Military Department

or the FBI for investigation.

C2.4.5. Overseas Personnel Security Investigations. Personnel security investigations requiring investigation overseas shall be conducted under the direction and control of DIS by the appropriate Military Department investigative organization. Only post adjudication investigations involving an overseas subject may be referred by the requester directly to the Military Department investigative organization having investigative responsibility in the overseas area concerned (see Appendix 9) with a copy of the investigative request sent to DIS. In such cases, the Military Department investigative agency will complete the investigation, forward the completed report of investigation directly to DIS, with a copy to the requester.

C2.5. LIMITATIONS AND RESTRICTIONS

C2.5.1. Authorized Requesters and Personnel Security Determination Authorities. Personnel security investigations may be requested and personnel security clearances (including Special Access authorizations as indicated) granted only by those authorities designated in paragraph C5.1.2. and Appendix 5.

C2.5.2. Limit Investigations and Access. The number of persons cleared for access to classified information shall be kept to a minimum, consistent with the requirements of operations. Special attention shall be given to eliminating unnecessary clearances and requests for personnel security investigations.

C2.5.3. Collection of Investigative Data. To the greatest extent practicable, personal information relevant to personnel security determinations shall be obtained directly from the subject of a personnel security investigation. Such additional information required to make the necessary personnel security determination shall be obtained as appropriate from knowledgeable personal sources, particularly subjects peers, and through checks of relevant records including school, employment, credit, medical, and law enforcement records.

C2.5.4. Privacy Act Notification. Whenever personal information is solicited from an individual preparatory to the initiation of a personnel security investigation, the individual must be informed of:

C2.5.4.1. The authority (statute or Executive Order that authorized solicitation);

C2.5.4.2. The principal purpose or purposes for which the information is to be used;

C2.5.4.3. The routine uses to be made of the information;

C2.5.4.4. Whether furnishing such information is mandatory or voluntary;

C2.5.4.5. The effect on the individual, if any, of not providing the information; and

C2.5.4.6. That subsequent use of the data may be employed as part of an a periodic, random process to screen and evaluate continued eligibility for access to classified information.

C2.5.5. Restrictions on Investigators. Investigations shall be carried out insofar as possible to collect only as much information as is relevant and necessary for a proper personnel security determination. Questions concerning personal and domestic affairs, national origin, financial matters, and the status of physical health should be avoided unless the question is relevant to the criteria of paragraph C2.2.1. of this Regulation. Similarly, the probing of a person's thoughts or beliefs and questions about conduct that have no personnel security implications are unwarranted. When conducting investigations under the provisions of this Regulation, investigators shall:

C2.5.5.1. Investigate only cases or persons assigned within their official duties.

C2.5.5.2. Interview sources only where the interview can take place in reasonably private surroundings.

C2.5.5.3. Always present credentials and inform sources of the reasons for the investigation.. Inform sources of the subjects accessibility to the information to be provided and to the identity of the sources providing the information. Restrictions on investigators relating to Privacy Act advisements to subjects of personnel security investigations are outlined in paragraph C2.5.4., above.

C2.5.5.4. Furnish only necessary identity data to a source, and refrain from asking questions in such a manner as to indicate that the investigator is in possession of derogatory information concerning the subject of the investigation.

C2.5.5.5. Refrain from using, under any circumstances, covert or surreptitious investigative methods, devices, or techniques including mail covers, physical or photographic surveillance, voice analyzers, inspection of trash, paid informants, wiretap, or eavesdropping devices.

C2.5.5.6. Refrain from accepting any case in which the investigator knows of circumstances that might adversely affect his fairness, impartiality, or objectivity.

C2.5.5.7. Refrain, under any circumstances, from conducting physical searches of subject or his property.

C2.5.5.8. Refrain from attempting to evaluate material contained in medical files. Medical files shall be evaluated for personnel security program purposes only by such personnel as are designated by DoD medical authorities. However, review and collection of medical record information may be accomplished by authorized investigative personnel.

C2.5.6. Polygraph Restrictions. The polygraph may be used as a personnel security screening measure only in those limited instances authorized by the Secretary of Defense in DoD Directive 5210.48, (reference (p)).

C3. CHAPTER 3

PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS

C3.1. SENSITIVE POSITIONS

C3.1.1. Designation of Sensitive Positions. Certain civilian positions within the Department of Defense entail duties of such a sensitive nature including access to classified information, that the misconduct, malfeasance, or nonfeasance of an incumbent in any such position could result in an unacceptably adverse impact upon the national security. These positions are referred to in this Regulation as sensitive positions. It is vital to the national security that great care be exercised in the selection of individuals to fill such positions. Similarly, it is important that only positions which truly meet one or more of the criteria set forth in paragraph C3.1.2., below, be designated as sensitive.

C3.1.2. Criteria for Security Designation of Positions. Each civilian position within the Department of Defense shall be categorized, with respect to security sensitivity, as either nonsensitive, noncritical-sensitive, or critical-sensitive.

C3.1.2.1. The criteria to be applied in designating a position as sensitive are:

C3.1.2.1.1. Critical-sensitive

C3.1.2.1.1.1. Access to Top Secret information.

C3.1.2.1.1.2. Development or approval of plans, policies, or programs that affect the overall operations of the Department of Defense or of a DoD Component.

C3.1.2.1.1.3. Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

C3.1.2.1.1.4. Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.

C3.1.2.1.1.5. Fiduciary, public contact, or other duties demanding the highest degree of public trust.

C3.1.2.1.1.6. Duties falling under Special Access programs.

C3.1.2.1.1.7. Category I automated data processing (ADP) positions.

C3.1.2.1.1.8. Any other position so designated by the Head of the DoD Component or designee.

C3.1.2.1.2. Noncritical-sensitive

C3.1.2.1.2.1. Access to Secret or Confidential information.

C3.1.2.1.2.2. Security police/provost marshal-type duties involving the enforcement of law and security duties involving the protection and safeguarding of DoD personnel and property.

C3.1.2.1.2.3. Category II automated data processing positions.

C3.1.2.1.2.4. Duties involving education and orientation of DoD personnel.

C3.1.2.1.2.5. Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DoD personnel and property.

C3.1.2.1.2.6. Any other position so designated by the Head of the DoD Component or designee.

C3.1.2.2. All other positions shall be designated as nonsensitive.

C3.1.3. Authority to Designate Sensitive Positions. The authority to designate sensitive positions is limited to those authorities designated in paragraph AP5.7., Appendix 5. These authorities shall designate each position within their jurisdiction as to its security sensitivity and maintain these designations current vis-a-vis the specific duties of each position.

C3.1.4. Limitation of Sensitive Positions. It is the responsibility of those authorities authorized to designate sensitive positions to insure that (1) only those positions are designated as sensitive that meet the criteria of paragraph C3.1.2. above and (2) that the designation of sensitive positions is held to a minimum consistent with

mission requirements. Designating authorities shall maintain an accounting of the number of sensitive positions by category, i.e., critical or non-critical sensitive. Such information will be included in annual report required in Chapter 9.

C3.1.5. Billet Control System For Top Secret

C3.1.5.1. To standardize and control the issuance of Top Secret clearances within the Department of Defense, a specific designated billet must be established and maintained for all DoD military and civilian positions requiring access to Top Secret information. Only persons occupying these billet positions will be authorized a Top Secret clearance. If an individual departs from a Top Secret billet to a billet/position involving a lower level clearance, the Top Secret clearance will be administratively rescinded. This Top Secret billet requirement is in addition to the existing billet structure maintained for SCI access.

C3.1.5.2. Each request to DIS for a BI or SBI that involves access to Top Secret or SCI information will require inclusion of the appropriate billet reference, on the request for investigation. Each Component head should incorporate, to the extent feasible, the Top Secret billet structure into the component Manpower Unit Manning Document. Such a procedure should minimize the time and effort required to maintain such a billet structure.

C3.1.5.3. A report on the number of established Top Secret billets will be submitted each year to the DUSD(P) as part of the annual clearance report referred to in Chapter 11.

C3.2. CIVILIAN EMPLOYMENT

C3.2.1. General. The appointment of each civilian employee in any DoD Component is subject to investigation, except for reappointment when the break in employment is less than 12 months. The type of investigation required is set forth in this section according to position sensitivity.

C3.2.2. Nonsensitive Positions. In accordance with the OPM Federal Personnel Manual, (reference (cc)) a NACI shall be requested not later than 3 working days after a person is appointed to a nonsensitive position. Although there is normally no investigation requirement for per diem, intermittent, temporary or seasonal employees in nonsensitive positions provided such employment does not exceed an aggregate of 120 days in either a single continuous or series of appointments, a NAC may be requested of DIS where deemed appropriate by the employing activity.

C3.2.3. Noncritical-Sensitive Positions

C3.2.3.1. An NACI shall be requested and the NAC portion favorably completed before a person is appointed to a noncritical-sensitive position (for exceptions see paragraph C3.2.5.). An ENTNAC, NAC or DNACI conducted during military or contractor employment may also be used for appointment provided a NACI has been requested from OPM and there is no more than 12 months break in service since completion of the investigation.

C3.2.3.2. Seasonal employees (including summer hires) normally do not require access to classified information. For those requiring access to classified information the appropriate investigation is required. The request for the NAC (or NACI) should be submitted to DIS by entering "SH"(summer hire) in red letters approximately one inch high on the DD Form 398-2, "Personnel Security Questionnaire (National Agency Checklist)." Additionally, to ensure expedited processing by DIS, summer hire requests should be assembled and forwarded to DIS in bundles, when appropriate.

C3.2.4. Critical-Sensitive Positions. A BI shall be favorably completed prior to appointment to critical-sensitive positions (for exceptions see paragraph C3.2.5.). Certain critical-sensitive positions require a preappointment SBI in accordance with section C3.5. of this chapter. Preappointment BIs and SBIs will be conducted by DIS.

C3.2.5. Exceptions

C3.2.5.1. Noncritical-sensitive. In an emergency, a noncritical-sensitive position may be occupied pending the completion of the NACI if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made part of the record. In such instances, the position may be filled only after the NACI has been requested.

C3.2.5.2. Critical-sensitive. In an emergency, a critical-sensitive position may be occupied pending completion of the BI (or SBI, as appropriate) if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made a part of the record. In such instances, the position may be filled only when the NAC portion of the BI (or SBI) or a previous valid NACI, NAC or ENTNAC has been completed and favorably adjudicated.

C3.2.6. Mobilization of DoD Civilian Retirees. The requirements contained in paragraph C3.2.1. of this section, regarding the type of investigation required by position sensitivity for DoD civilian retirees temporary appointment when the break in employment is greater than 12 months, should either be expedited or waived for the purposes of mobilizing selected reemployed annuitants under the provisions of Title 5, United States Code, depending upon the degree of sensitivity of the position to which assigned. Particular priority should be afforded to newly assigned personnel assigned to the defense intelligence and security agencies with respect to granting security clearances in an expeditious manner under paragraph C3.2.1. of this section.

C3.3. MILITARY APPOINTMENT, ENLISTMENT, AND INDUCTION

C3.3.1. General. The appointment, enlistment, and induction of each member of the Armed Forces or their Reserve components shall be subject to the favorable completion of a personnel security investigation. The types of investigation required are set forth in this section.

C3.3.2. Entrance Investigation

C3.3.2.1. An ENTNAC shall be conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. A DNACI shall be conducted on each commissioned officer, except as permitted by paragraph C3.3.4. of this section, warrant officer, cadet, midshipman, and Reserve Officers Training Candidate, at the time of appointment. A full NAC shall be conducted upon reentry of any of the above when there has been a break in service greater than 12 months.

C3.3.2.2. If an officer or warrant officer candidate has been the subject of a favorable NAC or ENTNAC and there has not been a break in service of more than 12 months, a new NAC is not authorized. This includes ROTC graduates who delay entry onto active duty pending completion of their studies.

C3.3.2.3. All derogatory information revealed during the enlistment or apppointment process that results in a moral waiver will be fully explained on a written summary attached to the DD Form 398-2.

C3.3.3. Reserve Components and National Guard. Reserve component and National Guard personnel not on active duty are subject to the investigative requirements of this chapter.

C3.3.4. Exceptions for Certain Commissioned Officers of Reserve Components.

The requirements for entrance investigation shall be rigidly adhered to except as follows. Healthcare professionals, chaplains, and attorneys may be commissioned in the Reserve components prior to completion of a DNACI provided that:

C3.3.4.1. A DNACI is initiated at the time an application for a commission is received; and

C3.3.4.2. The applying health professional, chaplain, or attorney agrees in writing that, if the results of the investigation are unfavorable, he or she will be subject to discharge if found to be ineligible to hold a commission. Under this exception, commissions in Reserve Components other than the National Guard may be tendered to immigrant alien health professionals, chaplains, and attorneys.

C3.3.5. Mobilization of Military Retirees. The requirements contained in paragraph C3.3.2. of this section, regarding a full NAC upon reentry to active duty of any officer or enlisted regular/reserve military retiree or Individual Ready Reserve who has been separated from service for a period of greater than 12 months, should be waived for the purposes of partial or full mobilization under provisions of Title 10, (Title 14, pertaining to the U.S. Coast Guard as an element of the Navy) United States Code, to include the period of prescribed service refresher training. Particular priority should be afforded to military retirees mobilized and assigned to the defense intelligence and security agencies communities.

C3.4. SECURITY CLEARANCE

C3.4.1. General

C3.4.1.1. The authorities designated in paragraph AP5.1., Appendix 5 are the only authorities authorized to grant, deny or revoke DoD personnel security clearances. The granting of such clearances shall be limited to only those persons who require access to classified information for mission accomplishment.

C3.4.1.2. Military, DoD civilian, and contractor personnel who are employed by or serving in a consultant capacity to the Department of Defense, may be considered for access to classified information only when such access is required in connection with official duties. Such individuals may be granted either a final or interim personnel security clearance provided the investigative requirements set forth below are complied with, and provided further that all available information has been adjudicated and a finding made that such clearance would be clearly consistent with the interests of national security.

C3.4.2. Investigative Requirements for Clearance

C3.4.2.1. Top Secret

C3.4.2.1.1. Final Clearance:

C3.4.2.1.1.1. BI.

C3.4.2.1.1.2. Established billet per paragraph C3.1.5. (except contractors).

C3.4.2.1.2. Interim Clearance:

C3.4.2.1.2.1. Favorable NAC, ENTNAC, DNACI, or NACI completed.

C3.4.2.1.2.2. Favorable review of DD Form 398/SF-86/SF-171/DD Form 49.

C3.4.2.1.2.3. BI or SBI has been initiated.

C3.4.2.1.2.4. Favorable review of local personnel, base/military police, medical, and other security records as appropriate.

C3.4.2.1.2.5. Established billet per paragraph C3.1.5. (except contractors).

C3.4.2.1.2.6. Provisions of paragraph C3.2.5. have been met regarding civilian personnel.

C3.4.2.2. Secret

C3.4.2.2.1. Final Clearance:

C3.4.2.2.1.1. DNACI: Military (except first-term enlistees) and contractor employees.

C3.4.2.2.1.2. NACI: Civilian employees.

C3.4.2.2.1.3. ENTNAC: First-term enlistees.

C3.4.2.2.2. Interim Clearance:

C3.4.2.2.2.1. When a valid need to access Secret information is established, an interim Secret clearance may be issued in every case, provided that the steps outlined in subparagraphs C3.4.2.2.2.2. through C3.4.2.2.2.5., below, have been complied with.

C3.4.2.2.2.2. Favorable review of DD Form 398-2/SF-85/SF-171/DD Form 48.

C3.4.2.2.2.3. NACI, DNACI, or ENTNAC initiated.

C3.4.2.2.2.4. Favorable review of local personnel, base military police, medical, and security records as appropriate.

C3.4.2.2.2.5. Provisions of paragraph C3.2.5. have been complied with regarding civilian personnel.

C3.4.2.2.3. Confidential

C3.4.2.2.3.1. Final Clearance:

C3.4.2.2.3.1.1. NAC or ENTNAC: Military and contractor employees (except for Philippine national members of the United States Navy on whom a BI shall be favorably completed).

C3.4.2.2.3.1.2. NACI: Civilian employees (except for summer hires who may be granted a final clearance on the basis of a NAC).

C3.4.2.2.3.2. Interim Clearance

C3.4.2.2.3.2.1. Favorable review of DD Form 398-2/SF 85/SF 17 1/DD Form 48.

C3.4.2.2.3.2.2. NAC, ENTNAC or NACI initiated.

C3.4.2.2.3.2.3. Favorable review of local personnel, base military police, medical, and security records as appropriate.

C3.4.2.2.3.2.4. Provisions of paragraph C3.2.5. have been complied with regarding civilian personnel.

C3.4.2.2.4. Validity of Previously Granted Clearances: Clearances granted under less stringent investigative requirements retain their validity; however, if a

higher degree of clearance is required, investigative requirements of this Regulation will be followed.

C3.4.3. Access to Classified Information by Non-U.S. Citizens

C3.4.3.1. Only U.S. citizens are eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to an immigrant alien or a foreign national. Such individuals may be granted a "Limited Access Authorization" (LAA) in those rare circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed in pursuit of a specific DoD requirement involving access to specified classified information for which a cleared or clearable U.S. citizen is not available.

C3.4.3.2. Limitations

C3.4.3.2.1. LAAs shall be limited only to individuals who have a special skill or technical expertise essential to the fulfillment of a DoD requirement that cannot reasonably be filled by a U.S. citizen.

C3.4.3.2.2. LAAs shall not be granted to personnel who perform routine administrative or other support duties, such as secretaries, clerks, drivers, or mechanics, unless it has been clearly established that those duties cannot be performed by a U.S. citizen.

C3.4.3.2.3. Personnel granted LAAs shall not be permitted uncontrolled access to areas where classified information is stored or discussed. Classified information shall be maintained in a location that will be under the continuous control and supervision of an appropriately cleared U.S. citizen.

C3.4.3.2.4. LAA personnel shall not be designated as a courier or escort for classified material outside the location in which access is permitted unless they are accompanied by an appropriately cleared U.S. person.

C3.4.3.3. Authorized Access Levels

C3.4.3.3.1. LAAs may be granted only at the SECRET and CONFIDENTIAL level. LAAs for TOP SECRET are prohibited. Interim access is not authorized pending approval of a LAA.

C3.4.3.3.2. The information the non-U S. citizen may have access to must

be approved for release to the persons country or countries of citizenship, in accordance with DoD Directive 5230.11 (reference (ll)).

C3.4.3.3.3. Access to classified information shall be limited or related to a specific program or project; the LAA shall be canceled or rejustified as described herein upon completion of the program or project.

C3.4.3.3.4. Access to classified information outside the scope of the approved LAA shall be considered a compromise of classified information and shall be investigated, in accordance with DoD 5200.1-R (reference (q)).

C3.4.3.4. Requirements

C3.4.3.4.1. The LAA granting authority (Appendix 5) may consider issuing an LAA only after a written determination is made that access is essential for a critical mission and no U.S. citizen is available to perform the duties.

C3.4.3.4.2. When a non-U.S. citizen who is nominated for an LAA is a citizen of a country with which the United States has an agreement providing for security assurances based on that countries investigative requirements, which are commensurate with the standards provided herein, an LAA may be issued at the requisite level.

C3.4.3.4.3. In addition to the above, a favorably completed (within the last 5 years) and adjudicated SSBI is required prior to granting an LAA. If the SSBI cannot provide full investigative coverage, a polygraph examination (if there are no host country legal prohibitions) to resolve the remaining personnel security issues (see DoD Directive 5210.48 (reference (p))), must be favorably completed before granting access.

C3.4.3.4.4. If geographical, political or medical situations prevent the full completion of the SSBI or prevent the than full SSBI, a LAA may be granted only with approval of the ASD(C3I).

C3.4.3.4.5. If an LAA is withdrawn and the individual subsequently is considered for an LAA, the provisions of this paragraph shall apply concerning an SSBI and polygraph examination. The scope of the SSBI normally shall cover the period since the previous background investigation or 10 years, whichever is shorter.

C3.4.3.4.6. A PR shall be conducted on every individual with a LAA 5 years from the date of the last PR or SSBI, as appropriate.

C3.4.3.4.7. All requests for initial LAAs shall contain a detailed justification and plan describing the following:

C3.4.3.4.7.1. The location of the classified material (security containers) in relationship to the location of the foreign national.

C3.4.3.4.7.2. The compelling reason for not employing a cleared or clearable U.S. citizen.

C3.4.3.4.7.3. A synopsis of an annual continuing assessment program to evaluate the individuars continued trustworthiness and eligibility for access.

C3.4.3.4.7.4. A plan to control access to secure areas and to classified and controlled unclassified information.

C3.4.3.5. LAA Determination Authority

C3.4.3.5.1. LAA determinations may only be made by an official listed in paragraph AP5.2., Appendix 5. The designated single authorizing official for the Military Departments, the Combatant Commands, and the DIS precludes an LAA determination by any other official at the major command level, or equivalent.

C3.4.3.5.2. LAA determinations for employees of the Military Departments shall be the sole authority of the Secretary of the Military Department or a single designee such as the Service central adjudication facility. Field elements must submit their recommendations for access to the designated official for approval, along with affiliated information in support of the action.

C3.4.3.5.3. The Commander of a Combatant Command, or single designee (flag officer or civilian equivalent) responsible for implementation of the personnel security program, shall be authorized to issue, deny, or revoke an LAA. LAA determinations by the Combatant Commands shall be reported to the central adjudicative facility of the Military Department in accordance with the assigned responsibilities in DoD Directive 5100.3 (reference (mm)) for inclusion in the DCII.

C3.4.3.5.4. All LAA determinations, favorable and unfavorable, shall be entered into the DCII

C3.4.3.5.5. The administrative action procedures in Chapter 8 do not apply to LAA determinations.

C3.4.3.6. Record

C3.4.3.6.1. The LAA granting authority shall ensure that a record is

created on issuance and maintained for 5 years from the date the LAA ceases. The record shall include the following:

C3.4.3.6.1.1. The identity of the individual granted the LAA, to include the full name, date and place of birth, current citizenship(s), any SSN, and any national identifying number issued by the individual's country or countries of citizenship;

C3.4.3.6.1.2. The individual's status as an immigrant alien or foreign national; if an immigrant alien, the date and place such status was granted;

C3.4.3.6.1.3. The classification level of the LAA; i.e., SECRET or CONFIDENTIAL;

C3.4.3.6.1.4. Date and type of most recent background investigation or PR and the investigating Agency.

C3.4.3.6.1.5. Whether a polygraph examination was conducted; if so, the date and administering Agency for the most recent examination.

C3.4.3.6.1.6. The nature and identity of the classified program materials to which access is authorized and the precise duties performed.

C3.4.3.6.1.7. The compelling reasons for granting access to the information.

C3.4.3.6.2. All LAA SSBIs and PRs shall be conducted under the auspices of the DIS and shall comply with the requirements of Appendix 1. The DIS shall initiate leads to the respective Military Department investigative agencies overseas as well as the Department of State (DOS). The results of all investigations, to include those conducted by the DOS, shall be returned to the DIS for review and entry into the DCII and return to the designated granting official for adjudication. (To expedite matters, the investigation may be initiated locally provided the necessary paperwork has been submitted to the DIS for assignment of a case control number and initiation of such other checks as needed.)

C3.4.3.6.3. The Combatant Commands shall report LAAs they issue to the applicable DoD Component CAF for entry into the DCII. The Combatant Commands shall ensure that all investigative paperwork for the initiation of the SSBI or PR is submitted to the DIS through the designated single-approval authority responsible for adjudication and issuance of the LAA.

C3.4.3.6.4. All LAA nominees must agree to undergo a polygraph

examination at any time during the period the LAA is in effect, if there is no host-country legal prohibition.

C3.4.3.7. All LAAs shall be reviewed annually by the issuing component to determine if continued access is in compliance with DoD policy. A report on all LAAs in effect, including the data required in paragraph C3.4.3.6.1. shall be furnished to the DASD(I&S) within 60 days after the end of each fiscal year (see subsection C11.1.3., below).

C3.4.4. Access by Persons Outside the Executive Branch

C3.4.4.1. Access to classified information by persons outside the Executive Branch shall be accomplished in accordance with Chapter VII, DoD 5200.1-R (reference (q)). The investigative requirement shall be the same as for the appropriate level of security clearance, except as indicated below.

C3.4.4.2. Members of the U.S. Senate and House of Representative do not require personnel security clearances. They may be granted access to DoD classified information that relates to matters under the jurisdiction of the respective Committees to which they are assigned and is needed to perform their duties in connection with such assignments.

C3.4.4.3. Congressional staff members requiring access to DoD classified information shall be processed for a security clearance in accordance with DoD Directive 5142.1 (reference (oo)) and the provisions of this Regulation. The Director, Washington Headquarters Services (WHS) will initiate the required investigation (initial or reinvestigation) to DIS, adjudicate the results and grant, deny or revoke the security clearance, as appropriate. The Assistant Secretary of Defense (Legislative Affairs) will be notified by WHS of the completed clearance action.

C3.4.4.4. State governors do not require personnel security clearances. They may be granted access to specifically designated classified information, on a "need-to-know" basis, based upon affirmation by the Secretary of Defense or the Head of a DoD Component or single designee, that access, under the circumstances, serves the national interest. Staff personnel of a governor's office requiring access to classified information shall be investigated and cleared in accordance with the prescribed procedures of this Regulation when the Head of a DoD Component, or single designee, affirms that such clearance serves the national interest. Access shall also be limited to specifically designated classified information on a "need-to-know" basis.

C3.4.4.5. Members of the U.S. Supreme Court, the Federal judiciary and the

Supreme Courts of the individual States do not require personnel security clearances. They may be granted access to DoD classified information to the extent necessary to adjudicate cases being heard before these individual courts.

C3.4.4.6. Attorneys representing DoD military, civilian or contractor personnel requiring access to DoD classified information to properly represent their clients, shall normally be investigated by DIS and cleared in accordance with the prescribed procedures in paragraph C3.4.2. This shall be done upon certification of the General Counsel of the DoD Component involved in the litigation that access to specified classified information, on the part of the attorney concerned, is necessary to adequately represent his or her client. In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of paragraph C3.4.2., access may be granted with the written approval of an authority designated in Appendix 5 provided that as a minimum: (a) a favorable name check of the FBI and the DCII has been completed, and (b) a DoD Non-Disclosure Agreement has been executed. In post-indictment cases, after a judge has invoked the security procedures of the Classified Information Procedures Act (CIPA) (reference (m)), the Department of Justice may elect to conduct the necessary background investigation and issue the required security clearance, in coordination with the affected DoD Component.

C3.4.5. Restrictions on Issuance of Personnel Security Clearance. Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements.

Personnel security clearances shall normally not be issued:

C3.4.5.1. To persons in nonsensitive positions.

C3.4.5.2. To persons whose regular duties do not require authorized access to classified information.

C3.4.5.3. For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.

C3.4.5.4. To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel firemen, doctors, nurses, police, ambulance drivers, or similar personnel.

C3.4.5.5. To persons working in shipyards whose duties do not require access to classified information.

C3.4.5.6. To persons who can be prevented from accessing classified information by being escorted by cleared personnel.

C3.4.5.7. To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

C3.4.5.8. To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.

C3.4.5.9. To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.

C3.4.5.10. To perimeter security personnel who have no access to classified information.

C3.4.5.11. To drivers, chauffeurs and food service personnel.

C3.4.6. Dual Citizenship. Persons claiming both United States and foreign

citizenship shall be processed: under paragraph C3.4.2., above, and adjudicated in accordance with the "Foreign Preference" standard in Appendix 8.

C3.4.7. One-Time Access. Circumstances may arise where an urgent operational or contractual exigency exists for cleared DoD personnel to have one-time or short duration access to classified information at a higher level than is authorized by the existing security clearance. In many instances, the processing time required to upgrade the clearance would preclude timely access to the information. In such situations, and only for compelling reasons in furtherance of the DoD mission, an authority referred to in subparagraph C3.4.7.1., below, may grant higher level access on a temporary basis subject to the terms and conditions prescribed below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level clearance. Procedures and conditions for effecting emergency one-time access to the next higher classification level are as follows:

C3.4.7.1. Authorization for such one-time access shall be granted by a flag or general officer, a general court martial convening authority or equivalent Senior Executive Service member, after coordination with appropriate security officials.

C3.4.7.2. The recipient of the one-time access authorization must be a U.S. citizen, possess a current DoD security clearance, and the access required shall be limited to classified information one level higher than the current clearance.

C3.4.7.3. Such access, once granted, shall be canceled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the granting authority.

C3.4.7.4. The employee to be afforded the higher level access shall have been continuously employed by a DoD Component or a cleared DoD contractor for the preceding 24-month period. Higher level access is not authorized for part-tune employees.

C3.4.7.5. Pertinent local records concerning the employee concerned shall be reviewed with favorable results.

C3.4.7.6. Whenever possible, access shall be confined to a single instance or at most, a few occasions. The approval for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval of the granting authority is

required. At such time as it is determined that the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been approved, such access shall be canceled at or before 90 days from original date of access.

C3.4.7.7. Access at the higher level shall be limited to information under the control and custody of the authorizing official and shall be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision shall be responsible for:

C3.4.7.7.1. Recording the higher-level information actually revealed,

C3.4.7.7.2. The date(s) such access is afforded, and

C3.4.7.7.3. The daily retrieval of the material accessed.

C3.4.7.8. Access at the next higher level shall not be authorized for COMSEC, SCI, NATO, or foreign government information.

C3.4.7.9. The exercise of this provision shall be used sparingly and repeat use within any 12 month period on behalf of the same individual is prohibited. The approving authority shall maintain a record containing the following data with respect to each such access approved:

C3.4.7.9.1. The name, and SSN of the employee afforded higher level access.

C3.4.7.9.2. The level of access authorized.

C3.4.7.9.3. Justification for the access, to include an explanation of the compelling reason to grant the higher level access and specifically how the DoD mission would be furthered.

C3.4.7.9.4. An unclassified description of the specific information to which access was authorized and the duration of access along with the date(s) access was afforded.

C3.4.7.9.5. A listing of the local records reviewed and a statement that no significant adverse information concerning the employee is known to exist.

C3.4.7.9.6. The approving authority's signature certifying C3.4.7.9.1. through C3.4.7.9.5., above.

C3.4.7.9.7. Copies of any pertinent briefings/debriefings administered to the employee.

C3.4.8. Access by Retired Flag and/or General Officers

C3.4.8.1. Upon determination by an active duty flag/general officer that there are compelling reasons, in furtherance of the Department of Defense mission, to grant a retired flag/general officer access to classified information in connection with a specific DoD program or mission, for a period not greater than 90 days, the investigative requirements of this Regulation may be waived. The access shall be limited to classified information at a level commensurate with the security clearance held at the time of retirement -- not including access to SCI.

C3.4.8.2. The flag/general officer approving issuance of the clearance shall, provide the appropriate DoD Component central clearance facility a written record to be incorporated into the DCII detailing:

C3.4.8.2.1. Full identifying data pertaining to the cleared subject;

C3.4.8.2.2. The classification of the information to which access was authorized.

C3.4.8.3. Such access may be granted only after the compelling reason and the specific aspect of the DoD mission which is served by granting such access has been detailed and under the condition that the classified materials involved are not removed from the confines of a Government installation or other area approved for storage of DoD classified information.

C3.5. SPECIAL ACCESS PROGRAMS

C3.5.1. General. It is the policy of the Department of Defense to establish, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding established requirements are authorized only when mandated by statute, national regulations, or international agreement or Executive Order 12968 or its successor. In this connection, there are certain special access programs (SAPs) originating at the national or international level that require personnel security investigations and procedures of a special nature. Those programs and the special investigative requirements imposed by them are described in this section. A SAP is any program designed to control access, distribution, and protection of particularly sensitive information established pursuant to E. O. 12958

(reference (j)) and prior Executive Orders. DoD Directive O-5205.7 (reference (qq)) prescribes policy and procedures for establishment, administration and reporting of Departmental SAPs.

C3.5.2. Sensitive Compartmented Information (SCI)

C3.5.2.1. The investigative requirements for access to SCI is an SBI (see paragraph AP1.1.1.4., Appendix 1) including a NAC on the individual's spouse or cohabitant. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family (or other persons to whom the individual is bound by affection or obligation) to the extent necessary to permit a determination by the adjudication agency that the Personnel Security standards of DCID 1/14 (reference (l)) are met.

C3.5.2.2. A previous investigation conducted within the past five years which substantially meets the investigative requirements prescribed by this section may serve as a basis for granting access approval provided that there has been no break in the individuals Military Service, DoD civilian employment, or access to classified information under the Industrial Security Program greater than 24 months. The individual shall submit one copy of an updated PSQ covering the period since the completion of the last SBI and/or SSBI and certify any substantive changes that may have occurred.

C3.5.2.3. In accordance with DCID 1/14 (reference (l)), a TOP SECRET security clearance shall not be a prerequisite for access to SCI. Determination of eligibility for access to SCI under reference (l) shall include eligibility for access to TOP SECRET and below.

C3.5.3. Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI). The investigative requirement for access to SIOP-ESI is an SBI, including a NAC on the spouse and the individual's immediate family who are 18 years of age or over and who are United States citizens other than by birth or who are resident aliens.

C3.5.4. Presidential Support Activities

C3.5.4.1. DoD Directive 5210.55 (reference (r)) prescribes the policies and procedures for the nomination, screening, selection, and continued evaluation of DoD military and civilian personnel and contractor employees assigned to or utilized in Presidential Support activities. The type of investigation of individuals assigned to Presidential Support activities varies according to whether the person investigated qualifies for Category One or Category Two as indicated below:

C3.5.4.1.1. Category One

C3.5.4.1.1.1. Personnel assigned on a permanent or full-time basis to duties in direct support of the President (including the office staff of the Director, White House Military Office, and all individuals under his control):

C3.5.4.1.1.1.1. Presidential air crew and associated maintenance and security personnel.

C3.5.4.1.1.1.2. Personnel assigned to the White House communications activities and the Presidential retreat.

C3.5.4.1.1.1.3. White House transportation personnel.

C3.5.4.1.1.1.4. Presidential mess attendants and medical personnel.

C3.5.4.1.1.1.5. Other individuals filling administrative positions at the White House.

C3.5.4.1.1.2. Personnel assigned on a temporary or part-time basis to duties supporting the President:

C3.5.4.1.1.2.1. Military Social Aides.

C3.5.4.1.1.2.2. Selected security, transportation, flight-line safety, and baggage personnel.

C3.5.4.1.1.2.3. Others with similar duties.

C3.5.4.1.1.3. Personnel assigned to the Office of the Military Aide to the Vice President.

C3.5.4.1.2. Category Two

C3.5.4.1.2.1. Personnel assigned to honor guards, ceremonial units, and military bands who perform at Presidential functions and facilities.

C3.5.4.1.2.2. Employees of contractors who provide services or contractors employees who require unescorted access to Presidential Support areas, activities, or equipment-including maintenance of the Presidential retreat communications, and aircraft.

C3.5.4.1.2.3. Individuals in designated units requiring a lesser degree of access to the President or Presidential Support activities.

C3.5.4.2. Personnel nominated for Category One duties must have been the subject of an SBI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are United States citizens other than by birth or who are resident aliens. The SBI must have been completed within the 12 months preceding selection for Presidential Support duties. If such an individual marries subsequent to the completion of the SBI, the required spouse check shall be made at that time.

C3.5.4.3. Personnel nominated for Category Two duties must have been the subject of a BI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are United States citizens other than by birth or who are resident aliens. The BI must have been completed within the 12 months preceding selection for Presidential Support duties. It should be noted that duties (separate and distinct from their Presidential Support responsibilities) of some Category Two personnel may make it necessary for them to have special access clearances, which require an SBI.

C3.5.4.4. The U.S. citizenship of foreign-born immediate family members of all Presidential Support nominees must be verified by investigation.

C3.5.4.5. A limited number of Category One personnel having especially sensitive duties have been designated by the Director, White House Military Office as "Category A." These personnel shall be investigated under special scoping in accordance with the requirements of reference (ii).

C3.5.5. Nuclear Weapon Personnel Reliabilily Program (PRP)

C3.5.5.1. DoD Directive 5210.42 (reference (s)) sets forth the standards of individual reliability required for personnel performing duties associated with nuclear weapons and nuclear components. The investigative requirement for personnel performing such duties is:

C3.5.5.1.1. Critical Position: BI. In the event that it becomes necessary to consider an individual for a critical position and the required BI has not been completed, interim certification may be made under carefully controlled conditions as set forth below.

C3.5.5.1.1.1. The individual has had a favorable DNACI, NAC (or

ENTNAC) within the past 5 years without a break in service or employment in excess of 1 year.

C3.5.5.1.1.2. The BI has been requested.

C3.5.5.1.1.3. All other requirements of the PRP screening process have been fulfilled.

C3.5.5.1.1.4. The individual is identified to supervisory personnel as being certified on an interim basis.

C3.5.5.1.1.5. The individual is not used in a two-man team with another such individual.

C3.5.5..1.1.6. Justification of the need for interim certification is documented by the certifying official.

C3.5.5.1.1.7. Should the BI not be completed within 150 days from the date of the request, the certifying official shall query the Component clearance authority, who shall ascertain from DIS the status of the investigation. On the basis of such information, the certifying official shall determine whether to continue or to withdraw the interim certification.

C3.5.5.1.2. Controlled Position: DNACI/NACI

C3.5.5.1.2.1. An ENTNAC completed for the purpose of first term enlistment or induction into the Armed Forces does not satisfy this requirement.

C3.5.5.1.2.2. interim certification is authorized for an individual who has not had a DNACI/NACI completed within the past 5 years, subject to the following conditions:

C3.5.5.1.2.2.1. The individual has had a favorable ENTNAC/NAC, or higher investigation, that is more than 5 years old and has not had a break in service or employment in excess of 1 year.

C3.5.5.1.2.2.2. A DNACI/NACI has been requested at the time of interim certification.

C3.5.5.1.2.2.3. All other requirements of the PRP screening process have been fulfilled.

C3.5.5.1.2.2.4. Should the DNACI/NACI not be completed within 90 days from the date of the request, the procedures set forth in C3.5.5.1.1.7., above, for ascertaining the delay of the investigation in the case of a critical position shall apply.

C3.5.5.1.2.3. Additional requirements apply.

C3.5.5.1.2.3.1. The investigation upon which certification is based must have been completed within the last 5 years from the date of initial assignment to a PRP position and there must not have been a break in service or employment in excess of 1 year between completion of the investigation and initial assignment.

C3.5.5.1.2.3.2. In those cases in which the investigation was completed more than 5 years prior to initial assignment or in which there has been a break in service or employment in excess of 1 year subsequent to completion of the investigation, a reinvestigation is required.

C3.5.5.1.2.3.3. Subsequent to initial assignment to the PRP, reinvestigation is not required so long as the individual remains in the PRP.

C3.5.5.1.2.3.4. A medical evaluation of the individual as set forth in DoD Directive 5210.42 (reference (s)).

C3.5.5.1.2.3.5. Review of the individual's personnel file and other official records and information locally available concerning behavior or conduct which is relevant to PRP standards.

C3.5.5.1.2.3.6. A personal interview with the individual for the purpose of informing him of the significance of the assignment, reliability standards, the need for reliable performance, and of ascertaining his attitude with respect to the PRP.

C3.5.5.1.2.3.7. Service in the Army, Navy and Air Force Reserve does not constitute active service for PRP purposes.

C3.5.6. Access to North Atlantic Treaty Organization (NATO) Classified Information

C3.5.6.1. Personnel assigned to a NATO staff position requiring access to NATO COSMIC (TOP SECRET), SECRET or CONFIDENTIAL information shall have

been the: subject of a favorably adjudicated BI (10-year scope), DNACI/NACI or NACI ENTNAC, current within five years prior to the assignment, in accordance with USSAN Instruction 1-69 (reference (kk)) and paragraph C3.7.6., below.

C3.5.6.2. Personnel not assigned to a NATO staff position, but requiring access to NATO COSMIC, SECRET or in the normal course of their duties, must possess the equivalent final U.S. security clearance based upon the appropriate personnel security investigation (Appendix 1) required by paragraphs C3.4.2. and C3.7.10. of this Regulation.

C3.5.7. Other Special Acces Programs(SAPs). Special investigative requirements for SAPs not provided for in this paragraph may be established only as part of the written program approval of the Deputy Secretary of Defense in accordance with the SAP approval process prescribed for in DoD Directive O-5205.7 (reference (qq)).

C3.6. CERTAIN POSITIONS NOT NECESSARILY REQUIRING ACCESS TO CLASSIFIED INFORMATION

C3.6.1. General. DoD Directive 5200.8 (reference (t)) outlines the authority of military commanders under the Internal Security Act of 1950 to issue orders and regulations for the protection of property or places under their command. Essential to carrying out this responsibility is a commander's need to protect the command against the action of untrustworthy persons. Normally, the investigative requirements prescribed in this Regulation should suffice to enable a commander to determine the trustworthiness of individuals whose duties require access to classified information or appointment to positions that are sensitive and do not involve such access. However, there are certain categories of positions or duties which, although not requiring access to classified information, if performed by unworthy persons, could enable them to jeopardize the security of the command or otherwise endanger the national security. The investigative requirements for such positions or duties are detailed in this section.

C3.6.2. Access to Restricted Areas, Sensitive Information or Equipment Not Involving Access to Classified Information

C3.6.2.1. Access to restricted areas, sensitive information or equipment by DoD military, civilian or contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NAC (or ENTNAC) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NAC shall be conducted and favorably reviewed by the appropriate DoD Component Agency or activity prior to permitting such access. DoD Components shall not request, and shall not direct or permit their contractors to

request, security clearances to permit access to areas when access to classified information is not required in the normal course of duties or which should be precluded by appropriate security measures. In determining trustworthiness under this paragraph, the provisions of paragraph C2.2.1. and Appendix 8 will be utilized.

C3.6.2.2. In meeting the requirements of this paragraph, approval shall be obtained from one of the authorities designated in paragraph AP5.1., Appendix 5 of this Regulation, for authority to request NACs on DoD military, civilian or contractor employees. A justification shall accompany each request which shall detail the reasons why escorted access would not better serve the national security. Requests for investigative requirements beyond a NAC shall be forwarded to the Deputy Under Secretary of Defense for Policy for approval.

C3.6.2.3. NAC requests shall:

C3.6.2.3.1. Be forwarded to DIS in accordance with the provisions of paragraph AP2.2., Appendix 2,

C3.6.2.3.2. Contain a reference to this paragraph on the DD Form 398-2, and

C3.6.2.3.3. List the authority in Appendix 5 who approved the request.

C3.6.2.4. Determinations to deny access under the provisions of this paragraph must not be exercised in an arbitrary, capricious, or discriminatory manner and shall be the responsibility of the military or installation commander as provided for in DoD Directive 5200.8 (reference (t)).

C3.6.3. Nonappropriated Fund Employees. Each Nonappropriated Fund employee who is employed in a position of trust as designated by an official authorized in paragraph AP5.9., Appendix 5, shall have been the subject of a NAC completed no longer than 12 months prior to employment or a prior personnel security investigation with no break in Federal service or employment greater than 12 months in accordance with DoD 1401.1-M, (reference (u)). An individual who does not meet established suitability requirements may not be employed without prior approval of the authorizing official. Issuance of a CONFEDENTIAL or SECRET clearance will be based on a DNACI or NACI in accordance with paragraph C3.4.2.

C3.6.4. Customs Inspectors. DoD employees appointed as customs inspectors, under waivers approved in accordance with DoD 5030.49-R (reference (v)), shall have undergone a favorably adjudicated NAC completed within the past 5 years unless there has been a break in DoD employment greater than 1 year in which case a current NAC is

required.

C3.6.5. Red Cross/United Service Organizations Personnel (USO). A favorably adjudicated NAC shall be accomplished on Red Cross or United Service Organizations personnel as prerequisite for assignment with the Armed Forces overseas (DoD Directive 5210.25 (reference (w))).

C3.6.6. Officials Authorized to Issue Security Clearance. Any person authorized to adjudicate personnel security clearances shall have been the subject of a favorably adjudicated BI.

C3.6.7. Personnel Security Clearance adjudication Officials. Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorably adjudicated BI.

C3.6.8. Persons Requiring DoD Building Passes. Pursuant to DoD Directive 5210.46 (reference (z)), each person determined by the designated authorities of the DoD Components concerned as having an official need for access to DoD buildings in the National Capital Region shall be the subject of a favorably adjudicated NAC prior to issuance of a DoD building pass. Conduct of a BI for this purpose is prohibited unless approved in advance by ODUSD(P).

C3.6.9. Foreign National Employees Overseas Not Requiring Access to Classified Information. Foreign nationals employed by DoD organizations overseas, whose duties do not require access to classified information, shall be the subject of the following record checks, initiated by the appropriate Military Department investigative organization consistent with paragraph C2.4.5., prior to employment:

C3.6.9.1. Host-government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government; and

C3.6.9.2. DCII;

C3.6.9.3. FBI-HQ/ID (where information exists regarding residence by the foreign national in the United States for one year or more since age 18).

C3.6.10. Special Agents and Investigative Support Personnel. Special agents and those noninvestigative personnel assigned to investigative agencies whose official duties require continuous access to complete investigative files and material require an SBI.

C3.6.11. Persons Requiring Access to Chemical Agents. Personnel whose duties involve access to or security of chemical agents shall be screened initially for suitability and reliability and shall be evaluated on a continuing basis at the supervisory level to ensure that they continue to meet the high standards required. At a minimum, all such personnel shall have had a favorably adjudicated NAC completed within the last 5 years prior to assignment in accordance with the provisions of DoD Directive 5210.65 (reference (y)).

C3.6.12. Education and Orientation Personnel. Persons selected for duties in connection with programs involving the education and orientation of military personnel shall have been the subject of a favorably adjudicated NAC prior to such assignment. This does not include teachers/administrators associated with university extension courses conducted on military installations in the United States. Non-US citizens from a country listed in Appendix 8 shall be required to undergo a BI if they are employed in a position covered by this paragraph.

C3.6.13. Contract Guards. Any person performing contract guard functions shall have been the subject of a favorably adjudicated NAC prior to such assignment.

C3.6.14. Transportation of Arms, Ammunition and Explosives (AA&E). Any DoD military, civilian or contract employee (including commercial carrier) operating a vehicle or providing security to a vehicle @porting Category I, II or CONFIDENTIAL AA&E shall have been the subject of a favorably adjudicated NAC or ENTNAC.

C3.6.15. Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II and ADP-III. DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with Appendix 10) and investigated as follows:

ADP-I:	BI
ADP-II:	DNACI/NACI
ADP-III:	NAC/ENTNAC

Those personnel falling in the above categories who require access to classified information will, of course, be subject to the appropriate investigative scope contained in paragraph C3.4.2., above.

C3.6.16. Others. Requests for approval to conduct an investigation on other personnel, not provided for in paragraphs C3.6.2. through C3.6.14., above, considered to fall with the general provisions of paragraph C3.6.1., above, shall be submitted, detailing the justification therefor, for approval to the Deputy Under Secretary of Defense for

Policy. Approval of such requests shall be contingent upon an assurance that appropriate review procedures exist and that adverse determinations will be made at no lower than major command level.

C3.7. REINVESTIGATION

C3.7.1. General. DoD policy prohibits unauthorized and unnecessary investigations. There are, however, certain situations and requirements that necessitate reinvestigation of an individual who has already been investigated under the provisions of this regulation. It is the policy to limit reinvestigation of individuals to the scope contained in paragraph AP1.1.1.4., Appendix 1, to meet overall security requirements. Reinvestigation, generally, is authorized only as follows:

C3.7.1.1. To prove or disprove an allegation relating to the criteria set forth in paragraph C2.2.1. of this Regulation with respect to an individual holding a security clearance or assigned to a position that requires a unworthiness determination;

C3.7.1.2. To meet the periodic reinvestigation requirements of this Regulation with respect to those security programs enumerated below; and

C3.7.1.3. Upon individual request, to assess the current eligibility of individuals who did not receive favorable adjudicative action after an initial investigation, if a potential clearance need exists and there are reasonable indications that the factors upon which the adverse determination was made no longer exists.

C3.7.2. Allegations Related to Disqualification. Whenever questionable behavior patterns develop, derogatory information is discovered, or inconsistencies arise related to the disqualification criteria outlined in paragraph C2.2.1. that could have an adverse impact on an individual's security status, a Special Investigative Inquiry (SII), psychiatric, drug or alcohol evaluation, as appropriate, may be requested to resolve all relevant issues in doubt. If it is essential that additional relevant personal data is required from the investigative subject, and the subject fails to furnish the required data, the subject's existing security clearance or assignment to sensitive duties shall be terminated in accordance with paragraph C8.2.2. of this Regulation.

C3.7.3. Access to Sensitive Compartmented Information (SCI). Each individual having current access to SCI shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph AP1.1.1.4., Appendix 1.

C3.7.4. Critical-sensitive Positions. Each DoD civilian employee occupying a critical sensitive position shall be the subject of a PR conducted an a 5-year recurring,

basis scoped as set forth in paragraph AP1.1.1.4., Appendix 1.

C3.7.5. Presidential Support Duties. Each individual assigned Presidential Support duties shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph AP1.1.1.4., Appendix 1.

C3.7.6. NATO Staff. Each individual assigned to a NATO staff position requiring a COSMIC clearance shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph AP1.1.1.4., Appendix 1. Those assigned to a NATO staff position requiring a NATO SECRET clearance shall be the subject of a new NAC conducted on a 5-year recurring basis.

C3.7.7. Extraordinarily Sensitive Duties. In extremely limited instances, extraordinary national security implications associated with certain SCI duties may require very special comparanentation and other special security measures. In such instances, a Component SOIC may, with the approval of the Deputy Under Secretary of Defense for Policy, request PRs at intervals of less than 5 years as outlined in paragraph AP1.1.1.4., Appendix 1. Such requests shall include full justification and a recommendation as to the desired frequency. In reviewing such requests, the Deputy Under Secretary of Defense for Policy shall give due consideration to:

C3.7.7.1. The potential damage that might result from the individuals defection or abduction.

C3.7.7.2. The availability and probable effectiveness of means other than reinvestigation to evaluate factors concerning the individual's suitability for continued SCI access.

C3.7.8. Foreign Nationals Employed by DoD Organizations Overseas. Foreign nationals employed by DoD organizations overseas who have been granted a "Limited Access Authorization" shall be the subject of a PR, as set forth in paragraph AP1.1.1.4., Appendix 1, conducted under the auspices of DIS by the appropriate Military Department or other U.S. Government investigative agency consistent with paragraph C2.4.5. and Appendix 9 of this Regulation.

C3.7.9. Persons Accessing Very Sensitive Information Classified Secret

C3.7.9.1. Heads of DoD Components shall submit a request to the Deputy Under Secretary of Defense for Policy for approval to conduct periodic reinvestigations on persons holding Secret clearances who are exposed to very sensitive Secret information.

C3.7.9..2. Generally, the Deputy Under Secretary of Defense for Policy will only approve periodic reinvestigations of persons having access to Secret information if the unauthorized disclosure of the information in question could reasonably be expected to:

C3.7.9.2.1. Jeopardize human life or safety.

C3.7.9.2.2. Result in the loss of unique or uniquely productive intelligence sources or methods vital to the United States security.

C3.7.9.2.3. Compromise technologies, plans, or procedures vital to the strategic advantage of the United States.

C3.7.9.3. Each individual accessing very sensitive Secret information who has been designated by an authority listed in paragraph AP5.1., Appendix 5 as requiring periodic reinvestigation, shall be the subject of a PR conducted on a 5-year recurring basis scoped as stated in paragraph AP1.1.1.4., Appendix 1.

C3.7.10. Access Top Secret Information. Each individual having current access to Top Secret information shall be the subject of a PR conducted on a 5-year recurring basis scoped as outlined in paragraph AP1.1.1.4., Appendix 1.

C3.7.11. Personnel Occupying Computer Positions Designated ADP-I. All DoD military, civilians, consultants, and contractor personnel occupying computer positions designated ADP-I, shall be the subject of a PR conducted on a 5-year recurring basis as set forth in paragraph AP1.1.1.4., Appendix 1.

C3.8. AUTHORITY TO WAIVE INVESTIGATIVE REQUIRENMNTS

C3.8.1. Authorized Officials. Only an official designated in paragraph AP5.7., Appendix 5, is empowered to waive the investigative requirements for appointment to a sensitive position, assignment to sensitive duties or access to classified information pending completion of the investigation required by this chapter. Such waiver shall be based upon certification in writing by the designated official that such action is necessary to the accomplishment of a DoD mission. A minor investigative element that has not been met should not preclude favorable adjudication--nor should this require a waiver when all other information developed on an individual during the course of a prescribed investigation is favorable.

C4. CHAPTER 4

RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

C4.1. RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATIONS AND PERSONNEL SECURITY DETERMINATIONS

C4.1.1. General. Investigations conducted by DoD organizations or another Agency of the Federal Government shall not be duplicated when those investigations meet the scope and standards for the level of the clearance or access required. The DoD Components that grant access (SCI or SAP) or issue security clearances (TOP SECRET, SECRET, and CONFIDENTIAL) to civilian and/or military or contractor employees are responsible for determining whether such individuals have been previously cleared or investigated by the U.S. Government. Any previously granted security clearance or access, which is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance or access required, shall provide the basis for issuance of a new clearance and/or access without further investigation or adjudication. Previously conducted investigations and previously rendered personnel security determinations shall be accepted within the Department of Defense, in accordance with the policy in sections C4.1.2. through C4.1.4. below.

C4.1.2. Prior Personnel Security Investigations. As long as there is no break in Military Service and/or Federal employment greater than 24 months, any previous personnel security investigation that essentially is equivalent in scope to an investigation required by this Regulation will be accepted without requesting additional investigation. There is no time limitation as to the acceptability of such investigations, subject to the provisions of paragraphs C2.3.8. and C4.1.3.2. of this Regulation.

C4.1.3. Prior Personnel Security Determinations Made by DoD Authorities

C4.1.3.1. Adjudicative determinations for appointment in sensitive positions, assignment to sensitive duties or access to classified information (including those pertaining to SCI) made by designated DoD authorities will be mutually and reciprocally accepted by all DoD Components without requiring additional investigation, unless there has been a break in the individual's Military Service and/or Federal employment of greater than 24 months or unless derogatory information that occurred subsequent to the last prior security determination becomes known. A check of the DCII or other appropriate databases should be conducted to accomplish this task.

C4.1.3.2. Whenever a valid DoD security clearance or access eligibility is on record, Components shall not request DIS or other DoD investigative organizations to forward prior investigative files for review unless:

C4.1.3.2.1. Significant derogatory information or investigation completed subsequent to the date of last clearance and/or an access authorization, is known to the requester; or

C4.1.3.2.2. The individual concerned is being considered for a higher level clearance (e.g., Secret or Top Secret) or the individual does not have an access authorization and is being considered for one; or

C4.1.3.2.3. The most recent clearance or access authorization of the individual concerned was conditional or based on a waiver.

C4.1.3.3. Requests for prior investigative files authorized by this Regulation shall be made in writing, shall cite the specific justification for the request (i.e., upgrade of clearance, issue Special Access authorization, etc.), and shall include the date, level, and issuing organization of the individual's current or most recent security clearance or Special Access authorization.

C4.1.3.4. All requests for non-DoD investigative files, authorized under the criteria prescribed by paragraphs C4.1.3.1., C4.1.3.2.1., C4.1.3.2.2., C4.1.3.2.3., and C4.1.3.3., above, shall be:

C4.1.3.4.1. Submitted on DD Form 398-2 to DIS;

C4.1.3.4.2. Annotated as a "Single Agency Check" of whichever Agency developed the investigative file or to obtain the check of a single national agency.

C4.1.3.5. When further investigation is desired, in addition to an existing non-DoD investigative file, a DD Form 1879 will be submitted to DIS with the appropriate security forms attached. The submission of a Single Agency Check via DD Form 398-2 will be used to obtain an existing investigative file or check a single national agency.

C4.1.3.6. Whenever a civilian or military member transfers from one DoD activity to another, the losing organizations security office is responsible for advising the gaining organization of any pending action to suspend, deny or revoke the individual's security clearance as well as any adverse information that may exist in security, personnel or other files. In such instances the clearance shall not be reissued until the

questionable information has been adjudicated.

C4.1.4. Investigations Conducted and Clearances Granted by Other Agencies of the Federal Government

C4.1.4.1. Whenever a prior investigation or personnel security determination (including clearance for access to information classified under Executive Order 12356 (reference (j))) of another Agency of the Federal Government meets the investigative scope and standards of this Regulation, such investigation or clearance may be accepted for the investigative or clearance purposes of this Regulation, provided that the employment with the Federal Agency concerned has been continuous and there has been no break longer than 24 months since completion of the prior investigation, and further provided that inquiry with the Agency discloses no reason why the clearance should not be accepted. If it is determined that the prior investigation does not meet the provisions of this paragraph, supplemental investigation shall be requested.

C4.1.4.2. A NACI conducted by OPM shall be accepted and considered equivalent to a DNACI for the purposes of this Regulation.

C4.1.4.3. Department of Defense policy on reciprocal acceptance of clearances with the Nuclear Regulatory Commission and the Department of Energy is set for the in DoD Directive 5210.2 (reference (z)).

C5. CHAPTER 5

REQUESTING PERSONNEL SECURITY INVESTIGATIONS

C5.1. REQUESTING PERSONNEL SECURITY INVESTIGATIONS

C5.1.1. General. Requests for personnel security investigations shall be limited to those required to accomplish the Defense mission. Such requests shall be submitted only by the authorities designated in paragraph C5.1.2., below. These authorities shall be held responsible for determining if persons under their jurisdiction require a personnel security investigation. Proper planning must be effected to ensure that investigative requests are submitted sufficiently in advance to allow completion of the investigation before the time it is needed to grant the required clearance or otherwise make the necessary personnel security determination.

C5.1.2. Authorized Requesters. Requests for personnel security investigation shall be accepted only from the requesters designated below:

C5.1.2.1. Military Departments

C5.1.2.1.1. Army

C5.1.2.1.1.1. Central Clearance Facility.

C5.1.2.1.1.2. All activity commanders.

C5.1.2.1.1.3. Chiefs of recruiting stations.

C5.1.2.1.2. Navy (including Marine Corps)

C5.1.2.1.2.1. Central Adjudicative Facility.

C5.1.2..1.2.2. Commanders and commanding officers of organizations listed on the Standard Navy Distribution List.

C5.1.2.1.2.3. Chiefs of recruiting stations.

C5.1.2.1.3. Air Force

C5.1.2.1.3.1. Air Force Security Clearance Office.

C5.1.2.1.3.2. Assistant Chief of Staff for Intelligence.

C5.1.2.1.3.3. All activity commanders.

C5.1.2.1.3.4. Chiefs of recruiting stations.

C5.1.2.2. Defense Agencies--Directors of Security and activity commanders.

C5.1.2.3. Organization of the Joint Chiefs of Staff--Chief, Security Division.

C5.1.2.4. Office of the Secretary of Defense--Director for Personnel and Security, Washington Headquarters Services.

C5.1.2.5. Commanders of the Combatant Commands or their designees.

C5.1.2.6. Such other requesters approved by the Deputy Under Secretary of Defense for Policy.

C5.1.3. Criteria for Requesting Investigations. Authorized requesters shall use the tables set forth in Appendix 3 to determine the type of investigation that shall be requested to meet the investigative requirement of the specific position or duty concerned.

C5.1.4. Request Procedures. To insure efficient and effective completion of required investigations, all requests for personnel security investigations shall be prepared and forwarded in accordance with Appendix 2 and the investigative jurisdictional policies set forth in section C2.4. of this Regulation.

C5.1.5. Priority Requests. To insure that personnel security investigations are conducted in an orderly and efficient manner, requests for priority for individual investigations or categories of investigations shall be kept to a minimum. DIS shall not assign priority to any personnel security investigation or categories of investigations without written approval of the Deputy Under Secretary of Defense for Policy.

C5.1.6. Personal Data Provided by the Subject of the Investigation

C5.1.6.1. To conduct the required investigation, it is necessary that the investigative agency be provided certain relevant data concerning the subject of the investigation. The Privacy Act of 1974 (reference (m)) requires that, to the greatest extent practicable, personal information shall be obtained directly from the subject individual when the information may result in adverse determinations affecting an individual's rights, benefits, and privileges under Federal programs.

C5.1.6.2. Accordingly, it is incumbent upon the subject of each personnel security investigation to provide the personal information required by this Regulation. At a minimum, the individual shall complete the appropriate investigative forms, provide fingerprints of a quality acceptable to the FBI, and execute a signed release, as necessary, authorizing custodians of police, credit, education, employment, and medical and similar records, to provide relevant record information to the investigative agency. When the FBI returns a fingerprint card indicating that the quality of the fingerprints is not acceptable, an additional set of fingerprints wail be obtained from the subject. In the event the FBI indicates that the additional fingerprints are also unacceptable, no further attempt to obtain more fingerprints need be made; this aspect of the investigation will then be processed on the basis of the name check of the FBI files. As an exception, a minimum of three attempts will be made (1) for all Presidential Support cases, (2) for SCI access nominations if the requester so indicates, and (3) in those cases in which more than minor derogatory information exists. Each subject of a personnel security investigation conducted under the provisions of this regulation shall be furnished a Privacy Act Statement advising of (1) the authority for obtaining the personal data, (2) the principal purpose(s) for obtaining it, (3) the routine uses, (4) whether disclosure is mandatory or voluntary, (5) the effect on the individual if it is not provided, and (6) that subsequent use of the data may be employed as part of an a periodic review process to evaluate continued eligibility for access to classified information.

C5.1.6.3. Failure to respond within the time limit prescribed by the requesting organization with the required security forms or refusal to provide or permit access to the relevant information required by this Regulation shall result in termination of the individual's security clearance or assignment to sensitive duties utilizing the procedures of paragraph C8.2.2. or further administrative processing of the investigative request.

C6. CHAPTER 6

ADJUDICATION

C6.1. ADJUDICATION

C6.1.1. General

C6.1.1.1. The standard that must be met for clearance or assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

C6.1.1.2. The principal objective of the DoD personnel security adjudicative function, consequently, is to assure selection of persons for sensitive positions who meet this standard. The adjudication process involves the effort to assess the probability of future behavior, which could have an effect adverse to the national security. Since few, if any, situations allow for positive, conclusive evidence of certain future conduct, it is an attempt to judge whether the circumstances of a particular case, taking into consideration prior experience with similar cases, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security. It is invariably a subjective determination, considering the past but necessarily anticipating the future. Rarely is proof of trustworthiness and reliability or untrustworthiness and unreliability beyond all reasonable doubt.

C6.1.1.3. Establishing relevancy is one of the key objectives of the personnel security adjudicative process in evaluating investigative material. It involves neither the judgment of criminal guilt nor the determination of general suitability for a given position; rather, it is the assessment of a person's trustworthiness and fitness for a responsibility that could, if abused, have unacceptable consequences for the national security.

C6.1.1.4. While equity demands optimal uniformity in evaluating individual cases, assuring fair and consistent assessment of circumstances from one situation to the next, each case must be weighed on its own merits, taking into consideration all relevant facts, and prior experience in similar cases. All information of record, both

favorable and unfavorable, must be considered and assessed in terms of accuracy, completeness, relevance, seriousness,and overall significance. In all adjudications the protection of the national security shall be the paramount determinant.

C6.1.2. Central Adjudication

C6.1.2.1. To ensure uniform application of the requirement of this Regulation and to ensure that DoD personnel security determinations are effected consistent with existing statutes and Executive orders, the Head of each Military Department and Defense Agencies shall establish a single Central Adjudication Facility for his/her component. The function of such facility shall be limited to evaluating personnel security investigations and making personnel security determinations. The chief of each Central Adjudication Facility shall have the authority to act on behalf of the Head of the Component concerned with respect to personnel security determinations. All information relevant to determining whether a person meets the appropriate personnel security standard prescribed by this Regulation shall be reviewed and evaluated by personnel security specialists specifically designated by the Head of the Component concerned, or designee.

C6.1.2.2. In view of the significance each adjudicative decision can have on a person's career and to ensure the maximum degree of fairness and equity in such actions, a minimum level of review shall be required for all clearance/access determinations related to the following categories of investigations:

C6.1.2.2.1. BI/SBI/PR/ENAC/SII:

C6.1.2.2.1.1. Favorable: Completely favorable investigations shall be reviewed and approved by an adjudicative official in the civilian grade of GS-7/9 or the military rank of O-3.

C6.1.2.2.1.2. Unfavorable: Investigations that are not completely favorable shall undergo at least two levels of review by adjudicative officials, the second of which must be at the civilian grade of GS-11/12 or the military rank of O-4. When an unfavorable administrative action is contemplated under paragraph C8.2.2., the letter of intent (LOI) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS-13/14 or the military rank of O-5. A final notification of unfavorable administrative action, subsequent to the issuance of the LOI, must be approved and signed at the civilian grade of GS-14/15 or the military rank of O-6.

C6.1.2.2.2. NACI/DNACI/NAC/ENTNAC:

C6.1.2.2.2.1. Favorable: A completely favorable investigation may be finally adjudicated after one level of review provided that the decision making authority is at the civilian grade of GS-5/7 or the military rank of O-2.

C6.1.2.2.2.2. Unfavorable: Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS-7/9 or the military rank of O-3. When an unfavorable administrative action is contemplated under paragraph C8.2.2., the letter of intent to deny/ revoke must be signed by an adjudicative official at the civilian grade of GS-11/12 or the military rank of O-4. A final notification of unfavorable administrative action subsequent to the issuance of the LOI must be signed by an adjudicative official at the civilian grade of GS-13 or the military rank of O-5 or above.

C6.1.2.2.3. Exceptions to the above policy may only be granted by the Deputy Under Secretary of Defense for Policy.

C6.1.3. Evaluation of Personnel Security Information

C6.1.3.1. The criteria and adjudicative policy to be used in applying the principles at paragraph C6.1.1., above, are set forth in paragraph C2.2.1. and Appendix 8 of this Regulation. The ultimate consideration in making a favorable personnel security determination is whether such determination is clearly consistent with the interests of national security and shall be an overall common sense evaluation based on all available information. Such a determination shall include consideration of the following factors:

C6.1.3.1.1. The nature and seriousness of the conduct;

C6.1.3.1.2. The circumstances surrounding the conduct;

C6.1.3.1.3. The frequency and recency of the conduct;

C6.1.3.1.4. The age of the individual;

C6.1.3.1.5. The voluntariness of participation; and

C6.1.3.1.6. The absence or presence of rehabilitation.

C6.1.3.2. Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in Appendix 8. Adjudication policy for access to SCI is contained in DCID 1/14.

C6.1.4. Adjudicative Record

C6.1.4.1. Each adjudicative determination, whether favorable or unfavorable, shall be entered into the Defense Clearance and Investigations Index (DCII) on a daily basis but in no case to exceed 5-working days from the date of determination.

C6.1.4..2. The rationale underlying each unfavorable personnel security determination to include the appeal process, and each favorable personnel security determination where the investigation or information upon which the determination was made included significant derogatory information of the type set forth in paragraph C2.2.1. and Appendix 8 of this Regulation shall be maintained in written or automated form and is subject to the provisions of DoD Directives 5400.7 (reference (aa)) and 5400.11 (reference (bb)). This information shall be maintained for aminimum of 5 years from the date of determination.

C7. CHAPTER 7

ISSUING CLEARANCE AND GRANTING ACCESS

C7.1. ISSUING CLEARANCE AND GRANTING ACCESS

C7.1.1. General

C7.1.1.1. The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the individual case with respect to the subjects suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of paragraph C8.1.3.

C7.1.1.2. Only the authorities designated in paragraph AP5.1., Appendix 5 are authorized to grant, deny or revoke personnel security clearances or Special Access authorizations (other than SCI). Any commander or head of an organization may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in paragraph C8.1.3. of this Regulation are complied with.

C7.1.1.3. All commanders and Heads of DoD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this Regulation.

C7.1.2. Issuing Clearance

C7.1.2.1. Authorities designated in paragraph AP5.1., Appendix 5 shall record the issuance, denial, or revocation of a personnel security clearance in the DCII (see paragraph C6.1.4., above). A record of the clearance issued shall also be recorded in an individual's personnel/security file or official personnel folder, as appropriate.

C7.1.2.2. A personnel security clearance remains valid until (1) the individual is separated from the Armed Forces, (2) separated from DoD civilian employment, (3)

has no further official relationship with the Department of Defense, (4) official action has been taken to deny, revoke or suspend the clearance or access, or (5) regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties. If an individual resumes the original status of (1), (2), (3), or (5) above, no single break in the individual's relationship with the Department of Defense exists greater than 24 months, and/or the need for regular access to classified information at or below the previous level recurs, the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

C7.1.2.3. Personnel security clearances of DoD military personnel shall be granted, denied, or revoked only by the designated authority of the parent Military Department. Issuance, reissuance, denial, or revocation of a personnel security clearance by any DoD Component concerning personnel who have been determined to be eligible for clearance by another component is expressly prohibited. Investigations conducted on Army, Navy, and Air Force personnel by DIS will be returned only to the parent Service of the subject for adjudication regardless of the source of the original request. The adjudicative authority will be responsible for expeditiously transmitting the results of the clearance determination. As an exception, the employing DoD Component may issue an interim clearance to personnel under their administrative jurisdiction pending a final eligibility determination by the individual's parent DoD Component. Whenever an employing DoD Component issues an interim clearance to an individual from another DoD Component, written notice of the action shall be provided to the parent DoD Component.

C7.1.2.4. When an SSBI (or PR) for access to SCI is initiated on a military member, who is assigned to a Defense Agency (except DIA), OSD staff, or the Joint Staff, DIS will return the completed investigation to the appropriate Military Department CAF, in accordance with subsection C7.1.2.3., above, for issuance (or reissuance) of the SCI eligibility. The CAF shall be responsible for expeditiously transmitting the results of the SCI eligibility determination to the requesting Defense Agency. For military personnel assigned to the DIA, the completed investigation will be forwarded to the DIA for the SCI eligibility determination. The DIA will expeditiously transmit the results of the SCI eligibility determination to the appropriate Military Department CAF.

C7.1.2.5. When the Defense Industrial Security Clearance Office (DISCO) initiates an SSBI (or PR) for access to SCI on a contractor employee, DIS will return the completed investigation to the appropriate CAF with SCI cognizance. Following a favorable SCI eligibility determination, the CAF will notify DISCO of the outcome. If the SCI eligibility is denied or revoked, the CAF will complete all appropriate due

process and appeal procedures before forwarding the case and all relevant additional documentation to DISCO for appropriate action, to include referral to the Defense Office of Hearings and Appeals (DOHA) for possible action under DoD Directive 5220.6 (reference (c)).

C7.1.2.6. The interim clearance shall be recorded in the DCII (paragraph C6.1.4., above) by the parent DoD Component in the same manner as a final clearance.

C7.1.3. Granting Access

C7.1.3.1. Access to classified information shall be granted to persons whose official duties require such access and who have the appropriate personnel security clearance. Access determinations (other than for Special Access programs) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

C7.1.3.2. In the absence of derogatory information on the individual concerned, DoD commanders and organizational managers shall accept a personnel security clearance determination, issued by any DoD authority authorized by this Regulation to issue personnel security clearance, as the basis for granting access, when access is required, without requesting additional investigation or investigative files.

C7.1.3.3. The access level of cleared individuals will, wherever possible, be entered into the Defense Clearance and Investigations Index (DCII), along with clearance eligibility. However, completion of the DCII Access field is required effective October 1, 1993, in all instances where the adjudicator is reasonably aware of the level of classified access associated with a personnel security investigation. Agencies are encouraged to start completing this field as soon as possible.

C8. CHAPTER 8

UNFAVORABLE ADMINISTRATIVE ACTIONS

C8.1. REQUIREMENTS

C8.1.1. General. For purposes of this Regulation, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at paragraph DL1.1.2., and any unfavorable personnel security determination, as defined at paragraph DL1.1.29. This chapter is intended only to provide guidance for the internal operation of the Department of Defense and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

C8.1.2. Referral for Action

C8.1.2.1. Whenever derogatory information related to the criteria and policy set forth in paragraph C2.2.1. and Appendix 8 of this Regulation is developed or otherwise becomes available to any DoD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall insure that the appropriate Central Adjudicative Facility (CAF) of the individual concerned is informed promptly concerning (1) the derogatory information developed and (2) any actions taken or anticipated with respect thereto. However, referral of derogatory information to the commander or security officer shall in no way affect or limit the responsibility of the CAF to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with paragraph C8.2.2., below, if such action is warranted and supportable by the criteria and policy contained in paragraph C2.2.1. and Appendix 8. No unfavorable administrative action as defined in paragraphs DL1.1.28. and DL1.1.29. may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in paragraph C8.2.2., below, or, in the case of SCI, Annex B, DCID 1/14 (reference (l)).

C8.1.2.2. The Director DIS shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other

than through DoD command or industrial organization channels. Such access shall include utilization of the DoD Inspector General "hotline" to receive such reports for appropriate follow-up by DIS. DoD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DoD Components will augment the system when and where necessary. Heads of DoD Components will be notified immediately to take action if appropriate.

C8.1.3. Suspension.

C8.1.3.1. The commander or head of the organization shall determine whether, on the basis of all facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subjects security status unchanged or to take interim action to suspend subjects access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), if information exists which raises serious questions as to the individual's ability or intent to protect classified information or execute sensitive duties (or other duties requiring a trustworthiness determination) until a final determination is made by the appropriate authority designated in Appendix 5.

C8.1.3.2. Whenever a determination is made to suspend a security clearance for access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), the individual concerned must be notified of the determination in writing by the commander, or component CAF, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security.

C8.1.3.3. Component field elements must promptly report all suspension actions to the appropriate CAF, but not later than 10 working days from the date of the suspension action. The adjudicative authority will immediately update the DCII Eligibility and Access fields to alert all users to the individual's changed status.

C8.1.3.4. Every effort shall be made to resolve suspension cases as expeditiously as circumstances permit suspension cases exceeding 180 days shall be closely monitored and managed by the DoD Component concerned until finally resolved. Suspension cases pending in excess of 12 months will be reported to the DASD (I&S) for review and appropriate action.

C8.1.3.5. A final security clearance eligibility determination shall be made for all suspension actions and the determination entered in the DCII. If, however, the individual under suspension leaves the jurisdiction of the Department of Defense and no longer requires a clearance (or trustworthiness determination), entry of the "Z" Code

(adjudication action incomplete due to loss of jurisdiction) in the clearance eligibility field is appropriate. In no case shall a "suspension" code (Code Y) remain a permanent record in the DCII

C8.1.3.6. A clearance or access entry in the DCII shall not be suspended or downgaded based solely on the fact that a periodic reinvestigation was not conducted precisely within the 5-year time period for TOP SECRET/SCI or within the period prevailing for SECRET clearances under departmental policy. While every effort should be made to ensure that PRs are conducted within the prescribed timeframe, agencies must be flexible in their administration of this aspect of the personnel security program so as not to undermine the ability of the Department of Defense to accomplish its mission.

C8.1.4. Final Unfavorable Administrative Actions. The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in Appendix 5, except that the authority to terminate the employment of a civilian employee of a Military Department or Defense Agency is vested solely in the head of the DoD Component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DoD Components, on the basis of criteria listed in paragraph C2.2.1., C2.2.1.1. through C2.2.1.6., shall be coordinated with the of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence OASD(C3I) prior to final action by the Head of the DoD Component. DoD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this regulation if removal or separation can be effected under OPM regulations or administrative (nonsecurity) regulations of the Military Departments. However, actions contemplated in this regard shall not affect or limit the responsibility of the CAF to continue to process the individual for clearance, access to classified information, or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this Regulation.

C8.2. PROCEDURES

C8.2.1. General. No final unfavorable personnel security clearance or access determination shall be made on a Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person affiliated with the Department of Defense without granting the individual concerned the procedural benefits set forth in C8.2.2., below, when such determination results in an unfavorable administrative action (see paragraph C8.1.1.). As an exception, DoD contractor personnel shall be afforded the procedures contained in DoD Directive 5220.6 (reference (c)) and Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by DoD Directive 5210.25 (reference (w)). Procedures for to SAPs may differ from the procedures in this Regulation as authorized in E.O. 12968 and as approved by the Secretary of Defense or Deputy Secretary of Defense.

C8.2.2. Unfavorable Administrative Action Procedures. Except as provided for below, no unfavorable administrative action shall be taken under the authority of this Regulation unless the individual concerned has been:

C8.2.2.1. Provided a written statement of the reasons (SOR) as to why the unfavorable administrative action is being taken in accordance with the example at Appendix 11, which includes sample letters and enclosures. The SOR shall be as comprehensive and detailed as the protection of sources afforded confidentiality under provisions of the Privacy Act of 1974 (reference (m)) and national security permit. The statement will contain, 1) a summary of the security concerns and supporting adverse information, 2) instructions for responding to the SOR and 3) copies of the relevant security guidelines from Appendix 8. In addition, the CAF will provide within 30 calendar days, upon request of the individual, copies of releasable records of the personnel security investigation (the CAF must retain copies of the file for at least 90 days to ensure the ready availability of the material for the subject). If the CAF is unable to provide requested documents for reasons beyond their control, then the name and address of the Agency (Agencies) to which the individual may write to obtain a copy of the records will be provided.

C8.2.2.1.1. The head of the local organization of the individual receiving an SOR shall designate a point of contact (POC) to serve as a liaison between the CAF and the individual. The duties of the POC will include, but not necessarily be limited to, delivering the SOR, having the individual acknowledge receipt of the SOR; determining whether the individual intends to respond within the time specified; ensuring that the individual understands the consequences of the proposed action as well as the to respond in a timely fashion; explaining how to obtain time extensions, procure

copies of investigative records, and the procedures for responding to the SOR; and ensuring that the individual understands that he or she can obtain legal counsel or other assistance at his or her own expense.

C8.2.2.2. Afforded an opportunity to reply in writing to the CAF within 30 calendar days from the date to submit a timely response will result in forfeiture of all future appeal rights with regard to the unfavorable administrative action. Exceptions to this policy may only be circumstances where the individual's failure to respond to the SOR was due to factors beyond his or her control. The CAF must be notified of the individual's intent to respond, via the POC, within 10-calendar days of receipt of the SOR. An extension of up to 30-calendar days may be granted by the employing organization following submission of a written request from the individual. Additional extensions may only be granted by the CAF. Responses to the CAF must be forwarded through the head of the employing organization.

C8.2.2.3. Provided a written response by the CAF to any submission under subparagraph C8.2.2.2., above. stating the final reason(s) for the unfavorable administrative action, which shall be as specific as privacy and national security considerations permit and in accordance with the example of a letter of denial (IOD) and its enclosures at Appendix 11. Such response shall be as prompt as individual circumstances permit, not to exceed 60-calendar days from the date of receipt of the response submitted under subparagraph C8.2.2.2., above, provided no additional investigative action is necessary. If a final response cannot be completed within the time frame allowed, the individual must be notified in writing of this fact, the reasons therefor, and the date a final response is expected, which shall not normally exceed a total of 90 days from the date of receipt of the response under subparagraph C8.2.2.2.

C8.2.2.4. Afforded an opportunity to appeal an LOD, issued pursuant to paragraph C8.2.2.3., above to the DoD Component Personnel Security Appeals Board (PSAB). The PSAB shall consist of a minimum of three members and function in accordance with Appendix 12. If a decision is made to appeal the LOD, the individual may do so by one of the following methods:

C8.2.2.4.1. Appeal Without a Personal Appearance: Advise the PSAB within 10-calendar days of receipt of the LOD, of the intent to appeal. Within 40-calendar days of receipt of the LOD, write to the appropriate PSAB stating reasons why the LOD should be overturned and providing any additional, relevant information that may have a bearing on the final decision by the PSAB;

C8.2.2.4.2. Appeal With a Personal Appearance: Advise the Defense Office of Hearings and Appeals (DOHA) within 10-calendar days of receipt of the LOD

that a personal appearance before a DOHA Administrative Judge (AJ) is desired in order to provide additional, relevant information, which may have a bearing on the final decision by the PSAB. DOHA will promptly schedule a personal appearance and will provide a recommendation to the PSAB generally within 60 days of receipt of the requesting the personal appearance. Procedures governing the conduct of the personal appearance before a DOHA AJ are contained at Appendix 13.

C8.2.2.5. Provided a final written decision by the PSAB, including a rationale, to any submission under subparagraph C8.2.2.4., above, stating the final disposition of the appeal. This will nominally be accomplished within 60-calendar days of receipt of the written appeal from the individual if no personal appearance was requested, or within 30-calendar days from receipt of the AJ's recommendation if a personal appearance was requested.

C8.2.3. Due Process Review. The due process and appeal procedures will be reviewed one year after implementation. The above procedures will become effective no later than 120 days after the date of this change.

C8.2.4. Exceptions to Policy. Notwithstanding paragraph C8.2.2., above or any other provision of this Regulation, nothing in this Regulation shall be deemed to limit or affect the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national security so requires, pursuant to Section 7532, Title 5, United States Code (reference (pp)). Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph C8.2.2., above, are not appropriate. Such determination shall be conclusive.

C8.3. REINSTATEMENT OF CIVILIAN EMPLOYEES

C8.3.1. General. Any person whose civilian employment in the Department of Defense is terminated under the provisions of this Regulation shall not be reinstated or restored to duty or reemployed in the Departmentof Defense unless the Secretary of Defense, or the Head of a DoD Component, finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of national security. Such a finding shall be made part of the personnel security record.

C8.3.2. Reinstatement Benefits. A DoD civilian employee whose employment has been suspended or terminated under the provisions of this Regulation and who is reinstated or restored to duty under the provisions of Section 3571 of Title 5, U.S.

Code (reference (dd)) is entitled to benefits as provided for by Section 3 of Public Law 89-380 (reference (ee)).

C9. CHAPTER 9

CONTINUING SECURITY RESPONSIBILITIES

C9.1. EVALUATING CONTINUED SECURITY ELIGIBILITY

C9.1.1. General. A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood-of the individual preserving the national security. Obviously it is not possible at a given point to establish with certainty that any human being will remain trustworthy. Accordingly, the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, there is the clear need to assure that, after the personnel security determination is reached, the individual's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the individual's supervisor and, to a large degree, the individual himself. Therefore, the Heads of DoD Components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within a command is considered in the personnel security process.

C9.1.2. Management Responsibility

C9.1.2.1. Commanders and heads of organizations shall insure that personnel assigned to sensitive duties (or other duties requiring a trustworthiness determination under the provisions of this Regulation) are initially indoctrinated and periodically instructed thereafter on the national security implication of their duties and on their individual responsibilities.

C9.1.2..2. The Heads of all DoD Components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect to such areas as financial, medical or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long term, job-related security problems.

C9.1.3. Supervisory Responsibility. Security programs shall be established to

insure that supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern. Specific instructions should be disseminated concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect the interests of national security as well as to provide any necessary help to the individual concerned to correct any personal problem which may have a bearing upon the individuals continued eligibility for access.

C9.1.3.1. In conjunction with the submission of PRs stated in Section C3.7., Chapter 3, and paragraph AP1.1.1.4., Appendix 1, supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's continued eligibility for access to classified information is omitted.

C9.1.3.2. If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package.

"I am aware of no information of the type contained at Appendix 5, DoD 5200.2-R, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information."

C9.1.3.3. If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package:

"I am aware of information of the type contained in Appendix E, DoD 5200.2-R, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s)."

C9.1.3.4. In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with paragraphs

C9.1.3.2. and C9.1.3.3., above, as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their Component guidance.

C9.1.4. Individual Responsibility

C9.1.4.1. Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust in this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.

C9.1.4.2. Moreover, individuals having access to classified information must report promptly to their security office:

C9.1.4.2.1. Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee's official activities, in which:

C9.1.4.2.1.1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

C9.1.4.2.1.2. The employee is concerned that he or she may be the target of exploitation by a foreign entity.

C9.1.4.2.2. Any information of the type referred to in paragraph C2.2.1. or Appendix 8.

C9.1.5. Coworker Responsibility. Coworkers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information employed in a sensitive position.

C9.2. SECURITY EDUCATION

C9.2.1. General. The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DoD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DoD personnel security program. Accordingly, Heads of

DoD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

C9.2.2. Initial Briefings

C9.2.2.1. All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this Regulation shall be given an initial security briefing. The briefing shall be in accordance with the requirements of paragraph 10-102., DoD 5200.1-R (reference (q)) and consist of the following elements:

C9.2.2.1.1. The specific security requirements of their particular job.

C9.2.2.1.2. The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

C9.2.2.1.3. The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.

C9.2.2.1.4. The penalties that may be imposed for security violations.

C9.2.2.2. If an individual declines to execute Standard Form 312, "Classified Information Nondisclosure Agreement" (replaced the Standard Form 189). the DoD Component shall initiate action to deny or revoke the security clearance of such person in accordance with paragraph C8.1.3., above.

C9.2.3. Refresher Briefing. Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in paragraph 10-101. DoD 5200.1-R (reference (q)) shall be tailored to fit the needs of the experienced personnel.

C9.2.4. Foreign Travel Briefing. While world events during the past several years have diminished the threat to our national security from traditional cold-war era foreign intelligence services, foreign intelligence services continue to pursue the unauthorized acquisition of classified or otherwise sensitive U.S. Government information, through the recruitment of U.S. Government employees with access to such information. Through security briefings and education, the Department of Defense continues to provide for the protection of information and technology considered vital to the national security interests from illegal or unauthorized acquisition by foreign intelligence

services.

C9.2.4.1. DoD Components will establish appropriate internal procedures requiring all personnel possessing a DoD security clearance to report to their security office all contacts with individuals of any nationality, whether within or outside the scope of the employee's official activities in which:

C9.2.4.1.1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

C9.2.4.1.2. The employee is concerned that he or she may be the target of exploitation by a foreign entity.

C9.2.4.2. The DoD security manager, security specialist, or other qualified individual will review and evaluate the reported information. Any facts or circumstances of a reported contact with a foreign national that appear to:

C9.2.4.2.1. Indicate an attempt or intention to obtain unauthorized access to proprietary, sensitive, or classified Information or technology,

C9.2.4.2.2. Offer a reasonable potential for such, or

C9.2.4.2.3. Indicate the possibility of continued contact with the foreign national for such purposes, shall be promptly reported to the appropriate counterintelligence agency.

C9.2.5. Termination Briefing

C9.2.5.1. Upon termination of employment administrative withdrawal of security clearance or contemplated absence from duty or employment for 60 days or more DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. This statement shall include:

C9.2.5.1.1. An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD Regulations applicable to the safeguarding of classified information to which the individual has had access and understands the implications thereof.

C9.2.5.1.2. A declaration that the individual no longer has any documents or material containing classified information in his or her possession;

C9.2.5.1.3. An acknowledgment that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

C9.2.5.1.4. An acknowledgment that the individual will report without delay to the FBI or DoD Component concerned any attempt by any unauthorized person to solicit classified information.

C9.2.5.2. When an Individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal to sign a Security Termination Statement shall be reported to the Director, Defense Investigative Service, who shall ensure that it is recorded in the Defense Clearance and Investigations Index.

C9.2.5.3. The Security Termination Statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's records retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

C9.2.5.4. In addition to the provisions of subparagraphs C9.2.5.1., C9.2.5.2., and C9.2.5.3., above, DoD Components shall establish a central authority to be responsible for ensuring that Security Termination Statements are executed by senior personnel (general officers, flag officers and GS-16s and above). Failure on the part of such personnel to execute a Security Termination Statement shall be reported immediately to the Deputy Under Secretary of Defense for Policy.

C10. CHAPTER 10

SAFEGUARDING PERSONNEL SECURITY INESTIGATIVE RECORDS

C10.1. SAFEGUARDING PERSONNEL SECURITY INESTIGATIVE RECORDS

C10.1.1. General. In recognition of the sensitivity of personnel security reports and records, particularly with regard to individual privacy, it is Department of Defense policy that such personal information shall be handled with the highest degree of discretion. Access to such information shall be afforded only for the purpose cited herein and to persons whose official duties require such information. Personnel security investigative reports may be used only for the purposes of determining eligibility of DoD military and civilian personnel, contractor employees, and other persons affiliated with the Department of Defense, for access to classified information, assignment or retention in sensitive duties or other specifically designated duties requiring such investigation, or for law enforcement and counterintelligence investigations. Other uses are subject to the specific written authorization of the Deputy Under Secretary of Defense for Policy.

C10.1.2. Responsibilities. DoD authorities responsible for administering the DoD personnel security program and all DoD personnel authorized access to personnel security reports and records shall ensure that the use of such information is limited to that authorized by this Regulation and that such reports and records are safeguarded as prescribed herein. The Heads of DoD Components and the Deputy Under Secretary of Defense for Policy for the Office of the Secretary of Defense shall establish internal controls to ensure adequate safeguarding and limit access to and use of personnel security reports and records as required by paragraph C10.1.3. and C10.1.4., below.

C10.1.3. Access Restrictions. Access to personnel security investigative reports and personnel security clearance determination information shall be authorized only in accordance with DoD Directives 5400.7 and 5400.11 (references (aa) and (bb)) and with the following:

C10.1.3.1. DoD personnel security investigative reports shall be released outside of the Department of Defense only with the specific approval of the investigative agency having authority over the control and disposition of the reports.

C10.1.3.2. Within the Department of Defense, access to personnel security investigative reports shall be limited to those designated DoD officials who require access in connection with specifically assigned personnel security duties, or other

activities specifically identified under the provisions of paragraph C10.1.1., above.

C10.1.3.3. Access by subjects of personnel security investigative reports shall be afforded in accordance with DoD Directive 5400.11 (reference (bb)).

C10.1.3.4. Access to personnel security clearance determination information shall be made available, other than provided for in C10.1.3.3., above, through security channels, only to the Department of Defense or other officials of the Federal Government who have an official need for such information.

C10.1.4. Safeguarding Procedures. Personnel security investigative reports and personnel security determination information shall be safeguarded as follows:

C10.1.4.1. Authorized requesters shall control and maintain accountability of all reports of investigation received.

C10.1.4.2. Reproduction, in whole or in part, of personnel security investigative reports by requesters shall be restricted to the minimum number of copies required for the performance of assigned duties.

C10.1.4.3. Personnel security investigative reports shall be stored in a vault, safe, or steel file cabinet having at least a lock or and an approved three-position dial-type combination padlock or in a similarly protected area/container.

C10.1.4.4. Reports of DoD personnel security investigations shall be sealed in double envelopes or covers when transmitted by mail or when carried by persons not authorized access to such information. The inner cover shall bear a notation substantially as follows:

C10.1.4.5. An individual's status with respect to a personnel security clearance or a Special Access authorization is to be protected as provided for in paragraph 6.3.6., DoD Directive 5400.7 (reference (aa)).

C10.1.5. Records Disposition

C10.1.5.1. Personnel security investigative reports, to include OPM NACIs may be retained by DoD recipient organizations, only for the period necessary to complete the purpose for which it was originally requested. Such reports are considered to be the property of the investigating organization and are on loan to the recipient organization. All copies of such reports shall be destroyed within 90 days after completion of the required personnel security determination. Destruction shall be accomplished in the same manner as for classified information in accordance with

paragraph 9-101., DoD 5200.1-R (reference (q)).

C10.1.5.2. DoD record repositories authorized to file personnel security investigative reports shall destroy PSI reports of a favorable or of a minor derogatory nature 15 years after the date of the last action. That is, after the completion date of the investigation or the date on which the record was last released to an authorized user--whichever is later. Personnel security investigative reports resulting in an unfavorable administrative personnel action or court-martial or other investigations of a significant nature due to information contained in the investigation shall be destroyed 25 years after the date of the last action. Files in this latter category that are determined to be of possible historical value and those of widespread public or congressional interest may be offered to the National Archives after 15 years.

C10.1.5.3. Personnel security investigative reports on persons who are considered for affiliation with the Department of Defense will be destroyed after 1 year if the affiliation is not completed.

C10.1.6. Foreign Source Information. Information that is classified by a foreign government is exempt from public disclosure under the Freedom of Information and Privacy Acts. Further, information provided by foreign governments requesting an express promise of confidentiality shall be released only in a manner that will not identify or allow unauthorized persons to identify the foreign agency concerned.

C11. CHAPTER 11

PROGRAM MANAGEMENT

C11.1. PROGRAM MANAGEMENT

C11.1.1. General. To ensure uniform implementation of the DoD personnel security program throughout the Department, program responsibility shall be centralized at the DoD Component level.

C11.1.2. Responsibilities

C11.1.2.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) shall have primary responsibility for providing guidance, oversight, development and approval for policy and procedures governing personnel security program matters within the Department:

C11.1.2.1.1. Provide program management through isuance of policy and operating guidance.

C11.1.2.1.2. Provide staff assistance to the DoD Components and Defense Agencies in resolving day-to-day security policy and operating problems.

C11.1.2.1.3. Conduct inspections of the DoD Components for implementation and compliance with DoD security policy and operating procedures.

C11.1.2.1.4. Provide policy, oversight, and guidance to the Component adjudication functions.

C11.1.2.1.5. Approve, coordinate and oversee all DoD personnel security research initiatives and activities.

C11.1.2.2. The General Counsel shall ensure that the program is administered in a manner consistent with the laws; all proceedings are promptly initiated and expeditiously completed; and that the rights of individuals involved are protected, consistent with the Interests of national security. The General Counsel shall also ensure that all relevant decisions of the courts and legislative initiatives of the Congress are obtained on a continuing basis and that analysis of the foregoing is accomplished and disseminated to DoD personnel security program management authorities.

C11.1.2.3. The Heads of the CoDComponents shall ensure that:

C11.1.2.3.1. The DoD personnel security program is administered within their area of responsibility in a manner consistent with this Regulation.

C11.1.2.3.2. A single authority within the office of the Head of the DoD Component is assigned responsibility for administering the program within the Component.

C11.1.2..3.3. Information and recommendations are provided the ASD(C3I) and the General Counsel at their request concerning any aspect of the program.

C11.1.3. Reporting Requirements

C11.1.3.1. The OASD(C3I) shall be provided personnel security program management data by the Defense Data Manpower Center (DMDC) by 31 December each year for the preceding fiscal year. To facilitate accurate preparation of this report, all adjudicative determinations must be entered into the DCII by all DoD central adjudication facilities no later than the end of the fiscal year. The information required below is essential for basic personnel security program management and in responding to requests from the Secretary of Defense and Congress. The report shall cover the preceding fiscal year, broken out by clearance category, according to military (officer or enlisted), civilian or contractor status and by the central adjudication facility that took the action, using the enclosed format:

C11.1.3..1.1. Number of Top Secret, Secret, and Confidential clearances issued;

C11.1.3.1.2. Number of Top Secret, Secret, and Confidential clearances denied;

C11.1.3.1.3. Number of Top Secret, Secret, and Confidential clearances revoked;

C11.1.3.1.4. Number of SCI access determinations issued;

C11.1.3.1.5. Number of SCI access determinations denied;

C11.1.3.1.6. Number of SCI access determinations revoked; and

C11.1.3.1.7. Total number of personnel holding a clearance for Top Secret, Secret, Confidential, and Sensitive Compartmented Information as of the end of the fiscal year.

C11.1.3.2. The Defense Investigative Service (DIS) shall provide the OASD(C3I) a quarterly report that reflects investigative cases opened and closed during the most recent quarter by case category type, and by major requester. The information provided by DIS is essential for evaluating statistical data regarding investigative workload and the manpower required to perform personnel security investigations. Case category types include National Agency Checks (NACs); Expanded NACS; Single Scope Background Investigations; Periodic Reinvestigations (PRs); SECRET Periodic Reinvestigations (SPRs); Post Adjudicative; Special Investigative Inquiries (SlIs); and Limited Inquiries. This report shall be forwarded to OASD(C3I) within 45 days after the end of each quarter.

C11.1.3.3. The reporting requirement for DMDC and DIS has been assigned Report Control Symbol DD-C31(A)1749.

C11.1.4. Inspections. The Heads of DoD Components shall assure that personnel security program matters are included in their administrative inspection programs.

C12. CHAPTER 12

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII)

C12.1. DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII)

C12.1.1. General

C12.1.1.1. The Defense Clearance and Investigations Index (DCII) is the single, automated central repository that identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities.

C12.1.1.2. The DCII database consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects, in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are maintained, by subject, in the DCII.

C12.1.1.3. DoD investigative and adjudicative authorities report information which is used for investigative, adjudicative, statistical, research and other purposes as authorized by OASD(C3I) approval.

C12.1.2. Access. The DCII is operated and maintained by the Defense Investigative Service (DIS). Access is nominally limited to the Department of Defense and other Federal Agencies with adjudicative, investigative, and/or counterintelligence (CI) missions. Agencies wishing to gain access to the DCII must submit a written request outlining specific requirements with corresponding justification, as stated in paragraph C12.1.2.1. through C12.1.2.4., below. On approval, a Memorandum of Understanding (MOU) addressing equipment, maintenance, security, privacy, and other Agency responsibilities shall be forwarded to the requester by DIS for signature.

C12.1.2.1. Military Departments. Requests from Military Departments or organizations must be submitted for approval and endorsement through the following offices to DIS, Director, National Computer Center, P.O. Box 1211, Baltimore, MD 21203-1211.

C12.1.2.1.1. Air Force. Administrative Assistant to the Secretary of the Air Force, Pentagon, Room 4D881, Washington, DC 20330-4000.

C12.1.2.1.2. Army. Director, Counterintelligence and Security Countermeasures, Office of the Deputy Chief of Staff for Intelligence, Department of the Army, Pentagon, Room 2D481, Washington, DC 20301-1050.

C12.1.2.1.3. Navy and Marine Corps. Director, Information and Personnel Security Policy Directorate, Naval Criminal Investigative Service, Chief of Naval Operations (OP-09N), Washington, DC 20350-2000.

C12.1.2.2. Combatant Commands. Requests from Combatant Commands must be submitted for approval to DIS, Director, National Computer Center through the Joint Chiefs of Staff, Chief, Security Division, Directorate for Information and Resource Management, The Joint Staff, Room 1B738, The Pentagon, Washington, DC 20318-9300.

C12.1.2.3. Defense Agencies. Requests from DoD Agencies must be submitted through, and with the approval of, the Agency's Security Headquarters Office to DIS, Director, National Computer Center, P.O. Box 1211, Baltimore, MD 21203-1211.

C12.1.2.4. Non-DoD Agencies. Requests from Non-DoD Agencies must be submitted to the Deputy Assistant Secretary of Defense (Intelligence and Security), Attn: Counterintelligence and Security Programs, Room 3C281, 6000 Defense Pentagon, Washington, DC 20301-6000. On approval, those requests shall be forwarded to the DIS for action.

C12.1.3. Investigative Data. Contributors to the DCII shall ensure that all investigative data on an individual is entered into the DCII.

C12.1.3.1. An entry shall be made to indicate a pending investigation when an investigation is opened.

C12.1.3.2. When an investigation has been completed, the contributor shall change the DCII status to reflect a completed investigation, including the date (year) of the investigation.

C12.1.3.3. Changes or additions to existing files must, whenever appropriate, all be reflected in the DCII.

C12.1.3.4. Investigative file tracings may be deleted from the DCII when the retention period is over and the record file has been destroyed.

C12.1.4. Adjudicative Data. All adjudicative determinations on personnel with access to classified information or performing sensitive duties shall be indexed in the DCII.

C12.1.4.1. Specifically, a DCII clearance entry shall be created or updated as follows:

C12.1.4.1.1. Immediately upon suspension of access.

C12.1.4.1.2. When interim access has been authorized by the CAF or employing activity.

C12.1.4.1.3. Immediately following the granting, denial, or revocation of a clearance or access.

C12.1.4.1.4. Following the receipt, review, and adjudication of information received subsequent to the prior clearance or access determination.

C12.1.4.2. DCII entries shall inform the DoD Components of the clearance eligibility and/or access status of an individual or the presence of an adjudicative file.

C12.1.4.3. An adjudicative determination shall remain in the DCII as long as the subject is affiliated with the Department of Defense. The determination may be deleted 2 years after the employment and/or clearance eligibility ends. The deleted DCII data shall be retained by the DIS in a historical file for a minimum of 5 years after deletion by the contributor.

C12.1.4.4. The date of the DCII clearance and/or access entry shall always be the same as or subsequent to the date of the most recent investigation.

C12.1.4.5. DoD Components will notify the CAF of applicable personnel changes to ensure the accuracy of the DCII database.

C12.1.5. Notification to Other Contributors. Whenever a DoD contributor to the DCII becomes aware of significant unfavorable information about an individual with a clearance and/or access entry from another DoD contributor, immediate notification must be made to the latter along with copies of all relevant information.

C12.1.6. Security Requirements for the DCII

C12.1.6.1. The DCII is an unclassified system that meets the C-2 level of

protection under the Computer Security Act of 1987. Contributors may enter only unclassified information.

C12.1.6.2. Information contained in the DCII receives the protection required by the Privacy Act of 1974 (reference (m)).

C12.1.6.2.1. Due to the sensitive nature of the information, positions having direct (password) access to a DCII terminal are considered to be ADP-1 Critical Sensitive Positions.

C12.1.6.2.2. Individuals authorized access to the DCII must have a favorably completed SSBI (or BI and/or SBI).

C12.1.6.2.3. DoD activities and other Federal Agencies that have been authorized "Read Only" access to the DCII must also comply with those investigative requirements.

C12.1.6.3. Each authorized contributor is responsible for the accuracy of the data it enters. Contributors may enter, modify or delete only data originated by them. The DCII shall not allow one contributor to alter or delete another contributor's information.

C12.1.6.4. To prevent unauthorized access or tampering during nonworking hours, DCII terminals must be located in an area that is secured by guard personnel, an alarm system, or appropriate locking device.

C12.1.6.5. When the DCII terminal is operational, access to DCII information shall be controlled and limited to those persons authorized access to that information.

C12.1.7. Disclosure of Information. The Privacy Act of 1974 requires an accounting of the disclosure of personal information when it is provided to another Agency. For accessing the DCII, the Department of Defense is considered a single Agency. Disclosure of personal information in the Department of Defense does not require specific accounting for each disclosure. All releases of information obtained from the DCII to any non-DoD source must be recorded in the DCII Disclosure Accounting System (DDAS) by the Agency that releases the information. A contributor may disclose only the DCII data originated by that contributor to the subject of the data. Requests for release of investigative reports or adjudicative files are handled as Privacy Act requests by contributors.

AP1. APPENDIX 1

INVESTIGATIVE SCOPE

AP1.1.1. This appendix prescribes the scope of the various types of personnel security investigations.

AP1.1.1.1. National Agency Check. The scope for NAC is five years or to age 18, whichever is the shorter period. At a minimum, the first three of the described Agencies (DCII, FBLIHQ, and FBI/ID), below, shall be included in each complete NAC; however, a NAC may also include a check of any or all of the other described Agencies, if appropriate.

AP1.1.1.1.1. The DCII database consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects, in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are maintained, by subject, in the DCII. DCII records will be checked on all subjects of DoD investigations.

AP1.1.1.1.2. FBI/HQ has on file copies of investigations conducted by the FBI. The FBI/HQ check, included in every NAC, consists of a review of files for information of a security nature and that developed during applicant-type investigations.

AP1.1.1.1.3. An FBI/ID check, included in every NAC (but not ENTNAC), is based upon a technical fingerprint search that consists of a classification the subject's fingerprints and comparison with fingerprint cards submitted by law enforcement activities. If the fingerprint card is not classifiable, a "name check only" of these files is automatically conducted.

AP1.1.1.1.4. OPM. The files of OPM contain the results of investigations conducted by OPM under E.O. 9835 and 10450 (references (ff) and (g)), those requested by the Nuclear Regulatory Commission (NRC), the Department of Energy (DOE), and those requested since August 1952 to serve as a basis for "Q" clearances. OPM records are checked on all persons who are, or who have been, civilian employees of the U.S. Government; or U.S. citizens who are, or who have been, employed by a United Nations organization or other public international organization; and on those who have been granted security clearances by the NRC or the DOE.

AP1.1.1.1.5. Immigration and Naturalization Service (I&NS). The files

of I&NS contain (or show where filed) naturalization certificates, certificates of derivative citizenship, all military certificates of naturalization, repatriation files, petitions for naturalization and declaration of intention, visitors' visas, and records of aliens (including government officials and representatives of international organizations) admitted temporarily into the U.S. I&NS records are checked when the subject is:

AP1.1.1.1.5.1. An alien in the United States, or

AP1.1.1.1.5.2. A naturalized citizen whose naturalization has not been verified, or

AP1.1.1.1.5.3. An immigrant alien, or

AP1.1.1.1.5.4. A U.S. citizen who receives derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

AP1.1.1.1.6. State Department. The State Department maintains the following records:

AP1.1.1.1.6.1. Security Division (S/D) files contain information pertinent to matters of security, violations of security, personnel investigations pertinent to that agency, and correspondence files from 1950 to date. These files are checked on all former State Department employees.

AP1.1.1.1.6.2. Passport Division (P/D) shall be checked if subject indicates U.S. citizenship due to birth in a foreign country of American parents. This is a check of State Department Embassy files to determine if subject's birth was registered at the U.S. Embassy in the country where he was born. Verification of this registration is verification of citizenship.

AP1.1.1.1.7. Central Intelligence Agency (CIA). The CIA maintains the following records:

AP1.1.1.1.7.1. Directorate of Operations (CIA-DO/IMS) maintains the Foreign Intelligence/Counterintelligence database. This database shall be checked for all aliens residing outside the United States requiring access to classified information (i.e., LAA). If the requester provides complete personal identifying information (Complete Name, Date of Birth, Place of Birth, and Citizenship), all alien co-subjects (on SSBIS) residing outside the United States are also checked. In addition, this database shall be queried on the Subject any time there is a counterintelligence

concern raised during the conduct of the personnel security investigation.

AP1.1.1.1.7.2. Office of Security (CIA-SEC) maintains information on present and former employees, including members of the Office of Strategic Services (OSS), and applicants for employment. These files shall be checked if subject has been an employee of the CIA or when other sources indicate that CIA may have pertinent information.

AP1.1.1.1.8. Military Personnel Record Center files are maintained by separate Departments of the Armed Forces, General Services Administration and the Reserve Records Centers. They consist of the Master Personnel Records of retired, separated, Reserve, and active duty members of the Armed Forces. These records shall be checked when the requester provides required identifying data indicating service during the last 5 years.

AP1.1.1.1.9. Treasury Department. The files of Treasury Department Agencies (Secret Service, Internal Revenue Service, and Bureau of Customs) will be checked only when available information indicates that an Agency of the Treasury Department may be reasonably expected to have pertinent information.

AP1.1.1.1.10. The files of other Agencies, such as the National Guard Bureau, the Defense Industrial Security Clearance Office (DISCO), etc., will be checked when pertinent to the purpose for which the investigation is being conducted.

AP1.1.1.2. Single Scope Background Investigation (SSBI): The following SSBI scope reflects the requirements of National Security Directive 63 (reference (rr)).

AP1.1.1.2.1. Scope: The period of investigation for an SSBI is the last ten (10) years or to age 18, whichever is the shorter period, provided that the investigation covers at least the last 2 full years of the subject's life. No investigation will be conducted for the period prior to an individual's 16th birthday. Emphasis shall be placed on peer coverage whenever interviews are held with personal sources in making education, employment, and reference (including developed) contact.

AP1.1.1.2.2. Expansion of Investigation. The investigation may be expanded as necessary, to resolve issues and/or address employment standards unique to individual agencies.

AP1.1.1.2.3. NAC. Checks on subject and spouse/cohabitant of investigative and criminal history files of the Federal Bureau of Investigation, including submission of fingerprint records on the subject, and such other national Agencies

(DCII, INS, OPM, CIA, etc.). In addition to conducting a NAC on the subject of the investigation, the following additional requirements apply.

AP1.1.1.2.3.1. A DCII, FBLID name check only and FBI/HQ check shall be conducted on subject's spouse or cohabitant. In addition, such other national agency checks as deemed appropriate based on information on the subject's PSQ shall be conducted.

AP1.1.1.2.3.2. A check of FBI/HQ files on members of subject's immediate family who are 18 years of age or older and who are non-U.S. citizens shall be conducted. As used throughout the Regulation, members of subject's immediate family include the following:

AP1.1.1.2.3.2.1. Current spouse.

AP1.1.1.2.3.2.2. Adult children, 18 years of age or older, by birth, adoption, or marriage.

AP1.1.1.2.3.2.3. Natural, adopted, foster, or stepparents.

AP1.1.1.2.3.2.4. Guardians.

AP1.1.1.2.3.2.5. Brothers and sisters either by birth, adoption, or remarriage of either parent.

AP1.1.1.2.3.2.6. Cohabitant.

AP1.1.1.2.3.3. The files of CIA shall be reviewed on non-U.S. citizens of subject's immediate family who are 18 years of age or older.

AP1.1.1.2.3.4. I&NS files on members of subject's immediate family 18 years of age or older shall be reviewed when they are:

AP1.1.1.2.3.4.1. Non-U.S. citizens, or

AP1.1.1.2.3.4.2. Naturalized U.S. citizens whose naturalization has not been verified in a prior investigation, or

AP1.1.1.2.3.4.3. U.S. citizens born in a foreign country of American parent(s) or U.S. citizens who received derivative citizenship through the naturalization of one or both parents, provided that such citizenship has not been verified in a prior investigation.

AP1.1.1.2.4. Subject Interview. Required in all cases and shall be conducted by trained security, investigative, or counterintelligence personnel to ensure full investigative coverage. An additional personal interview shall be conducted when necessary to resolve any significant information and/or inconsistencies developed during the investigation. In Departments or Agencies with policies sanctioning the use of polygraph for personnel security purposes, the personal interview may include a polygraph examination, conducted by a qualified polygraph examiner;

AP1.1.1.2.5. Birth. Independent certification of date and place of birth received directly from appropriate registration authority if not otherwise verified under A1.1.1.2.6., below, or if a variance is developed.

AP1.1.1.2.6. Citizenship. Subject must be a U.S. citizen. Independent verification of citizenship received directly from appropriate registration authority. For foreign-born immediate family members 18 years of age or older, verification of citizenship or, legal status is also required. Subject's citizenship status must be verified in all cases. U.S. citizens who are subjects of investigation will be required to produce documentation that will confirm their citizenship. Normally such documentation should be presented to the DoD Component concerned prior to the initiation of the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that the designated authority in the DoD Component will be provided with the documentation prior to the issuance of a clearance. DIS will not check the BVS for native-born U.S. citizens except as indicated in AP1.1.1.2.5., above. In the case of foreign-born U.S. citizens, DIS will check I&NS records. The citizenship status of all foreign-born members of subject's immediate family shall be verified. Additionally, when the investigation indicates that a member of subject's immediate family has not obtained

U.S. citizenship after having been eligible for a considerable period of time, an attempt should be made to determine the reason. The documents listed below are acceptable for proof of U.S. citizenship for personnel security determination purposes:

AP1.1.1.2.6.1. A birth certificate must be presented if the individual was born in the United States. To be acceptable, the certificate must show that the birth record was filed shortly after birth and must be certified with the registrar's signature and the raised, impressed, or multicolored seal of his office except for States or jurisdictions which, as a matter of policy, do not issue certificates with a raised or impressed seal. Uncertified copies of birth certificates are not acceptable.

AP1.1.1.2.6.1.1. A delayed birth certificate (a record filed more than one year after the date of birth) is acceptable provided that it shows that the report of birth was supported by acceptable secondary evidence of birth as described in subparagraph A1.1.1.2.6.1.2., below.

AP1.1.1.2.6.1.2. If such primary evidence is not obtainable, a notice from the registrar stating that no birth record exists should be submitted. The notice shall be accompanied by the best combination of secondary evidence obtainable. Such evidence may include a baptismal certificate, a certificate of circumcision, a hospital birth record, affidavits of persons having personal knowledge of the facts of the birth, or other documentary evidence such as early census, school, or family bible records, newspaper files and insurance papers. Secondary evidence should have been created as close to the time of birth as possible.

AP1.1.1.2.6.1.3. All documents submitted as evidence of birth in the United States shall be original or certified documents. Uncertified copies are not acceptable.

AP1.1.1.2.6.2. A certificate of naturalization shall be submitted if the individual claims citizenship by naturalization.

AP1.1.1.2.6.3. A certificate of citizenship issued by the I&NS shall be submitted if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

AP1.1.1.2.6.4. A "Report of Birth Abroad of A Citizen of The United States of American" (Form FS-240), a "Certification of Birth" (Form FS-545 or DS-1350), or a "Certificate of Citizenship" is acceptable if citizenship was acquired by birth abroad to a U.S. citizen parent or parents.

AP1.1.1.2.6.5. A passport or one in which the individual was included

will be accepted as proof of citizenship.

AP1.1.1.2.7. Education: Independent verification of most recent or most significant claimed attendance and/or degree/diploma within the scope of investigation via sealed transcript received directly from the institution. If all education is outside of the investigative scope, the last education above high school level will be verified.

AP1.1.1.2.8. Employment: Direct verification through records of all periods of employment within scope but in any event the most recent two (2) years. Personal interviews of two sources (supervisor/coworkers) for each employment of six months or more shall be attempted. In the event that no employment exceeds six months, interviews of supervisor/coworkers shall be attempted. All periods of unemployment in excess of sixty (60) days shall be verified through records and/or sources. All prior Federal/Military service and type of discharge(s) shall be verified.

AP1.1.1.2.8.1. Non-Federal Employment. Verify all employment within the period of investigation to include seasonal, holiday, Christmas, part-time, and temporary employment. Interview one supervisor and one coworker at subject's current place of employment as well as at each prior place of employment during the past 10 years of six months duration or longer. The interview requirement for supervisors and coworkers does not apply to seasonal, holiday, Christmas, part-time, and temporary employment (4 months or less) unless there are unfavorable issues to resolve or the letter of inquiry provides insufficient information.

AP1.1.1.2.8.2. Federal Employment. All Federal employment will be verified within the period of investigation to include Christmas, seasonal temporary, summer hire, part-time, and holiday employment. Do not verify Federal employment through review of records if already verified by the requester. If Federal employment has not been verified by the requester, then subject's personnel file at his/her current place of employment will be reviewed. All previous Federal employment will be verified during this review. In the case of former Federal employees, records shall be examined at the Federal Records Center in St. Louis, Missouri. Interview one supervisor and one coworker at all places of employment during the past 10 years if so employed for 6 months or more.

AP1.1.1.2.8.3. Military Employment. Military service for the last 10 years shall be verified. The subject's duty station, for the purpose of interview coverage, is considered as a place of employment. One supervisor and one coworker shall be interviewed at subject's current duty station if subject has been stationed there for 6 months or more; additionally, a supervisor and a co-worker at subject's prior duty stations where assigned for 6 months or more during the past 5 years shall be

interviewed. Do not verify military employment through review of local records if already verified by the requester.

AP1.1.1.2.8.4. Unemployment. Subject's activities during all periods of unemployment in excess of 60 consecutive days, within the period of investigation, that are not otherwise accounted for shall be determined.

AP1.1.1.2.8.5. When an individual has resided outside the United States continuously for over one year, attempts will be made to confirm overseas employments as well as conduct required interviews of a supervisor and co-worker.

AP1.1.1.2.9. References: Four required (at least three of which are developed). To the extent practical, all should have social knowledge of subject and collectively span the entire scope of the investigation. As appropriate, additional interviews may include cohabitants(s), ex-spouses, and relative(s). Interviews with psychological/medical personnel are to be accomplished as required to resolve issues. Three developed character references who have sufficient knowledge of subject to comment on his background, suitability, and loyalty shall be interviewed. Efforts shall be made to interview developed references whose combined association with subject covers the full period of the investigation with particular emphasis on the last 5 years. Employment, education, and neighborhood references, in addition to the required ones, may be used as developed references provided that they have personal knowledge concerning the individual's character, discretion, and loyalty. A listed character reference will be interviewed only when developed references are not available or when it is necessary to identify and locate additional developed character references or when it is necessary to verify subject's activities (e.g., unemployment).

AP1.1.1.2.10. Neighborhood: Interviews with neighbors for the last five years if residence exceeds six months. Confirmation of current residence shall be accomplished regardless of length to include review of rental records if necessary. In the event no residence exceeds six months, interview of neighbors should be undertaken at current residence. During each neighborhood investigation, interview two neighbors who can verify subject's period of residence in that area and who were sufficiently acquainted to comment on subject's suitability for a position of trust. Neighborhood investigations will be expanded beyond this 5-year period only when there is unfavorable information to resolve in the investigation. Neighborhood investigations are not required outside the United States and Puerto Rico.

AP1.1.1.2.11. Credit: Verification of the subject s financial status and credit habits at all locations where subject has resided, been employed, or attended school for six months or more for the last seven (7) years. Conduct credit bureau

check in the 50 States, the District of Columbia, Puerto Rico and overseas (where APO/FPO addresses are provided) at all places where subject has resided (including duty stations and home ports), been employed, or attended school for 6 months or more, on a cumulative basis, during the last 7 years or during the period of the investigation, whichever is shorter. Financial responsibility, including unexplained affluence, will be stressed in all reference interviews.

AP1.1.1.2.12. Local Agency Checks: A check of appropriate police records, including state central criminal history record repositories, covering all locations where subject has resided, been employed, or attended school for six months or more during the scope of investigation, to include current residence regardless of duration. In the event that no residence, employment, or education exceeds six months, local agency checks should be conducted at the current residence, current employment, and last educational institution attended.

AP1.1.1.2.13. Foreign Travel. If subject has been employed, educated, traveled or resided outside of the United States for more than 90 days during the period of investigation, except under the auspices of the U.S. Government, additional record checks during the NAC shall be made in accordance with paragraph A1.1.1.2.6.of this Appendix. In addition, the following requirements apply:

AP1.1.1.2.13.1. Foreign travel not under the auspices of the U.S. Government. When employment education, or residence has occurred overseas for more than 90 days during the past 10 years or since age 18, which was not under the auspices of the U.S. Government, a check of records will be made at the Passport Office of the Department of State and other appropriate Agencies. Efforts shall be made to develop sources, generally in the United States, who knew the individual overseas to cover significant employment, education, or residence and to determine whether the individual has worked or lived outside of the United States continuously for over one year, the investigation will be expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

AP1.1.1.2.13.2. Foreign travel under the auspices of the U.S. Government. When employment, education, or residence has occurred overseas for a period of more than one year, under the auspices of the U.S. Government, a record check will be made at the Passport Office of the Department of State and other appropriate Agencies. Efforts shall be made to develop sources (generally in the United States) who knew the individual overseas to cover significant employment, education, or residence and to determine whether any lasting foreign contacts or connections were established during this period. Additionally, the investigation will be

expanded to cover fully this period through the use of such investigative assets and checks of record sources as may be available to the U.S. Government in the foreign country in which the individual resided.

AP1.1.1.2.14. Foreign Connections. All foreign connections (friends, relatives, and/or business connections) of subject and immediate family in the United States or abroad, except where such association was the direct result of subject's official duties with the U.S. Government, shall be ascertained. Investigation shall be directed toward determining the significance of foreign connections of the part of subject and the immediate family, particularly where the association is or has been with persons whose origin was within a country whose national interests are inimical to those of the United States

AP1.1.1.2.15. Organizations. Efforts will be made during reference interviews and record reviews to determine if subject and/or the immediate family has, or formerly had, membership in, affiliation with, sympathetic association towards, or participated in any foreign or domestic organization, association, movement, group, or combination of persons of the type described in paragraphs C2.2.1.1. through C2.2.1.4. of this Regulation.

AP1.1.1.2.16. Military Service. All Military Service and types of discharge during the last 10 years shall be verified.

AP1.1.1.2.17. Medical Records. Medical records shall not be reviewed unless:

AP1.1.1.2.17.1. The requester indicates that subject's medical records were unavailable for review prior to submitting the request for investigation, or

AP1.1.1.2.17.2. The requester indicates that unfavorable information is contained in subject's medical records, or

AP1.1.1.2.17.3. The subject lists one or more of the following on the PSQ:

AP1.1.1.2.17.3.1. A history of mental or nervous disorders.

AP1.1.1.2.17.3.2. That subject is now or has been addicted to the use of habit-forming drugs such as narcotics or barbiturates or is now or has been a chronic user to excess of alcoholic beverages.

AP1.1.1.2.18. Public Records: Verification of divorce(s), bankruptcy,

etc., and any other court (civil or criminal) actions to which subject has been or is a party within the scope of investigation, when known or developed. Divorces, annulments, and legal separations of subject shall be verified only when there is reason to believe that the grounds for the action could reflect on subject's suitability for a position of trust.

AP1.1.1.2.19. Ex-spouse Interview. If the subject of investigation is divorced, the ex-spouse will be interviewed when the date of final divorce action is within the scope of investigation.

AP1.1.1.2.20. Polygraph: Agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary.

AP1.1.1.2.21. Select Scoping. When the facts of the case warrant, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

AP1.1.1.2.22. Transferability: Investigations satisfying the scope and standards specified above are transferable between Agencies and shall be deemed to meet the investigative standards for access to Collateral TOP SECRET/National Security Information and Sensitive Compartmented Information. No further investigation or reinvestigation prior to revalidation every five years will be undertaken unless the Agency has substantial information indicting that the transferring individual may not satisfy eligibility standards for clearance or the Agency head determines in writing that to accept the investigation would not be in the national security interest of the United States.

AP1.1.1.2.23. Updating a Previous Investigation to SSBI Standards. If a previous investigation does not substantially meet the minimum standards of an SSBI or if it is more than 5 years old, a current investigation is required but may be limited to that necessary to bring the individual's file up to date in accordance with the investigative requirements of an SSBI. Should new information be developed during the current investigation that bears unfavorably upon the individual's activities covered by the previous investigation, the current inquiries shall be expanded as necessary to develop full details of this new information.

AP1.1.1.3. Periodic Reinvestigation (PR)

AP1.1.1.3.1. Each DoD military, civilian, consultant, and contractor employee occupying a critical sensitive position or possessing a TOP SECRET

clearance, or occupying a special access program position and non-U.S. citizens (foreign nationals and/or immigrant aliens) holding a limited access authorization shall be the subject of a PR initiated 5 years from the date of completion of the last investigation. The PR shall cover the period of the last 5 years.

AP1.1.1.3.2. Minimum Investigative Requirements. A PR shall include the following minimum scope.

AP1.1.1.3.2.1. NAC. A valid NAC on the SUBJECT will be conducted in all cases (NOTE: only a name check of the FBIJID will be conducted unless records indicate that a technical fingerprint check was not done previously). Checks of DCII, FBI/HQ, FBMD name check only, and other Agencies deemed appropriate, will be conducted on the Subject's current spouse or cohabitant, if not previously conducted. Additionally, NACs will be conducted on immediate family members, 18 years of age or older, who are non-U.S. citizens, if not previously accomplished.

AP1.1.1.3.2.2. Credit. Credit bureau checks covering all places where the SUBJECT resided for 6 months or more, on a cumulative basis, during the period of investigation, in the 50 States, District of Columbia, Puerto Rico and overseas (where APO/FPO addresses are provided), will be conducted.

AP1.1.1.3.2.3. Subject Interview. The interview should cover the entire period of time since the last investigation, not just the last 5-year period. Significant information disclosed during the interview, which has been satisfactorily covered during a previous investigation, should not be explored again unless additional relevant information warrants further coverage.

AP1.1.1.3.2.4. Employment. Current employment will be verified. Military and Fderal service records will not routinely be checked, if previously checked by the requester when the PR was originally submitted. Also, employment records will be checked wherever employment interviews are conducted.

Records need be checked only when they are locally available, unless unfavorable information had been detected.

AP1.1.1.3.2.5. Employment References. Two supervisors or coworkers at the most recent place of employment or duty station of 6 months; if the current employment is less than 6 months employment reference interviews will be conducted at the next prior place of employment, which was at least a 6-month duration.

AP1.1.1.3.2.6. Developed Character References (DCRs). Two developed character references who are knowledgeable of the SUBJECT will be interviewed. Developed character references who were previously interviewed will only be reinterviewed when other developed references are not available.

AP1.1.1.3.2.7. Local Agency Checks (LACs). DIS will conduct local agency checks on the SUBJECT at all places of residence, employment, and education during the period of investigation, regardless of duration, including overseas locations (except overseas locations from which military members have transferred).

AP1.1.1.3.2.8. Neighborhood Investigation. Conduct a neighborhood investigation to verify subject's current residence in the United States. Two neighbors who can verify subject's period of residence in that area and who are sufficiently acquainted to comment on the subject's suitability for a position of trust will be interviewed. Neighborhood investigations will be expanded beyond the current residence when unfavorable information arises.

AP1.1.1.3.2.9. Ex-Spouse Interview. If the subject of investigation is divorced, the ex-spouse will be interviewed when the date of final divorce action is within the period of investigation.

AP1.1.1.3.2.10. Polygraph: Agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary.

AP1.1.1.3.2.11. Select Scoping. When the facts of the case warrant, additional select scoping will be accomplished, as necessary, to fully develop or resolve an issue.

AP1.1.1.4. Secret Periodic Reinvestigation (S-PR)

AP1.1.1.4.1. Each DoD military, civilian, consultant, and contractor employee with current access to SECRET information shall be the subject of a S-PR initiated 10 years from the date of completion of the last investigation. The PR shall

cover the period of the last 5 years.

AP1.1.1.4.2. Minimum Investigative Requirements. The S-PR shall include the following minimum scope.

AP1.1.1.4.2.1. NAC. A NAC with a name check of the FBI Identification Division, a check of the FBI Investigative Files, as well as other Agencies' indices, e.g., DoD, OPM, CIA, State, INS, etc., as appropriate. (NOTE: A technical fingerprint check of the FBI Identification Division will be conducted vice a name check if one was not done previously);

AP1.1.1.4.2.2. Credit. Conduct credit bureau checks at all locations where subject has resided, been employed, or attended an institution of higher Teaming for a period of six months or more during the period of coverage;

AP1.1.1.4.2.3. The investigation may be expanded as necessary to fully develop or resolve an issue.

AP2. APPENDIX 2

REQUEST PROCEDURES

AP2.1. GENERAL

To conserve investigative resources and to insure that personnel security investigations are limited to those essential to current operations and are clearly authorized by DoD policies, organizations requesting investigation must assure that continuing command attention is given to the investigative request process.

In this connection, it is particularly important that the provision of Executive Order 12356 (reference (j)) requiring strict limitations on the dissemination of official information and material be closely adhered to and limited to those that investigations requested for issuing clearances are instances in which an individual has a clear need for access to classified information. Similarly, investigations required to determine eligibility for appointment or retention in the Department of Defense, in either a civilian or military capacity, must not be requested in frequency or scope exceeding that provided for in this Regulation.

In view of the foregoing, the following guidelines have been-developed to simplify and facilitate the investigative request process:

AP2.1.1. Limit requests for investigation to those-that are essential to current operations and clearly authorized by DoD policies and attempt to utilize individuals who, under the provisions of this Regulation, have already met the security standard;

AP2.1.2. Assure that military personnel on whom investigative requests are initiated will have sufficient time remaining in service after completion of the investigation to warrant conducting it;

AP2.1.3. Insure that request forms and prescribed documentation are properly executed in accordance with instructions;

AP2.1.4. Dispatch the request directly to the DIS Personnel Investigations Center;

AP2.1.5. Promptly notify the DIS Personnel Investigations Center if the investigation is no longer needed (notify OPM if a NACI is no longer needed); and

AP2.1.6. Limit access through strict need-to-know, thereby requiring fewer investigations.

In summary, close observance of the above-cited guidelines will allow the DIS to operate more efficiently and permit more effective, timely, and responsive service in accomplishing investigations.

AP2.2. NATIONAL AGENCY CHECK (NAC)

When a NAC is requested an original only of the DD Form 398-2 (National Agency Check Request) and a completed YD 258 (Applicant Fingerprint Card) are required. If the request is for an ENTNA.NC, an original only of the DD Form 398-2 and a completed DD Form 2280 (Armed Forces Fingerprint Card) are required. Those forms should be sent directly to:

Personnel Investigation Center
Defense Investigative Service
P.O. Box 1083
Baltimore, Maryland 21203

AP2.3. NATIONAL AGENCY CHECK PLUS WRITTEN INQUIRIES (NACI)

When a NACI is requested, an original and one copy of the SF 85 (Data for Nonsensitive or Noncritical-sensitive Position), an SF 171 (Personal Qualifications Statement), and an SF 87 (U.S. Civil Service Commission Fingerprint Chart) shall be sent directly to:

Office of Personnel Management
Bureau of Personnel Investigations
NACI Center
Boyers, Pennsylvania 16018

The notation "ALL REFERENCES" shall be stamped immediately above the title at the top of the Standard Form 85.

AP2.4. DoD NATIONAL AGENCY CHECK WITH INQUIRIES (DNACI)

AP2.4.1. When a DNACI is requested, one copy of DD Form 1879, an original and two copies of the DD Form 398-2 (National Agency Check Request), two copies of FD 258 (Fingerprint Card), and an original of DD Form 2221 (Authority for Release of Information and Records) shall be sent directly to:

Personnel Investigations Center
Defense Investigative Service
P.O. Box 1083
Baltimore, Maryland 21203

AP2.4.2. The DD Form 398-2 must be completed to cover the most recent five year period. All information, to include items relative to residences and employment, must be complete and accurate to avoid delays in processing.

AP2.5. SPECIAL BACKGROUND INVESTIGATION (SBI)/BACKGROUND INVESTIGATION (BI)

AP2.5.1. When requesting a BI or SBI, one copy of DD Form 1879 (Request for Personnel Security Investigation), an original and four copies of DD Form 398 (Statement of Personnel History), two copies of YD 258, and an original of DD Form 2221 Authority for Release of Information and Records) shall be sent directly to the:

Personnel Investigations Center
Defense Investigative Service
P.O. Box 454
Baltimore, Maryland 21203

AP2.5.2. For the BI and SBI, the DD Form 398 must be completed to cover the most recent five and 15 year period, respectively, or since the 18th birthday, which ever is shorter.

AP2.6. PERIODIC REINVESTIGATION (PR)

AP2.6.1. PRs shall be requested only in such cases as are authorized by paragraphs C3.7.1. through C3.7.11. of this Regulation.

AP2.6.1.1. For a PR requested in accordance with paragraph C3.7.1. and C3.7.11., the DD Form 1879 must be accompanied by the following documents:

AP2.6.1.1.1. Original and four copies of DD Form 398.

AP2.6.1.1.2. Two copies of FD-258.

AP2.6.1.1.3. Original copy of DD Form 2221

AP2.6.1.2. In processing PRs, previous investigative reports will not be requested by the requesting organization, unless significant derogatory or adverse information, postdating the most recent favorable adjudication, is developed during the course of reviewing other locally available records. In the latter instance, requests for previous investigative reports may only be made if it is determined by the requesting organization that the derogatory information is so significant that a review of previous investigative reports is necessary for current adjudicative determinations.

AP2.6.2. No abbreviated version of DD Form 398 may be submitted in connection with a PR.

AP2.6.3. The PR request shall be sent to the address in paragraph AP2.5.1., above.

AP2.7. ADDITIONAL INVESTIGATION TO RESOLVE DEROGATORY OR ADVERSE INFORMAITON

AP2.7.1. Requests for additional investigation-required to resolve derogatory or adverse information shall be submitted by DD Form 1879 (Request for Personnel Security Investigation) to the:

Defense Investigative Service
P.O. Box 454
Baltimore, Maryland 21203

Such requests shall set forth the basis for the additional investigation and describe the specific matter to be substantiated or disproved.

AP2.7.2. The request should be accompanied by an original and four copies of the DD Form 398, where appropriate, two copies of FD-258 and an original copy of DD Form 2221, unless such documentation was submitted within the last 12 months to DIS as part of a NAC or other personnel security investigation. If pertinent, the results of a

recently completed NAC, NACI, or other related investigative reports available should also accompany the request.

AP2.8. OBTAINING RESULTS OF PRIOR INVESTIGATIONS

Requesters requiring verification of a specified type of personnel security investigation, and/or requiring copies of prior investigations conducted by the DIS shall submit requests by letter or message to:

Defense Investigative Service Investigative Files Division
P.O. Box 1211
Baltimore, Maryland 21203

Message Address: DIS PIC BALTIMORE MD/ /D0640

The request will include subject's name, grade, social security number, date and place of birth, and DIS case control number, if known.

AP2.9. REQUESTING POST-ADJUDICATION

AP2.9.1. Requests pertaining to issues arising after adjudication of an investigation (post-adjudication cases) shall be addressed to DIS on a DD Form 1879 accompanied by a DD Form 398, where appropriate.

AP2.9.2. All requests for initial investigations will be submitted to PIC regardless of their urgency. If, however, there is an urgent need for a post-adjudication investigation, or the mailing of a request to PIC for initiation of a post-adjudication case would prejudice timely pursuit of investigative action, the DD Form 1879 may be directed for initiation, in CONUS, to the nearest DIS Field Office, and in overseas locations, to the military investigative service element supporting the requester (Appendix 9). The field element (either DIS or the military investigative agency) will subsequently forward either the DD Form 1879 or completed investigation to PIC.

AP2.9.3. A fully executed DD Form 1879 and appropriate supporting documents may not be immediately available. Further, a case that is based on sensitive security issues may be compromised by a request that the subject submit a DD Form 398. A brief explanation should appear on DD Form 1879s, which does not include complete supporting documentation.

AP2.10. REQUESTS INVOLVING CONTRACTOR EMPLOYEES

To preclude duplicative investigative requests and double handling of contractor employee cases involving access to classified information, all requests for investigation of contractor personnel must be submitted, using authorized industrial security clearance forms, for processing through the Defense Industrial Security Clearance Office, except for programs in which specific approval has been obtained from the Deputy Under Secretary of Defense for Policy to utilize other procedures.

AP2.11. RESPONSIBILITIES FOR PROPER DOCUMENTATION OF REQUESTS

The official signing the request for investigation shall be responsible for insuring that all documentation is completed in accordance with these instructions.

AP3. APPENDIX 3

TABLES FOR REQUESTING INVESTIGATIONS
GUIDE FOR REQUESTING BACKGROUND INVESTIGATIONS (BI)

TABLE 1

A	B	C
If the individual is a:	and duties require:	then a BI is required before:
U.S. national military member, civilian, consultant, or contractor employee	Top Secret clearance	granting final clearance
U.S. national civilian employee	assignment to a "Critical" sensitive position	assignment to the position
U.S. national military member, DoD civilian or contractor employee	occupying a "critical" position in the Nuclear Weapon Personnel Reliability Program (PRP) (reference (s))	occupying a "critical" position
U.S. national military member or civilian employee	granting, denying clearances	performing clearance functions
U.S. national military member or civilian employee	membership on security screening, hearing, or review board	appointment to the board
immigrant alien	limited access to Secret or Confidential information	issuing limited access authorization (Note 1)
non-U.S. national employee excluding immigrant alien	limited access to Secret or Confidential information	issuing limited access authorization
non-U.S. national employee for military education and orientation program (from a country listed at Appendix 7)	education and orientation of military personnel	before performing duties

NOTE 1 - will cover a 10-year scope.

TABLE 1 (continued)

If the individual is a:.	and duties require:	then a BI is required before:
U.S. national military member, DoD civilian or contractor employee	assignment to a category two Presidential Support position	assignment
U.S. national military member, DoD civilian or contractor employee assigned to NATO	access to NATO COSMIC information	access may be granted

TABLE 2
GUIDE FOR REQUESTING SPECIAL BACKGROUND INVESTIGATIONS (SBI)

A	B	C
If the individual is a:	and duties require:	then a SBI is required before:
U.S. national military member, DoD civilian, consultant, or contractor employee	access to SCI	granting access
	assignment to a category one Presidential Support position	assignment
	access to SIOP-ESI	granting access
	assignment to the National Security Agency	assignment
	access to other Special Access programs approved under paragraph C3.5.7.	granting access
	assignment to personnel security, counterintelligence, or criminal investigative or direct investigative support duties	assignment

TABLE 3
GUIDE FOR REQUESTING PERIODIC REINVESTIGATIONS (PR)

A	B	C
If the individual is a:	and duties require:	then a PR is required:
U.S. national military member, DoD civilian, consultant, or contractor employee	access to SCI	5 years from date of last SBI/BI or PR
	Top Secret Clearance	5 years from date of last SBI/BI or PR
	access to NATO COSMIC	5 years from date of last SBI/BI or PR
	assignment to Presidential Support activities	5 years from date of last SBI/BI or PR
U.S. national civilian employee	assignment to a "Critical" sensitive position	5 years from last SBI/BI or PR
Non-U.S. national employee	current limited access authorization to Secret or Confidential information	5 years from last SBI/BI or PR

TABLE 4

GUIDE FOR REQUESTING DoD NATIONAL AGENCY CHECK WITH INQUIRIES (DNACI) OR NACI

A	B	C
If the individual is a:	and duties require:	Then DNACI/NACI is required:
U.S. national military member or contractor employee	Secret clearance	before granting clearance (note 1)
	Interim Secret Clearance	may be automatically issued (note 2)
U.S. national civilian employee or consultant	Secret clearance	before granting clearance
	Interim Secret Clearance	may be automatically issued (note 3)
	Appointment to "Non Critical" sensitive position	before appointment
U.S. national military member, DoD civilian or contractor employee	occupying a "controlled" position in the Nuclear Weapon PRP (reference (s))	before assignment
applicant for appointment as a commissioned officer	commission in the Armed Forces	before appointment (after appointment for health professionals, chaplains, and attorneys, under conditions authorized by paragraph C3.3.4. of this Regulation)

TABLE 4 (continued)

A	B	C
If the individual is a:	and duties require:	then a DNACI/NACI is required:
Naval Academy Midshipman, Military Academy Cadet, or Air Force Academy Cadet	enrollment	to be initiated 90 days after entry
Reserve Officer Training Corps Cadet or Midshipman	entry to advanced course or College Scholarship Program	then a DNACI is required to be initiated 90 days after entry

NOTE 1 - First-term enlistees shall require an ENTNAC.

NOTE 2 - Provided DD Form 398-2 is favorably reviewed, local records check favorably accomplished, and DNACI initiated.

NOTE 3 - Provided an authority designated in Appendix 5 finds delay in such appointment would be harmful to national security; favorable review of DD Form 398-2; NACI initiated; favorable local records check accomplished.

TABLE 5
GUIDE FOR REQUESTING NATIONAL AGENCY CHECKS (NAC)

A	B	C
If the individual is a:	and duties require:	then a NAC is required:
a first-term enlistee	retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT three (3) work days after entry (note 1)
prior service member reentering military service after break in Federal employment exceeding 1 year	Retention in the Armed Forces (including National Guard and Reserve)	to be initiated NLT three (3) work days after reentry
nominee for military education and orientation program	education and orientation of military personnel	before performing duties (note 2)
U.S. national military, DoD civilian, or contractor employee	access to restricted areas, sensitive information, or equipment as defined in paragraph C3.6.2.	before authorizing entry
nonappropriated fund instrumentality (NAFI) civilian employee (reference (u))	appointment as NAFI custodian	before appointment
	accountability for nonappropriated funds	before completion of probationary period
	fiscal responsibility as determined by NAFI custodian	before completion of probationary period
	other "positions of trust"	before appointment
Persons requiring access to chemical agents chemical agents	access to or security of chemical agents	before appointment

NOTE: 1 - Request ENTNAC only.

NOTE: 2 - Except where personnel whose country of origin is a country listed at Appendix 7, a BI will be required (See paragraph C3.6.12.).

TABLE 5 (continued)

A	B	C
If the individual is a:	and duties require:	then a NAC is required:
U.S. national, civilian employee nominee for customs inspection duties	waiver under provisions of paragraph C3.6.4.	before appointment (note 3)
Red Cross/United Services Organization personnel	assignment with the Armed Forces overseas	before assignment (see note 4 for foreign national personnel)
U.S. national	DoD building pass	prior to issuance
Foreign national employed overseas	no access to classified information	prior to employment (note 4)

NOTE: 3 - A NAC not over 5 years old suffices unless there has been a break in employment over 12 months. Then a current NAC is required.

NOTE: 4 - In such cases, the NAC shall consist of: (a) Host government law enforcement and security agency record checks at the city, state (province), and national level, and (b) DCII.

AP4. APPENDIX 4

REPORTING OF NONDEROGATORY CASES

AP4.1.1. Background Investigation (BI) and Special Background Investigation (SBI) shall be considered as devoid of significant adverse information unless they contain information listed below:

AP4.1.1.1. Incidents, infractions, offenses, charges, citations, arrests, suspicion or allegations of illegal use or abuse of drugs or alcohol, theft or dishonesty, unreliability, irresponsibility, immaturity, instability or recklessness, the use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions.

AP4.1.1.2. All indications of moral turpitude, heterosexual promiscuity, aberrant, deviant, or bizarre sexual conduct or behavior, transvestitism, transsexualism, indecent exposure, rape, contributing to the delinquency of a minor, child molestation, wife-swapping, window-peeping, and similar situations from whatever source. Unlisted full-time employment or education; full-time education or employment that cannot be verified by any reference or record source or that contains indications of falsified education or employment experience. Records or testimony of employment, education, or military service where the individual was involved in serious offenses or incidents that would reflect adversely on the honesty, reliability, trustworthiness, or stability of the individual.

AP4.1.1.3. Foreign travel, education, visits, correspondence, relatives, or contact with persons from or living in a foreign country of foreign intelligence service.

AP4.1.1.4. Mental, nervous, emotional, psychological, psychiatric, or character disorders/behavior or treatment reported or alleged from any source.

AP4.1.1.5. Excessive indebtedness, bad checks, financial difficulties or irresponsibility, unexplained affluence, bankruptcy, or evidence of living beyond the individual's means.

AP4.1.1.6. Any other significant information relating to the criteria included in C2.2.1.1. through C2.2.1.17. or Appendix 8 of this Regulation.

AP5. APPENDIX 5

DoD SECURITY CLEARANCE AND/OR SCI ACCESS DETERMINATION AUTHORITIES

AP5.1. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE PERSONNEL SECURITY CLEARANCES (TOP SECRET, SECRET, AND CONFIDENTIAL)

AP5.1.1. Secretary of Defense and/or single designee.

AP5.1.2. Secretary of the Army and/or single designee. [1]

AP5.1.3. Secretary of the Navy and/or single designee. [1]

AP5.1.4. Secretary of the Air Force and/or single designee. [1]

AP5.1.5. Chairman of the Joint Chiefs of Staff and/or single designee.

AP5.1.6. Director, Washington Headquarters Services, and/or single designee.

AP5.1.7. Director, National Security Agency, and/or single designee. [1, 2]

AP5.1.8. Director, Defense Intelligence Agency, and/or single designee. [1]

AP5.1.9. Deputy General Counsel, Legal Counsel, OGC, and/or single designee (for contractors under the Defense Industrial Security Program (DISP))

AP5.1.10. Director, Defense Investigative Service, and/or single designee, (may grant security clearances only for contractor personnel under the DISP)

---

[1] Authority to grant, deny or revoke access to SCI is a function of the Senior Officials of the Intelligence Community (SOIC), or their designated representative, as identified in E.O. 12333 (reference (h)) and Director of Central Intelligence Directive (DCID) 1/14 (reference (l)). The authority for making SCI access determinations may also be the same official making security clearance determinations.

[2] Reference to the Director, NSA or single designee is not intended to infringe upon the authorities or responsibilities contained in DoD Directive 5210.45, "Personnel Security in the National Security Agency," reference (i).

AP5.2. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE LAA

Officials listed in subsection AP5.1.1. through AP5.1.10., above, and the Commanders of the Combatant Commands, or their single designee, (must be at general officer, flag rank or civilian equivalent).

AP5.3. OFFICIALS AUTHORIZED TO CERTIFY PERSONNEL UNDER THEIR JURISDICTION FOR ACCESS TO CRITICAL NUCLEAR WEAPON DESIGN INFORMATION

See enclosure to DoD Directive 5210.2 (reference (z)).

AP5.4. OFFICIAL AUTHORIZED TO APPROVE PERSONNEL FOR ASSIGNMENT TO PRESIDENTIAL SUPPORT ACTIVITIES

The Executive Secretary to the Secretary of Defense and the Deputy Secretary of Defense, or designee.

AP5.5. OFFICIALS AUTHORIZED TO GRANT ACCESS TO SIOP-ESI

AP5.5.1. Director of Strategic Target Planning

AP5.5.2. Director, Joint Staff.

AP5.5.3. Chief of Staff, U.S. Army.

AP5.5.4. Chief of Naval Operations.

AP5.5.5. Chief of Staff, U.S. Air Force.

AP5.5.6. Commandant of the Marine Corps.

AP5.5.7. Commanders of the Combatant Commands.

AP5.5.8. The authority may be further delegated in writing by the officials in subsections AP5.5.1. through AP5.5.7. to the applicable subordinates.

AP5.6. FINAL DETERMINATIONS

Three member PSAB shall be formed under the auspices of the following officials to render final determinations when an unfavorable personnel security determination is appealed under paragraph C8.2.2.4. of this Regulation.

AP5.6.1. Secretary of the Army.

AP5.6.2. Secretary of the Air Force.

AP5.6.3. Secretary of the Navy.

AP5.6.4. Chairman of the Joint Chiefs of Staff.

AP5.6.5. Director, NSA.

AP5.6.6. Director, DIA.

AP5.6.7. Director, WHS.

AP5.6.8. General Counsel, Department of Defense (contractors only).

AP5.7. OFFICIALS AUTHORIZED TO SUSPEND ACCESS TO CLASSIFIED INFORMATION

AP5.7.1. Security Clearances

AP5.7.1.1. Contractor Personnel. The Director, Counterintelligence and Security Programs; ODASD(I&S); OASD(C3I); and the Deputy General Counsel (Legal Counsel), Office of General Counsel, OSD.

AP5.7.1.2. Military and/or Civilian Personnel. Commander and/or Agency head, Head of the Component, or adjudicative authority.

AP5.7.2. SCI. Cognizant SOICs, or their designees.

AP5.8. OFFICIALS AUTHORIZED TO ISSUE INTERIM CLEARANCES

AP5.8.1. Interim TOP SECRET clearances may be issued by the officials listed in section AP5.1., above. That may be further delegated on determination by the Head of the Agency.

AP5.8.2. Interim SECRET and/or CONFIDENTIAL clearances may be issued by the officials listed in section AP5.1., above, as well as by organizational commanders.

AP5.9. OFFICIALS AUTHORIZED TO DESIGNATE NONAPPROPRIATED FUND POSITIONS OF TRUST

The Heads of the DoD Components, or their designees.

AP6. APPENDIX 6

GUIDELINES FOR CONDUCTING PRE-NOMINATION PERSONAL INTERVIEWS

AP6.1. PURPOSE

The purpose of the personal interview is to assist in determining the acceptability of an individual for nomination and further processing for a position requiring an SBI.

AP6.2. SCOPE

Questions asked during the course of a personal interview must have a relevance to a security determination. Care must be taken not to inject improper matters into the personal interview. For example, religious beliefs and affiliations, beliefs and opinions regarding racial matters, political beliefs and affiliations of a nonsubversive nature, opinions regarding the constitutionality of legislative policies, and affiliations with labor unions and fraternal organizations are not proper subjects for inquiry. Department of Defense representatives conducting personal interviews should always be prepared to explain the relevance of their inquiries. Adverse inferences shall not be drawn from the refusal of a person to answer questions the relevance of which has not been established.

AP6.3. THE INTERVIEWER

Except as prescribed in section AP6.2., above, persons conducting personal interviews normally will have broad latitude in performing this essential and important function and, therefore, a high premium must necessarily be placed upon the exercise of good judgment and common sense. To insure that personal interviews are conducted in a manner that does not violate lawful civil and private rights or discourage lawful political activity in any of its forms, or intimidate free expression, it is necessary that interviewers have a keen and well-developed awareness of and respect for the rights of interviewees. Interviewers shall never offer an opinion as to the relevance or significance of information provided by the interviewee to eligibility for access to SCI. If explanation in this regard is required, the interviewer will indicate that the sole function of the interview is to obtain information and that the determination of relevance or significance to the individual's eligibility will be made by other designated officials.

AP6.4. INTERVIEW PROCEDURES

AP6.4.1. The Head of the DoD Component concerned shall establish uniform procedures for conducting the interview that are designed to elicit information relevant to making a determination of whether the interviewee, on the basis of the interview and other locally available information (DD 398, "Personnel Security Investigation Questionnaire," personnel records, security file, etc.), is considered acceptable for nomination and further processing.

AP6.4.2. Such procedures shall be structured to insure the interviewee his full rights under the Constitution of the United States, the Privacy Act of 1974 (reference (m)), and other applicable statutes and regulations.

AP6.5. PROTECTION OF INTERVIEW RESULTS

All information developed during the course of the interview shall be maintained in personnel security channels and made available only to those authorities who have a need-to-know in connection with the processing of an individual's nomination for duties requiring access to SCI or those who need access to information either to conduct the required SBI or to adjudicate the matter of the interviewee's eligibility for access to SCI, or as otherwise authorized by Executive order or statute.

AP6.6. ACCEPTABILITY DETERMINATION

AP6.6.1. The determination of the interviewee's acceptability for nomination for duties requiring access to sensitive information shall be made by the commander, or designee, of the DoD organization that is considering nominating the interviewee for such duties.

AP6.6.2. Criteria guidelines contained in DCID 1/14 (reference (l)), upon which the acceptability for nomination determination is to be based shall be provided to commanders of DoD organizations who may nominate individuals for access to SCI and shall be consistent with those established by the Senior Officer of the Intelligence Community of the Component concerned with respect to acceptability for nomination to duties requiring access to SCI.

AP7. APPENDIX 7

(RESERVED FOR FUTURE USE)

AP8. APPENDIX 8

ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMAITON

PURPOSE

The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs, and are to be used by Government Departments and Agencies in all final clearance determinations.

ADJUDICATIVE PROCESS

The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole person concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- The nature, extent, and seriousness of the conduct.
- The circumstances surrounding the conduct, to include knowledgeable participation.
- The frequency and recency of the conduct.
- The individual's age and maturity at the time of the conduct.
- The voluntariness of participation.
- The presence or absence of rehabilitation and other pertinent behavioral changes.
- The motivation for the conduct.
- The potential for pressure, coercion, exploitation, or duress.
- The likelihood of continuation or recurrence.

Each case must be judged on its own merits and final determination remains the responsibility of the specific Department or Agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security and considered final.

The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following:

A. Allegiance to the United States
B. Foreign influence
C. Foreign preference
D. Sexual behavior
E. Personal conduct
F. Financial considerations
G. Alcohol consumption
H. Drug involvement
I. Emotional, mental, and personality disorders
J. Criminal conduct
K. Security violations
L. Outside activities
M. Misuse of Information Technology Systems

Each of the foregoing should be evaluated in the context of the whole person.

Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior.

However, notwithstanding the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(1) voluntarily reported the information;
(2) sought assistance and followed professional guidance, where appropriate;
(3) resolved or appears likely to favorably resolve the security concern;
(4) has demonstrated positive changes in behavior and employment;
(5) should have his or her access temporarily suspended pending final adjudication of the information.

If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

The information in bold print at the beginning of each adjudicative guideline provides a brief explanation of its relevance in determining whether it is clearly consistent with the interest of national security to grant or continue a persons eligibility for access to classified information.

ADJUDICATIVE GUIDELINES

ALLEGIENCE TO THE UNITED STATES

An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

Conditions that could raise a security concern and may be disqualifying include:

(1) involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

(2) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

(3) association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any State or subdivision, by force or violence or by other unconstitutional means;

(4) involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State.

Conditions that could mitigate security concerns include:

(1) the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

(2) the individual's involvement was only with the lawful or humanitarian aspects of such an organization;

(3) involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

(4) the person has had no recent proscribed involvement or association with such activities.

FOREIGN INFLUENCE

A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are: (1) not citizens of the United States or (2) may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Conditions that could raise a security concern and may be disqualifying include:

(1) an immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

(2) sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

(3) relatives, cohabitants, or associates who are connected with any foreign government;

(4) failing to report, where required, associations with foreign nationals;

(5) unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

(6) conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

(7) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

(8) a substantial financial interest in a country, or in any foreign-owned or operated business that could make the individual vulnerable to foreign influence.

Conditions that could mitigate security concerns include:

(1) a determination that the immediate family member(s), cohabitant, or associate(s) in question would not constitute an unacceptable security risk;

(2) contacts with foreign citizens are the result of official U.S. Government business;

(3) contact and correspondence with foreign citizens are casual and infrequent;

(4) the individual has promptly reported to proper authorities all contacts, requests, or threats from persons or organizations from a foreign country, as required;

(5) foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

FOREIGN PREFERENCE

When an individual acts m such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

Conditions that could raise a security concern and may be disqualifying include:

(1) the exercise of dual citizenship;
(2) possession and/or use of a foreign passport;
(3) military service or a willingness to bear arms for a foreign country;
(4) accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;
(5) residence in a foreign country to meet citizenship requirements;
(6) using foreign citizenship to protect financial or business interests in another country;
(7) seeking or holding political office in the foreign country;
(8) voting in foreign elections; and
(9) performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

Conditions that could mitigate security concerns include:

(1) dual citizenship is based solely on parents' citizenship or birth in a foreign country;

(2) indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

(3) activity is sanctioned by the United States;

(4) individual has expressed a willingness to renounce dual citizenship.

SEXUAL BEHAVIOR

Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, subjects the individual to undue influence or coercion, or reflects lack of judgment or discretion.[1] (Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.)

Conditions that could raise a security concern and may be disqualifying include:

(1) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(2) compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;

(3) sexual behavior that causes an individual to be vulnerable to undue influence or coercion;

(4) sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

Conditions that could mitigate security concerns include:

(1) the behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

(2) the behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

(3) there is no other evidence of questionable judgment, irresponsibility, or emotional instability;

(4) the behavior no longer serves as a basis for undue influence or coercion.

---

[1] The adjudicator should also consider guidelines pertaining to criminal conduct (criterion J); or emotional, mental, and personality disorders (criterion I), in determining how to resolve the security concerns raised by sexual behavior.

PERSONAL CONDUCT

Conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(1) refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

(2) refusal to complete required security forms, releases, or provide full, frank and true answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

Conditions that could raise a security concern and may be disqualifying also include:

(1) reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

(2) the deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(3) deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

(4) personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or pressure;

(5) a pattern of dishonesty or rule violations[2];

(6) association with persons involved in criminal activity.

Conditions that could mitigate security concerns include:

(1) the information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

(2) the falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

(3) the individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

(4) omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

(5) the individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or pressure;

(6) a refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;

(7) association with persons involved in criminal activities has ceased.

---

[2] To include violation of any written or recorded agreement made between the individual and the Agency.

FINANCIAL CONSIDERATIONS

An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Conditions that could raise a security concern and may be disqualifying include:

(1) a history of not meeting financial obligations;
(2) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filling deceptive loan statements, and other intentional financial breaches of trust;
(3) inability or unwillingness to satisfy debts;
(4) unexplained affluence;
(5) financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include:

(1) the behavior was not recent;
(2) it was an isolated incident;
(3) the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);
(4) the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;
(5) the affluence resulted from a legal source; and
(6) the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

ALCOHOL CONSUMPTION

Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

Conditions that could raise a security concern and may be disqualifying include:

(1) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other incidents related to alcohol use;

(2) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

(3) diagnosis by a credentialed medical professional[3] of alcohol abuse or alcohol dependence;

(4) habitual or binge consumption of alcohol to the point of impaired judgment;

(5) consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional[3] and following completion of an alcohol rehabilitation program

Conditions that could mitigate security concerns include:

(1) the alcohol related incidents do not indicate a pattern;

(2) the problem occurred a number of years ago and there is no indication of a recent problem;

(3) positive changes in behavior supportive of sobriety;

(4) following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional.[3]

---

[3] credentialed medical professional: licensed physician, licensed clinical psychologist, or board-certified psychiatrist.

DRUG INVOLVEMENT

Improper or illegal involvement with drugs, raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

Drugs are defined as mood and behavior altering:

(a) drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens) and

(b) inhalants and other similar substances.

Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Conditions that could raise a security concern and may be disqualifying include:

(1) any drug abuse (see above definition);

(2) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

(3) failure to successfully complete a drug treatment program prescribed by a credentialed medical professional.[3] Current drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will normally result in an unfavorable determination

Conditions that could mitigate security concerns include:

(1) the drug involvement was not recent;
(2) the drug involvement was an isolated or infrequent event;
(3) a demonstrated intent not to abuse any drugs in the future;
(4) satisfactory completion of a drug treatment program prescribed by a credentialed medical professional.[3]

---

[3] credentialed medical professional: licensed physician, licensed clinical psychologist, or board-certified psychiatrist.

EMOTIONAL, MENTAL, AND PERSONALITY DISORDERS

Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability.

When appropriate, a credentialed mental health professional,[4] acceptable to or approved by the Government, should be consulted so that potentially disqualifying and mitigating information may be fully and properly evaluated.

Conditions that could raise a security concern and may be disqualifying include:

(1) a diagnosis by a credentialed mental health professional [4] that the individual has a disorder that could result in a defect in psychological, social, or occupational functioning;

(2) information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a diagnosed disorder, e.g., failure to take prescribed medication;

(3) a pattern of high-risk, irresponsible, aggressive, anti-social, or emotionally unstable behavior;

(4) information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

Conditions that could mitigate security concerns include:

(1) there is no indication of a current problem;

(2) recent diagnosis by a credentialed mental health professional[4] that an individual's previous emotional, mental, or personality disorder is cured or in remission and has a low probability of recurrence or exacerbation;

(3) the past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

---

[4] credentialed mental health professional: licensed clinical psychologist, licensed social worker, or board-certified psychiatrist.

CRIMINAL CONDUCT

A history or pattern of criminal activity creates doubt about a persons judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying include:

(1) any conduct, regardless of whether the person was formally charged;
(2) a single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

(1) the behavior was not recent;
(2) the crime was an isolated incident;
(3) the person was pressured or coerced into committing the act and those pressures are no longer present in that persons life;
(4) the person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;
(5) there is clear evidence of successful rehabilitation.

SECURITY VIOLATIONS

Noncompliance with security regulations raises doubt about an individual's trustworthiness, and ability to safeguard classified information.

Conditions that could raise a security concern and may be disqualifying include:

(1) unauthorized disclosure of classified information;
(2) violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

(1) were inadvertent;
(2) were isolated or infrequent;
(3) were due to improper or inadequate training;
(4) demonstrate a positive attitude towards the discharge of security responsibilities.

OUTSIDE ACTITIVITIES

Involvement in certain types of outside employment or activities is of security concern if it poses conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Conditions that could raise a security concern and may be disqualifying include:

Any service, whether compensated, volunteer, or employment with:

(1) a foreign country;
(2) any foreign national;
(3) a representative of any foreign interest;
(4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Conditions that could mitigate security concerns include:

(1) evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;
(2) the individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

Information Technology Systems include all related equipment used for the communication, mission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying include:

(1) Illegal or unauthorized entry into any information technology system;
(2) Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;
(3) Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;
(4) Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

Conditions that could mitigate security concerns include:

(1) The misuse was not recent or significant;
(2) The conduct was unintentional or inadvertent;
(3) The introduction or removal of media was authorized;
(4) The misuse was an isolated event;
(5) The misuse was followed immediately by a prompt, good faith effort to correct the situation.

AP9. APPENDIX 9

OVERSEAS INVESTIGATIONS

AP9.1. PURPOSE

The purpose of this appendix is to establish, within the framework of this Regulation, DoD Directive 5105.42, and Defense Investigative Service Manual 20-1-M (references (hh) and (ii)), standardized procedures for the military investigative agencies to follow when they perform administrative and investigative functions on behalf of DIS at overseas locations.

AP9.2. TYPE INVESTIGATION

This Regulation describes in detail Background Investigations (BI) which are conducted for Limited Access Authorizations (LAA) and those Special Investigative Inquiries (SII) conducted for post-adjudicative purposes. Hereafter they are referred to as LAA and post-adjudicative cases and are briefly described in paragraphs AP9.2.1. and AP9.2.2., below:

AP9.2.1. Limited Access Authorization (LAA). A level of access to classified defense information that may be granted to a non-US citizen under certain conditions, one of which is that a BI must have been completed with satisfactory results. Paragraph C3.4.4. further describes LAA cases.

AP9.2.2. Post-Adjudication Investigation. A Personnel Security Investigation (PSI) predicated on new, adverse or questionable security, suitability or hostage information that arises and requires the application of investigation procedures subsequent to adjudicative action on a DoD-affiliated person's eligibility for continued access to classified information, assignment to or retention in sensitive duties or other designated duties requiring such investigation. While these cases are normally predicated on the surfacing of unfavorable information subsequent to favorable adjudication, they may also be opened when favorable information is offered to counter a previous unfavorable adjudication. Paragraph C2.4.3.3. further describes these cases.

AP9.3. GENERAL

AP9.3.1. As a rule, investigative activity in most PSIs occurs in the United States even when the Subject is at an overseas location. Therefore, the submission of requests for investigation to the Personnel Investigation Center (PIC) at Baltimore is a required procedure as it ensures uniform application of DoD PSI policy and the efficient dispatch and coordination of leads.

AP9.3.2. When the purpose of the investigation is for an LAA or post-adjudication on a Subject overseas, much, if not all of the leads are at an overseas location. While these cases also may be submitted directly to PIC for action, there is an inherent delay in the mailing of the request, the exchange of leads and reports with PIC, and transmittal of the reports back to the requestor. To avoid this delay, the military investigative agencies, when acting for DIS overseas in accordance with DoD Directive 5105.42 (reference (hh) may, with their Headquarters approval, accept these requests for investigations, initiate them and disseminate the results from the same level as they open, close, and disseminate their own cases. Usually this will greatly improve response time to the requester.

AP9.3.3. Under the procedures in paragraph AP9.3.2., above, DIS will not often be in a position to directly exercise its responsibility for control and direction until the case or lead is in progress or even completed; therefore, adherence to the policy stated in referenced documents, and as modified herein, is mandatory. When the policy of the military investigative agency is at variance with the above, the matter will be referred to the respective headquarters for resolution.

AP9.3.4. Since DIS is ultimately responsible for the personnel security product, it must be kept informed of all such matters referred to in this appendix. For instance, when the investigative agency overseas receives a DD Form 1879, "Request for Personnel Security Investigation," which sets forth an issue outside DIS jurisdiction, it will reject the request, inform the requester of the reason and furnish an information copy of the DD Form 1879 and rejection letter to PIC. When the issue/jurisdiction is unclear to the investigative agency, the DD Form 1879 and the perceived jurisdictional question should be promptly forwarded to DIS for action and, if appropriate, to the Component' s headquarters for information. Questions on the interpretation of DIS or DoD policy and Directives pertaining to individual PSI cases can usually be resolved through direct communications with PIC.

AP9.3.5. DoD Directive 5105.42 (reference (hh)), establishes the supporting relationship of the military investigative agencies to DIS in overseas areas, and DIS provides these Agencies with copies of relevant policy and interpretive guidance. For

these reasons, the investigative agency vice the requester, is responsible for evaluating the request, processing it, collecting and evaluating the results within their jurisdiction for sufficiency, and forwarding the completed product to the appropriate activity.

AP9.3.6. The magnitude of operations at PIC requires that methods of handling LAA and post-adjudicative cases be consistent to the maximum extent possible. For this reason, the procedures for LAA cases are nearly identical to those for post-adjudicative cases. Briefly, the main exceptions are:

AP9.3.6.1. The notification to PIC that a post-adjudication case has been opened will be by message, since an issue is present at the outset, whereas notification of an LAA case should normally be by mail.

AP9.3.6.2. The scope of the LAA investigation is 10 years or since the person's 18th birthday, whichever is shortest, whereas the leads in a post-adjudication case are limited to resolving the issue.

AP9.4. JURISDICTION

AP9.4.1. As set-forth in DoD Directive 5105.42 (reference (hh), DIS is responsible for conducting all DoD PSIs in the 50 States, District of Columbia, and Puerto Rico, and will request the Military Departments to accomplish investigative requirements elsewhere. The military investigative agencies in overseas locations routinely respond to personnel security investigative leads for DIS.

AP9.4.2. DIS jurisdiction also includes investigation of subversive affiliations, suitability information, and hostage situations when such inquiries are required for personnel security purposes; however, jurisdiction will rest with the military investigative agencies, FBI and/or civil authorities as appropriate when the alleged subversion or suitability issue represents a violation of law or, in the case of a hostage situation, there is an indication that the person concerned is actually being pressured, coerced, or influenced by interests inimical to the United States, or that hostile intelligence is taking action specifically directed against that person. Specific policy guidance on the applicability of these procedures and the jurisdictional considerations are stated in C2.4.

AP9.5. CASE OPENING

AP9.5.1. A request for investigation must be submitted by using DD Form 1879 and accompanied by supporting documentation unless such documentation is not immediately available, or the obtaining of documentation would compromise a sensitive investigation. Upon receipt of the request, the military investigative component will identify the issue(s), scope the leads, and ensure that the proposed action is that which is authorized for DIS as delineated in this Regulation, DoD Directive 5105.42 and Defense Investigative Service 20-1-M (references (hh) and (ii)).

AP9.5.2. Upon such determination, the Component will prepare an Action Lead Sheet (ALS), which fully identifies the Subject and the scope of the case, and specifies precisely the leads that each investigative Component (including DIS/PIC when appropriate) is to conduct.

AP9.5.3. Case opening procedures described above are identical for LAA and post-adjudication cases except with respect to notification of case opening to PIC:

AP9.5.3.1. Post-Adjudication Cases. These cases, because they involve an issue, are potentially sensitive and must be examined as early as possible by PIC for conformity to the latest DoD policy. Accordingly, the initial notification to PIC of case openings will always be by message. The message will contain at a minimum:

AP9.5.3.1.1. Full identification of the subject;

AP9.5.3.1.2. A narrative describing the allegation/facts in sufficient detail to support opening of the case; and

AP9.5.3.1.3. A brief listing of the leads that are planned. The DD Form 1879 and supporting documents, along with the Agency's ALS, should be subsequently mailed to PIC.

AP9.5.3.2. LAA Cases. The notification to PIC of case opening will normally be accomplished by mailing the DD Form 1879, DD Form 398, "Personal History Statement," a copy of the ALS, and any other supporting documents to PIC. Message notification to PIC in LAA cases will only be required if there is a security or suitability issue apparent in the DD Form 1879 or supporting documents.

AP9.5.4. Beyond initial actions necessary to test allegation for investigative merit and jurisdiction, no further investigative action should commence until the notification of case opening to PIC has been dispatched.

AP9.5.5. PIC will promptly respond to the notification of case opening by mail or message specifying any qualifying remarks along with a summary of previously existing data. PIC will also provide a DIS case control number (CCN). This number must be used by all Components on all case-related paperwork/reports.

(The investigating agency may assign its unique Service CCN for interim internal control; however, the case will be processed, referenced, and entered into the DCII by the DIS case control number.) The first five digits of the DIS CCN will be the Julian date of the case opening when received at DIS.

AP9.6. CASE PROCESSING

AP9.6.1. The expected completion time for leads in LAA cases is 50 calendar days and for post-adjudication cases, 30 days, as computed from the date of receipt of the request. If conditions preclude completion in this time period, a pending report of the results to date, along with an estimated date of completion will be submitted to PIC.

AP9.6.2. Copies of all ALSs will be furnished to PIC. In addition, PIC will be promptly notified of any significant change in the scope of the case, or the development of an investigative issue.

AP9.6.3. The procedures for implementing the Privacy Act in PSI cases are set in DIS 20-1-M (reference (ii)). Any other restrictions on the release of information imposed by an overseas source or by regulations of the country where the inquiry takes place will be clearly stated in the report.

AP9.6.4. The report format for these cases will be that used by the military investigative agency.

AP9.6.5. Investigative action outside the jurisdictional area of an investigative component office may be directed elsewhere by ALS as needed in accordance with that Agency's procedures and within the following geographical considerations:

AP9.6.5.1. Leads will be sent to PIC if the investigative action is in the United States, District of Columbia, Puerto Rico, American Samoa, Bahama Islands, the U.S. Virgin Islands, and the following islands in the Pacific: Wake, Midway, Kwajalin, Johnston, Carolines, Marshalls, and Eniwetok.

AP9.6.5.2. Leads to areas not listed above may be dispatched to other units of the investigative agency or even to another military agency's field units if there is an

agreement or memorandum of understanding that provides for such action. For case accountability purposes, copies of such "lateral" leads must be sent to the PIC.

AP9.6.5.3. Leads that cannot be dispatched as described in subparagraph AP9.6.5.2., above, and those that must be sent to a non-DoD investigative agency should be sent to PIC for disposition.

AP9.6.6. The Defense Investigative Manual (reference (ii)) calls for obtaining PIC approval before conducting a Subject interview on a post-adjudicative investigation. To avoid the delay that compliance with this procedure would create, a military investigative component may conduct the interview provided:

AP9.6.6.1. All other investigative leads have been completed and reviewed.

AP9.6.6.2. The CCN has been received, signifying DIS concurrence with the appropriateness of the investigation.

AP9.6.6.3. Contrary instructions have not been received from the PIC.

AP9.6.6.4. The interview is limited to the resolution of the relevant issues disclosed by the investigation.

AP9.6.7. Notwithstanding the provisions of paragraph AP9.6.1. through AP9.6.4., above, if time is of the essence due to imminent transfer of the subject, a subject interview may be conducted at the discretion of the investigative agency.

AP9.7. CASE RESPONSIBILITY: LAA and PA

Section AP9.3., above, describes the advantages of timely handling that accrue when the military investigative components act for DIS overseas. These actions for DIS may, however, be limited by the Component's staffing and resource limitations, especially since some cases require more administration and management than others. Post-adjudication case leads, for instance, will normally be within the geographical jurisdiction of the Component that accepted the request for investigation; therefore, relatively little case management is required. In contrast, LAA cases may require leads world-wide, and, therefore, create more complex case management and administration, especially in the tracking, monitoring and reviewing of leads outside the Component's geographical area. Accordingly, an investigative Component will accept the case from the requester, but only assign itself the appropriate leads within its own geographical jurisdiction and send the balance to PIC for appropriate disposition in accordance with the following:

AP9.7.1. The investigative agency will accept the request for investigation (thereby saving time otherwise lost in mailing to PIC) but limit its involvement in case management by extracting only those leads it will conduct or manage locally.

AP9.7.2. The Agency should then prepare an ALS that shows clearly what leads it will cover and send PIC a copy of this ALS, along with the request for investigation and any other appropriate documentation. It must be clear in the ALS that PIC is to act on all those leads that the unit has not assigned to itself.

AP9.7.3. PIC, as case manager, will assume responsibility for the complete investigative package and, upon receipt of the last lead, will send the results to the appropriate activity.

AP9.7.4. The Agency that accepted the case and assigned itself leads may send a copy of its report to the activity in the "Results to" block at the same time it sends the originals to PIC. If so, the letter of transmittal must inform the recipient that these reports are only a portion of the investigation, and that the balance will be forthcoming from PIC. Similarly, PIC must be informed of which investigative reports were disseminated. (This is normally done by sending PIC a copy of the letter of transmittal.)

AP9.8. SCOPE

AP9.8.1. LAA. The scope of investigation is 10 years or from age 18, whichever is the shortest period.

AP9.8.2. Post-Adjudication Cases. There is no standard scope. The inquiries conducted will be limited to those necessary to resolve the issue(s).

AP9.9. CASE CLOSING: LAA and PA

AP9.9.1. Whether the investigative Component or PIC closes out an investigation, there are three key elements to consider:

AP9.9.1.1. The investigative results must be reviewed for quality and conformance to policy.

AP9.9.1.2. The results must be sent to the activity listed in the "Results to" block of the DD Form 1879.

AP9.9.1.3. PIC must be informed whether or not any dissemination was made

by the investigative agency and, if so, what reports were furnished.

AP9.9.2. Investigative results may also be sent to a requester or higher level activity that makes a statement of need for the results. In such instances, a copy of the letter requesting the results and the corresponding letter of transmittal must be sent to PIC for retention.

AP9.9.3. When an investigative agency disseminates reports for PIC, it may use the transmittal documents, letters, or cover sheets it customarily uses for its own cases.

AP9.9.4. The material that is to be provided to PIC will consist of: The originals of all reports, and all other case documentation such as original statements, confidential source sheets, interview logs, requests for investigation, letters of transmittal to adjudicaters/requesters, or communications with the requester, such as those that modify the scope of the investigation.

AP9.9.5. For DIS to fulfill its responsibilities under DoD 5220.22-R (reference (a)) and the Privacy Act of 1974 (reference (m)), all inquires conducted in its behalf must be set forth in an ROI for the permanent file, whether the case is completed, terminated early or referred to another Agency.

AP9.10. REFERRAL

A case may require premature closing at any time after receipt of the DD Form 1879 by the investigative Component if the information accompanying the request, or that which is later developed, is outside DIS jurisdiction. For example, alleged violations of law, a counterintelligence matter, or actual coercion/influence in a hostage situation (see paragraph AP9.4.2., above) must be referred to the appropriate Agency, and DIS involvement terminated. The requester will be informed by letter or endorsement to the DD Form 1879 of the information developed that, due to jurisdictional consideration, the case was referred to (fill in appropriate address) and that the DIS case is closed. The Agency to which referral was made and PIC will be furnished with the results of all investigations conducted under DIS auspices. DIS, however, has an interest in the referral Agency's actions and no information should be solicited from that Agency.

AP10. APPENDIX 10

ADP POSITION CATEGORIES AND CRITERIA FOR DESIGNATING POSITIONS

AP10.1. ADP POSITION CATEGORIES AND CRITERIA FOR DESIGNATING POSITIONS

OMB Circular A-71 (and Transmittal Memo #1), July 1978; OMB Circular A-130, December 12, 1985; and FPM Letter 732, November 14, 1978, contain the criteria for designating positions under the existing categories used in the personnel security program for Federal civilian employees as well as the criteria for designating ADP and ADP-related positions. This policy is outlined below:

AP10.2. ADP POSITION CATEGORIES

AP10.2.1. Critical-Sensitive Positions

AP10.2.1.1. ADP-I positions. Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

AP10.2.2. Noncritical-Sensitive Positions

AP10.2.2.1. ADP-II positions. Those positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to insure the integrity of the system.

AP10.2.3. Nonsensitive Positions

AP10.2.3.1. ADP-III positions. All other positions involved in computer activities. In establishing the categories of positions, other factors may enter into the determination, permitting placement in higher or lower categories based on the Agency's judgement as to the unique characteristics of the system or the safeguards protecting the system.

AP10.3. CRITERIA FOR DESIGNATING POSITIONS

Three categories have been established for designating computer and computer-related positions -- ADP-I, ADP-II, and ADP-III. Specific criteria for assigning positions to one of these categories is as follows:

Category	Criteria
ADP-I	Responsibility or the development and administration of Agency computer security programs, and also including direction and control of risk analysis and/or threat assessment.
	Significant involvement in life-critical or mission-critical systems.
	Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
	Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lesser amounts if.the activities of the individual are not subject to technical review by higher authority in the ADP-I category to insure the integrity of the system.
	Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
	Other positions as designated by the Agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.
ADP-II	Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP-I category, includes, but is not limited to:
	(1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;
	(2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year. Other positions are designated by the Agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP-I positions.
ADP-III	All other positions involved in Federal computer activities.

AP11. APPENDIX 11

LIST OF SAMPLE NOTIFICATIONS

Initial Package to Notify Organization and Individual

Package to Inform Organization and Individual of Denial

Local Organization Letter with Statement of Reasons (SOR)

From: Director, (Component) Central Adjudication Facility
To: Director, Service Graphics Facility, Washington, DC

Subject: RESPONSIBILITY FOR HANDLING STATEMENT OF REASONS (SOR)

Reference: (a) (Component Personnel Security Regulation)

Enclosure: 1. SOR
2. SOR Receipt and Statement of Intention
3. Form for Requesting (Personnel Security Investigation)

1. The purpose of this letter is to provide instructions for actions required by your organization related to the individual named in the enclosed SOR. Since denial or revocation of access eligibility can have a severe impact on individuals and their careers, procedures required by reference (a) must be closely followed to ensure that both security and fairness requirements are met.

2. Your organization is responsible for completing the following actions with regard to the individual named in the SOR:

a. Consider whether or not to suspend access to classified information and assignment of the individual to nonsensitive duties pending a final personnel security decision. Failure to do so could result in an increased level of security risk.

b. Designate a person from your organization as the point of contact (POC) in this matter pursuant to paragraph 8-201(a), reference (a), above. This person will serve as a liaison between the (Component) Central Adjudication Facility (CAF) and the individual.

3. The POC from your organization should:

a. Promptly deliver enclosure (1) to this letter, the SOR and its enclosures, to the named individual.

b. Complete and forward enclosure (2) to this letter to the CAF within 10 calendar days. Ensure that Parts I, II, and III are all completed. This form notifies the CAF whether the individual intends to respond to the SOR and whether your organization has granted a time extension.

c. Advise the individual that he or she should not attempt to communicate directly with the CAF except in writing, and that, if necessary, he or she should seek the assistance of your organization's designated POC. Also, ensure that the individual understands that he or she is entitled to obtain legal counsel or other assistance but that this must be done at the individual's own expense.

d. Ensure that the individual understands the consequences of being found ineligible for access to classified information and performance of sensitive duties and the serious effect such a determination could have on his or her career.

e. Take particular care to ensure that the individual fully understands that the proposed denial or revocation action will become final if your organization notifies the CAF via enclosure (2) that the individual does not intend to respond to the SOR. Ensure that the individual understands that failure to submit a timely reply will result in forfeiture of any further opportunity to contest this unfavorable personnel security determination.

f. Explain procedures for requesting a time extension for responding to the SOR. If the individual requires additional time to obtain copies of investigative records and/or to prepare his or her response, your organization may grant an extension of up to 30 additional calendar days. The CAF must be notified of such an extension using enclosure (2). See reference (a) for more detail.

g. Assist the individual in obtaining applicable references and copies of pertinent investigative files. The SOR is usually based on investigative information from the Defense Investigative Service (DIS) and/or another investigative agency. If the individual desires copies of releasable information pertinent to this SOR, a request may be submitted to the CAF using the receipt at enclosure (2). If the individual wants to obtain a copy of the complete investigative file, provide him or her with enclosure (3) which is the form for requesting [DIS and/or other investigative agency] records under the Privacy Act (5 U.S.C. 552a.).

4. Ensure that the individual's response to the SOR is promptly endorsed by appropriate authority and immediately forwarded to the CAF. Submissions to the CAF are deemed to have been made when actually received by the CAF, or postmarked, whichever is sooner. This endorsement should include observations and comments regarding the person's judgment, reliability and trustworthiness as well as a recommendation regarding the decision at hand. An endorsement that does not include comments and a recommendation will be taken to mean that your organization concurs with the unfavorable personnel security determination.

5. (Additional component-specific requirements)

6. If you have any questions, the point of contact at the CAF is Mr. John Doe, DSN 000-0000 or commercial (000) 000-0000, e-mail doejohn@caf.dod.

Statement of Reasons (SOR)

From: Director, [Component] Central Adjudication Facility
Through: Director, Service Graphics Facility, Washington, DC
To: Mr. John Doe, SSN 000-00-0000

Subject: INTENT TO (DENY/REVOKE) ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT IN SENSITIVE DUTIES

Reference: (a) Component Personnel Security Regulation

Enclosure: 1. Security Concerns and Supporting Adverse Information
2. Instructions for Responding to a Statement of Reasons
3. Applicable Personnel Security Guidelines

1. A preliminary decision has been made to (deny/revoke) your eligibility for access to classified information or employment in sensitive duties. Adverse information from an investigation of your personal history has led to the security concerns listed in enclosure (1) and has raised questions about your trustworthiness, reliability, and judgment. If this preliminary decision becomes final, you will not be eligible for access to classified information or employment in sensitive duties as defined by reference (a).

2. You may challenge this preliminary decision by responding, in writing, with any information or explanation which you think should be considered in reaching a final decision. Enclosure (2) is provided to assist you if you choose to respond. Enclosure (3) provides an extract from reference (a) of the specific personnel security guidelines used in the preliminary decision to (deny/revoke) your eligibility for access to classified information employment in sensitive duties. The preliminary decision will become final if you fail to respond to this letter. You may obtain legal counsel or other assistance; however, you must do so at your own expense.

3. You must notify your (Component) Central Adjudication Facility (CAF) via the head of your organization within 10 calendar days as to whether or not you intend to respond. If you choose not to respond, you will forfeit an opportunity to contest this unfavorable personnel security determination. Should you choose to respond, your response must be submitted via the head of your organization within 30 calendar days from the date you received this letter. Your organization may grant up to 30 additional calendar days if you submit a written request to your security office. Additional time extensions may only be granted by the CAF. Contact the point of contact with the CAF for help in preparing and forwarding your notice of an intent to respond and your response and if you wish to obtain releasable investigative records used in your case.

4. If you currently have access to classified information, this access (is/may be) suspended pending the final decision. Please direct questions regarding this letter to your security officer or the point of contact with the CAF.

Security Concerns and Supporting Adverse Information

Subject of Investigation: (Mr. John Doe, 000-00-0000)

Statement of Reasons

1. Available information tends to show criminal or dishonest conduct on your part:

   a. You were arrested on 28 March 1985 in Arlington, VA, for assault on a police officer. You were found guilty and fined $4,000.

   b. You were arrested on 10 January 1993 in Fairfax, VA, and charged with interfering with an arrest. You were released on $300 bail which you forfeited for failure to appear.

   c. You were arrested on 22 June 1994 in Fairfax, VA, on a bench warrant and charged with failure to appear (as set forth above). You were found guilty of interfering with an arrest on 10 January 1993 (as set forth above) and fined $400. The charge of failure to appear was dismissed.

2. Available information tends to show financial irresponsibility on your part:

   a. You filed for Bankruptcy under Chapter 7 in the U.S. District Court, Washington, DC on 10 August 1987. You were discharged from debts

   b. A judgment was entered against you for $2,500 on 20 July 1992, in the Superior Court, Washington, DC. As of 30 January 1995, the judgment had not been paid.

   c. As of 20 July 1994, your credit account with the Hecht Company, Washington, DC was $350 overdue and referred for collection.

   d. As of 20 July 1994, your credit account with J.C. Penney Co., Arlington, VA, was $500 overdue and referred for collection.

Instructions for Responding to a Statement of Reasons (SOR)

A preliminary decision has been made to deny or revoke your eligibility for access to classified information or employment in sensitive duties. This preliminary decision will automatically become final if you fail to notify the Central Adjudication Facility (CAF) within 10 days that you intend to respond to the SOR. You will also lose your right to appeal that final decision if you do not submit a timely response. If this decision becomes final, you will not be eligible to handle classified information or perform sensitive duties. This could prevent you from continuing in your present position or pursuing your current career.

The SOR is based on adverse information revealed by an investigation into your personal history. Specific security concerns about your conduct or background, along with supporting adverse information, are listed in enclosure (1) to the Statement of Reasons.

These instructions are intended to help you provide the most accurate and relevant information as to why the preliminary decision should be overturned. However, it is only a guide. You should provide whatever information you think ought to be considered in reaching the final decision.

It is in your best interest to provide the most complete and accurate information possible at this stage in the decision-making process. Therefore, if you decide to challenge the preliminary decision, you must respond to the statement of reasons as completely as possible.

A. Before Responding

(1) Follow the instructions. The SOR and these instructions provide specific requirements and deadlines for compliance. You will forfeit your right to appeal if you fail to follow these instructions. You must notify the CAF via the point of contact (POC) within 10 calendar days as to whether or not you intend to respond. Should you choose to respond, your response must be submitted via the head of your organization within 30 calendar days from the date you received the SOR, unless you requested and were granted an extension of time.

(2) Review adverse information. You should carefully read the security concerns and supporting adverse information (enclosure 1) to the SOR to determine if the findings are accurate and whether there are circumstances that were not included and which might have a favorable bearing in your case. You may obtain relevant investigative or other information pertinent to the adverse information listed in enclosure (1) to the SOR. In addition, you may obtain a complete copy of releasable investigative records concerning your personal history under the provisions of the Privacy Act. Your security officer or point of contact with the CAF can help you obtain copies of these records. If you do submit a request for your investigative records, make sure to ask the POC for a time extension to the deadline for responding to the SOR since it may take up to 30 calendar days to receive these records.

(3) Obtain and organize supporting documents. Gather any documentation that supports your case. Documentation should be organized according to the security concerns presented in enclosure (1). The most useful documents will be those that refute, correct, explain, extenuate,

mitigate, or update the adverse information presented in enclosure (1). Examples of useful documentation include copies of correspondence; court records with details or dispositions of arrests and status of probation; receipts; copies of canceled checks or letter from creditors verifying the status of delinquent accounts; certificates of completion for rehabilitation programs; releases from judgment or attachment; transcripts of court testimony taken under oath; probation reports; copies of negotiated plea bargains; etc. Mere statements, such as "I paid those bills," "I didn't do it," or "It wasn't my fault," will not carry as much weight as supporting documentation. You may provide statements from co-workers, supervisors, your commander, friends, neighbors and others concerning your judgment, reliability and trustworthiness, and any other information that you think ought to be considered before a final decision is made.

(4). Seek assistance. An individual at your organization has been designated as a point of contact with the CAF on this matter. If this person cannot answer your questions, he or she can request assistance from higher authority. The process is designed so that individuals can represent themselves. Nonetheless, you may obtain legal counsel or other assistance in preparing your response. However, if you obtain assistance, it must be at your own expense.

Remember -- it is up to you to decide whether to respond. You are responsible for the substance of your response and it must be signed by you.

B. Writing a Response

(1) Your response should be in the form of a letter from you to the CAF. You should address each security concern separately. You should admit or deny each security concern and admit or deny each item of supporting adverse information.

(2) It is essential that you address each security concern and the adverse information cited to support it. Provide any information that explains, refutes, corrects, extenuates, mitigates or updates each security concern. Include, wherever possible, copies of the types of documents described above. Organize supporting documents in the order that they are referred to in your letter and enclose copies with your letter. Finally, be sure to sign and date your letter.

(3) The impact of your response will depend on the extent to which you can specifically refute, correct, extenuate, mitigate, or update security concerns and adverse information presented in enclosure (1). Information that is untrue should be specifically refuted. If you believe that the adverse information, though true, does not support the security concern or presents an incomplete picture, you should provide information that explains your case. This additional information could help you disprove or lessen the security concern.

(4) Personnel security guidelines are used by decision-makers to determine whether certain adverse information is of security concern. The guidelines pertinent to security concerns in your case are listed in enclosure (3) to the SOR. These guidelines are general rules used by decision-makers in determining whether an individual should be granted eligibility for access to classified information or permitted to perform sensitive duties. The guidelines provide a framework for weighing all available information, both favorable information as well as adverse information

that is of security concern. The guidelines help decision-makers make a common-sense determination concerning an individual's eligibility for access to classified information and performance of sensitive duties based upon all that is known about an individual's personal history.

(5) Place your written response and supporting documents in a single envelope or package and forward it to the CAF via the head of your organization. Your organization will add its comments at that time. An endorsement by your organization that does not include substantive comments and a recommendation will be interpreted to mean that your organization concurs with the SOR. Be sure to meet the time deadlines. You will be notified in writing of the final decision. In most cases this decision will be made within 60 days. If the decision is in your favor, your access eligibility will be granted or restored. If not, you may appeal the decision to a higher authority.

Applicable Personnel Security Guidelines

The relevant personnel security guidelines are listed below for each area of security concern in your case. The security concerns and supporting adverse information are provided in enclosure (1).

Security Concern: Available information tends to show criminal conduct on your part.

A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness. Conditions that signal security concern and may be disqualifying include: (1) any criminal conduct, regardless of whether the person was formally charged; (2) a single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include: (1) the criminal behavior was not recent; (2) the crime was an isolated incident; (3) the person was pressured or coerced into committing the act and those pressures are no longer present in that person's life; (4) the person did not intentionally commit the act and the factors leading to the unintentional violation are not likely to recur; (5) there is clear evidence of successful rehabilitation.

Security Concern: Available information tends to show financial irresponsibility or unexplained affluence on your part.

An individual who is financially overextended is at greater risk of having to choose between significantly reducing lifestyle or engaging in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts. Conditions that signal security concern and may be disqualifying include: (1) a history of not meeting financial obligations resulting in bankruptcy; (2) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust; (3) being unable to satisfy debts incurred to creditors; (4) unexplained affluence; (5) financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include: (1) the behavior was not recent; (2) it was an isolated incident; (3) the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation); (4) the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control; (5) the affluence resulted from a legal source; and (6) the individual initiated a good-faith effort to repay overdue creditors.

SOR Receipt and Statement of Intention

From: Director, Service Graphics Facility
To: Director, (Component) Central Adjudication Facility

Subject: Acknowledgment of Receipt for Statement of Reasons

1. I acknowledge receipt and delivery of your Statement of Reasons (SOR) to Mr. John Doe, SSN 000-00-0000. Parts I, II, III and IV of this form have been completed as requested.

PART I

I have received an SOR on this date from the (Component) Central Adjudication Facility.

_____

(Signature) (Date)

PART II

I intend to:

a. ( ) submit no reply to the SOR.

b. ( ) respond to the SOR but have requested an extensionfor the following reasons:

_____

_____

_____

_____

c. ( ) respond via my organization head within 30 calendar days of the date I acknowledged receipt of the SOR.

_____

_____

(Signature) (Date)

PART III

Check one of the following:

a. ( ) I request relevant copies of documents and records upon which the SOR is based;

b. ( ) I do not desire relevant copies of documents and records upon which the SOR is based.

PART IV

This organization

a. ( ) has not granted an extension.

B. ( ) has granted an extension until

_____

(Date)

Point of Contact:

_____

(Print Name) (Position)

Local Organization Letter with LOD

From: Director, (Component) Central Adjudication Facility
To: Director, Service Graphic Facility, Washington, DC

Subject: RESPONSIBILITIES FOR HANDLING LETTER OF (DENIAL/REVOCATION)

Enclosure: 1. Letter of Denial/Revocation (LOD)
2. LOD Receipt

1. A decision has been made by the Central Adjudication Facility (CAF) to (deny/revoke) the (security clearance, SCI access, employment in sensitive duties) of the individual named in the enclosed LOD. The purpose of this letter is to provide instructions for actions required by your organization.

2. If not already accomplished, your organization is responsible for completing the following actions with regard to the individual named in the LOD:

a. Terminate access to classified information and/or assignment to sensitive duties.

b. Designate a person from your organization as the point of contact in this matter.

3. Your point of contact (POC) on this matter should promptly deliver enclosure (1) to the named individual. Have the individual sign and date enclosure (2) upon receipt of the LOD. This signature verifies receipt of the LOD and should be retained by your organization until the final disposition of the appeal.

4. If the subject responded to the statement of reasons, your POC should:

a. Ensure the individual understands that he has 10 calendar days, from receipt of the LOD, to submit a notice of intent to appeal and to elect whether to appeal in writing to the Personnel Security Appeals Board (PSAB) or to appear in person before a Defense Office of Hearings and Appeals (DOHA) Administrative Judge (AJ). He must notify your organization of his intended action. Any extensions to this deadline must be submitted in writing to the PSAB.

b. Ensure that the individual understands that he may elect to appeal in writing directly to the PSAB or to request a personal appearance before a DOHA AJ. If the individual desires a personal appearance, the request must be in writing. It must be sent to DOHA within 10 calendar days of the individual's receipt of the LOD. If the individual desires to appeal in writing directly to the PSAB, it must be filed within 30 calendar days of receipt of the LOD. A form for the notice of intent to appeal has been provided as an enclosure to the LOD.

5. If the subject did not respond to the statement of reasons, your POC should inform the individual the decision is final and the appeal process is concluded. Exceptions may only be granted by the CAF.

6. If your organization or the named individual has any questions, the POC should communicate with the President, PSAB, at DSN 000-0000 or commercial 000-00-0000, or the Director, DOHA, at Autovon 226-4598 or commercial 703-696-4598.

Letter of Denial/Revocation(LOD)

From: Director (Component)Central Adjudication Facility
Through: Director, Service Graphic Facility, Washington, D.C.
To: Mr. John Doe, SSN 000-00-0000

Subject: FINAL (DENIAL/REVOCATION) OF ELIGIBILITY FOR ACCESS TO CLASSIFIED
INFORMATION OR (EMPLOYMENT IN SENSITIVE DUTIES)

Reference: (a) Our ltr (Ser XXX) of (date)
(b) Personnel Security Regulation
(c) Your ltr of (date)

Enclosure: 1. Notice of Intent to Appeal
2. Instructions for Appealing a Letter of (Denial/Revocation)

1. Reference (a) informed you of our intent to [deny/revoke] your eligibility for access to classified information (or employment in sensitive duties). An enclosure of this reference listed security concerns and supporting adverse information supporting this preliminary decision. The contents of your response have been carefully considered. Our final assessment of the security concerns presented in reference (a) is as follows:

a. Criminal conduct - The information you provided successfully mitigated the security concerns related to your arrest on 28 March 1985. However, you did not sufficiently address or provide any new information to explain or mitigate the other adverse information (items 1b and 1c). Your criminal conduct is still of security concern.

b. Financial irresponsibility - While you provided an explanation for the Superior Court Judgment, you did not sufficiently address or provide any new information to explain the other adverse information (items 2a, 2c and 2d). Your financial irresponsibility is still of security concern.

2. Given the remaining security concerns, effective this date, we have (denied/revoked) your eligibility for access to classified information and for assignment to a sensitive position using the provisions of reference (b).

3. You may appeal this letter of denial (LOD) in one of two ways: (1) by notifying the Personnel Security Appeal Board (PSAB) within 10 calendar days after you receive this LOD of your intent to appeal directly to the PSAB and by providing the PSAB within the next 30 calendar days with any supporting material not already provided as to why the LOD should be overturned; or (2) by requesting a personal appearance before an Administrative Judge to present your case. If you request a personal appearance, it must be sent to the Director, Defense Office of Hearings and

Appeals (DOHA), Post Office Box 3656, Arlington, Virginia, 22203 (FAX No. 703-696-6865) within 10 calendar days of your receipt of the LOD. A form (enclosure 1) for requesting a personal appearance is appended. In either case, inform the head of your employing organization that you are submitting an appeal. Instructions for preparing and executing an appeal are provided at enclosure 2.

4. If you appeal, the case file including all of the information you supplied in accordance with reference (c) will be forwarded to either the PSAB or the DOHA for consideration. If you require an extension to a deadline, you must make your request in writing to the PSAB or the DOHA and notify the head of your organization.

5. Questions regarding this LOD should be directed to POC designated by your organization.

Use The Following If The Individual Did Not Respond To SOR:

1. Reference (a) informed you of our intent to (deny/revoke) your eligibility for access to classified information and for assignment to sensitive duties.

2. Reference (a) further informed you that the unfavorable personnel security decision would become automatically final if you failed to submit a timely response.

3. Because we have received no timely response, your eligibility for access to classified information or performance of sensitive duties is hereby (denied/revoked). This decision is final and is not subject to further appeal.

Notice of Intent to Appeal

PART I

I, (last name), (first name), (middle initial), social security number (000-00-0000), received a Letter of Denial/Revocation from (Name of CAF) dated MMDDYY. I elect (check one of the following):

( ) to appeal directly to PSAB

( ) a personal appearance before a DOHA Administrative Judge

PART II

The following information is provided so that I can be contacted by the PSAB or DOHA:

a. Duty Address:

b. Duty Phone:

c. Home Address:

d. Home Phone:

PART III

This Notice must be sent to the President of the PSAB (address), or the Director, Defense Office of Hearings and Appeals, Post Office Box 3656, Arlington, Virginia 22203 (FAX No. (703)-696-6865) within 10 calendar days from receipt of the Letter of Denial/Revocation (LOD).

_____

Signature Date

Instructions for Appealing a Letter of Denial/Revocation (LOD)

A decision has been made to deny or revoke your eligibility for access to classified information or performance of sensitive duties. This means that your are not eligible to handle classified information or perform sensitive duties. This could prevent you from continuing in your present position or pursuing your current career. The letter of denial or revocation (LOD) explains this decision. It is based on adverse information which raises security concerns about your trustworthiness, reliability or judgment.

A. How to Appeal

The LOD can be appealed in one of two ways:

1. You may request a personal appearance before an administrative judge (AJ) from the Defense Office of Hearings and Appeals (DOHA). This appearance is intended to provide you with an additional opportunity to present a full picture of your situation. You will have an opportunity to orally respond to the security concerns noted in the LOD and submit supporting documentation to the AJ who will make a recommendation to the Personnel Security Appeal Board (PSAB). The PSAB will consider both your written record and the results of the personal appearance in making its final decision.

2. You may, however, prefer to submit a written appeal to the PSAB and forego the personal appearance. If you submit a written appeal, you may also provide supporting documentation. Having or not having a personal appearance will not bias the PSAB in making a fair determination in your case.

You must elect either (1) or (2); you may not do both.

B. Appealing Without a Personal Appearance

If you choose to appeal without a personal appearance, your written response should provide whatever information you think ought to be considered in the final decision. You should try to specifically explain, refute, extenuate, mitigate or update the security concerns presented in the LOD.

You should review enclosure (2) to the SOR, "Instructions for Responding to a Statement of Reasons (SOR)" to make sure that your appeal follows the guidelines outlined in that document. It will help you understand how to develop and write your appeal so that it can best address the security concerns in your case. Supporting documents should be provided in the order referred to in your written response.

Place your written appeal and supporting documents in a single envelope or package and forward it to the PSAB via the head of your organization. Be sure to sign and date your appeal and submit it within 30 calendar days of your notice of appeal.

C. Appealing with a Personal Appearance

If you choose to have a personal appearance, you must provide DOHA with your request within 10 calendar days of receipt of the LOD. You will receive a notice designating the time, date and place for the personal appearance, which generally with be held within 30 calendar days after your request. The personal appearance generally will be conducted at or near your duty station if it is in the lower 48 states. For people stationed elsewhere, it will be held at or near your duty station or at a DOHA facility in the Washington, D.C. or Los Angeles, California metropolitan area.

At the appearance you will have an opportunity to present oral and documentary information on your own behalf. While the personal appearance is designed so that you can represent yourself, you may obtain legal counsel or other assistance at your own expense to be present at the appearance. If you desire counsel, arrange for it now. Postponement of the personal appearance can be granted only for good cause.

In getting ready for the personal appearance, make sure that you are prepared to address all of the security concerns and supporting adverse information. Also, make sure that your supporting documents are organized and readily accessible for presentation to the AJ presiding at the appearance and for use in answering questions.

The AJ presiding at the appearance will have already reviewed your case file. Therefore, your goal should be to clarify your reasons for overturning the LOD and adding additional information and documentation when appropriate rather than merely to repeat material that you previously submitted. You will not have the opportunity to present or cross-examine witnesses. If you want the views of others presented, make sure that you obtain these views in writing (e.g., letters of reference, letters from medical authorities, etc.) and that you present these documents to the AJ.

During the appearance, you will be allowed to make an oral presentation and submit documentation. You may be asked questions. Answer clearly, completely, and honestly. The AJ is not there to present the government's security concerns but rather to listen to any explanations that you may have concerning your case. This individual did not make the unfavorable personnel security determination set forth in the LOD, and is there to give you an opportunity to present your case as fully as possible.

At the end of the personal appearance, you will be given an opportunity to make a closing statement. You should stress the highlights rather than review your entire case. Try to show how the weight of all available information supports overturning the unfavorable personnel security determination in your case.

The AJ will review the case file, listen to your comments and review any additional documentation that you submit, and then make a recommendation to the PSAB as to whether the clearance, access, or employment in sensitive duties should be denied, revoked or reinstated. The PSAB is not bound by the recommendation of the AJ but will consider it, as well as any additional information you present at your appearance.

AP12. APPENDIX 12

STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD

AP12.1. STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD

Component Personnel Security Appeal Boards (PSABS) shall be structured and function to meet the following requirements:

AP12.1.1. The PSAB will be comprised of three members at the minimum military grade of O-5 or civilian grade of GM/GS-14. In cases where the appellant is at or above the grade of military O-5 or GM/GS- 14, at least one member of the board will be equivalent or senior in grade to the appellant.

AP12.1.2. One of the three members will be a permanent board member and serve as board president. This person should have a thorough knowledge of and experience in the field of personnel security.

AP12.1.3. One of the three members will be an attorney, unless the board has access to legal counsel, and not more than one member shall be from the security career field.

AP12.1.4. The composition of the board may be changed if an appellant works for a Component without a PSAB. A senior official of that Component will be entitled, but not required, to occupy one of the three board positions during consideration of the case.

AP12.1.5. Officials from the Central Adjudication Facility will neither serve as a member of the board nor communicate with board members concerning the merits of an open case.

AP12.1.6. Component PSABs will meet regularly to ensure timely disposition of appeals.

AP12.1.7. Each case shall be reviewed by all three PSAB members. Appeals will be decided by majority vote of the board members present at a meeting to discuss and vote on the case.

AP12.1.8. Component PSABs will render a final determination and notify the individual (via the individual's local organization) in writing. The PSAB will generally notify individuals within 60 calendar days of the receipt of appeal (without personal appearance) or 30 calendar days of receipt of the recommendation of the Administrative Judge (if a personal appearance is requested). This written notification will provide the reasons that the PSAB either sustained or overturned the original determination of the Component Central Adjudication Facility. The PSAB determination will be final and will conclude the appeal process.

AP12.1.9. The PSAB shall maintain a redacted file of all decisions which will be subject to review in accordance with the Freedom of Information Act.

AP13. APPENDIX 13

CONDUCT OF A PERSONAL APPEARANCE BEFORE AN ADMINISTRATIVE JUDGE (AJ)

AP13.1.1. A person appealing a Letter of Denial (LOD) may request a personal appearance by notifying the Defense Office of Hearings and Appeals (DOHA) in writing at the following address: Director, Defense Office of Hearings and Appeals, Post Office Box 3656, Arlington, Virginia 22203 (FAX No. (703) 696-6865). The request must be sent to DOHA within 10 calendar days of receipt of the LOD. An extension of time may be granted by the Director, DOHA, or designee, for good cause demonstrated by the appellant.

AP13.1.2. Upon receipt of a request for a personal appearance, DOHA shall promptly request the appellant's case file from the appropriate CAF, assign the case to an AJ, and provide a copy of the request to the appropriate PSAB. The CAF shall provide the case file to DOHA normally within 10 calendar days.

AP13.1.3. The AJ will schedule a personal appearance generally within 30 calendar days from receipt of the request and arrange for a verbatim transcript of the proceeding. For appellants at duty stations within the lower 48 States, the personal appearance will be conducted at the appellant's duty station or a nearby suitable location. For individuals assigned to duty stations outside the lower 48 States, the personal appearance will be conducted at the appellant's duty station or a nearby suitable location, or at DOHA facilities located in the Washington, DC metropolitan area or the Los Angeles, California metropolitan area, as determined by the Director, DOHA, or designee.

AP13.1.4. Travel costs for the appellant will be the responsibility of the employing organization.

AP13.1.5. The AJ will conduct the personal appearance proceeding in a fair and orderly manner:

AP13.1.5.1. The appellant may be represented by counsel or personal representative at his own expense;

AP13.1.5.2. The appellant may make an oral presentation and respond to questions posed by his counsel or personal representative, and shall respond to questions asked by the AJ;

AP13.1.5.3. The appellant may submit documents relative to whether the LOD should be overturned;

AP13.1.5.4. The appellant will not have the opportunity to present or cross-examine witnesses;

AP13.1.5.5. Upon completion of the personal appearance, the AJ will generally forward within 30 calendar days, a written recommendation to the appropriate PSAB whether to sustain or overturn the LOD, along with the case file and any documents submitted by the appellant. A copy of the AJ's recommendation will be provided to the CAF.

AP13.1.6. The PSAB will render a final written determination stating its rationale and notify the individual in writing (via the individual's employing organization) generally within 30 calendar days of receipt of the recommendation from DOHA. This decision will be final and will conclude the appeal process.

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

AFI31-401_AFGM1
29 February 2012

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: AF/A4/7
1030 Air Force Pentagon
Washington DC 20330

SUBJECT: Air Force Guidance Memorandum to AFI 31-401, *Information Security Program Management*

By Order of the Secretary of the Air Force, this is an Air Force Guidance Memorandum (AFGM) immediately changing AFI 31-401. Compliance with this AFGM is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails in accordance with AFI 33-360, *Publications and Forms Management*.

In advance of rewrite of AFI 31-401, or publication of AFI 16-1401, *Enterprise Information Protection*, the attachment to this AFGM provides guidance changes that are effective immediately.

The AFGM guidance becomes void after 180 days have elapsed from the date of this AFGM, or upon incorporation by interim change to AFI 31-401, rewrite of AFI 31-401, or publication of AFI 16-1401, whichever is earlier.

JUDITH A. FEDDER
Lieutenant General, USAF
DCS/Logistics, Installations & Mission Support

Attachment:
Guidance Changes

The below changes to AFI 31-401, dated 1 November 2005, through Interim Change 1, dated 19 August 2009, are effective immediately.

(Replace) 1.3.7.1. Establish criteria, evaluate, and rate all civilian and military employees who are original classification authorities, security managers or specialists, and other personnel whose duties primarily involve the creation of or handling of classified information on their performance of security responsibilities. Include the designation and management of classified information as a critical element, item, or assessment for these personnel. If the mandated performance form does not permit defining a new critical element, the performance reviewer will include an assessment of this area in an existing text block. *[Reference EO 13526 §5.4 and DOD 5200.1-R, C1.1.2.1.]*.

(Replace) 1.4.1. MAJCOMs will incorporate information protection (IP) into the Air Force Inspection System (AFIS). The IP inspection will occur every four (4) years and will be known as the Information Protection Management Evaluation (IPME). Until a permanent solution is reached, MAJCOM IP Directors will provide IP augmentees to the MAJCOM IG team. To preclude perceived conflicts of interest, inter-MAJCOM IP exchanges of qualified IP personnel to augment IG CUI teams is encouraged. If an exchange is not feasible, MAJCOM IP Directors may select MAJCOM, center, or wing-level IP augmentees; however, selected personnel will not be members of the wing or center being inspected.

1.4.1.1. DELETED

1.4.1.1.1. DELETED

1.4.1.1.2. DELETED

1.4.1.1.3. DELETED

(Replace) 1.4.2. The Chief, Information Protection (CIP), may request a Staff Assistance Visit (SAV) from the MAJCOM/FOA/DRU IP Director at any time. A SAV is an assistance-oriented visit, not an inspection. The MAJCOM/FOA/DRU IP Director will coordinate the SAV through the MAJCOM/FOA/DRU Gatekeeper.

(Replace) 1.4.3. Installation CIPs will conduct Local Information Protection Management Evaluations (LIPMEs):

(Replace) 1.4.3.1. No less frequently than annually for activities on the installation, and any others serviced by the IP staff, that store or handle classified material. If an organization clearly demonstrated a highly effective, discrepancy-free approach to managing IP during a previous IPME (MAJCOM CUI) or LIPME, the CIP, with the concurrence of the Wing CV, may elect to extend that organization's next LIPME out to 24 months.

(Replace) 1.4.3.2. No less frequently than once every 24 months, or under unit Commander's Inspection Program (CCIP) guidelines, for activities on the installation and any others serviced by the IPO that do not store or handle any classified material.

(Add New) 1.4.3.3. LIPMEs are assistance-oriented oversight visits performed by CIPs or designated representative(s) on subordinate IPOs and/or unit security programs. LIPMEs are not rated but are conducted to determine effectiveness, benchmark processes and/or products, and identify problem areas and required corrective action.

(Add New) 1.4.3.4. LIPMEs will focus on IP Enterprise efforts, inclusive of the information, personnel, and industrial security disciplines. LIPMEs will include collateral classified material and Controlled Unclassified Information (CUI) (excluding Computer Security Act of 1987 information and technical documents) holdings.

(Add New) 1.4.3.5. Collateral material and CUI kept within a Sensitive Compartmented Information Facility (SCIF) or Special Access Program Facility (SAPF) does not fall within the purview of a LIPME, and responsibility for such material rests with the applicable owner/user.

(Add New) 1.4.3.6. The CIP will provide the inspected unit Commander with written review results within 15 duty days of the review outbrief.

(Add New) 1.4.3.6.1. If the review report requires a response to identified shortfalls, the inspected unit Commander will provide written response to the CIP within 30 duty days of the review report date.

(Add New) 1.4.3.6.2. If the first response does not close all action items, the inspected unit Commander will provide reports to the CIP every 30 days thereafter until all actions are resolved or closed.

(Replace) 1.4.4. Commanders of units responsible for processing or holding classified information will ensure unit personnel conduct semiannual security self-inspections to evaluate information security program effectiveness.

(Add New) 1.4.4.1. Unit commanders will appoint an individual(s) in writing to conduct a semiannual security inspection.

(Add New) 1.4.4.2. Neither the unit security manager nor members of the IP staff will be appointed to conduct the inspection.

(Add New) 1.4.4.3. If the CIP conducted a LIPME or SAV in a unit within the last 12 months, that event will count as one of the semiannual self-inspections for that 12-month period; i.e., the unit would have to conduct only one self-inspection during the same period.

(Add New) 1.4.5. SAF/AAP, Information Protection Directorate, personnel will visit MAJCOM IP organizations as necessary to review management of the MAJCOM Enterprise IP environment.

(Replace) 1.7.1.1. Organizations sample data for Part D, Derivative Classification Decisions, during a consecutive 2-week period each fiscal year quarter (Oct-Dec, Jan-Mar, Apr-Jun, and Jul-Sep). In the last quarter, the 2-week period must be set early since the reports are required by 15 October. Calculations will be annualized. For example, multiply the figure representing 8

weeks' worth of actual data x 6.5 to achieve a figure reflecting 52 weeks' worth of annualized data. If less than 100% of the population is surveyed, identify the percentage surveyed and annotate the mathematical calculation used to arrive at a 100% figure. Interagency Report Control Number 0230-GSA-AN applies to this information collection requirement.

(Replace) 1.7.1.1.1. Count the number of classification decisions in finished products for dissemination or retention, regardless of the media. Include classified work stations (such as SIPRNET) when compiling data.

(Add New) 1.7.1.2. Effective with the FY12 SF 311 report, the actual number of decisions made must be reported under Part C, "Original Classification Decisions." Each OCA will report the number of his or her original classification decisions throughout the year for each Part C category and how each decision was documented. A separate list citing specific Part C data for each category for each OCA will be provided to SAF/AAP with the annual SF 311.

(Replace) 1.9. See paragraph 1.4.4. of this AFI *[Reference DOD 5200.1-R, C1.7.]*.

(Delete) 2.1. and all subordinate elements. Replace with new text which follows.

(New) 2.1. Original Classification Authority (OCA) *[Reference EO 13526 § 1.3 and 32 CFR 2001.11]*

(New) 2.1.1. The Secretary of the AF (SECAF) is a Presidentially-delegated Top Secret OCA IAW EO 13526 § 1.3(a)(2). The SECAF may further delegate, in writing, Top Secret, Secret, and Confidential AF authorities, but only to the minimum number required to carry out EO 13526.

(New) 2.1.2. Per the SECAF, SAF/AA is a SECAF-designated Top Secret OCA who may further delegate Secret and Confidential authorities on behalf of the SECAF, but only to the minimum number required to carry out EO 13526.

(New) 2.1.3. No OCA, other than the SECAF or SAF/AA, can further delegate OCA.

(New) 2.1.4. OCAs are senior military or civilian positions (usually General Officer or Senior Executive Service, respectively) at the first or second echelon of command responsible for carrying out a unique mission in one of eight EO 13526 § 1.4 classification categories.

(New) 2.1.4.1. OCA is delegated to a position, not a person. Incumbents assume the authority granted to the position. Deputies, vice commanders, chiefs of staff, and other similar OCA subordinates are empowered to act as the OCA when they assume that duty position in an "acting" capacity and have certified in writing that they have been trained, prior to exercising the authority, in OCA responsibilities and classification principles in addition to the basic security training on the proper safeguarding of classified information and the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.

(New) 2.1.4.2. When permanent incumbents change, notify SAF/AAP of the new incumbent's name within 15 calendar days of the effective date.

(New) 2.1.4.3. OCA is not automatically delegated to, or retained by, any position simply because delegation authority exists. Retaining delegated OCA is based on demonstrable and continuing need per EO 13526.

(New) 2.1.4.4. Revoked or relinquished OCA may be requested consistent with mission changes.

(New) 2.1.5. Sensitive Compartmented Information (SCI). The only AF OCA for SCI is AF/A2. No other AF OCAs can originally classify SCI.

(New) 2.1.6. North Atlantic Treaty Organization (NATO).

(New) 2.1.6.1. AF OCAs do not originally classify NATO information but rather US information in NATO records under the guidelines set forth in DoD-level INFOSEC guidance and this AFI.

(New) 2.1.6.2. For AF officials holding both AF positions and NATO positions, DoD-level INFOSEC guidance and this AFI pertain to information classified for exclusive US use. Applicable NATO security regulations pertain to information classified for exclusive NATO use. These officials derive NATO classification authority through Headquarters (HQ) Supreme Headquarters Allied Powers Europe (SHAPE) as a result of their position in NATO and not the AF.

(New) 2.1.7. Forward OCA requests, signed by the MAJCOM Commander or Vice, through MAJCOM IP channels to SAF/AAP. Requests will include the information below. Upon review, SAF/AAP may require additional information prior to processing the request.

(New) 2.1.7.1. The full position title, functional office symbol, and level of OCA requested.

(New) 2.1.7.2. A detailed explanation of why the position requires OCA. Discuss how the requested OCA affects the MAJCOM or Air Staff organization's OCA portfolio. State if this OCA replaces an existing OCA or is additive. Describe how this change supports the EO 13526 requirement to restrict OCA delegations to the minimum number necessary to carry out the EO.

(New) 2.1.7.3. Number and type (collateral, SCI, SAP) of Security Classification Guides (SCGs) for which the OCA is (or will be) responsible.

(New) 2.1.7.4. Description and estimate of the anticipated annual use of the delegated authority.
(New) 2.1.7.5. If the OCA request is for a new organization (or organization that has recently moved/changed names), provide an explanation.

(New) 2.1.8. OCA training.

(New) 2.1.8.1. Initial OCA training will be completed before exercising any original classification decisions, or within 60 calendar days of appointment, whichever is sooner. Notify SAF/AAP through MAJCOM/FOA/DRU IP channels of training completion date. *[Reference 32 CFR § 2001.70.]*

(New) 2.1.8.2. OCAs will complete annual OCA refresher training. Failure to complete annual training will result in suspension and may result in revocation of OCA. Notify SAF/AAP through MAJCOM/FOA/DRU IP channels of training completion date. *[Reference 32 CFR § 2001.70.]*

(New) 2.1.9. SAF/AAP will maintain the master list of Air Force OCAs and post it on the SAF/AAP Portal. If a position is not listed on the master list, that position has not been delegated OCA and cannot perform OCA functions. SAF/AAP will monitor demonstrable and continuing need and may request validation from the MAJCOM/FOA/DRU IP Directors.

(Replace) 2.2.2. Classification may be applied only to information that is owned or produced by, or for, or is under the control of the United States Government. Information may be considered for classification only if it concerns one of the categories specified in Section 1.4 of EO 13526. *[Reference DTM 11-004, C2.3.2.]*

(New) 2.3.5. Those who perform derivative classification must complete derivative classification training at least once every two years. *[Reference EO 13526 § 2.1(d)]*

(Replace) 2.4.1. Under no circumstances shall information be classified, continue to be maintained as classified, or fail to be declassified in order to (1) conceal violations of the law, inefficiency, or administrative error; (2) to prevent embarrassment to a person, organization, or agency; or (3) to restrain competition. *[Reference EO 13526§1.7; DTM 11-04, C2.4.3.1.1.]*

(Add) 2.4.3. Reclassification after declassification and release to the public under proper authority will be IAW DTM 11-004, C2.4.3.2. *[Reference EO 13526§1.7(c)]*

(Add) 2.4.3.1. MAJCOM/FOA/DRU commanders will make requests for reclassification after declassification and release through IP channels to SECAF.

(Add) 2.4.3.1.1. Identify the specific information for which reclassification is requested.

(Add) 2.4.3.1.2. Identify how the information will be reasonably recovered without attracting undue attention to the information.

(Add) 2.4.3.1.3. Identify whether the information is in the custody of the National Archives and Records Administration (NARA).

(Add) 2.4.3.1.4. Identify all information necessary for the original classification process IAW DoD 5200.1-R, C2.3.

(Add) 2.4.3.2. If reclassification is approved, SECAF will notify the National Security Advisor, the Director of ISOO, and the USD(I); and the requestor will ensure applicable security classification guidance is updated.

(Add) 2.4.3.3. If the records have been available for public use through NARA, public access will be suspended pending approval of the reclassification action by the ISOO Director. Should the ISOO Director disapprove the declassification action, SECAF may appeal the decision to the President through the National Security Advisor.

(Add) 2.4.3.3.1. If appealed, the requestor will provide to SECAF, through IP channels, a clearly articulated justification describing the compelling national security reasons for reclassifying the information, in rebuttal to the ISOO rationale for denying the request. SAF/AAP will notify USD(I) of the appeal.

(Add) 2.4.3.3.2. Once a final decision is rendered, the requestor will consider the need to update applicable security classification guidance.

(Add) 2.4.4. Reclassification or classification of information not previously disclosed under proper authority will be IAW DTM 11-004, C2.4.3.3.

(Add) 2.4.4.1. OCAs will submit requests for reclassification after declassification and release through IP channels to SAF/AA.

(Add) 2.4.4.2. OCAs will identify all information necessary for the original classification process IAW DoD 5200.1-R, C2.3.

(Add) 2.4.4.3. Once a decision is rendered, OCAs will update applicable security classification guidance as necessary.

(Replace) 2.6.1.4. Provide the date of issuance or last review. The date of the original classification will be clearly identified and carried forward in SCG reissuances.

(Replace) 2.6.1.6. State which classification level applies to each element of information and, when useful, specify the elements of information that are unclassified. Where an element may qualify for more than one classification level, criteria will be provided for determining which classification level is applicable.

(Replace) 2.6.2.2.1. Release of program data on the World Wide Web. Extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. The search and data mining capabilities of Web technology must be assessed from a risk-management perspective. Information intended for publication on publicly accessible or unprotected web sites must be cleared for public release prior to publication according to AFI 35-102, *Security and Policy Review Process*. If there are any doubts, do not release the information.

(Replace) 2.6.2.3. Coordinate SCG review with the servicing Foreign Disclosure Office and CIP and/or MAJCOM/FOA/DRU IP Director.

(Replace) 2.6.2.4. SCGs shall be reviewed and updated as circumstances require but at least once every five years. Note: The AF will conduct an initial Fundamental Classification Guidance Review (including SCGs) by 29 February 2012. Thereafter, review SCGs at least once every five years. *[Reference 32 CFR § 2001.16.]*.

(Replace) 2.6.3.1. To extend classification beyond 25 years, proper approval authority must first be obtained IAW DTM 11-004, C4.3.

(Add) 2.6.3.1.1. For specific information or records, the OCA will request exemption through IP channels to SAF/AA. Requests will include items identified in DTM 11-004, C4.3.3.3.1.1. – C4.3.3.3.1.3. If approved, SAF/AA will notify the Interagency Security Classification Appeals Panel (ISCAP) of the decision, and will provide USD(I) an informational copy.

(Add) 2.6.3.1.2. For file series, the OCA will request exemption through IP channels to SECAF. Requests will include items identified in DTM 11-004, C4.3.3.3.2.1. – C4.3.3.3.2.3. If approved, SECAF will notify ISCAP of the decision and will provide USD(I) an informational copy.

(Add) 2.6.3.1.3. ISCAP may direct SECAF or SAF/AA not to exempt the specific information or file series or may direct an earlier declassification date. If required, SECAF may appeal the decision to the President through the National Security Advisor. An informational copy will be provided to USD(I).

(Replace) 2.6.3.2. Submit SCGs electronically through IP channels to SAF/AAP whenever an SCG is issued, revised, reviewed, or rescinded.

(Replace) 2.6.3.3. Report all SCG events on DD Form 2024, *DoD Security Classification Guide Data Elements*, through IP channels to SAF/AAP. Events include initial publication, revisions, reviews, changes, cancellations, etc. Submit all SCGs and DD Forms 2024 electronically through IP channels, in Adobe Portable Document Format (.pdf), to SAF/AAP:

(Replace) 2.6.3.3.1. Secret Internet Protocol Router Network (SIPRNET): saf.aap.workflow@af.pentagon.smil.mil, for Secret and below SCGs only. If possible, send all unclassified SCGs and DD Forms 2024 via SIPRNET. SIPRNET transmissions permit direct publication to the Manager of Online Security Archival Information Classified (MOSAIC) Community of Practice (CoP) and direct submission to DTIC.

(Replace) 2.6.3.3.2. Non-Secure Internet Protocol Router Network (NIPRNET): saf.aap.workflow@pentagon.af.mil, for unclassified SCGs only. Encrypt all transmissions.

(Replace) 2.6.3.4. SAF/AAP will process the SCG and DD Form 2024 and send it to the Air Force Declassification Office (AFDO) for further distribution to:

(Add) 2.6.3.4.1. Defense Technical Information Center (DTIC). TR@DTIC.smil.mil.

(Add) 2.6.3.4.2. MOSAIC.

(Replace) 2.6.4. Electronic Location of Guides. SAF/AAP maintains the master list of AF collateral SCGs. Collateral SCGs are posted on the AFDO-hosted MOSAIC SIPRNET CoP. Guides are also located on the DTIC web site. To access the DTIC web site, register for a DTIC account at: http://www.dtic.mil/dtic/registration.

(Replace) 3.2. Declassification. Note: Exemptions identified in this chapter are found in 32 CFR 2001.26.

(Replace) 3.2.1. Originally Classified Documents. The declassification decision determines the duration of protection *[Reference EO 13526 § 1.6.(a)(4) and 32 CFR 2001.26]*. *At the time an item of information is classified, original classifiers will determine which of the following four declassification instructions will be used, selecting whenever possible, the declassification instruction that will result in the shortest duration of classification.*

(Replace) 3.4. Automatic Declassification. *[Reference EO § 3.3, 32 CFR 2001.30, and DTM 11-004 C4.3]*.

(Replace) 3.4.1. The Air Force Declassification Office (AFDO) published the *AF Declassification Guide for Historical Records* providing the framework for AF compliance with 32 CFR § 2001.30. It pertains to information contained in 25-year-old Air Force records determined to be of permanent historical value. It is critical that records management and IP personnel collaborate to ensure mutual requirements are met for classified records to either be stored at federal records centers or accessioned to the National Archives.

(Replace) **3.8. Public Release.** When information is declassified, it is not releasable to the public until it has been approved for release through the security review process IAW AFI 35-102. The same holds true for declassified or unclassified information that will be placed on an Internet site that can be accessed by the public.

(Replace) 4.1. General. AF members, employees, and contractors will mark all classified products (i.e., paper documents, e-mails, slide presentations, web pages, etc.) IAW Controlled Access Program Coordination Office (CAPCO) standards. The CAPCO guide is available through the SAF/AAP Portal. In the event of conflict between CAPCO standards and this AFI, CAPCO takes precedence.

(Replace) 4.2.4. The reason for classification. Each originally classified document shall bear a concise statement of the reason for classification, as determined by the original classifier. *[Reference DOD 5200.1-R, C5.2.4.]* The classification categories are listed in EO 13526 § 1.4, and DTM 11-004, C2.3.2. *Example:* REASON: 1.4(e).

5.2.1. DELETED

5.2.1.1. DELETED

5.2.1.2. DELETED

5.2.1.3. DELETED

(Replace) 5.4.5.2.3. If the results of the NAC are favorable and AFHRA OL-A/HOR approves access, the researcher must sign an SF 312 and an agreement to submit any notes and manuscript(s) for security and policy review (AFI 35-102). This process is to ensure the documents do not contain any classified information and, if so, determine if they can be declassified. Send the SF 312 to AFHRA OL-A/HOR for retention. Classified information will not be removed from government facilities.

(Replace) 5.4.6.5. Obtains the individual's agreement to safeguard the information and to submit any notes and manuscript for a security review (AFI 35-102) to ensure that the documents do not contain classified information or to determine if any classified information should be declassified.

(Replace) 5.6. Preventing Public Release of Classified Information. See AFI 35-102 for guidance on security reviews to prevent people from publishing classified information in personal or commercial articles, presentations, theses, books or other products written for general publication or distribution.

(Replace) **9.7. Public Release.** Security incident reports cannot be released into the public domain until they have undergone a security review *[Reference AFI 35-102.]* Unauthorized disclosure of classified information to the public must be processed IAW DODD 5210.50.

(Replace) 9.8.3. The appointing authority will immediately notify the OCA, or the originator when the OCA is not known, when it is determined there is a compromise, potential compromise, or loss of classified information. Refer to paragraph 9.6.1. of this AFI for security classification marking requirements.

ATTACHMENT 1
GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References
(Delete) AFI 35-101, Public Affairs Policies and Procedures
(Add) AFI 35-102, Security and Policy Review Process

Abbreviations and Acronyms
(Add) IP—Information Protection
(Add) IPME—Information Protection Management Evaluation (performed by MAJCOM IG)
(Delete) ISPR—Information Security Program Review
(Add) LIPME—Local Information Protection Management Evaluation (performed by installation IP staff)

Administrative Changes

References throughout to "Executive Order (EO) 12958, as amended" are hereby changed to "Executive Order (EO) 13526, *Classified National Security Information*."

References throughout to "ISOO Directive 1" are hereby changed to "Title 32 Code of Federal Regulations (CFR) Part 2001, *Classified National Security Information*."

References throughout to "National Agency Check (NAC)" are hereby changed to "National Agency Check with Written Inquiries (NACI)."

References throughout to the "Information Protection Community of Practice (CoP)" are hereby changed to the "SAF/AAP Portal."

References throughout to "USSAN Instruction 1-69, *United States Implementation of NATO Security Procedures*," are hereby changed to "USSAN Instruction 1-07, *US Implementation of NATO Security Procedures*."

References throughout to "AFSSI 5020, *Remanence Security*," are hereby changed to "AFSSI 8580, *Remanence Security*."

References throughout to "Air Force Declassification Plan" are hereby changed to "Air Force Declassification Guide for Historical Records."

References throughout to "Information Security Program Review" are hereby changed to "Information Protection Management Evaluation."

References throughout to "IPSR" are hereby changed to "LIPME."

References throughout to "unclassified controlled information" are hereby changed to "Controlled Unclassified Information (CUI)."

References throughout to "AFI 35-101" are hereby changed to "AFI 35-102."

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-401

1 NOVEMBER 2005
Incorporating Change 1, 19 August 2009

Security

INFORMATION SECURITY
PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ USAF/XOS-FI

Certified by: HQ USAF/XO
(Lt Gen Carrol H. Chandler)

Supersedes: AFI 31-401,
1 November 2001

Pages: 91

This publication implements Air Force Policy Directive (AFPD) 31-4, Information Security. It prescribes and explains how to manage and protect unclassified controlled information and classified information. Use this instruction with Executive Order (EO) 12958, as amended, *Classified National Security Information*, 25 March 2003; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, *Classified National Security Information*, Executive Order 12829, National Industrial Security Program (NISP), DOD Manual 5220.22, *National Industrial Security Program Operating Manual*, January 1995; and, Department of Defense (DOD) 5200.1-R, *Information Security Program*, 14 Jan 97, for the management of the Air Force Information Security Program. Additional references include DOD Instruction (DODI) 5240.11, *Damage Assessments*, 23 Dec 91; DOD Directive (DODD) 5210.83, *Unclassified Controlled Nuclear Information (UCNI)*, 15 Nov 91; Air Force Policy Directive (AFPD) 31-4, *Information Security*. This instruction is applicable to contractors as prescribed in AFI 31-601, *Industrial Security Program*. All these references are listed at the end of each paragraph where applicable. This instruction is not to be used as a stand-alone document. HQ USAF/XOS-F is delegated approval authority for revisions to this AFI.

SUMMARY OF CHANGES

This interim change reflects new requirements for management of the Information Security Program at all echelons; transfers responsibility for Unclassified Controlled Nuclear Information; reflects the transfer of Information Security Program Manager (ISPM) duties and responsibilities

from the Chief, Security Forces or installation security official to the Chief of Information Protection at MAJCOM and installation levels and codifies staff office changes from that action; updates locations possible for overnight delivery of Secret information in urgent cases; updates references and deletes terms not used in the text; updates glossary of references and supporting information (**Attachment 1**); updates transmission procedures for unclassified controlled nuclear information (**Attachment 2**); deletes use of United States Postal System registered mail or Express Mail to transfer Secret or Confidential material (**Attachment 4**). An asterisk (|) indicates newly revised material.

Chapter 1

POLICY AND PROGRAM MANAGEMENT

1.1. Policy. It is Air Force policy to identify, classify, downgrade, declassify, mark, protect, and destroy its classified and unclassified information and material consistent with national policy. This general policy statement also applies to unclassified controlled information (**Attachment 2**) under the purview of relevant statutes, regulations and directives *[Reference DOD 5200.1-R, C1.1.]*.

1.2. Philosophy. Protecting information is critical to mission accomplishment. The goal of the Information Security Program is to efficiently and effectively protect Air Force information by delegating authority to the lowest levels possible; encouraging and advocating use of risk management principles; focusing on identifying and protecting only that information that requires protection; integrating security procedures into our business processes so that they become transparent; and, ensuring everyone understands their security roles and responsibilities.

1.3. Program Management. The strength of the Air Force Information Security Program is in its infrastructure. The infrastructure is important because it facilitates effective communication of our security policies and procedures to those performing the Air Force mission. With the support of commanders at all levels, this is accomplished predominantly through our Information Security Program Manager (ISPM) and security manager system. Both play an integral role in ensuring unit personnel know and understand their role in protecting classified information against unauthorized disclosure *[Reference DOD 5200.1-R, C1.2.]*.

1.3.1. Senior Security Official. The Administrative Assistant to the Secretary of the Air Force (SAF/ AA) is designated the Air Force Senior Security Official responsible for ensuring implementation of the Information Security Program.

1.3.2. Air Force Program Manager. The Director, Information Protection (SAF/AAP) is responsible for policy, resource advocacy, and oversight of this program.

1.3.3. Commanders of Major Commands (MAJCOM), Field Operating Agencies (FOAs), Direct Reporting Units (DRUs), and Installations. These commanders are responsible for:

1.3.3.1. Establishing information security programs.

1.3.3.2. Identifying requirements.

1.3.3.3. Executing their programs to comply with this policy.

1.3.4. The installation Chief of the Information Protection (IP) Office (IPO) or MAJCOM Director, Information Protection is designated the ISPM at each Air Force installation or site. Air Force Chiefs of Information Protection:

1.3.4.1. Implement the Information Security Program, for the Information, Personnel, and Industrial Security Programs on behalf of the installation commander. Assist in the program/technology protection planning process as it relates to information, personnel and industrial security, to include direction on physical security requirements

for the protection of assets during the various states, i.e., production, deployment, maintenance, test, or undergoing modifications.

1.3.4.2. Integrate on-base contractor operations into the installation's Information Security Program in accordance with (IAW) AFI 31-601.

1.3.4.2.1. Review pre-award and/or draft solicitations and contract documents associated with classified contract efforts; security classification guides and Department of Defense (DD) Form 254 to ensure appropriate security clauses and/or language is contained therein which address the protection of sensitive government information and resources.

1.3.4.2.2. Serve as technical OPR for the development and preparation of the Visitor Group Security Agreement (VGSA) or other security agreements as determined necessary by the installation commander.

1.3.4.2.3. Conduct security oversight of on-base designated "cleared facilities" as determined by the installation commander.

1.3.4.3. Provide oversight within their jurisdiction.

1.3.4.4. Provide and monitor training as required by **Chapter 8** of this AFI.

1.3.4.5. For organizations at the Wing level and below, conduct security manager meetings no less than semi-annually.

1.3.5. Unit Commanders or Equivalents, and Staff Agency Chiefs. NOTE: For the purpose of this instruction, staff agency chiefs are those individuals serving in 2-digit positions reporting to the commander or vice commander above the Wing level and 2 and 3 digit positions at Headquarters Air Force. These commanders or equivalents, and staff agency chiefs will:

1.3.5.1. Appoint a security manager to administer the unit's information security program. Alternate security managers may be appointed as necessary. Commanders or equivalents, and staff agency chiefs should consider Air Expeditionary Force rotation cycles, TDY, training requirements, and other assigned duties. Continuity should receive serious consideration in selection of security managers. Military security managers must have a favorable National Agency Check, local agency check, and credit check (NACLC); civilians a National Agency Check with written inquiries and credit check (ANACI), investigation or higher and eligibility for JPAS access before appointment. ***NOTE:*** Smaller organizations and staff agencies are encouraged to appoint primary and alternate security managers to serve multiple activities.

1.3.5.1.1. Contractors will not be appointed as primary or alternate security managers. However, they can be required to provide other security program support, under Air Force direction, such as, assisting the security manager, conducting end-of-day security checks, security training/briefings, etc.

1.3.5.2. Ensure security managers receive training required by **Chapter 8**.

1.3.5.3. Notify the ISPM in writing when either primary or alternate security managers are changed.

1.3.6. Security Managers:

1.3.6.1. Establish and manage the Information Security Program within their unit or staff agency.

1.3.6.2. Develop and update a unit security operating instruction.

1.3.6.3. Advise the unit commander or equivalents, and staff agency chief on security issues pertaining to the unit or staff agency.

1.3.6.4. Attend ISPM hosted security manager meetings.

1.3.6.5. Update and remind personnel of security policies and procedures.

1.3.6.6. Oversee the unit or staff agency information security self-inspection program.

1.3.6.7. Report security incidents immediately, but no later than by the end of the first duty day.

1.3.6.8. Assist the unit commander or equivalent, staff agency chief and ISPM in monitoring security incident investigations. Normally security managers will not conduct security incident inquiries.

1.3.6.9. Participate in security education training as defined in **Chapter 8**.

1.3.6.10. Manage the JPAS within their organization.

1.3.6.10.1. In-process and out-process all unit personnel.

1.3.6.10.2. Monitor and act on system notifications.

1.3.7. Supervisors:

1.3.7.1. Establish criteria, evaluate, and rate all Air Force employees on their performance of security responsibilities *[Reference DOD 5200.1-R, C1.1.2.1.]*.

1.3.7.1.1. Military. See AFI 36-2406, *Officer and Enlisted Evaluation Systems,* paragraph 1.3.7.

1.3.7.1.2. Civilian. See AFI 36-1001, *Managing the Civilian Performance Program,* paragraph A3.2.8.

1.3.7.2. Provide and ensure training as directed in **Chapter 8** of this AFI.

1.3.8. Foreign Disclosure. The Deputy Under Secretary of the Air Force, International Affairs, (SAF/ IA), 1080 Air Force Pentagon, Washington DC 20330-1080, oversees the release of all Air Force information to foreign governments, persons, and international organizations.

1.3.9. Historian. The Air Force Historian (HQ USAF/HO), 3 Brookley Avenue, Box 94, Bolling AFB DC 20032-5000, approves or disapproves historical researchers' access to classified information. *[Reference DOD 5200.1-R, C6.2.2.4.]*

1.4. Oversight. In addition to the reporting requirements of the Information Security Program (see **paragraph 1.7**), the following will be implemented *[Reference DOD 5200.1-R, C1.7.]*.

1.4.1. MAJCOMs will incorporate information protection issues into Inspector General (IG) inspections/reviews. In addition, MAJCOM Information Protection Offices (IPO) will

conduct oversight and assistance visits in the form of either an Information Security Program Review (ISPR) or Staff Assistance Visit (SAV) to subordinate IPOs at least every 36 months. MAJCOM IPO staffs are encouraged to explore oversight options to minimize resource impact.

1.4.1.1. ISPR.

1.4.1.1.1. An ISPR is an assistance-oriented oversight visit for the information security programs performed by an ISPM, or designated representative(s) on a subordinate ISPM or security manager. It is a non-rated review for policy and program effectiveness to benchmark processes/products, identify problem areas and corrective actions. A key component of the ISPR is an assessment of the effectiveness of the information security training program.

1.4.1.1.2. Air Force on-base contractor visitor groups will be integrated into the host installation's Information Security Program unless the mission, operational requirements, autonomous nature or other factors require them to establish and maintain their own security program as a cleared facility under the National Industrial Security Program Operating Manual (NIS- POM).

1.4.1.1.3. The ISPM will provide the commander or equivalent, and staff agency chief the ISPR results in writing.

1.4.2. Base level ISPMs will conduct ISPRs on an annual basis. ***EXCEPTION:*** An extension to 18 months may be granted by the ISPM for units that have demonstrated highly effective, discrepancy free programs during the previous ISPR. ISPRs/SAVs may be conducted every two years for activities or units that do not store classified information.

1.4.3. Security Self-Inspections: Unit commanders or equivalents, and staff agency chiefs involved with processing or holding classified information ensure personnel conduct semiannual security self-inspections to evaluate information security program effectiveness. ***EXCEPTION:*** Activities with a small volume of classified material may work with the ISPM to develop an oversight schedule consistent with risk management principles.

1.4.3.1. Unit commanders or equivalents, and staff agency chiefs will appoint an individual, in writing, other than the unit security manager to conduct a semiannual security inspection.

1.4.3.2. A program review may satisfy the requirement for one of the semiannual self-inspections.

1.4.4. SAF/AAP, Chief of Information Protection will visit MAJCOMs to review their information protection and associated security programs every 36 months.

1.5. Special Types of Information. *[Reference DOD 5200.1-R, C1.3.]*

1.5.1. Restricted Data (RD)/Formerly Restricted Data (FRD). *[Reference DODD 5210.2 and DOD 5200.1-R, C1.3.1.]*

1.5.1.1. General. RD is governed by DODD 5210.2, *Access to and Dissemination of Restricted Data,* 12 Jan 78. Air Force personnel will mark and safeguard RD according to DODD 5210.2. A list of Air Force Officials Authorized to Certify Access to RD is

located on the AFSFC web site. These officials are responsible for certifying access to RD using DoE Form 5631.20, *Request for Visit or Access Approval* (see **paragraph 5.5.1.2**). They may delegate this authority to the level they deem necessary for operational efficiency. Officials delegated the authority will sign in the "For" block on behalf of the access granting official. Air Force personnel may obtain DoE Form5631.20 from the DoE activity they are visiting or at the DoE Forms web site.

1.5.1.1.1. Activities must notify SAF/AAP through command IP channels of changes to the list of certifying officials as they occur. When doing so, they must also provide the position title, activity and office symbol of the affected authority. ***NOTE:*** When the change involves an activity name change, access-granting officials will sign forms authorizing access using the current activity name and a note that identifies the activity it superseded until the list of officials is updated.

1.5.1.1.2. SAF/AAP will periodically update a master list available at the Information Protection Directorate Community of Practice (CoP).

1.5.1.2. Critical Nuclear Weapon Design Information (CNWDI). RD that is particularly sensitive. Access is limited to the minimum number of people who need it to do their job.

1.5.1.2.1. CNWDI Approving Officials. These officials are responsible for granting CNWDI access. This authority is assigned to division chiefs and above at all levels of command.

1.5.1.2.2. Granting Access. Approving officials will ensure access and briefings are documented on AF Form 2583, *Request for Personnel Security Action*.

1.5.1.2.3. Protection. Air Force personnel will protect CNWDI in the same manner prescribed for collateral classified information. This includes limiting access to containers storing CNWDI to only those personnel who have been granted CNWDI access. *[Reference DODD5210.2, Paragraph 6]*

1.5.2. North Atlantic Treaty Organization (NATO). *[Reference DOD 5200.1-R, C1.3.4.]*

1.5.2.1. SAF/AAP is responsible for overall development, approval, and implementation of NATO security policy within the Air Force.

1.5.2.2. The HQ USAFE IP Office is responsible for developing and recommending NATO security policy for implementation within the Air Force.

1.5.3. For Official Use Only (FOUO). Unclassified information that is exempt from release under the Freedom of Information Act (FOIA) exemptions 2-9, may be designated "For Official Use Only." No other material shall be considered FOUO. FOUO is not authorized as an anemic form of classification to protect national security interests. *[Reference DOD Regulation 5400.7/AF Supplement, DOD Freedom of Information Act Program, C4.1.1]* The FOIA exemptions are detailed in *DOD Regulation 5400.7/AF Supplement,* Chapter 3.

1.5.4. Sensitive Compartmented Information (SCI). The Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2), 1480 Air Force Pentagon, Washington DC 20330-1480, is responsible for SCI policy. The provisions of this publication may not supersede the policies and guidance prescribed in the appropriate Director of Central Intelligence Directives governing the control, safeguarding, and dissemination of SCI as promulgated by the Cognizant Security Authority (CSA) for intelligence security

management. The CSA will, on behalf of the Senior Official of the Intelligence Community (SOIC), AF/A2, ensure appropriate resolution of actual or perceived conflicts regarding SCI and the provisions of this publication.

1.5.5. Special Access Program (SAP) Information. The Director of Security, Counterintelligence and Special Program Oversight (SAF/AAZ), 1480 Air Force Pentagon, Washington DC 20330-1480, is responsible for SAP policy and oversight of all Air Force SAPs. Should the policies and guidance in this instruction and those issued by DoD and/or the Air Force SAP Central Office (AFSAPCO) conflict, DoD and AFSAPCO policies and guidance will take precedence.

1.6. Waivers.

1.6.1. Commanders or equivalents, and staff agency chiefs send requests to waive provisions of DOD 5200.1-R, AFPD 31-4, or this AFI through command IP channels to SAF/AAP. FOAs also coordinate their requests with their respective functional head at Headquarters Air Force (HAF) before submitting to SAF/AAP [Reference DOD 5200.1- R, C1.4.2.].

1.6.2. Requests for waivers shall contain sufficient information to permit a complete and thorough analysis to be made of the impact on national security should the waiver be approved.

1.6.3. Waivers or exceptions to Special Access Program (SAP) requirements are forwarded through appropriate program channels to SAF/AAZ, 1480 Air Force Pentagon, Washington DC 20330-1480.

1.7. Reporting Requirements. *[Reference DOD 5200.1-R, C1.6.1.]*

1.7.1. MAJCOM and DRU IPs will submit the SF Form 311, Agency Security Classification Program Data, report to SAF/AAP by 1 October of each year.

1.7.1.1. Organizations sample data for Part C, Original Classification Decisions, and Part D, Derivative Classification Decisions during a consecutive 2-week period each fiscal year quarter (Oct-Dec, Jan-Mar, Apr-Jun, and Jul-Sep). In the last quarter the 2-week period must be set early since the reports are required by 15 October. Interagency Report Control Number 0230-GSA-AN applies to this information collection requirement.

1.7.1.1.1. Count the number of classification decisions in finished products for dissemination or retention, regardless of the media.

1.7.1.1.2. Do not count reproductions or copies.

1.8. Administrative Sanctions.

1.8.1. Send reports through command IP channels to SAF/AAP when someone knowingly, willfully, or negligently discloses classified information to unauthorized individuals as specified in EO 12958, as amended *[Reference DOD 5200.1-R, C1.5.]*.

1.8.2. Air Force commanders or equivalents and staff agency chiefs report unauthorized disclosures of classified information that violate criminal statutes to their servicing ISPM and Air Force Office of Special Investigations (AFOSI) offices *[Reference DOD 5200.1-R, C1.5.]*.

1.8.3. Commanders or equivalents, and staff agency chiefs take and process administrative sanctions/ actions for civilian appropriated fund employees IAW AFI 36-704, *Discipline and Adverse Actions*, AFMAN 34-310, *Nonappropriated Fund Personnel Program Management and Administration Procedures*, for nonappropriated fund employees, and IAW AFI 36-2907, *Unfavorable Information File (UIF) Program*, for military personnel. Contact the servicing civilian or military personnel flight office if assistance is needed. Commanders should consult their servicing legal office before taking action for serious violations.

1.9. Self-Inspection. See **paragraph 1.4** of this AFI *[Reference DOD 5200.1-R, C1.7.]*.

Chapter 2

ORIGINAL AND DERIVATIVE CLASSIFICATION

2.1. Original Classification Authority (OCA) *[Reference DOD 5200.1-R, C2.2.]*

2.1.1. The Secretary of the Air Force serves as the OCA and may further delegate this authority.

2.1.2. The process for delegating OCA authority is as follows:

2.1.2.1. Secretary of the Air Force delegates Top Secret, Secret, and Confidential authority.

2.1.2.2. SAF/AA delegates Secret and Confidential authority.

2.1.2.3. All requests for the delegation of OCA will be forwarded through command IP channels to SAF/AAP, Director of Information Protection, 1720 Air Force Pentagon, Washington, DC 20330-1340, for processing.

2.1.2.3.1. Address requests for original Top Secret authority to the Secretary of the Air Force.

2.1.2.3.2. Address requests for original Secret and Confidential authority to SAF/AA.

2.1.2.3.3. Only individuals in senior military or civilian positions (usually General Officer or Senior Executive Service level) at the first or second echelon of command carrying out a unique mission with responsibility for one of the eight subject areas prescribed by EO 12958, as amended, may be designated as an OCA.

2.1.2.3.4. OCA is assigned to a position, not a person. OCA will not be delegated other than identified in **paragraphs 2.1.2.1** and **2.1.2.2** above. However, deputies, vice commanders, chiefs of staff and similar other subordinates of an OCA are empowered to act as an OCA when they assume the duty position of an OCA in an "acting" capacity and have certified in writing that they have been trained in OCA responsibilities and classification principles in addition to the basic security training on the proper safeguarding of classified information and the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure before exercising this authority.

2.1.2.4. All requests will contain the full position title, functional office symbol, a detailed explanation of why the position requires OCA and an estimate of the annual use of the delegated authority.

2.1.3. SAF/AAP will maintain the master list of Air Force OCAs and post on the Information Protection Directorate Community of Practice (CoP). Periodically, SAF/AAP will request OCA validation from the MAJCOM/FOA/DRU IPMs.

2.1.3.1. Personnel will submit requests for changes or new requests through IP command channels as they occur.

2.1.3.2. See the Information Protection Directorate Community of Practice (CoP) web site for OCA training requirements.

2.2. Original Classification. *[Reference DOD 5200.1-R, Chapter 2 and Interim Information Security Guidance, April 16, 2004.]*

2.2.1. Original classification is the initial decision that an item of information could be expected to cause damage to the national security if subjected to unauthorized disclosure, and that the interests of the national security are best served by applying the safeguards of the Information Security Program to protect it. This decision may be made only by persons who have been specifically delegated the authority to do so, have received training in the exercise of this authority, and have program responsibility or cognizance over the information *[Reference: DOD 5200.1-R, C2.1.]*.

2.2.1.1. Before an original classification decision is made, it must be determined that classification guidance is not already available in the form of classification guides, plans or other memoranda.

2.2.1.2. OCAs are accountable to the Secretary of Defense for their classification decisions.

2.2.1.3. In those rare situations where the OCAs' decision must be rendered verbally due to the priorities of an on-going operation, written confirmation will be issued within seven days.

2.2.1.4. OCAs must notify users when there are changes to an original decision.

2.2.1.5. OCAs shall be prepared to present, as required, deposition and expert testimony in courts of law concerning classification of national security information and be prepared to defend and justify their original decisions.

2.2.2. Classification may be applied only to information that is owned by, produced by or for, or is under the control of the United States Government. Information may be considered for classification only if it concerns one of the categories specified in Section 1.4 of EO 12958, as amended.

2.3. Derivative Classification. The act of incorporating, paraphrasing, restating, or generating in a new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or a classification guide issued by an OCA. Within DOD, all cleared personnel can perform derivative classification.

2.3.1. Originating Agency's Determination Required (OADR). OADR is no longer an approved marking and should not be contained in any originally classified documents that have been created after October 14, 1995.

2.3.2. X1 through X8 are no longer approved markings and should not be contained in any originally classified documents that have been created on or after September 22, 2003.

2.3.3. When creating a derivatively classified document and using a source document that contains OADR or X1 through X8, the derivative classifier will place the following information in the Declassify On line:

DECLASSIFY ON: Source marked OADR (or X1 thru X8, whatever is applicable)

Date of source: 5 October 1993 (date of source document)

2.3.4. These documents will be subject to review for declassification 25 years after the date of the source document.

2.4. Classification Prohibitions and Limitations.

2.4.1. Under no circumstances shall information be classified in order to (1) conceal violation of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) prevent or delay the release of information that does not require protection in the interest of the national security *[Reference EO 12958, as amended, Section 1.7, DOD 5200.1-R, and Interim Information Security Guidance 16 April 2004]*.

2.4.2. The OCA having jurisdiction over the subject matter determines if information requested under the FOIA or the mandatory declassification review (MDR) provisions of EO 12958, as amended, should be declassified *[Reference DOD 5200.1-R, C2.4.3.5.]*

2.5. Classification Challenges. *[Reference DOD 5200.1-R, C4.9.]*

2.5.1. If holders of information have reason to believe that the information is improperly or unnecessarily classified, they shall communicate that belief to their commander or equivalent, staff agency chief, security manager, or supervisor.

2.5.2. Send formal challenges to classification, in writing, to the OCA with jurisdiction over the information in question.

2.5.3. Challenges to reclassification decisions are sent through command IP channels to SAF/AAP.

2.5.4. All classified information undergoing a challenge or a subsequent appeal will remain classified until a final resolution is reached.

2.6. Security Classification/Declassification Guides.

2.6.1. Required Elements. A security classification/declassification guide (see **Attachment 7** for sample format) is the written record of an original classification decision and appropriate declassification instructions and should be issued as early as practical in the life cycle of the classified system, plan, program or project. It shall, at a minimum:

2.6.1.1. Identify the subject matter of the classification guide.

2.6.1.2. Identify the OCA by name or personal identifier, and position.

2.6.1.3. Identify an agency Point of Contact (POC) (name, office symbol, mailing address, organizational e-mail address, DSN/commercial phone numbers) for questions regarding the classification guide.

2.6.1.4. Provide the date of issuance or last review.

2.6.1.5. State precisely the categories or elements of information to be declassified, to be downgraded, or not to be declassified.

2.6.1.6. State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified (***NOTE:*** Only one level of classification will be annotated for each element of information.)

2.6.1.7. State a concise reason for classification which, at a minimum, cites the applicable classification category or categories in Section 1.4 of EO 12958, as amended.

2.6.1.8. State, when applicable, special handling caveats.

2.6.1.9. Prescribe declassification instructions for each element of classified information.

2.6.1.10. Identify any related files series that have been exempted from automatic declassification pursuant to Section 3.3(c) of EO 12958, as amended.

2.6.1.11. To the extent a guide is used in conjunction with the automatic declassification provisions in Section 3.3 of EO 12958, as amended, state precisely the elements of information to be exempted from declassification to include:

2.6.1.11.1. The appropriate exemption category listed in section 3.3(b), and, when citing the exemption category listed in section 3.3(b)(9), specify the applicable statute, treaty or international agreement; and

2.6.1.11.2. A date or event for declassification IAW **section 1.5**.

2.6.2. OCA Responsibilities.

2.6.2.1. It is the responsibility of the OCA to publish classification/declassification guides to facilitate the proper and uniform derivative classification and declassification of their information. ***NOTE:*** In some cases, OCAs may determine that publishing classification guidance in other forms is more effective, e.g., program protection plans, system protection guides, AFIs. In these cases, the applicable publication will be considered the guide and the publishing requirements in **paragraph 3.3** still apply.

2.6.2.2. Each OCA will revise (IAW **paragraph 2.6.2.4** below) their security classification guides to include an advisory statement in the Release of Information section:

2.6.2.2.1. Release of program data on the World Wide Web. Extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. The search and data mining capabilities of Web technology must be assessed from a risk management perspective. Information intended for publication on publicly accessible or unprotected web sites must be cleared for public release prior to publication according to AFI 35-101, *Public Affairs Policy and Procedures*. If there are any doubts, do not release the information.

2.6.2.3. All guides will be reviewed by the servicing Foreign Disclosure Office before final approval.

2.6.2.4. Classification/declassification security guides shall be reviewed and updated, as circumstances require, but at least once every five years. ***NOTE:*** Due to the major changes implemented by EO 12958, as amended, all current Air Force classification/declassification guides will be reviewed no later than 31 December 2005, and every five years thereafter.

2.6.3. Publishing Requirements.

2.6.3.1. All guides which extend classification beyond 25 years must be approved by the Interagency Security Classification Appeals Panel (ISCAP). Once the OCA has signed the guide, the document will be sent to SAF/AAP who will forward it to the ISCAP for approval.

2.6.3.2. The OCA will report publication of or changes to security classification/ declassification guides to the Administrator, Defense Technical Information Center (DTIC) using DD Form 2024. DTIC will require an electronic copy of the guide.

2.6.3.3. OCAs must also forward a hard copy of the applicable publication or change to:

2.6.3.3.1. HQ AFHRA/RSA, 600 Chennault Circle, Maxwell AFB AL 36112-6424.

2.6.3.3.2. SAF/PA, 1690 Air Force Pentagon, Washington, DC 20330-1690.

2.6.3.4. All guides (to include any changes) will also be forwarded electronically to SAF/AAP at **SAF.AAP.workflow@pentagon.af.mil** and AFDO at **AFDO.Workflow@pentagon.af.mil** in PDF and Microsoft Word format.

2.6.4. Electronic Location of Guides. SAF/AAP will maintain the master list of all Air Force classification/declassification guides and will provide guides made available on the MOSIAC SIPRNET Community of Practice (CoP). Guides are also located on the DTIC web site. To access the DTIC web site you must have a DTIC account. The URL for this is **http://www.dtic.mil/dtic/registration**.

2.6.5. Nuclear Weapons Classification Policy. The DOD and the Department of Energy (DoE) issue joint security classification guidance for information relating to nuclear weapons. The Air Force issues security classification policy for information relating to nuclear weapons. Most of these products are classified and users will require the appropriate security clearance before accessing them. Users may obtain copies of Joint DOD/DoE classification guides through DTIC at a cost. Users forward requests for copies of these guides to SAF/AAP (1720 Air Force Pentagon, Washington DC 20330-1340) through command IP channels. Requests must include the name, address, and phone number of the activity POC, and the POC's level of access. IPs will validate this information before submitting the requests to SAF/AAP. For all other Air Force or other agency guides, go direct to the originator. Users refer to DOD 5200.1-I, DOD Index of Security Classification Guides, to determine what other guides relating to nuclear weapons classification guidance are needed. DOD 5200.1-I can be obtained from DTIC.

Chapter 3

DECLASSIFYING AND DOWNGRADING INFORMATION

3.1. Declassification and Downgrading Officials. Within the Air Force, only OCAs have the authority to declassify or downgrade classified information.

3.2. Declassification. Note: Exemptions identified in this chapter are found in *ISSO Directive Number 1, Section 2001.21(3)(i).*

3.2.1. Originally Classified Documents. The declassification decision determines the duration of protection *[Reference EO 12958, as amended, Section 1.6.(a)(4) and ISOO Directive Number 1, Section2001.12.]. At the time an item of information is classified, original classifiers will determine which of the following four declassification instructions will be used, selecting whenever possible, the declassification instruction that will result in the shortest duration of classification.*

3.2.1.1. A date or event less than 10 years from the date of the document; or, if unable to identify such a date or event;

3.2.1.2. A date 10 years from the date of the document;

3.2.1.3. A date greater than 10 and less than 25 years from the date of the document; or

3.2.1.4. A date 25 years from the date of the document.

3.2.2. Derivatively Classified Documents. The "Declassify on" line must include one of the following:

3.2.2.1. The date or event up to 25 years, as noted on the source document; or

3.2.2.2. Source marked OADR, date of source (cannot be a date after October 1995);

3.2.2.3. Source marked X1-X8, date of source (cannot be a date after September 2003);

3.2.2.4. 25X1 through 25X9, and a specific date or event for declassification; or

3.2.2.5. 25X1-human (the only category that does not require a date or event follow it).

3.3. Exceptions. RD/FRD *[Reference 10 CFR 1045.1 Subpart A]*. Documents containing RD or FRD are excluded from automatic declassification and do not require a declassification date. RD must be reviewed by the DoE prior to release. DoE and DOD must jointly review documents containing FRD prior to release.

3.4. Automatic Declassification. IAW EO 12958, as amended, Section 3.3, all Air Force activities that possess classified information that is of permanent historical value and is 25 years old or older should have completed a declassification review of these documents by 31 Dec 2006.

3.4.1. The Air Force Declassification Office (AFDO) has published the Air Force Declassification Plan that provides the framework for Air Force compliance with Section 3.3 of EO 12958, as amended. It pertains to all classified Air Force records that are 25 years old or older as of 31 December 2006, and have been determined under Federal law to have permanent historical value. The Air Force Declassification Plan is posted at the

AFDO web site (**http://www.afdo.hq.af.mil/Plan.htm**). It is critical that records management and information security personnel work together to ensure that requirements of both are met on classified records that are going to be sent to the National Archives or Federal Records Center.

3.4.2. All classified records shall be automatically declassified on 31 December of the year that is 25 years from the date of its original classification, unless it falls in one of the exemption categories (25X) listed in Section 3.3(b) of EO 12958, as amended.

3.4.3. The 25X categories *cannot* be used unless the specific information has been approved through the ISCAP process. This is usually done in the form of a security classification/declassification guide. (See **paragraph 2.6** and **Attachment 7**.) The Air Force has an approved list of exemption categories (listed in the Air Force Declassification Plan); however, the specific item must still be annotated in the security classification/ declassification guide before it is used on derivatively marked documents. For original classification decisions, no 25X marking, other than "25X1-human," is permitted on the "declassify on" line. All originally classified documents *will* contain either a date or event less than 10 years or a date from 10 to 25 years. The only exception is the marking "25X1-human." This marking may be used when the disclosure of the information could be expected to reveal the identity of a confidential human source or human intelligence source. This is the *only* 25X marking that does not require a date or event for declassification to be cited with the 25X marking.

3.5. Mandatory Review.

3.5.1. Mandatory review requests must identify the information requested with enough specificity to allow for location of the records with a reasonable amount of effort.

3.5.2. Send all requests for MDR to 11 CS/SCSL (MDR), 1000 Air Force Pentagon, Washington DC 20330-1000.

3.5.3. Send appeals to MDR decisions through 11 CS/SCSL (MDR) to SAF/AA, the Air Force Appellate Authority for MDRs.

3.6. Systematic Review for Declassification. Activities will set up an annual schedule for conducting systematic declassification reviews for the following records:

3.6.1. Records of permanent historical value prior to their twenty-fifth birthday. These records will be reviewed and appropriate action taken by 31 Dec of the same year that is 25 years from the date of its original classification.

3.6.2. Other records. Activities will set up a reasonable schedule for conducting declassification reviews for all other classified records.

3.7. Referrals. A referral is information that is subject to the provisions of EO 12958, as amended, Section 3.3, Automatic Declassification, and ISOO Directive No. 1, Section 2001.34, and has been referred to, within, or outside the Air Force for review. AFDO is the focal point for processing Air Force referrals. Detailed information regarding the referral process can be found in the Air Force Declassification Plan.

3.8. Public Release. When information is declassified, it is not releasable to the public until it has been approved for release through the security review process IAW AFI 35-101, Chapter

15. The same holds true for declassified or unclassified information that will be placed on an Internet site that can be accessed by the public.

3.9. Downgrading. Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level, and can be properly protected at a lower level. Any official who is authorized to classify or declassify the information and has authority over the information may downgrade information.

Chapter 4

MARKINGS

4.1. General. Air Force personnel who originally and derivatively classify information will mark those products according to DOD 5200.1-R and the ISOO Marking Booklet. Material other than ordinary paper documents, e.g., e-mail transmitted over a secure network, must have the same information either marked on it or made immediately available to holders by other means. *[Reference DOD 5200.1-R, C5.1.]*

4.2. Required Markings. Classified documents are required to have the following markings:

4.2.1. The overall classification of the document.

4.2.2. The agency, office of origin, and date of the document.

4.2.3. The office or source document that classified the information.

4.2.3.1. If it is originally classified, the document will reference the office. ***Example:*** **CLASSIFIED BY**: **SAF/AAP.**

4.2.3.2. If a document is derivatively classified, it will reference the source document or the security classification/declassification guide. ***Example:*** **DERIVED FROM**: **HQ USAF/A3/5 Memo dated 12 Jan 2008. Subj**: **Funding Problems.**

4.2.4. The reason for classification. Each originally classified document shall bear a concise statement of the reason for classification, determined by the original classifier. *[Reference DOD 5200.1-R, C5.2.4.]* The classification categories are listed in EO 12958, as amended, Section 1.4; DOD5200.1-R Interim Information Security Guidance, Chapter 2, Para 1. ***Example:*** **REASON: 1.4(e).**

4.2.4.1. If a document is derivatively classified, the "REASON" is not required to be carried over to the derivative document.

4.2.5. Declassification instructions, and any downgrading instructions that apply. ***Example:*** **DECLASSIFY ON: 15 MARCH 2010.**

4.2.5.1. If marking material that falls within one of the 25-year exemption categories, the correct marking will be as follows (NOTE: only derivatively classified documents will carry a 25X marking, with the exception of 25X1-human, which is allowed on originally classified documents):

DECLASSIFY ON: 25X5, 15 February 2010

4.2.6. Page and portion markings to identify the specific classified information in the document and its level of classification. When marking a document that is derivatively classified, ensure all markings and caveats are carried over from the source document to the derivative document.

4.2.7. Control notices and other markings that apply to the document.

4.2.8. When a document has been declassified or downgraded, the following markings shall be applied:

4.2.8.1. The word "Declassified" or the new classification if being downgraded.

4.2.8.2. The authority for the action (the OCA's office symbol and the identification of the correspondence or classification instruction that required it).

4.2.8.3. The date of declassification or downgrading action.

4.2.8.4. The overall classification markings that appear on the cover page or first page shall be marked through with a straight line. If downgraded, the new classification will be written in.

4.2.8.5. Page and portion markings will be remarked as required.

4.2.9. Notebooks, binders, folders, etc. containing classified documents will be conspicuously marked with the highest classification of the material contained. Affix the appropriate overall classification marking or classified cover sheet to the front and back of the notebook, binder, folder, etc.

4.3. Special Control and Similar Notices. *[Reference DOD 5200.1-R, C5.2.9.]*

4.3.1. Working Papers. Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information will be:

4.3.1.1. Dated when created.

4.3.1.2. Marked with the highest classification of any information contained in the document and annotated "WORKING PAPER".

4.3.1.3. Destroyed when no longer needed.

4.3.1.4. Protected IAW the assigned classification.

4.3.1.5. Marked in the same manner as a finished document at the same classification level when transmitted outside the facility or if retained for more than 180 days from the original creation date.

4.3.2. Communications Security (COMSEC). See AFI 33-211, *Communications Security (COMSEC) User Requirements,* for guidance on marking COMSEC documents and media.

4.3.3. Technical Documents. See AFI 61-204, *Disseminating Scientific and Technical Information,* for guidance on marking and disseminating technical documents. *[Reference DOD 5200.1-R, paragraph C5.2.9.8. and DODD 5230.24, Distribution Statements on Technical Documents.]*

4.3.4. SAPs. Documentation and information may be identified with the Phrase "Special Access Required" and the assigned nickname, codeword, trigraph, or digraph. See AFI 16-701, *Special Access Programs,* for additional guidance on SAP documents.

4.3.5. Restricted Data/Formerly Restricted Data (RD/FRD). *[Reference 10 CFR 1045.1, Subpart A.)*

4.3.5.1. Documents containing RD shall be marked:

RESTRICTED DATA

"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions."

4.3.5.2. Documents containing FRD shall be marked:

FORMERLY RESTRICTED DATA

"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954"

4.3.6. For Official Use Only (FOUO). See chapter 4 of DOD 5400.7/AF Supplement.

4.4. NATO. NATO documents should be marked in compliance with AFI 31-406, *Applying North Atlantic Treaty Organization (NATO) Protection Standards*, USSAN Instruction 1-69, *United States Implementation of NATO Security Procedures*, and C-M(2002)49, *Security Within the North Atlantic Treaty Organization (NATO)*. Any new policies, principles, standards, and procedures contained in C-M(2002)49 and it's supporting directives take precedence, where they conflict, over the guidelines expressed in USSAN 1-69, dated 21 April 1982.

4.5. Other Foreign Government Information (FGI).

4.5.1. Classification designations for FGI often do not parallel U.S. classification designations. Moreover, many foreign governments and international organizations have a fourth level of classification that generally translates as "Restricted," and a category of unclassified information that is protected by law in the originating country and is provided on the condition that it will be treated "in confidence." A table of U.S. and foreign government classification markings can be found in DOD 5200.1-R, Appendix 6.

4.5.2. Other foreign government classified documents shall be marked in English to identify the originating country and the applicable U.S. classification designation. If a classification designation has been applied to a foreign document by the originator, and it is the applicable U.S. English language designation, only the identity of the originating country need be applied to the document. ***Examples:***

A German document marked "Geheim" would be marked: **DEU SECRET**.

A UK document marked "SECRET" would be marked: **GBR SECRET**.

4.5.3. Foreign government documents that are marked with a classification designation that equates to Restricted, and unclassified foreign government documents that are provided to a DOD Component on the condition that they will be treated "in confidence," shall be marked to identify the originating government and whether they are Restricted or provided "in confidence." Additionally, they shall be marked "CONFIDENTIAL - Modified Handling".

Example:

A French document marked "Diffusion Restreinte" would be marked:

FRENCH RESTRICTED INFORMATION

Protect as:

CONFIDENTIAL - Modified Handling

4.5.3.1. **(Ref: DOD 5200.1-R, para C6.6.3.)** In order to ensure the protection of FGI provided in confidence (e.g., foreign government "Restricted," or foreign government unclassified information provided in confidence), such information must be classified under EO 12958, as amended. Provide a degree of protection to the FGI at least equivalent to that required by the foreign government or international organization that provided the information. If the foreign protection requirement is lower than the protection required for U.S. CONFIDENTIAL information, the following requirements shall be met:

4.5.3.1.1. The information shall be provided only to those individuals who have a need-to-know and access is required by official duties.

4.5.3.1.2. Individuals given access shall be notified of applicable handling instructions.

4.5.3.1.3. Documents shall be stored so as to prevent unauthorized access.

4.6. Marking of Foreign Government and NATO Information In DOD Documents.

4.6.1. When used in DOD documents, FGI must be marked to prevent premature declassification or unauthorized disclosure. To satisfy this requirement, U.S. documents that contain FGI shall be marked on the cover or first page, **"THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION."** In addition, the portions shall be marked to identify the classification level and the country of origin, e.g., **(GBR-C)**; **(DEU-C)**. If the identity of the foreign government must be concealed, the cover or first page of the document shall be marked, **"THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION,"** and applicable paragraphs shall be marked FGI together with the appropriate classification (**FGI-S**). The identity of the foreign government shall be maintained with the record copy, which must be appropriately protected.

4.6.2. The "Derived From" line shall identify the U.S. as well as foreign classification sources. If the identity of the foreign government must be concealed, the "Derived From" line shall contain the marking "Foreign Government information." In that case, the identity of the foreign government will be maintained with the record copy and protected appropriately. A U.S. document shall not be downgraded below the highest level of FGI contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations concerning downgrading or declassification shall be submitted through the DOD entity that created the document to the originating foreign government.

4.6.3. DOD classified documents that contain extracts of NATO classified information shall be marked as follows on the cover or first page: **"THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION."** Portions shall be marked to identify the NATO information (e.g., **NS**). When NATO or other foreign government RESTRICTED information is included in otherwise unclassified DOD documents, the following statement shall be affixed to the top and bottom of the page containing the information: **"This page contains (indicate NATO or country of origin) RESTRICTED information"**. The restricted portions shall be marked (e.g., **(NR) (GBR-R)**). The cover, (or first page, if no cover) of the document shall contain the following statement: **"This document contains NATO RESTRICTED information not marked for declassification (date of source) and shall be safeguarded in accordance with USSAN 1-69".**

4.6.4. Other foreign government classified documents should be marked in English to identify the originating country and the applicable U.S. classification designation.

4.6.5. Foreign government documents that are marked with a classification designation that equates to RESTRICTED, and unclassified foreign government documents that are provided to a DOD component, should be marked to identify the originating government and whether they are restricted or provided in confidence.

4.7. Audio and Video Tapes. Personnel responsible for marking and maintaining original classified audio and video tapes that document raw test data do not need to include footers/headers showing the applicable classification markings. However, the required classification markings must be placed on the outside of the container and reel. All copies made from the original tapes must include headers/footers that show the applicable classification markings. This will help ensure that valuable historical test data is not inadvertently erased during the classification marking process. *[Reference DOD 5200.1-R, C5.4.]*

4.8. Removable Information Systems Storage Media. Use SF Form 706, Top Secret ADP Media Classification Label; SF 707, Secret ADP Media Classification Label; SF Form 708, Confidential ADP Media Classification Label; SF 710, Unclassified Label, SF Form 711, ADP Data Descriptor Label, on removable information systems storage media. These are available through the Air Force Publications Distribution System. *[Reference DOD 5200.1-R, Paragraphs 5-407 and 5-409a-b.]*

4.8.1. Many new removable information systems storage media are of size and shape that precludes application of the standard forms. Such media storing classified information must be permanently marked to display the highest classification of stored information.

4.8.2. Designated Approving Authorities (DAA) have the authority to impose restrictions upon, and prohibit the use of, government owned removable information systems storage media for classified systems or networks. DAA approved restrictions will outline clearing, or destruction, procedures for unauthorized devices found in areas where classified processing takes place. Personally owned information systems storage media are prohibited in areas where classified is processed.

4.8.3. The inherent risk of loss of small storage devices should be considered before using them for storing or transporting classified information. Procedures to reduce the potential

for accidental loss must be included in local operating instructions. Include a review of these procedures in the semi-annual self-inspection and ISPRs.

4.9. Sensitive Compartmented Information (SCI). *[Reference DOD 5200.1-R, C5.4.11.]*

4.9.1. See AFI 14-302, *Control, Protection, and Dissemination of Sensitive Compartmented Information,* for Air Force policy on intelligence information.

4.9.2. The Special Security Office (SSO) is the focal point for release and dissemination of SCI. The Director of Central Intelligence Directive (DCID) 6/6, *Security Controls on the Dissemination of Intelligence Information* and *DCID 6/7, Intelligence Disclosure Policy* provide criteria for release of intelligence to foreign officials.

4.10. Authorized for Release To (REL TO) Markings. *[Reference DUSD(/)I Memo 27 Sep 2004, subject: Security Classification Marking Instructions.]*

4.10.1. "REL TO" identifies classified information that an originator has predetermined to be releasable based on guidance provided by an Air Force specifically designated foreign disclosure official or has been released, through established foreign disclosure procedures and channels, to the foreign country(ies)/international organizations indicated.

4.10.2. "REL TO" cannot be used with "Not Releasable to Foreign Nationals" (NOFORN) on page markings. When a document contains both NOFORN and REL TO portions, NOFORN takes precedence for the markings at the top and bottom of the page.

4.10.3. The full marking "REL TO USA//applicable country trigraph(s), international organization or coalition force tetragraph" shall be used after the classification and will appear at the top and bottom of the front cover, if there is one, the title page, if there is one, the first page and the outside of the back cover, if there is one. "REL TO" must include country code "USA" as the first country code listed. After the USA, country trigraphic code shall be listed in alphabetical order followed by international organization/coalition tetragraphic codes listed in alphabetical order.

4.10.4. Country codes shall be separated by a comma and a space with the last country code separated by a space, a lower case "and" and a space. ***EXAMPLE:*** TOP SECRET//REL TO USA, EGY and ISR.

4.10.5. When portion marking, countries do not need to be listed unless they are different from the countries listed in the "REL TO" at the top and bottom of the page. Text that is releasable to all the countries listed at the top and bottom of the page shall be portion marked "REL". ***EXAMPLE:*** (TS//REL).

4.10.6. If the information is releasable to countries that are different than those listed in the overall "REL TO" marking, the portion marking has the same format, but with the specific countries/organizations listed alphabetically. ***EXAMPLE:*** The overall document marking is 'SECRET//REL TO USA, NZL and NATO." However, the portion marking may be: (S//REL TO USA, AUS, NZL and NATO) to indicate that information contained in this portion is also releasable to Australia.

4.10.7. "NOFORN" is an authorized control marking for intelligence information IAW DCID 6/6, Security Controls on the Dissemination of Intelligence Information. Do not use the "NOFORN" dissemination control marking on any document, including derivatively

classified documents, without first verifying that the requirements of DCID 6/6 are met and that the marking is actually warranted.

4.10.8. Countries represented with the International Organization for Standardization (ISO) 3166 trigraphic codes can be obtained from the ISPM or from INTELINK on the SIPRNET.

4.11. Classified Electronic Mail (E-Mail).

4.11.1. All e-mails and documents accomplished on the SIPRNET, whether classified or unclassified, will contain the correct classification markings. Classified information may not be transmitted on the NIPRNET.

4.11.2. The first marking in the **Subject** line of the e-mail will be the overall classification of the e-mail using these symbols: (S) for Secret, (C) for Confidential, and (U) for Unclassified. Following this will be the subject title, followed by the classification of the subject title. ***Example:*** Subject: (S) Unclassified E-Mail Sample (U).

4.11.3. **Do not send classified messages or mark messages as classified on an unclassified network.**

4.11.4. Place the appropriate classification of the e-mail in all uppercase letters as the first line of the e-mail message text.

4.11.5. Begin the text of the message on the third line, leaving a blank line between the classification marking and the text.

4.11.6. All paragraphs and subparagraphs will be marked with the appropriate portion marking. Use the abbreviated classification symbol at the beginning of all paragraphs and subparagraphs.

4.11.7. Place the appropriate classification of the e-mail in all uppercase letters as the last line of the e-mail message text.

4.11.8. All attachments (if any) will be marked appropriately with overall and portion markings. Indicate the classification of the attachment by placing the abbreviated classification symbol in parentheses before the attachment icon.

4.11.9. Place classification, declassification, and downgrading instructions after the signature block on the left margin.

Chapter 5

SAFEGUARDING

Section 5A—Control Measures

5.1. General. Air Force personnel are responsible, both personally and officially, for safeguarding classified information for which they have access. Collecting, obtaining, recording, or removing, for any unauthorized use whatsoever, of any sensitive or classified information, is prohibited.

5.1.1. Everyone should be aware that advancing technology provides constantly changing means to quickly collect and transport information. The introduction of electronic storage or transmission devices into areas that store, process, and/or generate classified information increases the risk to that information.

5.1.2. Consult the servicing DAA for specific guidance concerning introduction into areas containing Information Systems (IS). *[Reference DODD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG).]*

Section 5B—Access

5.2. Granting Access to Classified Information. Personnel who have authorized possession, knowledge, or control of classified information grant individuals access to classified information when required for mission essential needs and when the individual has the appropriate clearance eligibility according to AFI 31-501, *Personnel Security Program Management*; has signed an SF 312, *Classified Information Nondisclosure Agreement (NdA)*, and has a need to know the information. Those granting access to classified information must gain the originator's approval before releasing the information outside the Executive Branch or as specified by the originator of the material. Also see **paragraph 5.4.1.1** of this AFI. *[References DOD 5200.1-R, C6.2., and EO 12958, as amended, Section 4.1(c.)]*

5.2.1. The Secretary of Defense directed all military members and civilian employees with Top Secret eligibility or access to a specially controlled access category or compartmented information to make a one time verbal attestation to the first paragraph of the SF 312. The verbal attestation must be witnessed by at least one individual in addition to the official who presides over the attestation and manages the process *[Reference DOD 5200.1-PH-1.]* The procedures for personal attestation include:

5.2.1.1. The statement, "Attestation completed on (date)," is placed in the bottom of the Organization block in Item 11 of the SF 312.

5.2.1.2. The individual making the verbal attestation will complete Item 11 of the SF 312. The witness will sign in the Witness block. The presiding official will sign in the Acceptance block.

5.2.1.3. Record the date of attestation in JPAS.

5.2.2. Confirm an individual's access level. The holder of the information must confirm valid need-to-know and must verify the level of access authorization. Those granting access to classified information will confirm a person's access level by:

5.2.2.1. Checking the person's access level, clearance eligibility, and date the person signed the SF 312 and completed Non-SCI Indoctrination, in JPAS; or

5.2.2.2. Confirming it through the employee's security manager, supervisor, or commander or equivalent, or staff agency chief; or

5.2.2.3. Receiving a visit request from a non-DOD visitor's security manager or supervisor. See **paragraph 5.5** for further guidance.

5.3. Nondisclosure Agreement (NdA). Signing the NdA is a prerequisite for obtaining access (see **paragraph 5.2**). Unit commanders or equivalents and staff agency chiefs are responsible for ensuring their employees have signed one by checking JPAS or the employee's personnel records. If they have not signed one, those responsible use DOD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Pamphlet*, to brief people on the purpose. Record the NdA on-line through JPAS prior to sending the signed form for retention. ***NOTE:*** When the employee's access level is passed to another office or activity, that office or activity can assume the employee has signed one.

5.3.1. Retention. Security managers mail the NdA to the following organizations who will retain the NdAs for 50 years.

5.3.1.1. For active military members, to HQ AFPC/DPFFCMI, 550 C St., W, Suite 21, Randolph AFB, TX 78150-4723.

5.3.1.2. For AFRC and ANG members, to HQ ARPC/DPSFR, 6760 E. Irvington Place, #4450, Denver, CO 80280-4450.

5.3.1.3. For retired flag or general officers or civilian equivalents receiving access under the provisions of AFI 31-501 and who do not already have a signed NdA in their retired file, ISPMs send NdAs to HQ AFPC/DPFFCMR, 550 C St., W, Suite 21, Randolph AFB TX 78150-4723.

5.3.1.4. For Air Force civilians, to the servicing civilian personnel office:

5.3.1.4.1. HQ AFPC/DPCMP, 550 C St, W, Suite 57, Randolph AFB, TX, 78150-4759.

5.3.1.4.2. Hill: OO-ALC/DPC (AFMC), 6053 Elm Lane, Hill AFB UT 84056-5819.

5.3.1.4.3. Tinker: 72 MSG/DPC (AFMC), 3001 Staff Drive Ste 1AH190B, Tinker AFB OK 73145-3014.

5.3.1.4.4. Robins: 78 MSG/DPC (AFMC), 215 Page Road Ste 325, Robins AFB GA 31098-1662.

5.3.1.4.5. 11 WG and the Pentagon: HQ 11 WG/DPC, 1460 Air Force Pentagon, Washington DC 20330-1460.

5.3.1.4.6. Wright-Patterson: 88 MSG/DPC (AFMC), 4040 Ogden Ave, Wright-Patterson AFB OH 45433-5763.

5.3.1.5. For persons outside the Executive Branch who receive access according to **paragraph 5.4**, the servicing ISPM to the activity granting access will file the NdA.

5.3.2. Refusal To Sign. When a person refuses to sign an NdA, the commander or equivalent, or staff agency chief:

5.3.2.1. Initiates security incident report, in JPAS, that the person refused to sign the NdA.

5.3.2.2. Denies the individual access to classified information.

5.3.2.3. Initiate actions to establish a Security Information File (SIF) according to AFI 31-501.

5.4. Access by Persons Outside the Executive Branch.

5.4.1. Policy. MAJCOM/FOA/DRU commanders and HAF 2-digits or their designees authorize individuals outside the executive branch to access Air Force classified material as follows unless otherwise provided in DOD 5200.1-R, paragraph C6.2.2.

5.4.1.1. Authorizing Officials (those cited in **paragraph 5.4.1** above) may grant access once they have:

5.4.1.1.1. Gained release approval from the originator or owner of the information. Normally, this is the same official identified in **paragraph 5.4.1.1.2.2** below.

5.4.1.1.2. Determined the individual has a current favorable personnel security investigation as defined by AFI 31-501 and a check of JPAS and a local files check (LFC) shows there is no unfavorable information since the previous clearance. A LFC must be processed according to AFI 31-501. ***EXCEPTION:*** In cases where there is no current personnel security investigation as defined in AFI 31-501, MAJCOM/FOA/DRU commanders and HAF 2-digits may request a National Agency Check (NAC) and grant access up to the Secret level before the NAC is complete when there is a favorable LFC and the Air Force Central Adjudication Facility (AFCAF) confirms there is no unfavorable information on the individual in JPAS. When applying this exception, follow the procedures outlined in AFI 31-501, paragraph 3.11. for interim security clearance eligibility.

5.4.1.1.2.1. Authority to grant access to persons outside the Executive Branch without a previous clearance may not be delegated below the listed positions in **paragraph 5.4.1.1.2**.

5.4.1.1.2.2. Before material is released to persons outside the Executive Branch without a previous clearance, the OCA must be contacted and approve the access.

5.4.1.1.3. Determined granting access will benefit the government.

5.4.1.2. Requests for access must include:

5.4.1.2.1. The person's name, SSAN, date and place of birth, and citizenship.

5.4.1.2.2. Place of employment.

5.4.1.2.3. Name and location of installation or activity where the person needs access.

5.4.1.2.4. Level of access required.

5.4.1.2.5. Subject of information the person will access.

5.4.1.2.6. Full justification for disclosing classified information to the person.

5.4.1.2.7. Comments regarding benefit(s) the U.S. Government may expect by approving the request.

5.4.1.3. The authorizing official will coordinate the processing of the NAC request with the nearest Air Force authorized requester of investigations.

5.4.1.4. Individuals with approval must sign an NdA before accessing information. Upon completion of access, individuals must sign an AF Form 2587, Security Termination Statement.

5.4.2. Congress. See AFI 90-401, *Air Force Relations with Congress*, for guidance when granting classified access to members of Congress, its committees, members, and staff representatives. *[Reference DOD 5200.1-R, C6.2.2.1]*

5.4.3. Government Printing Office (GPO). The GPO processes and confirms their personnel's access. *[Reference DOD 5200.1-R, C6.2.2.2]*

5.4.4. Representatives of the Government Accountability Office (GAO). See AFI 65-401, *Relations with the General Accounting Office*, for access requirements. *[Reference DOD 5200.1-R, C6.2.2.3.]*

5.4.5. Historical Researchers. AFHRA OL-A/HOR is the authority for granting access to historical researchers on behalf of the Air Force Historian (HQ USAF/HO). *[Reference DOD 5200.1-R, C6.2.2.4.]*

5.4.5.1. General. Requests for classified access by historical researchers will be processed only in exceptional cases wherein extraordinary justification exists. Access will be granted to the researcher only if the records cannot be obtained through available declassification processes (i.e., the FOIA and MDR processes) and when the access clearly supports the interests of national security.

5.4.5.2. Providing Access.

5.4.5.2.1. The researcher must apply to AFHRA OL-A/HOR in writing for the access. The application will fully describe the project including the sources of documentation that the researcher wants to access.

5.4.5.2.2. If AFHRA OL-A/HOR accepts the request for access, they will provide the researcher with written authorization to go to the nearest Air Force installation security forces office to complete a personnel security questionnaire for a NAC according to AFI 31-501.

5.4.5.2.3. If the results of the NAC are favorable and AFHRA OL-A/HOR approves access, the researcher must sign a SF 312 and an agreement to submit any notes and manuscript(s) for security and policy review (AFI 35-101). This process is to ensure the documents do not contain any classified information and, if so, determine if they can be declassified. Send the SF 312 to AFHRA OL-A/HOR for retention. Classified information will not be removed from government facilities.

5.4.5.2.4. Other Terms.

5.4.5.2.4.1. The access agreement is valid for two years. One two-year renewal is possible. A renewal will not be considered if the project appears to be inactive in the months before the end of the original agreement.

5.4.5.2.4.2. Access will be limited to those records 25 or more years of age.

5.4.5.2.4.3. Access based on a NAC is valid for Secret and Confidential information but does not meet the requirement for access to RD or SAP information. Access to Top Secret or SCI information is not authorized.

5.4.5.2.4.4. Access will be allowed only to Air Force records at AFHSO, AFHRA, and the National Archives and Records Administration (NARA).

5.4.5.2.4.5. Access to Air Force records still in the custody of the originating offices in the Washington National Capital Region must be approved in writing by the originating offices or their successors. It is the responsibility of the researcher to secure this approval.

5.4.6. Former Presidential Appointees. Persons who previously occupied policy-making positions to which the President appointed them may not remove classified information upon departure from office. All such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information they originated, received, reviewed, signed, or that was addressed to them while serving in their official capacity, provided the applicable Air Force OCA: *[Reference DOD 5200.1-R, C6.2.2.5.]*

5.4.6.1. Makes a written determination that such access is clearly consistent with the interests of national security;

5.4.6.2. Uses the same access determination procedures outlined in **paragraph 5.4** of this AFI;

5.4.6.3. Limits the access to specific categories of information over which the Air Force OCA has classification jurisdiction;

5.4.6.4. Maintains custody of the information or authorizes access to documents in the custody of the NARA; and,

5.4.6.5. Obtains the individual's agreement to safeguard the information and to submit any notes and manuscript for a security review (AFI 35-101, Chapter 15) to ensure that the documents do not contain classified information or to determine if any classified information should be declassified.

5.4.7. Judicial Proceedings. See AFI 51-301, *Civil Litigation,* for more information regarding the release of classified information in litigation.

5.4.8. Other Situations. Follow the guidance in **paragraph 5.4.1.1** above. *[Reference DOD 5200.1-R, C6.2.2.7.]*

5.4.9. Foreign Nationals, Foreign Governments, and International Organizations. Owners of classified information disclose it to foreign nationals, foreign governments, and international organizations only when they receive authorization from SAF/IAPD, 1080 Air Force

Pentagon, Washington DC 20330-1080. (See AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*, for more specific guidance.) See **Attachment 4** for guidance on transmitting classified information to foreign governments.

5.4.10. Retired Flag or General Officers or Civilian Equivalent. See AFI 31-501. These individuals need not sign a NdA if the original one is already filed in their retired file or JPAS. (see **paragraph 5.3.1.3**).

5.5. Access by Visitors. JPAS is the primary source for confirming access eligibility for DOD and DOD contractor personnel. Visit authorization letters will not be used to pass security clearance information unless JPAS is not available. *[Reference DOD 5200.1-R, C6.2.3.]*

5.5.1. Outgoing Visit Requests for Air Force Employees. When an Air Force employee requires access to classified information at:

5.5.1.1. A non-DOD contractor activity, the supervisor or security manager contacts the office to be visited to determine the desired clearance verification.

5.5.1.2. A DoE activity, the supervisor or security manager prepares and processes DoE Form 5631.20, according to DODD 5210.2, *Access to and Dissemination of Restricted Data*. Also see **paragraph 1.5.1** of this AFI.

5.5.2. Incoming Visit Requests. Air Force activity visit hosts serve as the approval authority for visits to their activities. Use JPAS to confirm security clearances of DOD personnel, including DOD contractors. Installation or activity commanders or equivalents, and staff agency chiefs receiving a visit request:

5.5.2.1. From non-DOD contractors, see DOD 5220.22-M, Chapter 6.

5.5.2.2. From foreign nationals or U.S. citizens representing a foreign government, process the visit request according to AFI 16-201.

5.6. Preventing Public Release of Classified Information. See AFI 35-101, Chapter 15, for guidance on security reviews to prevent people from publishing classified information in personal or commercial articles, presentations, theses, books or other products written for general publication or distribution.

5.7. Access to Information Originating in a Non-DOD Department or Agency. Holders allow access under the rules of the originating agency.

5.8. Administrative Controls.

5.8.1. Top Secret. The security of Top Secret material is paramount. Strict compliance with Top Secret control procedures take precedence over administrative convenience. These procedures ensure stringent need to know rules and security safeguards are applied to our most critical and sensitive information. The Air Force accounts for Top Secret material and disposes of such administrative records according to *WebRims Records Disposition Schedule*.

5.8.1.1. Establishing a Top Secret Control Account (TSCA). Unit commanders or equivalents, and staff agency chiefs who routinely originate, store, receive, or dispatch Top Secret material establish a Top Secret account and designate a Top Secret Control Officer (TSCO), with one or more alternates, to maintain it. The unit commander or

staff agency chief will notify the installation ISPM of the establishment of TSCAs and the names of thE TSCO. The TSCO uses AF Form143, **Top Secret Register Page**, to account for each document (to include page changes and inserts that have not yet been incorporated into the basic document) and each piece of material or equipment to include IS media. ***NOTE:*** For IS information systems or microfiche media, TSCOs must either describe each Top Secret document stored on the media on the AF Form 143 or attach a list of the documents to it. This will facilitate a damage assessment if the media are lost or stolen. ***EXCEPTIONS:***

5.8.1.1.1. Top Secret Messages. TSCOs do not use AF Form 143 for Top Secret messages kept in telecommunications facilities on a transitory basis for less than 30 days. Instead, use message delivery registers or other similar records of accountability.

5.8.1.1.2. Defense Courier Service (DCS) Receipts. TSCOs don't use AF Forms 143 as a receipt for information received from or delivered to the DCS. DCS receipts suffice for accountability purposes in these cases. Retain as prescribed by *WebRims Records Disposition Schedule*. ***NOTE:*** TSCOs may automate their accounts as long as all of the required information is included in the information system.

5.8.1.2. Top Secret Disclosure Records.

5.8.1.2.1. The TSCO uses AF Form 144, **Top Secret Access Record and Cover Sheet**, as the disclosure record and keeps it attached to the applicable Top Secret material. Each person that accesses the attached Top Secret information signs the form prior to initial access.

5.8.1.2.2. People assigned to an office that processes large volumes (i.e., several hundred documents) of Top Secret material need not record who accesses the material. ***NOTE:*** This applies only when these offices limit entry to assigned and appropriately cleared personnel identified on an access roster.

5.8.1.3. Top Secret Inventories. Unit commanders or equivalents, and staff agency chiefs:

5.8.1.3.1. Designate officials to conduct annual inventories for all Top Secret material in the account and to conduct inventories whenever there is a change in TSCOs. These officials must be someone other than the TSCO or alternate TSCOs of the TSCA being inventoried. The purpose of the inventory is to ensure all of the Top Secret material is accounted for, discrepancies resolved, and its status is correctly reflected on the corresponding AF Form 143.

5.8.1.3.2. Ensure necessary actions are taken to correct deficiencies identified in the inventory report.

5.8.1.3.3. Ensure the inventory report and a record of corrective actions taken are maintained with the account.

5.8.1.3.4. May authorize the annual inventory of Top Secret documents and material in repositories, libraries, or activities storing large volumes of Top Secret documents and material be limited to a random sampling using the percentage scale indicated

below. If account discrepancies are discovered the commander or equivalent, or staff agency chief must determine if the random sample percentage method will suffice or if a higher percentage inventory will be accomplished. If the higher percentage inventory is chosen, the inventory percentage will increase by no less than 20 percent.

5.8.1.3.4.1. One hundred percent, if there are fewer than 300 Top Secret documents.

5.8.1.3.4.2. No less than 90 percent if the holdings range from 301 to 400 Top Secret documents.

5.8.1.3.4.3. No less than 80 percent if the holdings range from 401 to 500 Top Secret documents.

5.8.1.3.4.4. No less than 70 percent if the holdings range from 501 to 600 Top Secret documents.

5.8.1.3.4.5. No less than 60 percent if the holdings range from 601 to 800 Top Secret documents.

5.8.1.3.4.6. No less than 50 percent if the holdings range from 801 to 1,000 Top Secret documents.

5.8.1.3.4.7. No less than 40 percent if the holdings range from 1,001 to 1,300 Top Secret documents.

5.8.1.3.4.8. No less than 30 percent if the holdings range from 1,301 to 1,800 Top Secret documents.

5.8.1.3.4.9. No less than 20 percent if the holdings range from 1,801 to 2,800 Top Secret documents.

5.8.1.3.4.10. No less than 10 percent if the holdings exceed 2,800 Top Secret documents.

5.8.1.4. Special Access Programs will follow the inventory and accountability requirements prescribed by the AFSAPCO.

5.8.1.5. Top Secret Receipts. TSCOs use AF Form 143 as a receipt when transferring Top Secret material from one TSCO to another on the same installation.

5.8.1.6. Top Secret Facsimiles. Top Secret facsimiles will be processed as another copy of the main Top Secret document in the TSCA. All the same rules apply except the register page and disclosure record will be faxed along with the document to the addressee. The addressee will sign and return them immediately to the sender for inclusion in the TSCA.

5.8.2. Secret. Unit commanders or equivalents, and staff agency chiefs set up procedures for internal control of Secret material. When entering Secret material into a mail distribution system, a receipt is required. Personnel may use AF Form 310, as a receipt.

5.8.3. Confidential. Individuals need not use a receipt for Confidential material unless asked to do so by the originating activity.

5.8.4. Foreign Government and NATO Information. See DOD 5200.1-R, C6.6., for receipting requirements.

5.8.5. Retention of Receipts. Retain receipt and other accountability records IAW *WebRims Records Disposition Schedule.*

Section 5C—Safeguarding

5.9. Care During Working Hours.

5.9.1. Personnel removing classified material from storage must:

5.9.1.1. For Top Secret material use AF Form 144, instead of SF Form 703, **Top Secret Cover Sheet** (see **paragraph 5.8.1.2.1**) except as specified in **paragraph 5.8.1.2.2** above. *[Reference DOD 5200.1-R, C6.3.2.1.]*

5.9.1.2. For Secret or Confidential material use SF Form 704, **Secret Cover Sheet**, or SF Form 705, **Confidential Cover Sheet**, as appropriate. These forms are available through the Air Force Publications Distribution system.

5.9.1.3. Use the SF Form 702, to record openings and closings for all General Services Administration (GSA)-approved security containers, vaults, and approved secure storage rooms.

5.9.2. The nature of the classified material typically stored within a secure room or vault may preclude the use of cover sheets. Use cover sheets when feasible.

5.10. End-of-Day Security Checks. Each unit and staff agency that processes, stores, or generates classified information will conduct an end-of-day security check to ensure classified material is stored appropriately. Personnel conducting these checks will do so at the close of each working day and record them on the SF Form 701, when security containers are present, even if the container was not opened that day. The "Checked By" column of the SF 702 does not require end-of-day documentation. Activities that are continuously staffed will establish local procedures to provide for daily security checks. Document those daily security checks on the SF 701. Note: Additional security and safety checks may be added in the blanks on the SF 701. All security containers will be listed on the SF 701 for end-of-day checks.

5.11. Residential Storage Arrangements.

5.11.1. SECAF and SAF/AA authorize the removal of Top Secret information from designated working areas. Requesters send requests through command IP channels to SAF/AAP [Reference DOD 5200.1-R, C6.3.7.1.].

5.11.2. MAJCOM/FOA/DRU commanders, or their ISPMs approve requests for removing Secret and Confidential material from designated work areas during non-duty hours *[Reference DOD 5200.1-R, C63.7.2.]*.

5.11.3. Contingency Plans. The written procedures will be developed as required by DOD 5200.1-R, C6.3.7.3. to include arrangements for notifying the responsible activity to pick up the classified container and material in the event something happens to the user *[Reference DOD 5200.1-R, C6.3.4.]*.

5.12. In-Transit Storage. Installation commanders:

5.12.1. Provide an overnight repository for classified material. A locally developed awareness program ensures operations dispatch, passenger services, base entry controllers, and billeting staff are aware of the availability.

5.12.2. Authorize the storage of Secret and Confidential material on the flightline during in-processing for deployment when the material is stored in a standard GSA-approved security container and the in-transit area is controlled and located on an Air Force installation.

5.13. Classified Meetings and Conferences. *[Reference DOD 5200.1-R, C6.3.8.]*

5.13.1. Classified information at meetings, conferences, symposia, portions or sessions of meetings, conferences, etc., during which classified information is to be disseminated shall be limited to appropriately cleared U.S. Government or U.S. Government contractor locations. Auditoriums, assembly halls, or gymnasiums that are primarily for public gatherings at cleared contractor facilities will not be used for a classified meeting at which Top Secret or Secret information would be disclosed, even though it is located on a portion of the contractor's cleared facility *[DOD 5220.22-R, Para C1.4.5.1]*.

5.13.2. Facility Approval Authority. Installation commanders or their designees assess the need to establish and approve secure conference and classified training facilities. Normally, secure conference or classified training facilities are only established at locations where frequent classified meetings or forums occur. If such a facility does not openly store classified information, secure construction requirements are not mandated. However, if installation commanders or their designees determine the local threat and security environment dictates more stringent construction requirements, they can use DOD 5200.1-R, Appendix 7 as a guide for constructing the facility.

5.13.3. Foreign Participation. Hosting officials refer to AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations,* for specific guidance.

5.13.4. Technical Surveillance Countermeasures (TSCM) Surveys. Commanders or equivalents, and staff agency chiefs or their designees determine to do TSCM surveys based on mission sensitivity and threat. See AFI 71-101, Volume 3, *The Air Force Technical Surveillance Countermeasures Program* for additional guidance.

5.14. Protecting Classified Material on Aircraft. Classified material and components are routinely carried on USAF aircraft. The purpose of this paragraph is to provide minimum standards for the protection of classified material and components while minimizing the impact on aircrew operations. The following minimum standards are established to provide cost effective security of classified material and components and to ensure detection of unauthorized access.

5.14.1. Aircraft commanders (owners/users) are responsible for the protection of classified material and components aboard their aircraft whether on a DOD facility, at a civilian airfield, or when stopping in foreign countries IAW DOD 5200.1-R, paragraph C6.3.9. Aircraft commanders should consult with the local ISPM or senior security forces representative for assistance in complying with these requirements.

5.14.2. To provide security-in-depth for classified components and material on aircraft, park the aircraft in an established restricted area or equivalent if the aircraft is designated Protection Level (PL) 1, 2, or 3. Refer to AFI 31-101, *Air Force Installation Security Program,* for details about protection levels.

5.14.2.1. Lock the aircraft, when possible, using a GSA-approved changeable combination padlock (Federal Specification FF-P-110) series available from GSA at 800-525-8027, under NSN 5340-00-285-6523 to secure the crew entry door, and/or

5.14.2.2. Place all removable classified material (e.g., paper documents, floppy disks, videotapes) in a storage container secured with a GSA-approved lock. The storage container must be a seamless metal (or similar construction) box or one with welded seams and a lockable hinged top secured to the aircraft. Hinges must be either internally mounted or welded. Containers installed for storage of weapons may also be used to store classified material even if weapons/ammunition are present, provided the criteria listed above have been met.

5.14.2.2.1. Have the aircraft and container checked for tampering every 12 hours. If unable to comply with the 12 hours due to crew rest, perform these checks no later than 1 hour after official end of crew rest.

5.14.2.2.2. Zeroize keyed COMSEC equipment as required by AFKAG-1N, *Air Force Communications Security (COMSEC) Operations*.

5.14.2.3. If the aircraft cannot be locked and is not equipped with a storage container, place the removable classified in an approved security container in an authorized U.S. facility. Classified components, attached to the aircraft, do not have to be removed.

5.14.3. To provide security-in-depth for classified components and material on PL 4 or non-PL aircraft, park the aircraft in a controlled area. PL 4 and non-PL aircraft should not be parked in a restricted area due to use of force limitations.

5.14.3.1. Lock the aircraft using a GSA-approved changeable combination padlock (Federal Specification FF-P-110) series available from GSA under NSN 5340-00-285-6523 to secure the crew entry door, and

5.14.3.2. Secure removable classified material IAW **paragraph 5.14.2.2** or **5.14.2.3**.

5.14.4. At non-U.S. controlled locations, host nation restricted/controlled areas may be used only if all material and components aboard the aircraft have been approved for release to the host nation by a cognizant foreign disclosure authority. Material should be secured IAW **paragraph 5.14.2** for restricted areas and **paragraph 5.14.3** for controlled areas.

5.14.5. If the aircraft cannot be parked in a restricted/controlled area:

5.14.5.1. Place removable classified material in a storage container and secure the container as described in **paragraph 5.14.2.2** Lock all aircraft egress points or secure them from the inside. Seal the aircraft with tamper proof seals such as evidence tape, numerically accountable metal, or plastic seals.

5.14.5.2. If the aircraft can be locked and sealed but there is no storage container, remove all removable classified material and store it in an approved security container in

an authorized U.S. facility. Classified components (e.g., AAR 47, ALE 47, etc.) may be stored in a locked and sealed aircraft.

5.14.5.3. If the aircraft cannot be locked and sealed and no storage container is available, off-load all classified material and components to an approved security container in an authorized U.S. facility.

5.14.5.4. If none of the above criteria can be met, U.S. cleared personnel must provide continuous surveillance. Foreign national personnel cleared by their government may be used if all material and components aboard the aircraft have been approved for release to the host nation by a cognizant foreign disclosure authority.

5.14.6. MAJCOM/FOA/DRUs determine specific risk management security standards for weather diverts and in-flight emergencies. Review AFKAG-1N if the classified information is COMSEC material.

5.14.7. If evidence exists of unauthorized entry, initiate a security investigation IAW **Chapter 9** of this AFI.

5.15. Information Processing Equipment.

5.15.1. Machines with Copying Capability. For copiers and facsimile machines or any machines with copying capability (e.g., microfiche machines), personnel consult their unit information manager (3A0X1) to determine if the machines are authorized for copying classified, and if so, determine if they retain any latent images when copying classified, and how to clear them when they do. Networked copiers present unique security hazards that require DAA approval. Also see **paragraph 5.24** for reproduction authority *[Reference DOD 5200.1-R, C6.3.10.]*.

5.15.2. Protect information system equipment or removable hard disk drive and the information system media at the highest security classification processed by the system *[Reference Air Force Special Security Instruction (AFSSI) 5020, paragraph 2.2.2.]*.

5.15.3. For any type of printer with a ribbon that has been used to print classified information, personnel remove the ribbon and store it as classified. See DOD 5200.1-R, Chapter 6 for storage requirements.

5.15.4. Used toner cartridges may be treated, handled, stored, and disposed of as unclassified, when removed from equipment that has successfully completed its last print cycle.

5.16. General Safeguarding Policy. *[Reference DOD 5200.1-R, C6.4.]*

5.16.1. See DOD 5200.1-R, C1.4 and **paragraph 1.6** when requesting waivers to provisions of DOD 5200.1-R, AFPD 31-4, or this publication.

5.16.2. The Air Force does not authorize use of security controls listed in DOD 5200.1-R, paragraph C6.8. *[Reference DOD 5200.1-R, Paragraph C6.8.]*

5.16.3. Use of Force for the Protection of Classified Material. See AFI 31-207, *Arming and Use of Force By Air Force Personnel.*

5.16.4. SCI Safeguarding Policy. See Air Force Manual (AFMAN) 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (supersedes USAFINTEL 201-1.).*

5.16.5. Retention of Classified Records. Personnel follow the disposition guidance in *WebRims Records Disposition Schedule.*

5.17. Standards for Storage Equipment. GSA-approved security containers must have a label stating "General Services Administration Approved Security Container" affixed to the front of the container usually on the control or top drawer.

5.17.1. If the label is missing or if the container's integrity is in question, the container shall be inspected by a GSA certified inspector.

5.17.2. Organizations without GSA certified inspectors must confirm that contractor inspectors have current GSA inspector training certificates prior to allowing them to determine the security integrity of GSA-approved containers.

5.17.3. Information on obtaining inspections and recertification of containers can be found in FED-STD -809A on the DoD lock program website at: (**https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks**) or by calling DSN 312-551-1212.

5.17.4. Inspecting personnel must note their findings and the source of confirmation on an AFTO Form 36**,** (available on the AFEPL), and retain that record in the container *[Reference DOD 5200.1-R, C6.4.]*.

5.18. Storage of Classified Information. *[Reference DOD 5200.1-R, C6.4.]*

5.18.1. Replacement of Combination Locks. Commanders or equivalents, and staff agency chiefs must ensure all combination locks on GSA-approved security containers and doors are replaced with those meeting Federal Specification FF-L-2740 starting with those storing the most sensitive information according to the priority matrix in DOD 5200.1-R, Appendix 7.

5.18.2. Due to operational necessity or the size and nature of some classified materials, it may be necessary to construct secure rooms for storage because GSA-approved containers or vaults are unsuitable or impractical. Secure rooms must be approved by the ISPM and be constructed IAW DOD 5200.1-R Appendix 7. Access to secure rooms must be controlled to preclude unauthorized access. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. The nature of the classified material typically stored within a secure room or vault may preclude the use of cover sheets.

5.19. Use of Key-Operated Locks *[Reference DOD 5200.1-R, C6.4.3.6.1.]*

5.19.1. The authority to determine the appropriateness of using key-operated locks for storage areas containing bulky Secret and Confidential material is delegated to the unit commanders or equivalents, and staff agency chiefs having this storage requirement. When key-operated locks are used, the authorizing official will designate lock and key custodians.

5.19.2. Lock and key custodians use AF Form 2427, (available on the AFEPL) to identify and keep track of keys.

5.20. Procurement of New Storage Equipment. *[Reference DOD 5200.1-R, C6.4.5.]*

5.20.1. Requesters of exceptions send their requests through command IP channels to SAF/AAP who will then notify USD/I of the exception *[Reference DOD 5200.1-R, C6.4.2.]*.

5.20.2. See AFMAN 23-110, Volume II, *Standard Base Supply Customer's Procedures [Reference DOD 5200.1-R, C6.4.2.]*.

5.21. Equipment Designations and Combinations.

5.21.1. See AFMAN 14-304 for guidance on marking security containers used to store SCI *[Reference DOD 5200.1-R, C6.4.1.]*.

5.21.2. Use SF Form 700, **Security Container Information** (available through the Air Force Publications Distribution system), for each vault or secure room door and security container, to record the location of the door or container, and the names, home addresses, and home telephone numbers of the individuals who are to be contacted if the door or container is found open and unattended. Applying classification marking to SF 700, Part 1, is not required when separated from Part 2 and 2a.

5.21.2.1. Affix the form to the vault or secure door or to the inside of the locking drawer of the security container. Post SF Form 700 to each individual locking drawer of security container with more than one locking drawer, if they have different access requirements.

5.21.2.2. The SF 700 contains Privacy Act information and must be safeguarded from casual view, but must be readily identifiable by anyone that finds the facility unsecured.

5.21.3. When SF Form 700, Part II, is used to record a safe combination, it must be:

5.21.3.1. Marked with the highest classification level of material stored in the security container; and,

5.21.3.2. Stored in a security container other than the one for which it is being used.

5.22. Repair of Damaged Security Containers *[Reference DOD 5200.1-R, C6.4.7.]*

5.22.1. Locksmiths or technicians must be GSA certified and either have a favorable NAC or must be continuously escorted while they are repairing security containers. See guidance for unescorted entry to restricted areas in AFI 31-501.

5.22.2. **(DELETED)**

5.22.3. Federal Standard 809, Neutralization and Repair Of GSA-approved Containers can be obtained from the NFESC, 1100 23rd Avenue, Code ESC66, Port Hueneme, California 93043-4370 or at: **http://locks.nfesc.navy.mil/pdf_files/fs809.pdf**.

5.22.4. Locksmiths or technicians who open or repair GSA approved containers must document their actions on an AFTO Form 36 retained in the container.

5.23. Maintenance and Operating Inspections. Personnel will follow maintenance procedures for security containers provided in AFTO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Security Type Equipment*. Commanders or equivalents and staff agency chiefs

may authorize trained security managers and security container custodians to perform inspections and preventive maintenance on safes and vaults. Note: Training is conducted by locksmiths or other personnel who are qualified as to technical construction, operation, maintenance, and purpose of such security type equipment *[Reference DOD 5200.1-R, C6.4.7.]*.

5.24. Reproduction of Classified Material.

5.24.1. Unit commanders or equivalents, and staff agency chiefs designate equipment for reproducing classified material.

5.24.2. The DAA approves networked equipment used to reproduce classified information. Information managers (3A0X1) issue procedures for clearing copier equipment of latent images.

5.24.3. Security managers:

5.24.3.1. Should display procedures for clearing latent images of equipment used to copy classified material in a location clearly visible to anyone using the equipment;

5.24.3.2. Develop security procedures that ensure control of reproduction of classified material; and,

5.24.3.3. Ensure personnel understand their security responsibilities and follow procedures.

5.25. Control Procedures. Unit commanders or equivalents and staff agency chiefs designate people/ positions to exercise reproduction authority for classified material in their activities *[Reference DOD 5200.1-R, C6.5.1.]*.

5.26. Emergency Authority. *(*See *EO 12958, as amended, Section 4.2(b) and ISOO Directive No. 1, Section 2001.51.)*

5.26.1. In emergency situations, in which there is an imminent threat to life or in defense of the homeland; Military Department or other DOD Component Agency, MAJCOM/FOA/DRU commanders may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

5.26.1.1. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;

5.26.1.2. Limit the number of individuals who receive it;

5.26.1.3. Transmit the classified information via approved federal government channels by the most secure and expeditious method according to DOD 5200.1-R, or other means deemed necessary when time is of the essence;

5.26.1.4. Provide instructions about what specific information is classified, how it should be safeguarded; physical custody of classified information must remain with an authorized federal government entity, in all but the most extraordinary circumstances;

5.26.1.5. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed NdA.

5.26.2. Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information and USD/I by providing the following information through ISPM channels;

5.26.2.1. A description of the disclosed information;

5.26.2.2. To whom the information was disclosed;

5.26.2.3. How the information was disclosed and transmitted;

5.26.2.4. Reason for the emergency release;

5.26.2.5. How the information is being safeguarded, and;

5.26.2.6. A description of the briefings provided and a copy of the signed NdA.

Section 5D—Disposition and Destruction of Classified Material

5.27. Retention of Classified Records.

5.27.1. Personnel follow the disposition guidance in *WebRims Records Disposition Schedule.*

5.27.2. Unit commanders or equivalents, and staff agency chiefs will designate a "clean-out day" once a year to ensure personnel are not retaining classified material longer than necessary *[Reference DOD 5200.1-R, C6.7.2.1.]*.

5.28. Disposition and Destruction of Classified Material *[Reference DOD 5200.1-R, C6.7.2.]*

5.28.1. Shredders purchased from an approved product list that produces a crosscut shred size of ½" x 1/32" or smaller, may continue to be used for destruction of collateral information until 1 October 2008. Employ compensatory measures such as mixing unclassified material with the shredding and stirring of the shredded material. Replacement shredders for destruction of classified information must be purchased from the National Security Agency (NSA)-approved Equipment Product List. Obtain information on approved destruction devices from the NSA Information Assurance web site (**http://www.nsa.gov/ia/government/mdg.cfm**). Please note that this list is FOUO and is updated quarterly on the restricted NSA site.

5.28.2. Records of Destruction Process.

5.28.2.1. Top Secret. TSCOs will ensure:

5.28.2.1.1. Two people with Top Secret access are involved in the destruction process;

5.28.2.1.2. Destruction is recorded on one of these forms: AF Form 143; AF Form 310; or, AF Form 1565, and,

5.28.2.1.3. The destruction record is attached to the AF Form 143 (used to account for the document) when the destruction is not recorded on the AF Form 143 itself.

5.28.2.2. Secret and Confidential. A record of destruction is not required. A cleared person must perform the destruction.

5.28.2.3. FGI. See DOD 5200.1-R, C6.6, for destruction of FGI.

5.28.2.4. Destruction of Information System Media. Dispose of information system media according to AFSSI 5020, *Remanence Security*.

5.28.2.5. Disposition of Destruction Records. Dispose of destruction records according to *WebRims Records Disposition Schedule.*

5.28.3. Central Destruction Facility (CDF). The installation commander determines the need for a CDF to destroy classified information, who manages the CDF, and who funds for maintenance. Usually, the decision is based on the amount of classified that is destroyed at the installation and the cost of building and maintaining a CDF, versus purchasing and maintaining other authorized equipment for destruction within individual units.

Chapter 6

TRANSMISSION AND TRANSPORTATION

Section 6A—Methods of Transmission or Transportation

6.1. General Policy.

6.1.1. Hand carrying Classified Material During Temporary Duty (TDY) Travel. Hand carrying classified material during TDY poses a risk and should be done as a last resort in critical situations. Whenever possible, personnel will use standard secure methods for relaying the data, e.g., mail through secure channels or through approved secure electronic means. Authorizing officials must assess the risk before authorizing the hand carrying of classified material. Some factors to consider during the risk assessment process are:

6.1.1.1. The environment in which the material will be handcarried. Consider the chances of the material being confiscated by unauthorized personnel. The servicing AFOSI office should be able to assist in determining the risks associated with the environment.

6.1.1.2. The sensitivity of the information. Consider the damage it could cause the United States if the information was compromised.

6.1.1.3. The availability of authorized facilities for storing the classified during overnight layovers, at the TDY location, etc. Consider storing the material at a U.S. military installation or other government facility.

6.1.2. Laptop Computers are High Risk. Because of their commercial value, laptop computers are an especially high risk when used to transport classified information. When using laptops to handcarry classified information, couriers must ensure both laptop and disks are prepared according to **paragraph 6.6.3**. In addition, as required for all classified material, couriers must take special care to ensure laptops and disks are kept under constant surveillance or in secure facilities/containers at all times.

6.1.3. Air Force Office of Primary Responsibility for Transmission and Transportation Policy. SAF/AAP establishes Air Force policy and procedures for transmission and transportation of classified information and material *[Reference DOD 5200.1-R, C7.1.1.1.]*.

6.1.4. Transmitting Classified Material by Pneumatic Tube Systems. Installation commanders approve the use of pneumatic tube systems and ensure that the equipment and procedures provide adequate security *[Reference DOD 5200.1-R, C7.1.1.1.]*.

6.1.5. Electronic Transmission and Physical Transportation of COMSEC Material. Personnel may acquire information on electronic transmission and physical transportation of COMSEC information and material from their supporting COMSEC manager. *[Reference AFI 33-201, AFI 33-211, AFI33-275, and DOD 5200.1-R, C7.1.1.2.]*

6.1.6. Releasing Other Agency Information Outside of the DoD. Personnel go direct to owners of other agency information to request permission to release the information outside the DoD *[Reference DOD 5200.1-R, C7.1.1.4.]*.

6.2. Transmission and Transporting Top Secret Information. *[Reference DOD 5200.1-R, C7.1.2.]*

6.2.1. Electronic Means. Obtain information about transmitting Top Secret information via electronic means from their Information Assurance office. See **paragraph 5.8** *[Reference DOD 5200.1-R, C7.1.2.2.]*.

6.2.2. DOD Component Courier Service. The Air Force does not have its own courier service *[Reference DOD 5200.1-R, C7.1.2.4.]*.

6.2.3. Department of State Diplomatic Courier Service. Personnel who need to transport classified material use the Department of State courier system when: *[Reference DOD 5200.1-R C7.1.2.5.]*

6.2.3.1. Transporting classified material through or within countries hostile to the United States or any foreign country that may inspect it.

6.2.3.2. Transporting Top Secret material to an installation serviced by diplomatic pouch. Personnel can find out if they are serviced by diplomatic pouch through their local military postal office.

6.3. Transmitting and Transporting Secret Information. *[Reference DOD 5200.1-R, C7.1.3.]*

6.3.1. Also see AFI 31-601 *[Reference DOD 5200.1-R, C7.1.3.2.]*.

6.3.2. The Air Force authorizes the use of the current holder of the GSA contract for overnight delivery of Secret information in urgent cases and when the delivery is between DOD Components and their cleared contractor facilities within the United States and its Territories. This applies to locations in Alaska, Hawaii, and Puerto Rico when overnight delivery is possible. USD/I has already ensured the conditions cited in DOD 5200.1-R, paragraph C7.1.3.3, have been met *[Reference DOD 5200.1-R, C7.1.3.3.]*

6.3.2.1. The Defense Security Service maintains a list of authorized GSA contract overnight delivery services at **http://www.dss.mil/isec/approved_overnight.htm**.

6.3.2.2. The carriers identified on the DSS list may be used for urgent overnight delivery of Secret and Confidential material within the continental United States (CONUS) when overnight delivery cannot reasonably be accomplished by the U.S. Postal Service. However, classified COMSEC information may not be transmitted overnight. Controlled Cryptographic Information (CCI) that is unclassified may be shipped overnight.

6.3.2.3. Carrier personnel should not be notified that the package contains classified material.

6.3.2.4. Packages are typically shipped on Monday through Thursday only. This ensures that the package does not remain in the possession of the carrier service over a weekend. However, the security manager may approve shipment on other days providing the receiver has appropriate procedures in place. These procedures must ensure that a cleared person will receive and sign for the package on Saturday, Sunday, or holidays, and that he or she is able to secure the package in approved storage. *[DOD 4525.8-M.]*

6.3.2.5. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and for verification of the correct mailing address.

6.3.3. For more information on protective security service carriers see DOD 5220.22-R, *Industrial Security Regulation*, AFI 31-601, AFPD 24-2, *Preparation and Movement of Air Force Materiel*, and AFI 24-201, *Cargo Movement. [Reference DOD 5200.1-R, C7.1.3.8.]*

6.3.4. Electronic Means. Obtain information about transmitting Secret information via electronic means from the supporting Information Assurance office.

6.4. Transmitting Confidential Information. *[Reference DOD 5200.1-R, C7.1.4.]*

6.4.1. Since first class mail bearing the "Return Service Requested" notice is an option for transmitting Confidential material, recipients must protect it as Confidential material unless they determine the contents are unclassified. ***EXCEPTION:*** Official Mail Center (OMC) and Activity Distribution Offices (ADO) will comply with the provisions of *DOD 4525.8-M/AF* Sup.

6.4.1.1. The outer envelope or wrapper shall be endorsed with "Return Service Requested" instead of "POSTMASTER: Do Not Forward".

6.5. Transmission of Classified Material to Foreign Governments. *[Reference DOD 5200.1-R , C7.1.5.]*

6.5.1. Also see AFI 31-601 and AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations [Reference DOD 5200.1-R, C7.1.5.1.]*.

6.5.2. US classified material will not be shipped from a US industrial activity to a foreign entity *[Reference DOD 5200.1-R, C7.1.5.1.]*.

Section 6B—Preparation of Material for Transmission

6.6. Envelopes or Containers. *[Reference DOD 5200.1-R, C7.2.]*

6.6.1. For the purpose of this policy, an activity is a facility *[Reference DOD 5200.1-R, C7.2.1.1.5.]*.

6.6.2. Receipts. See receipting requirements at **paragraph 5.8**.

6.6.2.1. Senders trace unacknowledged receipts:

6.6.2.1.1. Within 30 days for material sent within CONUS.

6.6.2.1.2. Within 45 days for material sent outside CONUS.

6.6.2.2. The recipient must immediately date, sign, correct, and return the receipt to the sender.

6.6.2.3. If recipients do not return the receipt and confirm they have not received the material, the sending activity must initiate security incident procedures according to **Chapter 9** of this AFI.

6.6.3. Laptop Computer and Disk Preparation Requirements. Couriers must ensure that:

6.6.3.1. Laptops are password protected.

6.6.3.2. Laptops and disks are marked according to DOD 5200.1-R, paragraphs C5.4.8, C5.4.9, and C5.4.10.

6.6.3.3. Laptops and disks containing classified information are kept under constant surveillance or stored in secure containers/facilities.

6.6.3.4. Classified media or systems will be wrapped or secured within a container if outer classification markings are visible.

Section 6C—Escort or Handcarrying of Classified Material

6.7. General Provisions. *[Reference DOD 5200.1-R, C7.3.]*

6.7.1. Authorization. *[Reference DOD 5200.1-R, C7.3.1.1.]*

6.7.1.1. The unit commander or equivalent, or staff agency chief authorizes appropriately cleared couriers to handcarry classified material on commercial flights. See DOD 5200.1-R, paragraph C7.3.1.2., for required documentation and this AFI, **paragraph 6.1.1**, for a cautionary statement regarding handcarrying classified material.

6.7.1.2. The unit commander or equivalent, staff agency chief, or security manager authorizes appropriately cleared couriers to handcarry classified material by means other than on commercial flights.

6.7.2. Security managers or supervisors brief each authorized member handcarrying classified material *[Reference DOD 5200.1-R, C7.3.1.2.]*.

6.7.3. Each Air Force activity or unit that releases classified material to personnel for handcarrying: *[Reference DOD 5200.1-R, C7.3.1.1.]*

6.7.3.1. Maintains a list of all classified material released.

6.7.3.2. Keeps the list until they confirm all the material reaches the recipient's activity or unit.

6.8. Documentation. Unit commanders or equivalents, staff agency chiefs, or security managers issue and control DD Form 2501 (Safeguard), **Courier Authorization** (available through the Air Force Publications Distribution system), for handcarrying classified material by means other than on commercial flights. This doesn't preclude the use of a courier authorization letter for infrequent courier situations. ***EXCEPTION:*** Documentation is not necessary when handcarrying classified information to activities within an installation (i.e., Air Force installation, missile field, or leased facilities within the local commuting area). ***NOTE:*** Account for DD Form 2501 (Safeguard) as prescribed in AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT) [Reference DOD 5200.1-R, C73.2.2.]*.

Chapter 7

SPECIAL ACCESS PROGRAMS (SAPS)

7.1. Control and Administration *[Reference DOD 5200.1-R, C8.1.3.3.]*

7.1.1. SAF/AAZ administers SAPs for the Air Force. See AFPD 16-7, *Special Access Programs.* ***EXCEPTION:*** HQ USAF/XOI controls SCI programs.

7.1.2. Contractor personnel associated with Special Access Programs (SAPs) administered under DOD 5220.22-M Sup 1 and AFI 16-701 may be nominated and approved by the cognizant Program Security Officer (PSO) to fulfill the roles and responsibilities of a security manager.

7.2. Code Words and Nicknames. Unit commanders or equivalents, and staff agency chiefs obtain code words and nicknames through channels from the servicing control point (normally, the MAJCOM/FOA/ DRU Information Management activity) *[Reference DOD 5200.1-R, C8.1.4.6.1]*.

Chapter 8

SECURITY EDUCATION AND TRAINING

Section 8A—Policy

8.1. General Policy. Effective information security training is a cornerstone of the Air Force Information Security Program. All Air Force personnel need information security training whether they have access to classified information or not. All Air Force personnel are individually responsible for protecting the national interests of the United States. All security infractions and/or violations must be immediately reported, circumstances examined and those responsible held accountable and appropriate corrective action taken. Commanders or equivalents, and staff agency chiefs are responsible for ensuring that personnel are knowledgeable and understand their responsibility to protect information and resources deemed vital to national security.

8.2. Methodology. The Air Force will provide information security training to its personnel and contractors, as appropriate, on a continuous basis using government and commercial training sources. Various training methods will be used to administer training, such as classroom instruction, one-on-one, computer-based, and other distant learning training media. The Air Force will maintain a cadre of trained professional career security personnel and security managers to administer, implement, and measure the program's effectiveness. When funds and resources permit, professional security personnel and security managers should attend in-residence type training courses.

8.3. Roles and Responsibilities.

8.3.1. These roles and responsibilities are in addition to those listed in **paragraph 1.3**.

8.3.2. SAF/AAP is responsible for coordinating development of Air Force specific information security training course materials and curriculums.

8.3.3. Commanders or equivalents, and staff agency chiefs are responsible for implementing the information security training program, developing supplemental training tools, and assessing the health of their programs on a continuous basis. In addition, they will:

8.3.3.1. Ensure appointed security managers receive training through the ISPM within 90 days of their assignment and that the training is annotated in the individual's official personnel file (OPF) or military training record.

8.3.3.2. Budget for security awareness training products, materials, and the formal training of security managers.

8.3.3.3. Actively support and monitor security education training.

8.3.3.4. Ensure records are maintained on a calendar year basis of personnel attending initial, refresher and specialized information security training. As a minimum, these records must reflect the date(s) training was conducted and the name of personnel in attendance.

8.3.4. Supervisors will conduct and/or ensure personnel receive training as required by this instruction, document it when required, and ensure credit is given for course completion or briefing attendance, as appropriate.

8.3.5. ISPMs that oversee security managers are responsible for:

8.3.5.1. Developing and overseeing implementation of information security training programs.

8.3.5.2. Assessing the effectiveness of training programs as part of the annual ISPR (see **para 1.4.2**).

8.3.5.3. Developing and conducting classroom or one-on-one training for newly appointed security managers.

8.3.5.4. Developing and distributing generic information security training lesson plans, which cover the basic information security work-center components (information, personnel and industrial security programs) to include installation specific security requirements.

8.3.5.5. Assisting security managers in the development of unit specific lesson plans, motivational materials and training aids.

8.3.5.6. Publicly recognizing the training efforts of effective security managers.

8.3.5.7. Providing civilian employees who complete information security managers training with a certificate, which they can use to enter course completion into their training file.

8.3.5.8. Providing military members who complete information security managers training with a certificate, which they can use to enter course completion into their on-the-job training record or other official records, as appropriate.

8.3.5.9. If full-time contractor performance or services is required or anticipated to support the Information Security work center or a specific security discipline (information, personnel, or industrial), the ISPM will assure the following language is inserted into the statement of work (SOW). "The contractor will be required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system."

8.3.5.10. When contractors require Information Security work center training, the ISPM must approve the contractor's enrollment in any web-based training course. In addition, the ISPM must notify, in writing, the 37 TRS/DORM Training Manager of this action, to include the contractor's name, SSAN, contract number, and contractor's cage code and contract performance location. The request may be Faxed to DSN 473-4150.

8.3.6. Security Managers are responsible for:

8.3.6.1. Ensuring security training is conducted as outlined in this AFI.

8.3.6.2. Developing organizational specific security lesson plans, as necessary.

8.3.6.3. Advising the commander on the status of the unit's security training program.

8.3.6.4. Ensuring training is documented and records are properly maintained, if applicable.

8.3.6.5. Providing security management, awareness, and training to on-base contractor visitor groups integrated into the organization unless the mission, operational requirements, autonomous nature or other factors require them to establish and maintain their own security program under the NISPOM.

Section 8B—Initial Security Orientation

8.4. Cleared Personnel.

8.4.1. Initial Training. Supervisors and security managers provide initial training to all cleared personnel. Supervisors are responsible for ensuring that their cleared personnel receive an initial security education orientation before they access classified information or within 90 days of assignment to the unit, whichever is shorter.

8.4.1.1. Initial training should ensure cleared personnel are knowledgeable of their security responsibilities as related to their jobs and the organization's mission. Note: Security manager records initial security training for cleared personnel in the appropriate JPAS "Indoctrinate Non-SCI Access" field. Document training of "Uncleared" personnel in local training records.

8.4.1.1.1. Indoctrinate to the investigation position code reflected in the Unit Manpower Document.

8.4.1.1.2. Verify that current eligibility meets or exceeds the access level.

8.4.1.1.3. Do not document indoctrination before the NdA execution has been recorded in JPAS.

8.4.1.2. The Air Force Information Security Training Standards establish initial information security training for cleared personnel, under column heading (C). ***Note:*** A standard lesson plan meeting the requirements of the training standard is available from the AFSFC web site that includes the NATO training prescribed below.

8.4.1.3. Due to the need for expeditious access to NATO classified information associated with ongoing operations and the Air Force's Aerospace Expeditionary Force (AEF) mission, all cleared military, civilian, and contractor personnel will receive a NATO security briefing. This does not mean every cleared military, civilian, or contractor will be granted access to NATO classified information. The access determination will be made by the access granting authority IAW AFI31-406, paragraph 4.2. A written acknowledgement of the NATO training will be maintained. If the member has access to NATO, also record in JPAS.

8.5. Uncleared Personnel.

8.5.1. Supervisors and security managers provide training to uncleared personnel. Supervisors are responsible for ensuring that all uncleared personnel receive an initial security education orientation within 90 days of assignment to the unit.

8.5.1.1. Initial orientation training must ensure that uncleared personnel are knowledgeable of their responsibilities and roles in the Air Force Information Security Program.

8.5.1.2. The Air Force Information Security Program Training Standards establish initial security education orientation training for uncleared personnel. ***NOTE:*** A standard lesson plan meeting the requirements of the training standard is available from the AFSFC web site: **https://www.mil.lackland.af.mil/afsf/** that includes the initial NATO training required of all uncleared personnel.

8.5.2. Initial training for uncleared personnel will be documented locally.

Section 8C—Special Requirements

8.6. Original Classification Authorities (OCAs). IPOs are responsible for administering specialized training to OCAs IAW DOD 5200.1-R. Training must be conducted prior to OCA authority being exercised. Personnel who propose, prepare, develop, or facilitate original classification decision actions for OCAs will be trained in original and derivative classification, marking, and preparation of security classification guidance. SAF/AAP has developed training standards for OCA training which can be found on the Information Protection Community of Practice (CoP) at: **https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SF-AF-10**. This specialized training is in addition to the other information security training also available on this CoP.

8.7. Derivative Classifiers, Security Personnel, and Others. Security managers are responsible for administering information security training to all personnel IAW DOD 5200.1-R. The training standards can be found on the Information Protection Community of Practice (CoP) at: **https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SF-AF-10**.

8.8. Restricted Data (RD)/Formerly Restricted Data (FRD). Within the DOD, an RD management official shall be appointed in each agency. SAF/AA is appointed the Air Force Management Official.

Section 8D—Continuing Security Education/Refresher Training

8.9. Continuing and Refresher Training. Commanders or equivalents, and staff agency chiefs ensure that each person receives continuing training throughout their duty assignment.

8.9.1. All personnel will receive Continuing Security Education/Refresher Training annually IAW the Air Force Information Security Training Standards.

8.9.2. Personnel performing specialized Classified National Security Information Program related functions, such as classification, declassification and derivative classification actions and security personnel, etc., will receive refresher training commensurate with their knowledge and proficiency in performing required tasks and the dissemination of new policy guidance.

8.9.3. Tailor training to mission needs.

8.9.4. Continuing Security Education/Refresher Training must include ensuring individuals have the most current security guidance applicable to their responsibilities. The annual Air Force Total Force Awareness Training (TFAT) Information Protection block of instruction is mandatory for all Air Force personnel, and meets the general security awareness required. Additional training relating to job requirements (functional, program, security clearances, etc.), or assignments (NATO, PCS, etc.) will be required.

8.9.5. Other related material to be considered include a general overview of the unclassified controlled information (**Attachment 2**), foreign disclosure, security and policy review processes and protection requirements.

Section 8E—Access Briefings and Termination Debriefings

8.10. Access Briefings.

8.10.1. Supervisors, security managers or designated officials conduct and document the following access briefings, as appropriate. The exception is **para 8.10.1.6** All documentation of SCI indoctrinations, debriefs, and NdAs are maintained only within the SSO.

8.10.1.1. Brief and execute the SF 312, prior to granting individual access to classified information. The SF 312 may also be used to document attestations. Both SF 312 completion and attestations will be recorded in JPAS *[Reference AFI 31-401,* **paragraph 5.3***]*.

8.10.1.2. Brief and execute the DD Form 2501 (Safeguard), Courier Authorization, as necessary, when an individual is authorized to escort or handcarry classified information. *[Reference AFI 31-401,* **paragraph 6.8***]*

8.10.1.3. Brief and execute the AF Form 2583, Request for Personnel Security Action, prior to granting an individual access to NATO classified information *[Reference AFI 31-406, paragraph 4.9.]*

8.10.1.4. Brief and execute the AF Form 2583, Request for Personnel Security Action, prior to granting an individual access to Critical Nuclear Weapons Design Information (CNWDI). *[Reference AFI 31-401, paragraph 1.5.1.3.]*

8.10.1.5. Brief and execute the AF Form 2583, Request for Personnel Security Action, prior to granting an individual access to SIOP-ESI. *[Reference AFI 10-1102, Safeguarding the Single Integrated Operational Plan (SIOP), paragraph 7.1.]*

8.10.1.6. The special security officer conducts the SCI indoctrination (in brief) prior to granting personnel access to SCI. The indoctrination is recorded in the DD Form 1847, Sensitive Compartmented Information Indoctrination Memorandum. The DD Form 1847-1, Sensitive Compartmented Information Nondisclosure Statement, is also executed at this time *[Reference DOD 5105.21-M-1, Chapter 2]*.

8.10.2. JPAS will also be used to record NATO, CNWDI, and SIOP-ESI access authorizations.

8.11. Termination Debriefings.

8.11.1. Supervisors, security managers or designated officials conduct and document the following termination debriefings, as appropriate:

8.11.1.1. Debrief individuals having access to classified information or security clearance eligibility when they terminate civilian employment, separate from the military service, have their access suspended, terminated, or have their clearance revoked or denied.

8.11.1.2. Use AF Form 2587, *Security Termination Statement*, to document the debriefing.

8.11.1.3. The debriefing must emphasize to individuals their continued responsibility to:

8.11.1.3.1. Protect classified and unclassified controlled information (**Attachment 2**) to which they have had access.

8.11.1.3.2. Report any unauthorized attempts to gain access to such information.

8.11.1.3.3. Adhere to the prohibition against retaining material upon departure.

8.11.1.3.4. Potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

8.11.2. For NATO access termination debriefing, see AFI 31-406, paragraph 4.10.

8.11.3. Commanders or equivalents, and staff agency chiefs ensure personnel accessed to SCI receive a termination debriefing from the Special Security Officer when access is no longer required, is suspended, or is revoked.

8.11.4. For SIOP-ESI termination briefing, see AFI 10-1102.

8.11.5. Dispose of AF Form 2587 according to *WebRims Records Disposition Schedule*.

8.11.6. Update JPAS to reflect termination of accesses.

8.12. Refusal to Sign a Termination Statement. When an individual willfully refuses to execute AF Form 2587, the supervisor, in the presence of a witness:

8.12.1. Debriefs the individual orally.

8.12.2. Records the fact that the individual refused to execute the termination statement and was orally debriefed.

8.12.3. Ensures the individual no longer has access to classified information.

8.12.4. Forwards the AF Form 2587 to the servicing ISPM for SIF processing according to AFI31-501.

Section 8F—Program Oversight

8.13. General.

8.13.1. Commanders or equivalents, and staff agency chiefs are responsible for ensuring systems are set up to determine training requirements, develop training, and evaluate effectiveness of the training.

8.13.2. ISPMs will make security education and training a special interest item during annual ISPRs.

8.13.3. Commanders or equivalents, and staff agency chiefs will ensure that their security education and training program is given close scrutiny during inspections, self-inspections and SAVs.

8.13.4. Personnel that have program oversight responsibilities should use a combination of approaches to assess the effectiveness of the security education program, such as, observations, quizzes, surveys, face-to-face interviews, practical demonstrations, etc.

Section 8G—Coordinating Requests for Formal Training

8.14. Coordinating Requests for Training.

8.14.1. Commanders or equivalents, and staff agency chiefs will ensure that requests for formal training are coordinated through unit, installation and MAJCOM training channels.

8.14.2. **(DELETED)**

Chapter 9

ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

9.1. Policy. *[Reference DOD 5200.1-R, C10.]*

9.1.1. It is Air Force policy that security incidents will be thoroughly investigated to minimize any possible damage to national security. The investigation will identify appropriate corrective actions that will be immediately implemented to prevent future security incidents. Further, if the security incident leads to the actual or potential compromise of classified information, a damage assessment will be conducted to judge the effect that the compromise has on national security.

9.1.2. Suspected instances of unauthorized public disclosure of classified information shall be reported promptly and investigated to determine the nature and circumstances of the suspected disclosure, the extent of the damage to national security, and the corrective and disciplinary action to be taken *[DODD 5210.50, Para 4.]*.

9.2. Definitions.

9.2.1. Security incidents as used in this AFI pertain to any security violation or infraction as defined in EO 12958, as amended. Security incidents may be categorized as:

9.2.1.1. Security Violation. Any knowing, willful or negligent action:

9.2.1.1.1. That could reasonably be expected to result in an unauthorized disclosure of classified information.

9.2.1.1.2. To classify or continue the classification of information contrary to the requirements of this order or its implementing directives.

9.2.1.1.3. To create or continue a SAP contrary to the requirements of EO 12958, as amended.

9.2.1.2. Security Infraction. Any knowing, willful or negligent action contrary to the requirements of EO 12958, as amended that is not a security violation.

9.2.2. A compromise of classified information occurs when unauthorized individuals have had access to the classified information. Unauthorized individuals include those individuals with the appropriate security clearance but do not have a valid need-to-know.

9.2.3. A potential compromise of classified information is when an investigating official concludes that a compromise of classified information has more than likely occurred as a result of a security incident.

9.3. Information System (IS) Deviations. Coordinate all security deviations involving information systems with the local ISPM and the supporting information assurance office to begin an evaluation on the impact of the incident to national security and the organization's operations. If COMSEC material is involved, refer to AFI 33-212, *Reporting COMSEC Deviations* (will be incorporated in AFI 33-201, Volume 3, *COMSEC User Requirements*).

9.4. Sensitive Compartmented Information (SCI) Incidents. Safeguard all SCI material and report incidents involving SCI to the Special Security Officer.

9.5. Special Access Program (SAP) Incidents Report security incidents involving DOD SAP materiel through local SAP channels to the Director, Special Programs OUSD(P).

9.6. Classification.

9.6.1. Classify security incident notices, appointment of inquiry official memorandums, and security incident reports at the same level of classification as the information compromised if they contain classified information or if they provide sufficient information that would enable unauthorized individuals to access the classified information in an unsecured environment. In the latter case, the documentation must remain classified until the information has been retrieved and appropriately safeguarded. Do not classify memorandums and reports pertaining to security incidents that have occurred in the information system environment when the system has been appropriately purged and the correspondence does not contain other classified information.

9.6.1.1. Classify security incident notices, memorandums, and reports according to the classified source from which they are derived. Refer to DOD 5200.1-R, Chapter 3.

9.6.1.2. Mark security incident notices, memorandums, and reports using derivative classification procedures. Refer to DOD 5200.1-R, Chapter 5.

9.6.2. All security incident reports will, as a minimum, be marked "For Official Use Only." Refer to DOD Regulation 5400.7/Air Force Supplement, *Freedom of Information Act Program*.

9.7. Public Release. Security incident reports cannot be released into the public domain until they have undergone a security review *[Reference AFI 35-101, Chapter 15.]* Unauthorized disclosure of classified information to the public must be processed IAW DODD 5210.50.

9.8. Reporting and Notifications.

9.8.1. Personnel who learn of a security incident must immediately report it to their commander or equivalent, supervisor, or security manager who will in-turn report the incident to the servicing ISPM by the end of the first duty day.

9.8.2. After assigning a case number beginning with calendar year, base, and sequential number for tracking purposes, the ISPM will:

9.8.2.1. Coordinate with the organization security manager to ensure the commander or equivalent, or staff agency chief has been briefed on the incident. The ISPM will brief the commander or equivalent, or staff agency chief if the security manager is unable to do so or when the incident is reported directly to the ISPM.

9.8.2.2. Report compromises/potential compromises for the following incidents through command IP channels to SAF/AAP:

9.8.2.2.1. Classified in the public media.

9.8.2.2.2. Foreign intelligence agencies.

9.8.2.2.3. Criminal activity.

9.8.2.2.4. NATO classified information.

9.8.2.2.5. FGI.

9.8.2.2.6. RD or FRD.

9.8.2.2.7. Disclosure to foreign nationals.

9.8.2.3. Notify the local AFOSI when the circumstances involve criminal activity or foreign intelligence agencies.

9.8.2.4. Notify SAF/AAZ through the appropriate SAP channels when the compromise involves special access information.

9.8.3. The appointing authority will notify the OCA, or the originator when the OCA is not known, when it is determined there is a compromise, potential compromise, or loss of classified information. Refer to **paragraph 9.6.1** of this AFI for security classification marking requirements.

9.9. Preliminary Inquiry. An informal inquiry to determine if classified information has been lost or compromised so that a damage assessment can be completed and the appropriate corrective action can be taken.

9.9.1. The commander or equivalent, or staff agency chief of the activity responsible for the security incident will appoint an inquiry official to conduct a preliminary inquiry. See **Attachment 5** for a sample appointment memorandum. Refer to **paragraph 9.6.1** of this AFI for appointment memorandum classification requirements. The guidelines for selection of the inquiry/investigative official are found in **paragraph 9.11.2**.

9.9.1.1. When security incidents occur because of unauthorized transmission of classified material, the sending activity appoints the inquiry official and conducts the inquiry.

9.9.1.2. Inquiry officials will coordinate their actions with the servicing ISPM and the staff judge advocate's office.

9.9.2. The preliminary inquiry will determine if classified material was compromised, the extent of the compromise, and the circumstances surrounding the compromise.

9.9.3. A preliminary inquiry report will be completed using the sample report format at **Attachment 6** and submitted to the appointing official through the ISPM. The ISPM will provide their concurrence/ non concurrence with the report and forward it to the appointing official for action. Refer to **paragraph 9.6** of this AFI for report classification requirements.

9.9.4. The report from the preliminary inquiry will be sufficient to resolve the security incident if:

9.9.4.1. The inquiry determines that loss or compromise of classified information has not occurred.

9.9.4.2. The inquiry determines that loss or compromise of classified information has occurred, but there is no indication of significant security weakness.

9.9.4.3. The appointing official determines that no additional information will be obtained by conducting a formal investigation.

9.9.5. If the report from the preliminary inquiry is not sufficient to resolve the security incident, the appointing authority initiates a formal investigation. The preliminary inquiry report will become part of any formal investigation. If the inquiry is closed out as a

compromise or potential compromise the appointing authority notifies the OCA to perform a damage assessment.

9.9.6. If the inquiry reveals suspected unauthorized disclosure to the public notify SAF/AAP through IP channels [DODD 5210.50, Para 5.2.1.]. Classify security incident notices, memorandums, and reports according to the classified source from which they are derived. Refer to DOD 5200.1-R, Chapter 3. Specifically address:

9.9.6.1. When, where, and how the incident occurred.

9.9.6.2. Was classified information compromised?

9.9.6.3. If compromise occurred, what specific classified information and/or material was involved?

9.9.6.4. If classified information is alleged to have been lost, what steps were taken to locate the material?

9.9.6.5. In what specific media article or program did the classified information appear?

9.9.6.6. To what extent was the compromised information disseminated?

9.9.6.7. Was the information properly classified?

9.9.6.8. Was the information officially released?

9.9.6.9. Are there any leads to be investigated that might lead to the identification of the person responsible for the compromise?

9.9.6.10. Will further inquiry increase the damage caused by the compromise?

9.9.7. Submit a completed Department of Justice (DoJ) Media leak Questionnaire, available from **https://wwwmil.lackland.af.mil/afsf/** through ISPM channels to USD(I), who will coordinate with DOD General Counsel to determine whether a referral to the DoJ for prosecution is warranted.

9.10. Damage Assessment.

9.10.1. A damage assessment is an analysis to determine the effect of a compromise of classified information on the national security. It will be initiated by the OCA upon notification of a potential or actual compromise to verify and reevaluate the information involved. Damage assessment reports will be classified and marked according to the classification guidance provided on the information being addressed in the reports.

9.10.2. The OCA must:

9.10.2.1. Verify the classification and duration of classification initially assigned to the information. If the OCA determines the information should be declassified, the reporting activity will be notified.

9.10.2.2. Set up damage assessment controls and procedures.

9.10.2.3. Provide a copy of the damage assessment to the inquiry or investigating official.

9.11. Formal Investigation.

9.11.1. A formal investigation is a detailed examination of evidence to determine the extent and seriousness of the compromise of classified information. The formal investigation will fix responsibility for any disregard (deliberate or inadvertent) of governing directives which led to the security incident.

9.11.2. The commander or equivalent, or staff agency chief of the activity responsible for the security incident, will appoint an investigative official to conduct an investigation.

9.11.2.1. The appointment letter provides authority to conduct an investigation, swear witnesses, and examine/copy documents, files and other data relevant to the inquiry.

9.11.2.2. The investigative official is the personal representative of the Appointing Authority and/ or the Commander. The investigative official must be impartial, unbiased, objective, thorough, and available.

9.11.2.3. The investigative official must be a commissioned officer, senior NCO (E-7 and above), or a civil service employee equivalent (GS-9 and above).

9.11.2.4. The investigation will be the investigative official's only duty (unless the Appointing Authority determines otherwise) until the report is completed and approved by the Appointing Authority.

9.11.2.5. Appointing Authorities will not appoint an investigative official who is retiring, separating, or being reassigned within 180 days.

9.11.3. The formal investigation will include the preliminary inquiry if one has been conducted.

9.12. Management and Oversight.

9.12.1. The inquiry/investigative official will route the completed report through the servicing ISPM for review before forwarding it to the appointing authority.

9.12.2. The appointing authority will:

9.12.2.1. Close the inquiry/investigation unless MAJCOM/FOA/DRU directives indicate otherwise.

9.12.2.2. Determine if administrative or disciplinary action is appropriate. See AFI 31-501, Chapter 8 and applicable military and civilian personnel publications.

9.12.2.3. Debrief anyone who has had unauthorized access, using AF Form 2587.

9.12.2.4. Forward a copy of the completed report to the ISPM identifying corrective actions taken.

9.12.2.5. Dispose of the report according to the instructions in *WebRims Records Disposition Schedule.*

9.12.3. The ISPM will:

9.12.3.1. Provide technical guidance and review of preliminary inquiry and formal investigation reports.

9.12.3.2. Monitor the status of security incidents.

9.12.4. Inquiry/investigative officials must complete inquiry/investigations within 30 duty days from appointment.

9.13. Unauthorized Absences. Report all unauthorized absences to the ISPM and appropriate AFOSI detachment *[Reference DOD 5200.1-R, C10.1.9.]*.

9.14. Prescribed Forms. These forms are prescribed throughout this AFI and are available through the Air Force Publications Distribution system:

AF Form 143, *Top Secret Register Page*

AF Form 144, *Top Secret Access Record and Cover Sheet*

AF Form 310, *Document Receipt and Destruction Certificate*

AF Form 349, *Receipt for Documents Released to Accredited Representatives of Foreign Nations*

AF Form 1565, *Entry, Receipt, and Destruction Certificate*

AF Form 2427, *Lock and Key Control Register*

AF Form 2587, *Security Termination Statement; Air Force Technical Order Form (AFTO) 36, Maintenance Record for Security Type Equipment*

SF 311, *Agency Security Classification Management Program Data*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

SF 703, *Top Secret Cover Sheet*

SF7 04, *Secret Cover Sheet*

SF 705, *Confidential Cover Sheet*

SF706, *Top Secret Label*

SF 707, *Secret Label*

SF 708, *Confidential Label*

DD Form 1847, *Sensitive Compartmented Information Indoctrination Memorandum*

DD Form 1847-1, *Sensitive Compartmented Information Nondisclosure Statement*

DD Form 1848, *Sensitive Compartmented Information Debriefing Memorandum*

DD Form 2024, *DOD Security Classification Guide Data Elements*

DD Form 2501 *(Safeguard), Courier Authorization*

DoE Form 5631.20, *Request for Visit or Access Approval*

9.15. Adopted Forms.

AF 349, AF 2587, 2427, and AFTO 36

CARROL H. CHANDLER, Lt. Gen, USAF
Deputy Chief of Staff Air & Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 12958, as amended. *Classified National Security Information*

Executive Order 12829, *National Industrial Security Program*

ISOO Directive Number 1, *Classified National Security Information*

10 C.F.R. 1045.1 Subpart A, *Program Management of the Restricted Data and Formerly Restricted Data Classification System*

DCID 6/6, *Security Controls on the Dissemination of Intelligence Information*

DCID 6/7, *Intelligence Disclosure Policy*

DOD 4000.25-8-M, *Military Assistance Program Address Directory System*

DOD 4528.8-M, *DOD Official Mail Manual*

DODD 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs*

DODD 5210.50, *Unauthorized Disclosure of Classified Information to the Public*

DOD 5200.1-H, *DOD Handbook for Writing Security Classification Guidance*

DOD 5200.1-R, *Information Security Program*

DOD 5200.1-PH, *DOD Guide to Marking Classified Documents*

DOD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (Standard Form 312)*

DODD 5210.2, *Access to and Dissemination of Restricted Data*

DODD 5210.83, *Unclassified Controlled Nuclear Information (UCNI)*

DODD 5230.24, *Distribution Statements on Technical Documents*

DOD 5220.22-M, *National Industrial Security Program Operating Manual*

DOD 5220.22-R, *Industrial Security Regulation*

DODI 5240.11, *Damage Assessments*

DOD 5400.7-R/Air Force Supplement, *DOD Freedom of Information Act Program*

DODD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG).]*

Naval Facilities Engineering Service Center Technical Data Sheet, TDS-2000-SHR, *Neutralizing "Locked-Out" Security Containers* (Available from DOD Lock Program website.)

AFI 14-302, *Control, Protection, and Dissemination of Sensitive Compartmented Information*

AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information,* (FOUO)

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*

AFPD 16-7, *Special Access Programs*

AFI 16-701, *Special Access Programs*

AFMAN 23-110, *USAF Supply Manual*

AFPD 24-2, *Preparation and Movement of Air Force Materiel*

AFI 24-201, *Cargo Movement*

AFI 31-101, *Air Force Installation Security Program*

AFI 31-207, *Arming and Use of Force by Air Force Personnel*

AFPD 31-4, *Information Security*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFPD 33-2, *Information Protection* (will be *Information Assurance)*

AFI 33-201, Volume 1, *Communications Security* (COMSEC)

AFI 33-201, Volume 2, *COMSEC User Requirements*

AFI 33-202 Volume 1, *Network and Computer Security*

AFI 33-204, *Information Assurance (IA) Awareness, Program*

AFI 33-211, *Communications Security (COMSEC) User Requirements (will be incorporated in AFI 33-201 V2,* COMSEC Users Requirements)

AFI 33-212, *Reporting COMSEC Deviations (will be incorporated in AFI 33-201 V2,* COMSEC Users Requirements

AFI 33-275, *Controlled Cryptographic Items (CCI)* (will be incorporated in AFI 33-201 V1)

AFI 33-360, *Air Force Privacy Act Program*

AFI 35-101, *Public Affairs Policies and Procedures*

AFI 36-1001, *Managing the Civilian Performance Program*

AFMAN 36-2108, *Enlisted Classification*

AFPD 36-22, *Air Force Military Training*

AFI 36-2201, Volume 1, *Training, Development, Delivery, and Evaluation*

AFI 36-2907, *Unfavorable Information File (UIF) Program*

AFMAN 36-505, *Skill Coding*

AFI 36-704, *Discipline and Adverse Actions*

AFI 36-2406, *Officer and Enlisted Evaluation Systems*

AFMAN 37-138, *Records Disposition – Procedures and Responsibilities*

AFI 51-301, *Civil Litigation*

AFI 61-204, *Disseminating Scientific and Technical Information*

AFI 61-205, *Sponsoring or Cosponsoring, Conducting, and Presenting DOD Related Scientific Technical Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*

AFI 65-401, *Relations with the General Accounting Office*

AFI 71-101, Volume I, *Criminal Investigations*

AFI 90-301, *Inspector General Complaints Resolution*

AFI 90-401, *Air Force Relations with Congress*

AFKAG-1N, *Air Force Communications Security (COMSEC) Operations*

AFTO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Security Type Equipment*

AFSSI 5020, *Remanence Security* (will be incorporated in forthcoming AFI 33-202 V3, *Network Security Program) WebRims Records Disposition Schedule*

Abbreviations and Acronyms

ADO—Activity Distribution Offices

ADP—Automatic Data Processing

AEF—Aerospace Expeditionary Force

AF—Air Force

AFCAF—Air Force Central Adjudication Facility

AFDO—Air Force Declassification Office

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFPDL—Air Force Publishing Distribution Library

AFSSI—Air Force Special Security Instruction

AFTO—Air Force Technical Order

ANACI—Access National Agency Check with Inquiry

AIS—Automated Information System

BITC—Base Information Transfer Center

CCI—Controlled Cryptographic Information

CDF—Central Destruction Facility

CNWDI—Critical Nuclear Weapon Design Information

COMSEC—Communications Security

CONUS—Continental United States

CSA—Cognizant Security Authority

DAA—Designated Approving Authority

DCID—Director Central Intelligence Directive

DCII—Defense Clearance and Investigations Index

DCS—Defense Courier Service

DD—Department of Defense (Used for DOD Forms)

DIA—Defense Intelligence Agency

DEA—Drug Enforcement Administration

DOD—Department of Defense

DODD—Department of Defense Directive

DODI—Department of Defense Instruction

DODSI—Department of Defense Security Institute (Now DSSA)

DoE—Department of Energy

DRU—Direct Reporting Unit

DSS—Defense Security Service (Formerly DIS and DODSI)

DSSA—Defense Security Service Academy

DTIC—Defense Technical Information Center

EES—Enlisted Evaluation System

EO—Executive Order

FGI—Foreign Government Information

FMS—Foreign Military Sales

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FRD—Formerly Restricted Data

GAO—Government Accountability Office

GILS—Government Information Locator System

GPO—Government Printing Office

GSA—General Services Administration

HAF—Headquarters Air Force

IDS—Intrusion Detection System

IG—Inspector General

IMT—Information Management Tool

INTELINK—Intelligence Link

IO—Investigating Officer

ISCAP—Interagency Security Classification Appeals Panel

ISO——International Organization for Standardization

ISOO—Information Security Oversight Office

ISPM—Information Security Program Manager

ISPR—Information Security Program Review

JPAS—Joint Personnel Adjudication System

LFC—local files check

MAJCOM—Major Command

MDR—Mandatory Declassification Review

MIS—Management Information System

NAC—National Agency Check

NACLC—National Agency Check, Local Agency Check, Credit Check

NARA—National Archives and Records Administration

NATO—North Atlantic Treaty Organization

NCR—National Capital Region

NdA—Nondisclosure Agreement

NFESC—Naval Facilities Engineering Services Center

NGA—National Geospatial-Intelligence Agency

NIMA—National Imagery and Mapping Agency

NIPRNET—Non-Secure Internet Protocol Router Network

NISPOM—National Industrial Security Program Operating Manual

NOFORN—Not Releasable to Foreign Nationals

NSA—National Security Agency

NSN—National Stock Number

OADR—Originating Agency's Determination Required

OCA—Original Classification Authority

OMB—Office of Management and Budget

OMC—Official Mail Center

OPF—official personnel file

ORCON—Originator Control

PA—Privacy Act

PCS—permanent change of station

PKI—Public Key Infrastructure

PL—Protection Level

POC—point of contact

RCS—Report Control Symbol

RD—Restricted Data

REL TO—Release To

SAF—Secretary of the Air Force

SAP—Special Access Program

SAV—staff assistance visit

SBU—Sensitive But Unclassified

SCG—Security Classification Guide

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facilities

SEI—Special Experience Identifier

SF—standard form

SIF—security information file

SIOP—ESI—Single Integrated Operational Plan-Extremely Sensitive Information

SIPRNET—Secret Internet Protocol Router Network

SOIC—Senior Official of the Intelligence Community

SSO—Special Security Office

TDS—technical data sheet

TDY—temporary duty

TSCA—Top Secret Control Account

TSCM—Technical Surveillance Countermeasures

TSCO—Top Secret Control Officer

UCNI—Unclassified Controlled Nuclear Information

URL—uniform resource locator

VAL—visit authorization letter

VGSA—visitor group security agreement

Terms

Access—the ability or opportunity to gain knowledge of classified information.

Agency—any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

Automated Information System (AIS)—Any telecommunications and/or computer- related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02).

Automatic Declassification—the declassification of information based solely upon (1) the occurrence of a specific date or event as determined by the OCA; or (2) the expiration of a maximum time frame for duration of classification established under EO 12958, as amended.

Classification—the determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

Classification/Declassification Guide—a documentary form of classification/declassification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Classification Guidance—any instruction or source that prescribes the classification of specific information.

Classified National Security Information or Classified Information—official information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Confidential Source—any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

Damage to The National Security—harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

Declassification—the determination that, in the interests of national security, classified information no longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation.

Declassification Authority—the official who authorized the original classification, if that official is still serving in the same position; the originator's current successor in function; a

supervisory official of either; or officials delegated declassification authority in writing by the agency head or the senior agency official.

Derivative Classification—the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Direct Reporting Unit (DRU)—A DRU has a specialized and restricted mission, and is directly subordinate to the Chief of Staff, United States Air Force or to his representative at HAF.

Document—any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Downgrading—a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Field Operating Agency (FOA)—A subdivision of the Air Force, directly subordinate to a HQ USAF functional manager. FOAs perform field activities beyond the scope of any of the major commands. Their activities are specialized or associated with an Air Force wide mission.

File Series—file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Foreign Government Information (FGI)—(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (3) information received and treated as ―foreign government information‖ under the terms of a predecessor order.

Formerly Restricted Data (FRD)—defined by the Atomic Energy Act as classified information which has been removed from the RD category after DoE and the DOD have jointly determined that it relates primarily to the military utilization of atomic weapons, and can be adequately safeguarded as national security information.

Information—any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of the United States Government. ―Control‖ means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information System (IS)—1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (***NOTE:*** This includes automated information systems). 2. (DOD) The entire infrastructure, organization, and

components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02).

Infraction—any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a violation, as defined below.

Integral File Block—a distinct component of a file series, as defined in this section, which should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

Integrity—the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Mandatory Declassification Review (MDR)—the review for declassification of classified information in response to a request for declassification.

Multiple Sources—two or more source documents, classification guides, or a combination of both.

National Security—the national defense or foreign relations of the United States.

Need—**To-Know—**a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Network—a system of two or more computers that can exchange data or information.

Original Classification—an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

Original Classification Authority (OCA)—an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

Records—the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

Records Having Permanent Historical Value—Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently IAW Title 44, United States Code.

Records Management—the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Restricted Data (RD—defined by the Atomic Energy Act as all data concerning design, manufacture, or utilization of atomic weapons, production of special nuclear material, and use of Special Nuclear Material in the production of energy.

Safeguarding—measures and controls that are prescribed to protect classified information.

Self—Inspection—the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

Sensitive But Unclassified (SBU) Information—information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under FOIA.

Source Document—an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Program (SAP)—a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Staff Agency Chief—For the purpose of this instruction, staff agency chiefs are those individuals serving in 2-digit positions reporting to the commander or vice commander above the Wing level, and 2 and 3 digit positions at HAF.

Systematic Declassification Review—the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value IAW title 44, United States Code.

Telecommunications—the preparation, transmission, or communication of information by electronic means.

Unauthorized Disclosure—a communication or physical transfer of classified information to an unauthorized recipient.

Violation—(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or (3) any knowing, willful, or negligent action to create or continue a SAP contrary to the requirements of this order.

Attachment 2

CONTROLLED UNCLASSIFIED INFORMATION

A2.1. For Official Use Only (FOUO). FOUO is a designation that is applied to unclassified information that is exempt from automatic release to the public under FOIA. See DOD 5400.7-R/AF Supplement for further guidance *[Ref: DOD 5200.1-R, Appendix 3, Para AP3.2.]*.

A2.1.1. Access to FOUO Information.

A2.1.1.1. No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.

A2.1.1.2. The final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge or control of the information and not on the prospective recipient.

A2.1.1.3. Information designated as FOUO may be disseminated within the DOD Components and between officials of DOD Components and DOD contractors, consultants, and grantees to conduct official business for the DOD, provided that dissemination is not further controlled by a Distribution Statement.

A2.1.1.4. DOD holders of information designated as FOUO are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a government function. If the information is covered by the Privacy Act, disclosure is only authorized if the requirements of AFI 33-332, Air Force Privacy Program, are satisfied.

A2.1.1.5. Release of FOUO information to Congress is governed by AFI 90-401, *Air Force Relations With Congress*. If the Privacy Act covers the information, disclosure is authorized if the requirements of DOD 5400.11-R are also satisfied.

A2.1.1.6. DOD Directive 7650.01, *General Accounting Office (GAO) and Comptroller General Access to Records*, governs release of FOUO information to the Government Accountability Office (GAO). If the Privacy Act covers the information, disclosure is authorized if the requirements of DOD 5400.11-R are also satisfied.

A2.1.2. Protection of FOUO Information.

A2.1.2.1. During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, store FOUO information in unlocked containers, desks or cabinets if Government or Government-contract building security is provided. If such building security is not provided, store the information in locked desks, file cabinets, bookcases, locked rooms, etc.

A2.1.2.2. FOUO information and material may be transmitted via first class mail, parcel post or, for bulk shipments, via fourth-class mail. Electronic transmission of FOUO information, e.g., voice, data or facsimile, e-mail, shall be by approved secure communications systems or systems utilizing access controls such as Public Key Infrastructure (PKI), whenever practical.

A2.1.2.3. FOUO information may only be posted to DOD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum, dated 25 November 1998, Subject: "*Web Site Administration*".

A2.1.2.4. Record copies of FOUO documents shall be disposed of according to the Federal Records Act and the DOD Component records management directives. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information.

A2.1.3. Unauthorized Disclosure. The unauthorized disclosure of FOUO does not constitute an unauthorized disclosure of DOD information classified for security purposes. However, appropriate administrative action shall be taken to fix responsibility for unauthorized disclosure of FOUO whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The Military Department or other DOD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

A2.2. FOR OFFICIAL USE ONLY Law Enforcement Sensitive.

A2.2.1. Law Enforcement Sensitive is a marking sometimes applied, in addition to/conjunction with the marking FOR OFFICIAL USE ONLY, by the Department of Justice and other activities in the law enforcement community. It is intended to denote that the information was compiled for law enforcement purposes and should be afforded appropriate security in order to protect certain legitimate government interests, including the protection of: enforcement proceedings; the right of a person to a fair trial or an impartial adjudication; grand jury information; personal privacy including records about individuals requiring protection under the Privacy Act; the identity of a confidential source, including a State, Local, or foreign agency or authority or any private institution which furnished information on a confidential basis; information furnished by a confidential source; proprietary information; techniques and procedures for law enforcement investigations or prosecutions; guidelines for law enforcement investigations when disclosure of such guidelines could reasonably be expected to risk circumvention of the law, or jeopardize the life or physical safety of any individual, including the lives and safety of law enforcement personnel.

A2.2.2. Markings.

A2.2.2.1. In unclassified documents containing Law Enforcement Sensitive information, the words "Law Enforcement Sensitive" shall accompany the words "FOR OFFICIAL USE ONLY" at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).

A2.2.2.2. In unclassified documents, each page containing FOR OFFICIAL USE ONLY Law Enforcement Sensitive information shall be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" at the top and bottom. Classified documents containing such information shall be marked as required by Chapter 5, DOD 5200.1-R except that pages containing Law Enforcement Sensitive information but no classified information will be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" top and bottom.

A2.2.2.3. Portions of DOD classified or unclassified documents that contain FOR OFFICIAL USE ONLY Law Enforcement Sensitive information shall be marked "(FOUO-LES)" at the beginning of the portion. This applies to classified, as well as to unclassified documents. If a portion of a classified document contains both classified and FOR OFFICIAL USE ONLY Law Enforcement Sensitive information, the appropriate classification designation is sufficient to protect the information.

A2.2.3. Access to FOR OFFICIAL USE ONLY Law Enforcement Sensitive. The criteria for allowing access to FOR OFFICIAL USE ONLY Law Enforcement Sensitive are the same as those used for FOUO information, except that if the information also bears the marking "Originator Control" or "ORCON" the information may not be disseminated beyond the original distribution without the approval of the originating office.

A2.2.4. Protection of FOR OFFICIAL USE ONLY Law Enforcement Sensitive. Within the DOD, FOR OFFICIAL USE ONLY Law Enforcement Sensitive shall be protected as required for FOUO information.

A2.3. Sensitive But Unclassified (SBU) Information. SBU information is information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under FOIA. When SBU information is included in DOD documents, it shall be marked as if the information were FOUO *[Ref: DOD 5200.1-R, Appendix 3, Para AP3.3.]*.

A2.4. Protection of Drug Enforcement Administration (DEA) Sensitive Information. Unclassified information that is originated by the DEA and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports *[Reference DOD 5200.1-R, Appendix 3, Para AP3.4.]*.

A2.5. Unclassified Controlled Nuclear Information (UCNI). Unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of Special Nuclear Material equipment or facilities *[Reference DOD 5200.1-R, Appendix 3, Para AP3.5.]*.

A2.5.1. The Director of Information Protection (SAF/AAP) has primary responsibility within the Air Force for the implementation of DODD 5210.83, *Department of Defense Unclassified Controlled Nuclear Information* (DOD UCNI).

A2.5.2. The following positions have been designated UCNI Officials within the Air Force:

A2.5.2.1. HAF staff agency chiefs.

A2.5.2.2. MAJCOM/FOA/DRU commanders, Chiefs of IP.

A2.5.2.3. Installation commanders and equivalent commander positions, Chiefs of IP.

A2.5.2.4. **(DELETED)**

A2.5.3. UCNI Officials' Responsibilities:

A2.5.3.1. Identify information meeting definition of UCNI.

A2.5.3.2. Determine criteria for access to UCNI and approve special access requests.

A2.5.3.3. Approve or deny the release of UCNI information.

A2.5.3.4. Ensure all UCNI information is properly marked, safeguarded, transmitted, and destroyed properly. Transmission of UCNI on the NIPRNet may only occur when the material is encrypted and digitally signed and the recipient has a ".mil" or ".gov" address extension.

A2.5.3.5. Document decisions and report them through their command IP channels to SAF/AAP. RCS Number DD-C3I(AR)1810 applies to this data collection.

A2.6. Sensitive Information (Computer Security Act of 1987). *The Computer Security Act of 1987* established requirements for protection of certain information in Federal Government AIS. It applies only to unclassified information that deserves protection and is concerned with protecting the availability and integrity, as well as the confidentiality, of information. See AFI 33-200 for Air Force policy on protecting information in Federal Government information systems *[Reference DOD 5200.1-R, Appendix 3, Para AP3.6.]*.

A2.7. Technical Documents. DOD Directive 5230.24 requires distribution statements to be placed on technical documents, both classified and unclassified. These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. See AFI 61-204 for Air Force policy on technical documents *[Reference DOD 5200.1-R, Appendix 3, Para AP3.7.]*.

A2.8. LIMITED DISTRIBUTION Information

A2.8.1. Description. LIMITED DISTRIBUTION is a caveat used by the National Imagery and Mapping Agency/National Geospatial-Intelligence Agency (NIMA/NGA) to identify a select group of sensitive but unclassified imagery or geospatial information and data created or distributed by NIMA/NGA or information, data, and products derived from such information. DOD Instruction 5030.59, *NATIONAL GEOSPATIAL- INTELLIGENCE AGENCY (NGA) LIMITED DISTRIBUTION GEOSPATIAL INTELLIGENCE*, contains details of policies and procedures regarding use of the LIMITED DISTRIBUTION caveat. These policies and procedures are summarized in **subparagraphs A2.8.2** through **A2.8.4**, below.

A2.8.2. Marking. Information or material designated as LIMITED DISTRIBUTION, or derived from such information or material shall, unless otherwise approved by the Director, NGA be marked with the notation shown in Figure A2.F1 as follows:

LIMITED DISTRIBUTION Notation

UNCLASSIFIED/LIMITED DISTRIBUTION

Distribution authorized to DOD, IAW 10 U.S.C. § 130 and 455. Release authorized to U.S. DOD Contractors IAW 48 C.F.R. §252.245-7000. Refer other requests to Headquarters, NGA, ATTN: Release Officer, Stop D-136. Destroy as "For Official Use Only." Removal of this caveat is prohibited.

A2.8.3. Access to LIMITED DISTRIBUTION Information or Material.

A2.8.3.1. Information bearing the LIMITED DISTRIBUTION caveat shall be disseminated by NGA to Military Departments or other DOD Components, and to authorized grantees for the conduct of official DOD business.

A2.8.3.2. DOD civilian, military and contractor personnel of a recipient DOD Component, contractor or grantee may be granted access to information bearing the LIMITED DISTRIBUTION caveat provided they have been determined to have a valid need to know for such information in connection with the accomplishment of official business for the DoD. Recipients shall be made aware of the status of such information, and transmission shall be by means to preclude unauthorized disclosure or release. Further dissemination of information bearing the LIMITED DISTRIBUTION caveat by receiving contractors or grantees to another Military Department, other DOD Component, contractor or grantee, or dissemination by any recipient Component, contractor, or grantee to any person, agency or activity outside DOD, requires the express written approval of the Director, NGA.

A2.8.3.3. Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be released, made accessible to or sold to foreign governments or international organizations, to include through Foreign Security Assistance transactions or arrangements, or transfer or loan of any weapon or weapon system that uses such information, or intended to be used in mission planning systems, or through the Foreign Military Sales (FMS) process, without the express, written approval of the Director, NGA.

A2.8.3.4. All FOIA requests for information bearing the LIMITED DISTRIBUTION caveat or derived there from, shall be referred to NGA consistent with DOD Instruction 5030.59.

A2.8.4. Protection of LIMITED DISTRIBUTION Information.

A2.8.4.1. Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be stored on systems accessible by contractors, individuals who are not directly working on a DOD contract, or those who do not require access to such information in connection with the conduct of official DoD business.

A2.8.4.2. LIMITED DISTRIBUTION information or derivative information, may only be posted to DOD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum dated December 1998. Such information shall not be transmitted over the World Wide Web or over other publicly accessible and unsecured systems. Electronic transmission of such information, e.g., voice, data or facsimile, shall be by approved secure communications systems or systems utilizing other protective measures such as PKI.

A2.8.4.3. During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, LIMITED DISTRIBUTION information may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided. If such building security is not provided, LIMITED DISTRIBUTION information shall be stored in locked buildings, rooms, desks, file cabinets, bookcases, or similar items. Store LIMITED DISTRIBUTION information in the same manner approved for FOUO.

A2.8.4.4. When no longer required, all LIMITED DISTRIBUTION information and copies, shall be returned to NIMA/NGA or destroyed in a manner sufficient to prevent its reconstruction.

Attachment 3

PHYSICAL SECURITY STANDARDS

A3.1. Intrusion Detection Systems (IDS) Standards. *[Reference DOD 5200.1-R, Appendix 7, AP7.2.]*

A3.1.1. Air Force IDS Standards. See AFI 31-101, *Air Force Installation Security Program*, Chapter 12, for Air Force policy on IDS.

A3.1.2. Trustworthiness Determinations. See AFI 31-501 for Air Force policy on trustworthiness determinations.

A3.2. Physical Security Design Guidelines. See the Military Handbook Design Guidelines for Physical Security of Facilities (MIL-HDBK-1013/1A) at **http://assist.daps.dla.mil/docimages/0000/57/10/54120.PD2** for facility design standards. DOD 5200.1-R, Appendix 7 provides vault and secure room construction standards.

A3.2.1. The ISPM certifies vaults and secure rooms in concert with appropriate engineering and communications technical representatives IAW DOD 5200.1-R, Appendix 7.

A3.2.2. Commander, equivalent, or staff agency chief approves open storage.

A3.2.3. Defense Intelligence Agency (DIA) standards for Sensitive Compartmented Information Facilities (SCIF) are included in Director Central Intelligence Agency Directive 6/9.

Attachment 4

TRANSMISSION TO FOREIGN GOVERNMENTS

A4.1. General. Comply with provisions of DOD 5200.1-R, Appendix 8 for movement of classified information or material to foreign governments. Air Force contracting officials ensure that US industrial activities have a government approved transportation plan or other transmission instructions.

A4.1.1. Receipts. Air Force personnel: *[Reference DOD 5200.1-R, Appendix 8, Paragraph a]*

A4.1.2. Use AF Form 349, Receipt for Documents Released to Accredited Representatives of Foreign Nations (available on the AFEPL);

A4.1.3. Show the complete unclassified title, description of a classified letter, minutes of meeting, and so on and any numerical identification of documents released on the form; and,

A4.1.4. **(DELETED)**

A4.2. Whenever possible, shippers should use military airlift for shipping classified to foreign recipients. ***NOTE:*** When Air Mobility Command airlift cannot deliver, determine an alternate secure method of direct delivery to a designated representative on a case-by-case basis *[Reference DOD 5200.1-R, AP8.1.1.3.]*

A4.3. Depot and contract administration officials review lists of freight forwarders specified by the recipient foreign government to confirm that DOD 4000.25-8-M, *Military Assistance Program Address Directory System,* Jul 95**,** shows them as authorized to transport classified information.

A4.4. See AFPD 24-2 and AFI 24-201 for instructions on "Report of Shipment."

A4.5. Foreign Military Sales (FMS). Air Force activities having primary management responsibility for processing FMS cases ensure that personnel include transmission instructions *[Reference DOD 5200.1-R, AP8.1.1.3.4.]*

A4.5.1. FMS processors must coordinate with ISPMs/IP and transportation officials on transportation plans submitted by foreign purchasers before giving final approval.

Attachment 5

APPOINTMENT OF INQUIRY OFFICIAL MEMORANDUM

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANUM FOR
FROM:
SUBJECT: Appointment of Inquiry Official, Incident No.

You are appointed to conduct a preliminary inquiry into security incident (number). The incident involves (provide a short summary). Refer to AFI 31-401, *Information Security Program Management*, **paragraph 9.5.**, for security classification requirements.

The purpose of this inquiry is to determine whether a compromise occurred and to categorize this security incident as either a security violation or a security infraction. You are authorized to interview those persons necessary to complete your findings. You are further authorized access to records and files pertinent to this inquiry. Your records indicate that you have a (Secret, Top Secret, etc.) security clearance. Should you determine this incident involved access to program information for which you are not authorized access, advise the Information Security Program Manager (ISPM).

Contact (name and phone number of the ISPM), for a briefing on your responsibilities, conduct of, and limitations of this inquiry. Your written report will be forwarded through the ISPM to me within 30 duty days from the date of your appointment. As a minimum, your report must contain the following:

a. A statement that a compromise or potential compromise did or did not occur.

b. Category of the security incident.

c. Cause factors and responsible person(s).

d. Recommended corrective actions needed to preclude a similar incident.

Notify me immediately at (phone number) if you determine that a compromise has occurred. You are required to obtain technical assistance from the ISPM and Staff Judge Advocate during the course of this inquiry whenever necessary.

(Signature Block of Commander, Staff Agency Chief, or equivalent)

Attachment 6

PRELIMINARY INQUIRY OF SECURITY INCIDENT REPORT

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR

FROM:

SUBJECT: Preliminary Inquiry of Security Incident No.

Authority: A preliminary inquiry was conducted (date) under the authority of the attached memorandum.

Matters investigated: The basis for this inquiry was that (provide a short summary of the security incident including the date it occurred, the classification of information involved, and the document control number if specific documents were involved). Refer to AFI 31-401, *Information Security Management Program Management*, **paragraph 9.5.**, for security classification requirements.

Personnel Interviewed: (list all personnel interviewed, position title, office symbol, and security clearance).

Facts: (list specific details answering who, what, why, where, and when questions concerning the security incident).

Conclusions: As a result of the investigation into the circumstances surrounding the security incident, interviews, and personal observations, it is concluded that: (list specific conclusions reached based on the facts and if a compromise or potential compromise did or did not occur). If a damage assessment is or has been done, provide the point of contact along with: the status of the assessment if it hasn't been completed; or, describe the outcome if it has been completed; or, provide a copy of the completed assessment report.

Recommendations: (list corrective actions needed to preclude a similar incident; the category of the incident; damage assessment; if the incident is a compromise, potential compromise or no compromise; and, if this inquiry should be closed without further investigation or with a recommendation for a formal investigation).

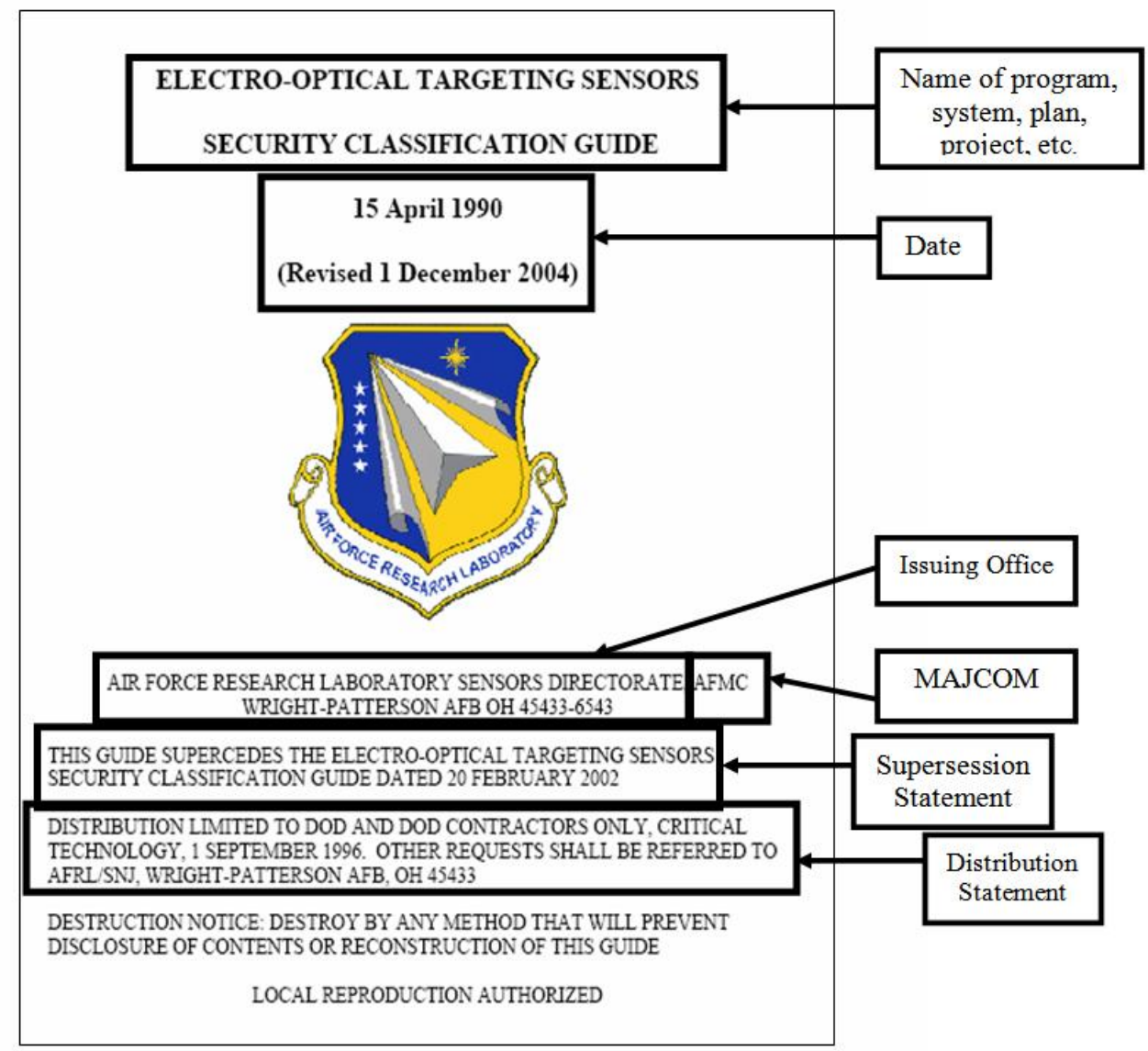
(Signature block of inquiry official)

Attachment:
Appointment of Inquiry Official Memo, (date)

Attachment 7

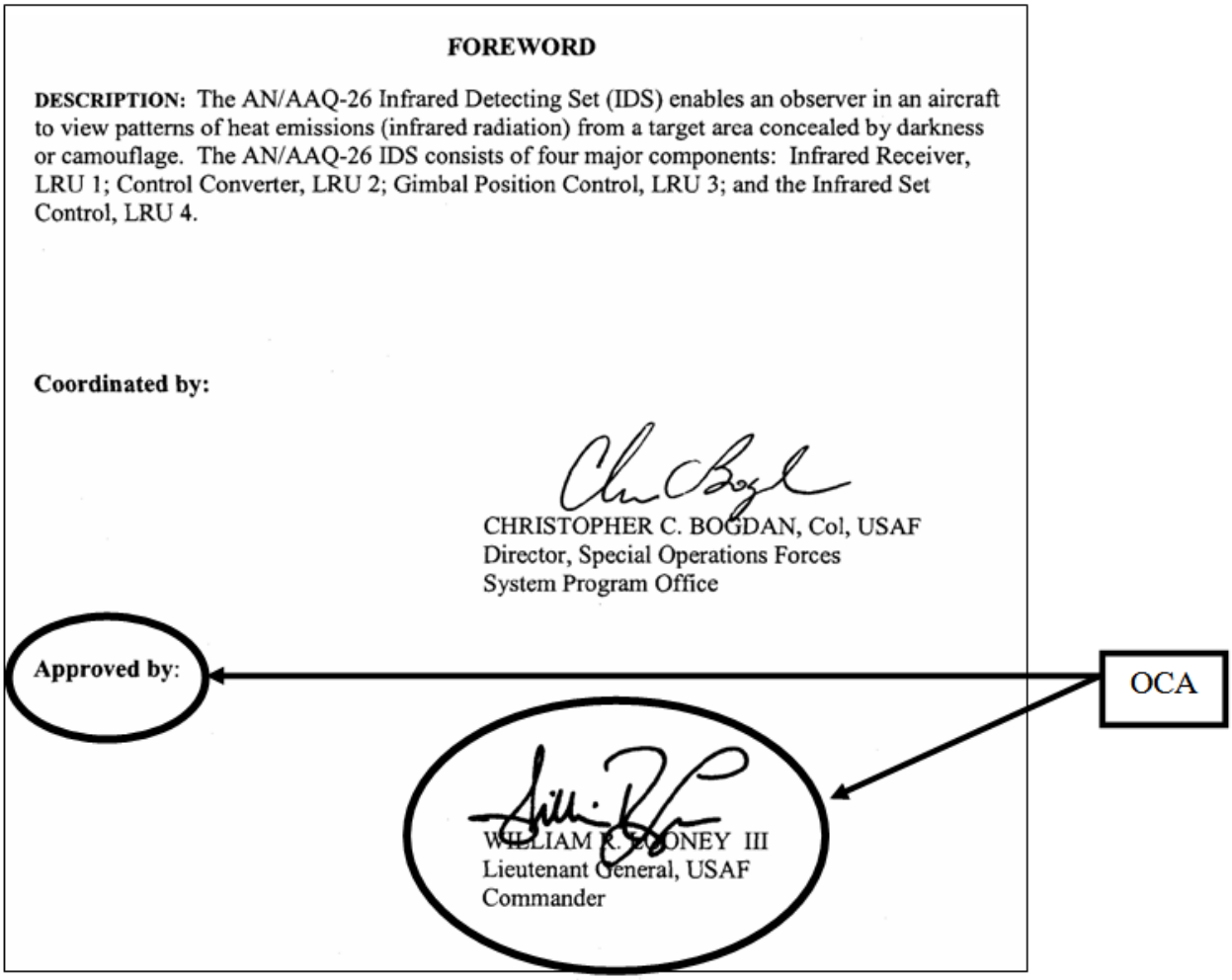
FORMAT FOR CLASSIFICATION/DECLASSIFICATION GUIDE

A7.1. Front page format:



SECTION 1

A7.2. General Instructions (Minimum Required Items Are Circled)



General Instructions Continued:

SECTION I

GENERAL INSTRUCTIONS

1. **Purpose.** This guide provides a basis for evaluating the degree of protection necessary for documentation, photographs, equipment, material, and information applicable to the AN/AAQ-26 IDS.

2. **Authority.** DoD 5200.1-R/AFI 31-401. Cite this guide as the basis for classifying, downgrading, or declassifying information about the AN/AAQ-26 IDS.

3. **Office of Primary Responsibility (OPR).** This guide is issued by ASC/LU, 1895 5th Street, Bldg 46, Wright-Patterson AFB OH 45433-7200, telephone COM (937) 255-4152/DSN 785-4152. Address all inquiries concerning content and interpretation to 88 SFS/SFA, 1801 Tenth Street, Room 103, Wright-Patterson AFB OH 45433-7625.

4. **Classification Recommendations.** Send completely documented and justified recommendations through 88 SFS/SFA, to the OPR if the security classifications or declassification instructions in this guide impose impractical requirements or when scientific or technological changes in the state of the art indicate a need for changes. Pending final decision, handle and protect the information at the highest of the present or the recommended classifications. All users of this guide are encouraged to assist in improving and maintaining the currency and adequacy of this guide.

5. **Classification Currency.** Changes to this guide will be affected by the issuance of a letter, Subject: Letter Change No. _____ to the AN/AAQ-26 IDS Security Classification Guide (SCG), 30 December 2004. This letter will indicate the appropriate change(s) and will constitute the authority for such change(s). Upon receipt of a letter change, the appropriate change(s) will be made and the letter of authority will be inserted in back of the guide.

6. **Reason for Classifying.** The reasons for classifying information are in accordance with Executive Order (EO) 12958, as amended by EO 13292. The categories for classification, as identified throughout the guide, are as follows:

Category 1.4g: Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security, which includes defense against and transnational terrorism.

7. **Explanation of Declassification Instructions.** Choose one of the following four declassification instructions, selecting, whenever possible, the declassification instruction that will result in the shortest duration of classification.

a. A date or event less than 10 years, or if unable to identify such a date or event;

b. a date 10 years from the date of the document; or

General Instructions Continued:

c. a date greater than 10 and less than 25 years from the date of the document; or

d. a date 25 years from the date of the document.

When determining the duration of classification, the Original Classification Authority should consider the four options listed above sequentially; first, consider the least amount of time that information needs to be classified, that is, a time frame that is less than 10 years; if unable to determine a date or event of less than 10 years then 10 years; third, between 10 years and up to 25 years based upon the sensitivity of the information as determined by the Original Classification Authority; and then finally, 25 years from the date of the decision.

All originally classified documents must contain a date or event of 25 years or less on the "Declassify on" line.

8. Prior Declassification Instructions. To comply with EO 12958, as amended by EO 13292, previously classified information with a declassification instruction of Originating Agency Determination Required (OADR) or X1 through X8 must be readdressed and now have a declassification date or event as identified in section 7 above. **NOTE**: The declassification date or event cannot exceed 25 years from the **original** classification date (the date the information was first classified).

9. Other Applicable Security Classification Guides. Refer to aircraft Security Classification Guides for aircraft/mission specific information.

10. Application, Reproduction, and Dissemination. Specified groups involved in the AN/AAQ-26 IDS program, including industrial activities, may make reproductions and extracts or selections of portions of this guide.

11. Manufacture, Test, and Assembly. During manufacture, test, or assembly processes, the classification as assigned by this guide shall apply at the earliest point where design, performance, or other classified characteristics can be derived and traced to the system(s) identified herein.

12. Disassembly and Repair. During disassembly and repair, the classification assigned by this guide no longer applies at the earliest point where design, performance, or other classified characteristics can no longer be derived from or traced to the system(s) identified herein.

13. Technology Transfer. A major goal of DoD classification policy is to deny our adversaries access to documents, hardware, and technologies that will accelerate their military programs and simultaneously cause an increase in our defense efforts and costs. During development of a system, numerous areas of advanced technology may be exploited. It is the intent of this guide to safeguard the following information:

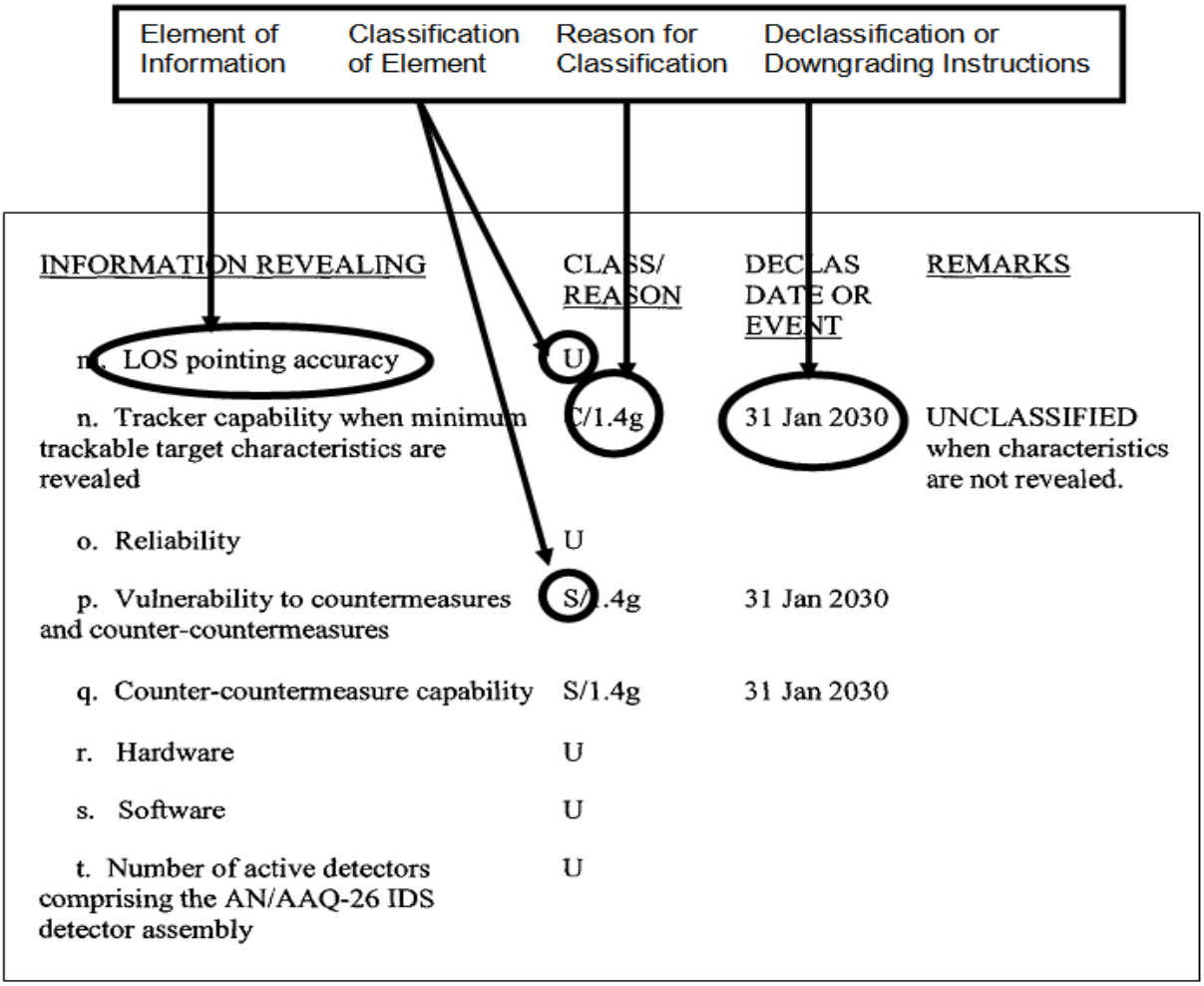
A7.3. Release Information:

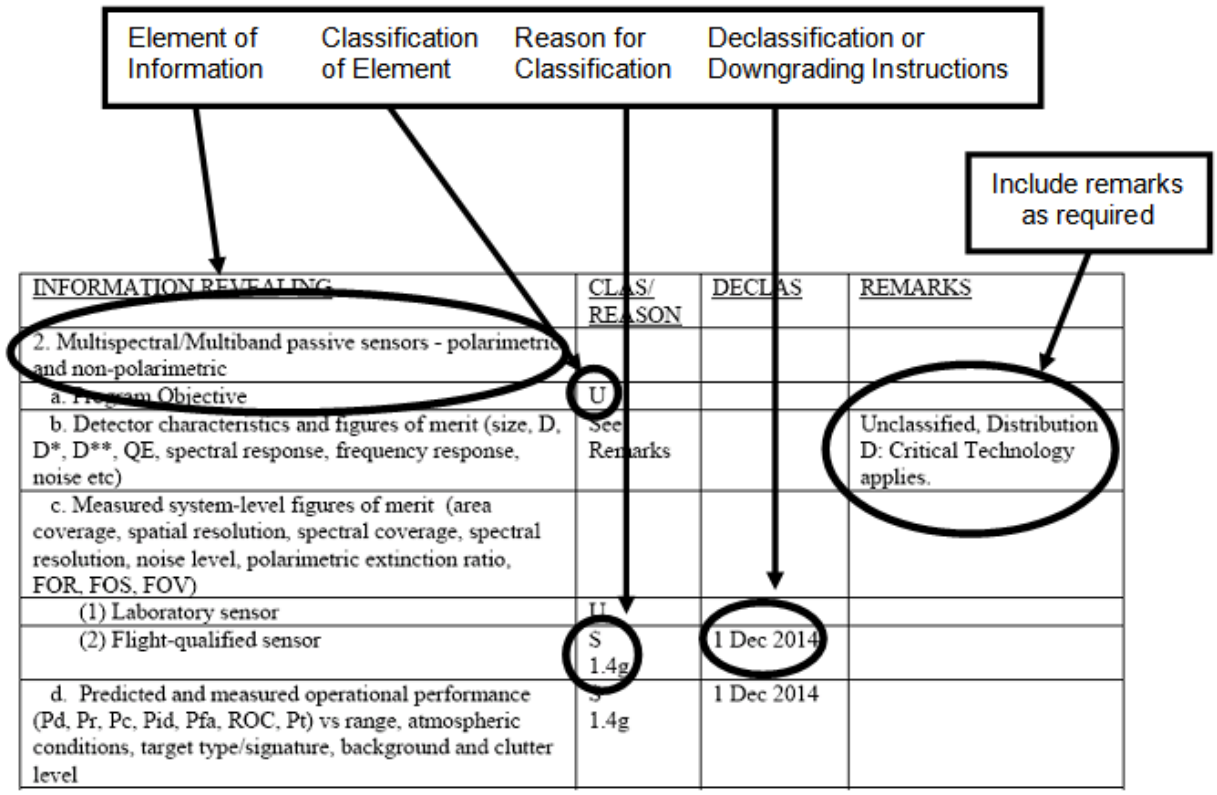
1. **Public Release of Official Information.** Although this guide shows certain details of information as unclassified, it does not permit automatic public release. Unclassified, unlimited distribution information proposed for public release about the AC-130U Gunship must be submitted to Aeronautical Systems Center Public Affairs; ATTN: Security and Policy Review (ASC/PA); Building 14, Room 240; 1865 4th Street; Wright-Patterson AFB OH 45433-7129, Telephone (937) 255-3334.

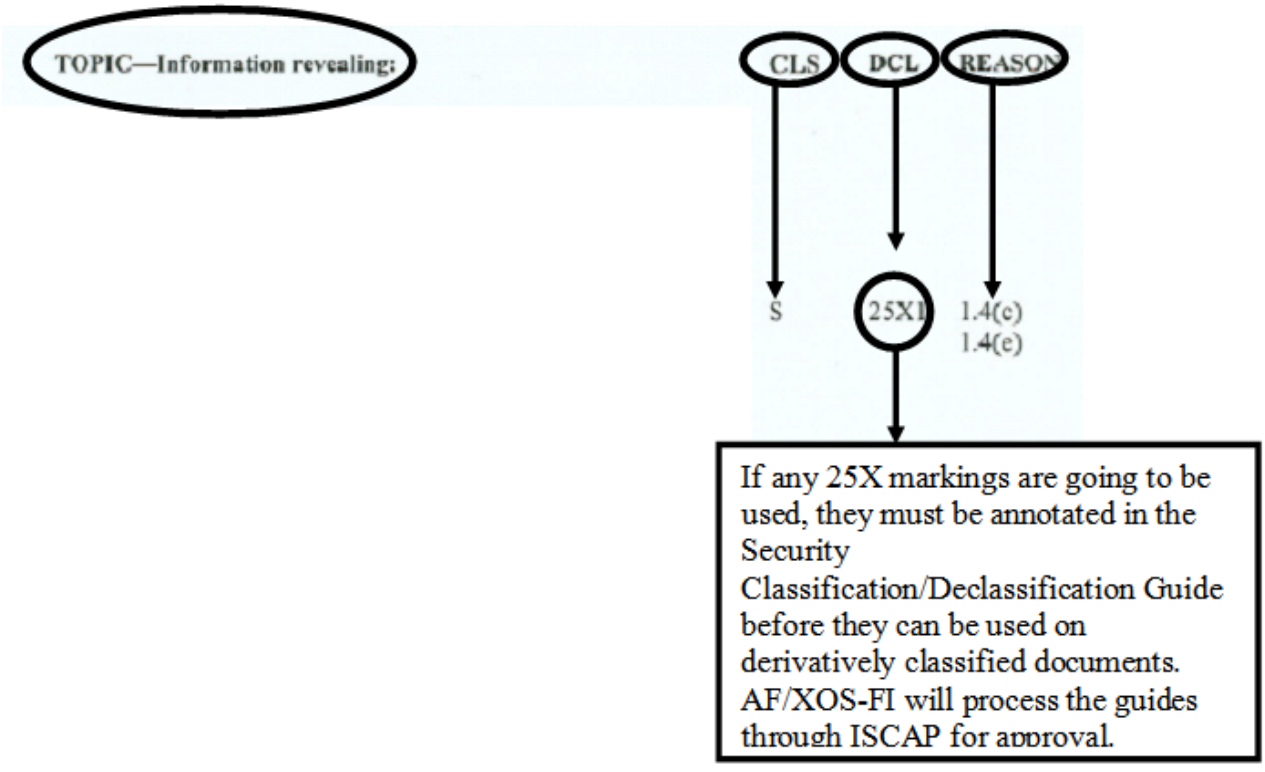
2. **Release of Program Data on the World Wide Web.** Extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web Sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. The search and data mining capabilities of Web technology must be assessed from a risk management perspective. If there are any doubts, do not release the information!

3. **Release of Classified and Unclassified Information to Foreign Governments or Their Representatives.** In accordance with AFI 16-201, Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations (C), advise a foreign national soliciting or requesting classified and/or unclassified USAF information to request it through their embassy in Washington DC. Any military activity or contractor receiving such a request from a foreign government, foreign contractor, or representative thereof must forward the request to ASC/XPD, 1865 4th St, Wright-Patterson AFB OH 45433-7127. Any military activity desiring to release classified and/or unclassified information to a foreign government, foreign contractor, or representative thereof, must forward the request to ASC/XPD according to AFI 16-201. Defense contractors desiring to release classified and/or unclassified information controlled by the International Traffic in Arms Regulation (ITAR) to a foreign government, foreign contractor, or representative thereof must request a munitions export license from: Department of State, Office of Defense Trade Control, PM/DTC Room 200, SA-6, Washington DC 20522.

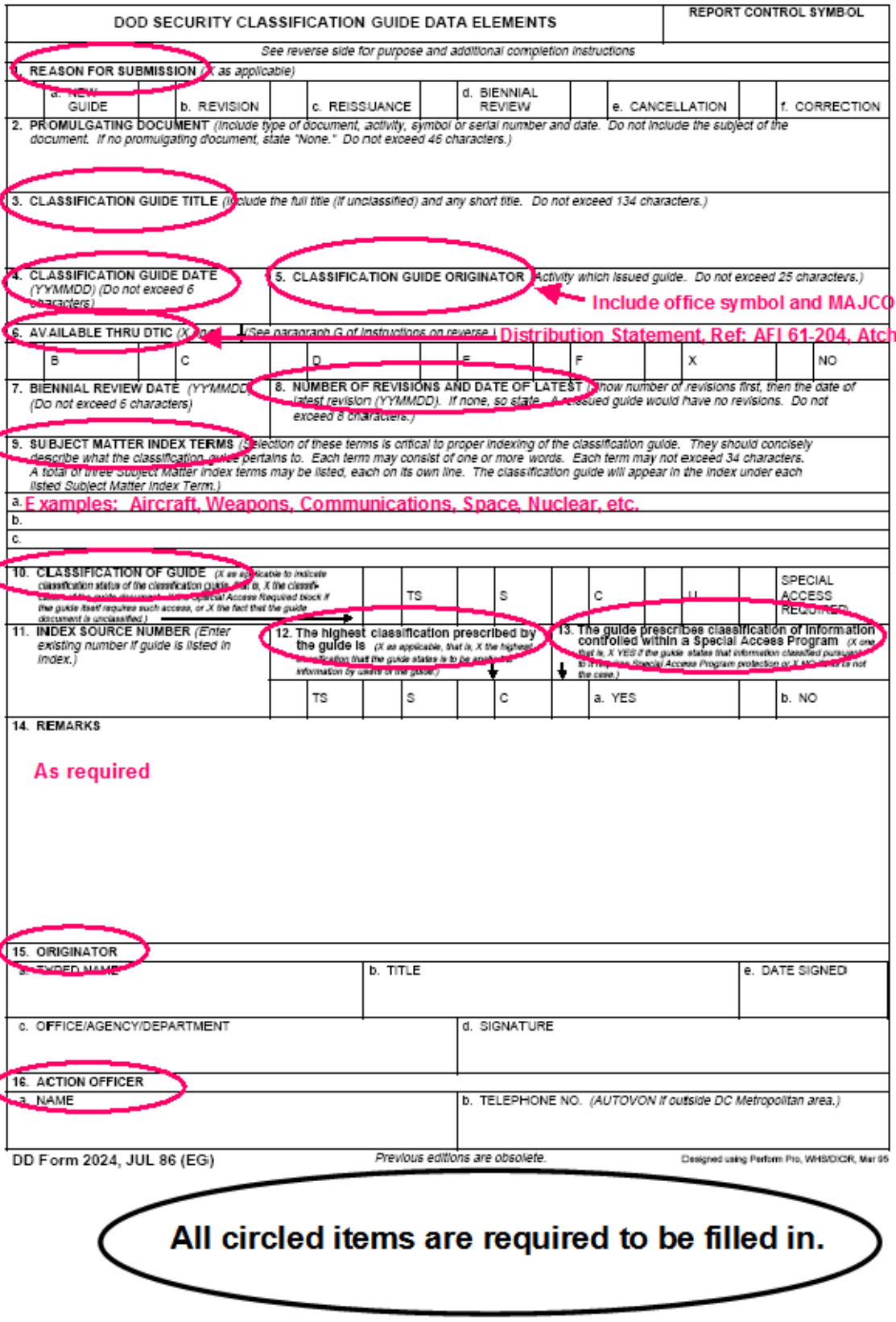
A7.4. Classification and Declassification Information:




Element of Information
Classification of Element
Reason for Classification
Declassification or Downgrading Instructions
Include remarks as required
INFORMATION REVEALING
CLAS/ REASON
DECLAS
REMARKS
2. Multispectral/Multiband passive sensors - polarimetric and non-polarimetric
a. Program Objective
U
b. Detector characteristics and figures of merit (size, D, D*, D**, QE, spectral response, frequency response, noise etc)
See Remarks
Unclassified, Distribution D: Critical Technology applies.
c. Measured system-level figures of merit (area coverage, spatial resolution, spectral coverage, spectral resolution, noise level, polarimetric extinction ratio, FOR, FOS, FOV)
(1) Laboratory sensor
U
(2) Flight-qualified sensor
S 1.4g
1 Dec 2014
d. Predicted and measured operational performance (Pd, Pr, Pc, Pid, Pfa, ROC, Pt) vs range, atmospheric conditions, target type/signature, background and clutter level
S 1.4g
1 Dec 2014


TOPIC—Information revealing:
CLS
DCL
REASON
S
25X1
1.4(c)
1.4(e)
If any 25X markings are going to be used, they must be annotated in the Security Classification/Declassification Guide before they can be used on derivatively classified documents. AF/XOS-FI will process the guides through ISCAP for approval.

A7.5. DD Form 2024, DOD Security Classification Guide Data Elements:



DOD SECURITY CLASSIFICATION GUIDE DATA ELEMENTS | REPORT CONTROL SYMBOL

See reverse side for purpose and additional completion instructions

1. REASON FOR SUBMISSION *(X as applicable)*

a. NEW GUIDE | b. REVISION | c. REISSUANCE | d. BIENNIAL REVIEW | e. CANCELLATION | f. CORRECTION

2. PROMULGATING DOCUMENT *(Include type of document, activity, symbol or serial number and date. Do not include the subject of the document. If no promulgating document, state "None." Do not exceed 46 characters.)*

3. CLASSIFICATION GUIDE TITLE *(Include the full title (if unclassified) and any short title. Do not exceed 134 characters.)*

4. CLASSIFICATION GUIDE DATE *(YYMMDD) (Do not exceed 6 characters)*

5. CLASSIFICATION GUIDE ORIGINATOR *(Activity which issued guide. Do not exceed 25 characters.)*

Include office symbol and MAJCOM

6. AVAILABLE THRU DTIC *(X one)* *(See paragraph G of Instructions on reverse.)*

Distribution Statement, Ref: AFI 61-204, Atch 2

B | C | D | E | F | X | NO

7. BIENNIAL REVIEW DATE *(YYMMDD) (Do not exceed 6 characters)*

8. NUMBER OF REVISIONS AND DATE OF LATEST *(Show number of revisions first, then the date of latest revision (YYMMDD). If none, so state. A reissued guide would have no revisions. Do not exceed 8 characters.)*

9. SUBJECT MATTER INDEX TERMS *(Selection of these terms is critical to proper indexing of the classification guide. They should concisely describe what the classification guide pertains to. Each term may consist of one or more words. Each term may not exceed 34 characters. A total of three Subject Matter Index terms may be listed, each on its own line. The classification guide will appear in the index under each listed Subject Matter Index Term.)*

a. Examples: Aircraft, Weapons, Communications, Space, Nuclear, etc.

b.

c.

10. CLASSIFICATION OF GUIDE *(X as applicable to indicate classification status of the classification guide. That is, X the classification of the guide document. Mark Special Access Required block if the guide itself requires such access, or X the fact that the guide document is unclassified.)* | TS | S | C | U | SPECIAL ACCESS REQUIRED

11. INDEX SOURCE NUMBER *(Enter existing number if guide is listed in index.)*

12. The highest classification prescribed by the guide is *(X as applicable, that is, X the highest classification that the guide states is to be applied to information by users of the guide.)* | TS | S | C

13. The guide prescribes classification of information controlled within a Special Access Program *(X one, that is, X YES if the guide states that information classified pursuant to it requires Special Access Program protection or X NO, if this is not the case.)* | a. YES | b. NO

14. REMARKS

As required

15. ORIGINATOR

a. TYPED NAME | b. TITLE | e. DATE SIGNED

c. OFFICE/AGENCY/DEPARTMENT | d. SIGNATURE

16. ACTION OFFICER

a. NAME | b. TELEPHONE NO. *(AUTOVON if outside DC Metropolitan area.)*

DD Form 2024, JUL 86 (EG) *Previous editions are obsolete.* Designed using Perform Pro, WHS/DIOR, Mar 95

All circled items are required to be filled in.

Executive Order 13526

From Wikisource

Executive Order 13526 of December 29, 2009

Classified National Security Information

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

NOW, THEREFORE, I, BARACK OBAMA, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1 — ORIGINAL CLASSIFICATION

Sec. 1.1. *Classification Standards*.

(a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. *Classification Levels*.

(a) Information may be classified at one of the following three levels:

EXECUTIVE ORDER 9397

NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL PERSONS

WHEREAS certain Federal agencies from time to time require in the administration of their activities a system of numerical identification of accounts of individual persons; and

WHEREAS some seventy million persons have heretofore been assigned account numbers pursuant to the Social Security Act; and

WHEREAS a large percentage of Federal employees have already been assigned account numbers pursuant to the Social Security Act; and

WHEREAS it is desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single unduplicated numerical identification system of accounts and avoid the unnecessary establishment of additional systems:

NOW, THEREFORE, by virtue of the authority vested in me as President of the United States, it is hereby ordered as follows:

1. Hereafter any Federal department, establishment, or agency shall, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize exclusively the Social Security Act account numbers assigned pursuant to Title 26, section 402.502 of the 1940 Supplement to the Code of Federal Regulations and pursuant to paragraph 2 of this order.

2. The Social Security Board shall provide for the assignment of an account number to each person who is required by any Federal agency to have such a number but who has not previously been assigned such number by the Board. The Board may accomplish this purpose by (a) assigning such numbers to individual persons, (b) assigning blocks of numbers to Federal agencies for reassignment to individual persons, or (c) making such other arrangements for the assignment of numbers as it may deem appropriate.

3. The Social Security Board shall furnish, upon request of any Federal agency utilizing the numerical identification system of accounts provided for in this order, the account number pertaining to any person with whom such agency has an account or the name and other identifying data pertaining to any account number of any such person.

4. The Social Security Board and each Federal agency shall maintain the confidential character of information relating to individual persons obtained pursuant to the provisions of this order.

5. There shall be transferred to the Social Security Board, from time to time, such amounts as the Director of the Bureau of the Budget shall determine to be required for reimbursement by any Federal agency for the services rendered by the Board pursuant to the provisions of this order.

6. This order shall be published in the FEDERAL REGISTER.

FRANKLIN D. ROOSEVELT

THE WHITE HOUSE
November 22, 1943

[F.R. Doc. 43-19051; Filed, November 27, 1943; 2:45 p.m.]
[8 Federal Register 16095, November 30, 1943]

Executive Order 10450--Security requirements for Government employment

Source: The provisions of Executive Order 10450 of Apr. 27, 1953, appear at 18 FR 2489, 3 CFR, 1949-1953 Comp., p. 936, unless otherwise noted.

WHEREAS the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U.S.C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U.S.C. 632, et seq.); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U.S.C. 118j); and the act of August 26, 1950, 64 Stat. 476 (5 U.S.C. 22-1, et seq.), and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

Section 1. In addition to the departments and agencies specified in the said act of August 26, 1950, and Executive Order No. 10237 of April 26, 1951, the provisions of that act shall apply to all other departments and agencies of the Government.[1]

Sec. 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

Sec. 3. (a) The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: *Provided*, that upon request of the head of the department or agency concerned, the Office of Personnel Management may, in its discretion, authorize such less investigation as may meet the requirements of the national security with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such

person a full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field investigation has been conducted: *Provided*, that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: *And provided further*, that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field pre-appointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

[Sec. 3 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 4. The head of each department and agency shall review, or cause to be reviewed, the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835 of March 21, 1947, and, after such further investigation as may be appropriate, shall re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, such of those cases as have not been adjudicated under a security standard commensurate with that established under this order.

Sec. 5. Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his representative, who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

Sec. 6. Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, the head of the department or agency concerned or his representative shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of the national security and, following such investigation and review as he deems necessary, the head of the department or agency concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with the said act of August 26, 1950.

Sec. 7. Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950, or pursuant to the said Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the Government, shall not be reinstated or restored to duty or reemployed in the same department or agency and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or

reemployment is clearly consistent with the interests of the national security, which finding shall be made a part of the records of such department or agency: *Provided,* that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except after a determination by the Office of Personnel Management that such person is eligible for such employment.

[Sec. 7 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

(1) Depending on the relation of the Government employment to the national security:

(i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

(ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, sexual perversion.

(iv) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.

(v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

(2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefore, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(4) Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

(5) Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State, or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(7) Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(8) Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his alleged disloyalty or other misconduct.

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Office of Personnel Management, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Office. The Office shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Office of Personnel Management, and other departments and agencies may use such facilities under agreement with the Office.

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information relating to any of the matters described in subdivisions (2) through (8) of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

[Sec. 8 amended by EO 10491 of Oct. 13, 1953, 18 FR 6583, 3 CFR, 1949-1953 Comp., p. 973; EO 10531 of May 27, 1954, 19 FR 3069, 3 CFR, 1954-1958 Comp., p. 193; EO 10548 of Aug. 2, 1954, 19 FR 4871, 3 CFR, 1954-1958 Comp., p. 200; EO 11785 of June 4, 1974, 39 FR 20053, 3 CFR, 1971-1975 Comp., p. 874; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 9. (a) There shall be established and maintained in the Office of Personnel Management a security-investigations index covering all persons as to whom security investigations have been conducted by any department or agency of the Government under this order. The central index established and maintained by the Office under Executive Order No. 9835 of March 21, 1947, shall be made a part of the security-investigations index. The security-investigations index shall contain the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an investigation concerning the person involved or has suspended or terminated the employment of such person under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950.

(b) The heads of all departments and agencies shall furnish promptly to the Office of Personnel Management information appropriate for the establishment and maintenance of the security-investigations index.

(c) The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of August 26, 1950, as may be required for the efficient conduct of Government business.

[Sec. 9 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 10. Nothing in this order shall be construed as eliminating or modifying in any way the requirement for any investigation or any determination as to security which may be required by law.

Sec. 11. On and after the effective date of this order the Loyalty Review Board established by Executive Order No. 9835 of March 21, 1947, shall not accept agency findings for review, upon appeal or otherwise. Appeals pending before the Loyalty Review Board on such date shall be heard to final determination in accordance with the provisions of the said Executive Order No. 9835, as amended. Agency determinations favorable to the officer or employee concerned pending before the Loyalty Review Board on such date shall be acted upon by such Board, and whenever the Board is not in agreement with such favorable determination the case shall be remanded to the department or agency concerned for determination in accordance with the standards and procedures established pursuant to this order. Cases pending before the regional loyalty boards of the Office of Personnel Management on which hearings have not been initiated on such date shall be referred to the department or agency concerned. Cases being heard by regional loyalty boards on such date shall be heard to conclusion and the determination of the board shall be forwarded to the head of the department or agency concerned: *Provided,* that if no specific department or agency is involved, the case shall be dismissed without prejudice to the applicant. Investigations pending in the Federal Bureau of Investigation or the Office of Personnel Management on such date shall be completed, and the reports thereon shall be made to the appropriate department or agency.

[Sec. 11 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 12. Executive Order No. 9835 of March 21, 1947, as amended, is hereby revoked.

[Sec. 12 amended by EO 11785 of June 4, 1974, 39 FR 20053, 3 CFR, 1971-1975 Comp., p. 874]

Sec. 13. The Attorney General is requested to render to the heads of departments and agencies such advice as may be requisite to enable them to establish and maintain an appropriate employee-security program.

Sec. 14. (a) The Office of Personnel Management, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, shall make a continuing study of the manner in which this order is being implemented by the departments and agencies of the Government for the purpose of determining:

(1) Deficiencies in the department and agency security programs established under this order which are inconsistent with the interests of, or directly or indirectly weaken, the national security.

(2) Tendencies in such programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or this order.

Information affecting any department or agency developed or received during the course of such continuing study shall be furnished immediately to the head of the department or agency concerned. The Office of Personnel Management shall report to the National Security Council, at least semiannually, on the results of such study, shall recommend means to correct any such deficiencies or tendencies, and shall inform the National Security Council immediately of any deficiency which is deemed to be of major importance.

(b) All departments and agencies of the Government are directed to cooperate with the Office of Personnel Management to facilitate the accomplishment of the responsibilities assigned to it by subsection (a) of this section.

(c) To assist the Office of Personnel Management in discharging its responsibilities under this order, the head of each department and agency shall, as soon as possible and in no event later than ninety days after receipt of the final investigative report on a civilian officer or employee subject to a full field investigation under the provisions of this order, advise the Office as to the action taken with respect to such officer or employee. The information furnished by the heads of departments and agencies pursuant to this section shall be included in the reports which the Office of Personnel Management is required to submit to the National Security Council in accordance with subsection (a) of this section. Such reports shall set forth any deficiencies on the part of the heads of departments and agencies in taking timely action under this order, and shall mention specifically any instances of noncompliance with this subsection.

[Sec. 14 amended by EO 10550 of Aug. 5, 1954, 19 FR 4981, 3 CFR, 1954-1958 Comp., p. 200; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 15. This order shall become effective thirty days after the date hereof.

[1] **Editorial note:** In *Cole* v. *Young*, 76 S.Ct. 861 (1955), section 1 of Executive Order 10450 was held to be invalid if applied to every department and agency.

Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors

There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.

Homeland Security Presidential Directive-12

August 27, 2004

SUBJECT: Policies for a Common Identification Standard for Federal Employees and Contractors

1. Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).
2. To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.
3. "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).
4. Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

5. Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.
6. This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.
7. Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.
8. The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

# # #

Last Published Date: *August 19, 2015*