SYSTEM NAME AND NUMBER: Personnel Security Clearance Case Files, 1703.03 AAFES.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Headquarters, Army and Air Force Exchange Service (Exchange), 3911 S. Walton Walker Boulevard, Dallas, TX 75236-1598.

SYSTEM MANAGER(S): Director/Chief Executive Officer, Army and Air Force Exchange Service, 3911 S. Walton Walker Boulevard, Dallas, TX 75236-1598; 800-527-6790.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 7103, Secretary of the Army; 10 U.S.C. 9013, Secretary of the Air Force; United States Presidential Executive Order (E.O.) 13526, Classified National Security; E.O. 10450, Security Requirements for Government Employment; Department of Defense Instruction (DoDI) 5200.01, DoD Information Security Program and Protection of Sensitive Compartmental Information; DoDI 5200.02, DoD Personnel Security Program (PSP); Army Regulation (AR) 380-67, Personnel Security Program; Air Force Instruction (AFI) 31-501, Personnel Security Program Management; AFI 31-401, Information Security Program Management; AR 215-8/AFI 34-211(I), Army and Air Force Exchange Service Operations; and E.O. 9397, (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: To assist in the processing of personnel security clearance actions, to record security clearances issued or denied, to verify eligibility for access to classified and sensitive information or positions. Records are used by Exchange executives for adverse personnel actions which may include removal from sensitive duties or employment, denial to a restricted or sensitive area, and revocation of security clearance. Records are also used to ensure that departing employees have been properly out-processed.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals affiliated with the Army and Air Force Exchange Service (Exchange) by assignment, employment, contractual relationship, or as the result of an inter-service support agreement on whom a personnel security clearance determination has been completed, is in process, or may be pending.

CATEGORIES OF RECORDS IN THE SYSTEM: Individual's full name, date of birth, Social Security Number (SSN); fingerprints; Department of Defense Identification Number (DoD ID Number), and ID card bar code value; Military Unit Identification Code (UIC); gender and marital status; addresses (home, billing, and shipping); e-mail address (personal and/or business) and telephone number (personal and/or business); personal automobile license plate number; military or civilian branch of service identifier and employment grade level; military or civilian status (active, reserve, retired, veteran, civilian, officer, enlisted, family member, survivor, foreign, local national, etc.); privilege identifier; financial information (bank account routing number and account number); job location; supervisor's name and contact information (phone and e-mail address); reason for departure; clearing office approval. This system also maintains pending and completed security clearance actions; briefing/debriefing statements for special programs, sensitive positions and other related information and documents required in connection with personnel security clearance adjudication, background investigation results, and security approvals or denials.

RECORD SOURCE CATEGORIES: From the individual, contractor/vendor, past employers, financial references, the Defense Enrollment Eligibility Reporting System (DEERS), Defense Manpower Data System (DMDC), and from investigative results furnished by the Defense Investigative Service and other Federal agencies such as Department of Defense, Department of Justice, Armed Forces Exchanges, Moral Welfare and Recreation (MWR), Defense Commissary Agency (DECA), and State, Local, Federal, and International law enforcement agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

b. To designated officers and employees of Federal, State, local, territorial or tribal, international, or foreign agencies maintaining civil, criminal, enforcement, or other pertinent information, such as current licenses, if necessary to obtain information relevant and necessary to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

c. To designated officers and employees of Federal, State, local, territorial, tribal, international, or foreign agencies in connection with the hiring or retention of an employee, the conduct of a suitability or security investigation, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter and the Department deems appropriate.

d. To contractors whose employees require suitability determinations, security clearances, and/or access to classified national security information, for the purpose of ensuring that the employer is appropriately informed about information that relates to and/or may impact a particular employee or employee applicant's suitability or eligibility to be granted a security clearance and/or access to classified national security information.

e. To foreign or international law enforcement, security, or investigatory authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

f. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or

homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

g. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

h. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

i. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

j. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

k. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

l. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

m. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

n. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORING OF RECORDS: Records are maintained in paper and electronic storage media, in accordance with the safeguards mentioned below.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: The records are retrieved by individual's full name. SSN, Military Unit Identification Code (UIC), DoD ID Number may be used for verification purposes.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: System records are retained and disposed of according to the National Archives and Records Administration (NARA) and the General Services Administration (GSA) regulations.

Security files for individuals not issued clearances are destroyed by shredding or erased from the server one year after consideration. Files associated with issued clearances are maintained for five years after their employment/contract relationship with the Exchange expires. Longer retention is authorized if required for business use.

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS: he Exchange has implemented the highest level of security controls and the system is assessed against Center for Internet Security (CIS) Configuration Baselines. Configuration scans are conducted monthly to monitor compliance. The Exchange secures information in secured buildings and behind controlled areas accessible only to employees with a right-to-know who have been screened, cleared for access, and have a role-based position for which places them in an arrangement that requires servicing, reviewing, or updated records. Administrative safeguards include periodic security audits, regular monitoring of individual security practices, and limiting access to personal information to those individuals who have a need to know to perform their official duties. Technical safeguards include individual user logins and passwords, intrusion detection system, encryption, and firewall protection. Physical safeguards include security guards, identification badges, key cards, safes, and cipher locks.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system should address written inquiries to the Director/Chief Executive Officer, Army and Air Force Exchange Service, Attention: Privacy Manager, 3911 S. Walton Walker Boulevard, Dallas, TX 75236-1598.

Signed written requests should include the individual's full name, telephone number, street or mailing address e-mail address, case number that appeared on correspondence received from the Exchange if applicable, name and number of this system of records notice, and signature.

In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United State of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The Army's rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 505, the Army Privacy Program and AR 25-22, The Army Privacy Program, or may be obtained from the system manager.

NOTIFICA**TION PROCEDURES:** Individuals seeking to determine if information about themselves is contained in this system should address written inquiries to the Director/Chief Executive Officer, Army and Air Force Exchange Service, Attention: Privacy Manager, 3911 S. Walton Walker Boulevard, Dallas, TX 75236-1598.

Signed, written requests should contain the individual's full name, telephone number, street or mailing address, e-mail address, case number that appeared on correspondence received from the Exchange if applicable, name and number of this system of records notice, and signature.

In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United State of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: August 09, 1996, 61 FR 41594. This system of records notice supersedes all versions previously published in the Federal Register.