U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL MANUAL	Number: 3140-001
SUBJECT: Management ADP Security Manual	DATE: July 19, 1984
	OPI: Agency Technical Services Division, Office of Information Resources Management

1 PURPOSE

This manual contains standards, guidelines, and procedures for the development and administration of ADP security programs mandated by DR 3140-1, ADP Security Policy.

2 APPLICABILITY

This manual applies to the management of all ADP resources of the Department of Agriculture. It applies to processing done on equipment that is:

> Government-owned or leased, whether Government or contractor operated; or accessed through commercial timesharing acquired under a USDA contract.

To the extent practicable, this manual shall also be applied to processing done on equipment that is:

> Accessed through commercial timesharing acquired under GSA schedule contracts; operated by a cooperator in accordance with a specific cooperative agreement, or a grantee in accordance with a specific grant, or employee-owned, when used to process USDA information. Processing of USDA information on employee-owned equipment must be authorized by the appropriate agency management.

This manual applies to the security and privacy of all automated information that is collected, transmitted, used, processed, stored, or disposed of by or under the direction of USDA or its designated agent.

3 REFERENCES - See Section 20

4 ABBREVIATIONS

A-71	OMB Circular A-71, Transmittal Memorandum No. 1
ADP	Automated Data Processing
DCC	Departmental Computer Center
FIPS PUBS	Federal Information Processing Standards Publications
FIRMR	Federal Information Resources Management Regulation
GOCO	Government Owned/Contractor Operated
OIG	Office of Inspector General
OIRM	Office of Information Resources Management
RJE	Remote Job Entry
RP-1	Standard Practice for the Fire Protection of Essential Electronic Equipment Operations
WP	Word Processing

5 EXPLANATION OF TERMS

Agencies. Agencies and Staff Offices.

Facility Types. Security requirements for ADP, research, word processing, and office automation facilities within USDA or at GOCO sites may vary, depending on several factors:

a The monetary value of equipment;
b The sensitivity of data;
c The criticality of processing performed;
d The number of users dependent on the facility; and
e The quality of protection external to the facility.

It is impossible to develop definitive standards which address the issues involved in assigning a facility type to aggregations of equipment. Prudent management dictates that facility attributes be reviewed annually and facilities redesignated if the reviews so indicate. A risk analysis, using an automated package, the FIPS PUS 65 method, or any other comprehensive approach should provide adequate results upon which to base a decision on redesignation.

The desired result of such reviews and studies is to determine the security features required to protect the particular installation or operation in question without expenditure of excessive resources.

In determining the facility type, only the actual functions performed by the facility should be taken into consideration, not the potential usages of the available hardware and software.

The required security is determined by the facility type and by the kind of processing done. For example, installations which communicate with other installations will, in general, need more security than a stand-alone computer. Installations processing sensitive data will require extra protection.

All USDA or GOCO ADP facilities shall be identified by type. The

facility types and attributes are:

Facility Type	Description
I	Is a Departmental Computer Center, the National Finance Center or another comparable large, typically multi-Agency, general purpose facility.
II	Has general purpose computer(s) which: Service multiple users concurrently as end processors, i.e., support self-contained processing using resident operating systems, compilers, peripheral devices, etc. Typically, Type II facilities serve one or a limited number of agencies.
III	Consists of other DP and WP equipment.

Formal security plans and risk analyses are mandatory for each type I and type II facility. Each agency is also required to develop an agency-wide security plan. Security plan requirements are detailed in Section 9.

Computers used for scientific research or process/laboratory control require separate consideration. Although such computers are often equivalent to Type II facility equipment in size and capability, their security requirements may differ.

Mandatory requirements for the special-purpose facilities described above are:

adequate physical security;
designated security officers;
annual security reviews;
security plans; and
backup and contingency plans for critical systems.

Facility managers may determine the need for:

software access controls;
data and software protection; and
audit trails.

Waivers from specific security standards are not required of special-purpose facilities. Facility managers must, however, make every reasonable effort to achieve and maintain security commensurate with the importance of processing done at the site.

Microcomputer. One of a variety of general purpose computers manufactured utilizing one or more microprocessors. Microcomputers

can range from computers with relatively small amounts of memory to computers with large amounts of random access memory and several peripheral devices. They normally require no special environmental site preparation. They are often called personal, professional, or end user computers.

Security. As used in this manual, ADP security.

Sensitive Information. Information which is: classified in the National Security; subject to the Privacy Act of 1974 (PL 93-579, 5 U.S.O. 552a); proprietary to a commercial firm; associated with fiduciary or financial transactions; associated with inventories, grants, or benefits; time- or market-critical; Types I or II systems software; related to agency plans or policies or future actions; and designated as vital records, as defined by FPMR 101-11.7.

Sensitive Processing. Application systems are designed to perform specific tasks. Incorporating security measures in application programs is one of the most effective ways to assure that the programs do exactly what is required and no more, no less. Proper control of data before, during, and after processing also is vital to achieving good system security.

In order to make a reasoned selection of controls for protecting a particular application, it is necessary to assess the sensitivity of the programs and related data which make up the system. The potential for loss, error, embarrassment, or delay inherent in the operation of the system must be considered.

The examples given below are not all-inclusive. For example, an agency's budgetary and planning material might be considered of vital importance--or it might not. Agencies must determine sensitivity through careful assessment of the potential for loss or harm that operation of a particular system poses.

Application systems, data management systems, and related data shall be designated sensitive if compromise could result in:

Any fraud, theft, or illegal gains from programs which issue payments, benefits, receipts, billings; which maintain inventories; or which produce commodity-related information;

Miscalculation of payments, benefits, receipts, billings, or inventories;

Failure to produce time-critical data on schedule;

Violation of National Defense disclosure requirements;

Unauthorized disclosure or misuse of private,

proprietary or trade-secret data;

Adverse effect on on-going investigations or agency operations; or

Adverse effect in life-threatening situations.

6 BACKGROUND

The Privacy Act of 1974 (PL 93-579, 5 U.S.O. 552a) imposes numerous requirements upon Federal agencies to prevent the misuse of information about individuals and assure its integrity and security. Protective measures must be employed to minimize the likelihood of unauthorized disclosure of such information or of any use of this data in other than routine use.

A-71, issued in July, 1978, requires (1) that security requirements be assessed and provided at several points in the development of sensitive application systems; (2) that adequate security features be included in all related documents for procurement of material or services and tested for completeness and quality before acceptance; (3) that risk analyses and physical security reviews be conducted at specified minimal intervals; (4) that adequate contingency plans be developed and tested; (5) that sensitive systems be evaluated and certified/ recertified at specified minimal intervals and subjected to rigorous ADP audit as deemed necessary; and (6) that personnel, including contractors, working in the ADP environment have proper personnel security clearances.

7 SECURITY PROGRAM REQUIREMENTS

Agencies must define the degree of protection needed for automated systems supporting their missions. Agencies will provide security requirements to management of the appropriate DCCs or agency facilities processing these systems and shall work with facility personnel to achieve the requisite level of protection. Agencies will determine security requirements by evaluation of the systems sensitivity, vulnerability, importance to agency missions, and cost to reconstruct. Protection against the following will be provided:

a Theft, fraud, waste, or abuse of ADP assets;

b Data loss or modification;

c Unauthorized data disclosure;

d Decreased operation reliability (interruption or loss of service; degraded system performance); and

e Asset loss (equipment, facilities, supplies, etc.).

Select safeguards on the basis of risk analyses, security reviews, and application evaluations, which will conform to applicable standards and guidelines. Document these safeguards in agency and

facility security plans.

Include adequate security provisions in specifications for the acquisition of hardware, software, and services. Agencies must certify the adequacy of these provisions and retain documentation in agency procurement files. (See DR 5020-2). Test security measures (when appropriate) and certify in writing prior to acceptance.

When it is not feasible to apply a particular standard to an existing ADP system without excessive costs, devise an alternate scheme for adequate protection. Agencies may then request a waiver from the standard, stating the reason for the request and describing the alternate scheme to be used. Address waiver requests to OIRM.

8 RESPONSIBILITIES

Responsibilities of Agency USDA Heads, OIRM, and ADP facility managers are detailed in DR 3140-1, ADP Security Policy. Each agency shall designate a qualified person to serve as the agency ADP Security Officer, who is responsible for oversight of the agency's ADP security program. OIRM strongly recommends that agency security officers be used as coordinators and consultants, in addition to their use as technicians. Agencies shall appoint deputy agency and facility security officers in appropriate numbers to assure proper coverage. Each DCC and each Type II facility will have a qualified facility security officer. Each Type III installation will have a designated security representative.

Agencies will furnish OIRM a current list of agency security officers and their deputies, giving names, mailing addresses, and telephone numbers.

a Responsibilities of Agency Heads, OIRM, and ADP facility managers are detailed in DR 3140-1.

b Specific responsibilities of security officers differ, depending on the mission of the unit. For example, in performing a DCC risk analysis, the facility officer will direct the effort; the agency officer most often will participate by furnishing information about agency data and processing.

The following security officer functions are necessary. An agency may assign specific duties to personnel other than the designated security officers, but all tasks must be performed by qualified individuals.

(1) Advise if management on policies and procedures to ensure data and system integrity; on employee access

to sensitive data; on personnel security clearances of individuals; and on proper operational control of the flow of sensitive data through the organization.

(2) Manage hardware, software, and data access mechanisms and authorizations.

(3) Assist the designated official responsible for meeting the requirements of the Privacy Act of 1974 (PL 93-579, 5 U.S.C. 552a).

(4) Develop the agency/facility ADP security plan(s) with the assistance of the deputy security officers.

(5) Monitor and test for vulnerability of security safeguards at irregular intervals, at least once a year.

(6) Participate in risk analyses.

(7) Assist in developing security requirements for acquisition of hardware/software/services and in testing security after installation; in the development of site preparation plans to assure inclusion of adequate security and safety provisions; in the application system evaluation and certification process; and in internal or external audits and physical inspections.

(8) Monitor remedial measures to correct deficiencies identified in audits or inspections.

(9) Coordinate or conduct all other systems security activities, including deputy and backup security officers training, security awareness training, employees and contractors briefing/debriefing, and facility security reviews.

(10) Maintain records of security problems and violations. If the capability to produce automated access violation reports exists, listings will be produced and analyzed. Significant violations and actions taken will be recorded and forwarded to appropriate. USDA officials, such as supervisors, Departmental security, or the OIG.

(11) Investigate system security breaches of any type and recommend emergency procedures deemed necessary. Report serious or potentially-serious breaches to OIG immediately.

(12) Report to management at least annually, when the agency security plan is prepared, or as a need dictates:

(a) Security program status.

(b) Actions required to improve security.

(c) Security training needs.

c All users of ADP facilities, at all organizational levels, share with facility personnel the responsibility to:

(1) Protect ADP assets and data from theft, fraud, misuse, loss, or unauthorized modification.

(2) Access or attempt to access only the data or resources specifically authorized. When granting access to another, the owner should limit the type and duration of access to the minimum necessary.

(3) Maintain confidentiality of data, including but not restricted to private, trade secret, National Defense, financial, proprietary, and market-sensitive information. If users have not been informed of the sensitivity of data and processing, they must ask management for clarification.

(4) Report promptly to proper authorities any violations of security or observed irregularities.

(5) Apply USDA security standards to processing done on remote terminals and microcomputers, to manual processing which is part of ADP systems, to word processing, and to processing in a telecommunications environment.

(6) Protect telephone numbers, passwords, and all other system access keys against unauthorized disclosure; change passwords frequently; use passwords which give no clue to names, content of data, or systems being protected; and protect input/output data from casual inspection or unauthorized retrieval.

(7) Recognize deviations from expected processing results or significant variations in input data. To this end, users should be aware of pertinent internal controls in their programs.

(8) Practice good housekeeping with all electronic equipment.

(9) Assure remote equipment logoff procedures are followed and that all data and equipment are secured.

(10) Use an alternate standard or procedure when a waiver from a Federal or USDA standard has been granted.

(11) If the required level of security is not available to the user, then the user must inform the

appropriate security officer of this fact and in the meantime take action to compensate for the deficiency by other means.

9 SECURITY PLANS

Each DCC and each agency will submit to OIRM an ADP security plan or an annual update to an existing plan by March 31 of each year.

These plans will be reviewed for suitability. The purpose of the plan is to:

a Provide management an assessment of security status, including future goals, training needs, and scheduled actions;

b Furnish guidance to newly-appointed security officers in administering the security program;

c Measure progress in achieving targeted goals; and

d Provide auditors and investigators with a status report.

Agency Security Plan. The agency security plan summarizes information contained in all agency facility security plans and addresses the security of all ADP processing, including microcomputers, remote terminals, and word processing operations.

It must contain a discussion of audits, reviews, or investigations performed and remedial actions taken; a record of evaluation of sensitive application systems and the status of application certification and other security-related programs; an account of participation in risk analyses on external facilities; agency facilities risk analysis summaries; and contingency plan(s). The security plan will follow the outline of topics as described below.

a Scope. A brief description of ADP operations, identifying ADP units covered by the plan.

b Definitions. Explanation of any items which might not be familiar for all readers.

c Overall Security Assessment. General discussion of agency policies and practices, addressing assignment of security responsibilities, personnel security clearance policies, audit reports, and training. This section should also contain an assessment of current security and planned activities for the next year.

d Appendices.

(1) List of sensitive application systems; give for each:

(a) Date of last system evaluation;

(b) Date of last system certification or recertification; and

(c) Date of next evaluation and recertification.

(2) Summary reports on all Types I and II risk analyses conducted or participated in.

(3) Agency contingency plan(s).

(4) Summary of microcomputer, terminal, and RJE area security review(s).

(5) Summary of training needs with action schedule.

(6) Other supporting documents (terminal security rules, local security procedures, etc.).

Facility Security Plan.

A facility security plan, required of Types I and II facilities, consists of a presentation of the current status of security in the facility; discussion of audits, reviews, or investigations performed and remedial actions taken; risk analysis documentation; a statement, of problems remaining and a list of scheduled corrective actions; and the contingency plan for the facility.

a Scope. A description of the site, giving location, configuration, and processing supported.

b Definition. Explanation of any terms which might not be familiar to all readers.

c Overall Security Assessment. General discussion of policies and practices, addressing assignment of security responsibilities, training, user interface, contingency planning, and other relevant issues. This section should include a discussion of audit reports, security problems, an assessment of current security, and plans for the next year.

d Appendices.

(1) Site plan and equipment schematic.

(2) Summary Risk Analysis Report.

(3) Facility contingency plan.

(4) Summary of training needs with action schedule.

(5) Other supporting documents (user handbooks, security procedures, etc).

Agency Type II facility plans need not be submitted to OIRM, for review.

Security plans should be considered a management tool. They should be candid and factual and should contain sufficient detail to give management a true picture of current security status in the facility or agency. Security plans are sensitive documents and must have minimal distribution. An adequate security plan is an important aid to internal auditors or investigators, however, and should be furnished on request.

10 SECURITY ASSESSMENT

A security assessment shall be conducted annually at each ADP processing site. The purpose of this review is to validate that safeguards remain adequate to prevent, detect, and recover from security failures.

There are three basic types of ADP facilities, ranging from large computer centers to simple data terminals. Type I and Type II facilities must perform risk analyses at intervals of 3 years or when hardware or systems software undergoes significant modification. Current risk analyses must be reviewed annually and updated as necessary. Type III facilities will perform security reviews annually.

Security review is a less formal process than risk analysis. It consists of an evaluation of physical security, operating procedures, and personnel practices. Generally, identified vulnerabilities can be countered by relatively simple and inexpensive measures. If potentially-serious security problems are identified, a risk analysis should be performed.

Use standard review checklists based on these standards and agency procedures.

Risk analysis is a formal, systematic approach to assessing vulnerability of ADP assets; identifying threats; quantifying the potential losses from threat realization; and developing countermeasures to reduce the amount of potential loss.

Countermeasures are selected on the basis of cost/benefit analysis.

The level of protection furnished ADP assets represents a prudent determination. It is based on the value and importance of the assets to be protected, a realistic assessment of threats, and the relative economy and effectiveness of alternate protection schemes.

Managers of ADP facilities should notify users of new protective measures installed or changes in procedures.

Appendix A contains a simplified method for performing risk analysis.

11 CONTINGENCY PLANS

Agencies shall develop contingency plans to meet emergencies and must assure that the plans cover all critical processing. Plans and plan implementation will be reviewed annually and updated as necessary and will be tested periodically, at intervals not to exceed one year.

Documents prepared for acquisition of ADP equipment and services must contain contingency requirements, if contingency plans require special features or services for that purpose.

Agencies are responsible for maintaining their application programs and data files current; identifying and establishing priority of critical jobs; and protecting data. Determine the criticality of jobs by evaluating the expected impact of processing degradation upon agency missions.

DCC Directors are responsible for locating, and executing agreements for use of alternate-site processing for DCC users. This action will be taken after agencies provide contingency requirements to the DCCs. Each DCC director will execute specific agreement(s) with an alternate site(s) and will notify agencies of these agreements. In case of serious interruption of service at a DCC, the Director will notify user management and agency security officers at the earliest possible time. Agencies will activate their contingency plans; DCCs will advise and assist. The transition to the DCC when the emergency has ended will be conducted by the DCC, based on a schedule coordinated with the agencies.

An effective contingency plan for emergency situations is probably the best insurance an ADP manager or user can have. The thorough planner will address all aspects of the following tasks which are pertinent to operations:

a Maintaining adequate materials at the backup or alternative site. These include current data, programs, run books, documentation, and support supplies;

b Handling the immediate emergency (fire-fighting, building evacuation, etc.);

c Maintaining liaison between facility management and users;

d Moving people, data, and support supplies to the previously-designated alternate site(s);

e Processing at the alternate site(s);

f Restoring the damaged facility; or relocating it; and

g Returning to the primary site in an orderly manner.

Users should give specific attention to any loss of processing capability which presents a serious problem to the agency. For example, a 12-hour delay in processing might be critical to one agency's operations, unimportant to another's.

Agencies must identify those applications which must be run immediately and/or continuously, those which can be delayed, and those which can be postponed indefinitely or done in another manner.

All DCCs furnish routine back-up services and off-site storage of critical material. User act evaluate the DCC backup schedules and request additional backup, beyond that routinely furnished, if needed. Off-site storage and schedules for maintenance of off-site files similarly require consultation with the DCC and execution of the require documents.

Users of agency or GOCO facilities or commercial computer services must also take the actions necessary to assure that backup and off-site storage are adequate. Assume, when developing the contingency plan, that the worst-case emergency would limit the users resources to materials stored off-site. These materials: data, documentation, programs, run books, and support supplies must be kept as complete and current at the backup or alternative site as good judgment dictates.

If processing is done at sites other than DCCS, specific agreement(s) between the agency and alternate processing site(s) must be executed by the agency. Minicomputer and microcomputer facilities which plan reciprocal backup should perform careful workload, compatibility, and telecommunications analyses. The combined workload a facility could carry must be defined.

Follow guidelines set forth in this document and in FIPS PUB 87, Guidelines for ADP Contingency Planning, in planning for continuity of vital operations in the event of emergency or disaster.

Contingency plans are a required element of both DCC and agency ADP

security plans. Advice on contingency planning can be obtained from the DCCs and ORIM.

12 APPLICATION CERTIFICATION AND RECERTIFICATION

The need for certification and recertification of the adequacy of security safeguards of sensitive computer applications is recognized by the Office of Management and Budget (OMB). A-71 requires Federal agencies to (a) certify the security of sensitive computer application systems after their initial development and (b) recertify operational sensitive applications at least every three years.

Section 17 discusses incorporation of controls in sensitive application systems, leading to initial certification.

USDA agencies and offices will conduct periodic audits or evaluations to certify and/or recertify the adequacy of security safeguards of each sensitive operational computer application system. The applications include those which process personal, proprietary, or other sensitive data, or which have a high potential for financial loss, such as automated decision-making applications.

Agencies will perform certification/recertification audits or evaluations, at time intervals determined by the agency. The scope of the effort should be commensurate with the sensitivity of information processed and the magnitude of loss or harm, that could result from improper operation. At a minimum, evaluations/ certifications will be conducted at least every three years.

Agencies will document all certification and recertification studies (e.g. evaluation plan, list of participants, threat and vulnerability assessment, list of internal controls and security provisions, investigation findings, evaluation report, certification statement) and maintain as part of the official documents of the agency.

NOTE: Sometimes the terms "certification" and "accreditation" are interchanged. For purposes of this document the term "certification" will be used.

Agency IRM Review Boards or similar bodies are responsible for system certifications and recertifications. The unit doing the certification should be independent of the user organization, especially the analysis/programming unit which is responsible for system development.

For additional guidance on certifying and recertifying application systems, refer to Appendix B.

There are basic requirements for assuring the integrity of even the least sensitive system. Even small, nonsensitive Programs, written for one-time or limited use, for example, can pose a threat to system stability. Such programs, which normally are not subjected to detailed analysis and formal development, will incorporate basic security features and will be teste(i before installation. These programs need not be certified, but should be entered in a perpetual log maintained by the office supervisor.

The designation of a system as nonsensitive holds for the life of the system, unless it is redesignated as sensitive or undergoes a significant modification which requires a change in status.

OMB Circular A-123. OMB Circular A-123 requires annual vulnerability assessment of the ADP portions of agency programs.

Certification of applications (which follows evaluation of internal controls, processing and user environments, and general management controls), should provide adequate basis for A-123 ADP vulnerability determination.

13 GENERAL SECURITY MANAGEMENT

In establishing an ADP facility, agencies should evaluate potential locations for vulnerability to natural disasters, fire, water leaks, external disruption, or other threats. Availability of alternate power, air-conditioning, and telecommunications are also important considerations.

Planners should address off-site storage requirements and develop contingency plans in conjunction with development of information systems.

Employee health and safety are sometimes overriding concerns in locating and operating ADP facilities. Safety requirements are not negotiable.

The goal of an agency security program is to provide a level of security, commensurate with their importance and value, to all ADP resources. If all standards cannot be met, alternative standards and procedures must be used.

Housekeeping.

a Proper care and maintenance of equipment protects the information and the equipment.

b Keep the work and storage areas neat and clean. Ban food and beverages from equipment and related support areas.

c Keep the equipment cleared of extraneous matter and unneeded documents.

d Personal computers, terminals, modems, magnetic storage media, and computing equipment and supplies are highly subject to theft and pilfering because of the increasingly widespread demand for these products in both the personal and business sectors. Control access to equipment. This will not prevent breaking and entering but will minimize opportunity for casual theft.

Workstations. Unattended operating equipment in open areas is vulnerable to unauthorized access and data and software compromise.

Close down and secure unattended equipment if access cannot be monitored.

Data Availability. An integral part of any information processing security system is to establish and implement backup (duplication) and recovery procedures. Store critical backup media in a room separate from routine storage areas.

All magnetic media are fragile and subject to physical damage for a variety of reasons. Incorporate the manufacturer's handling and storage instructions into the standard procedures of the site.

Accidents, operator error, equipment malfunctions, and theft are hazards to storage media. Make provision, in standard operating procedures, for handling and minimizing the adverse effects of these events.

Externally identify and properly file storage media. Minimum external identification: file name, date created, version, owner, information sensitivity, and retention time.

In order to give agencies considerable flexibility in meeting their security needs, the standards below are kept to a minimum.

Consequently, agencies should not assume that conformance to all the standards given here will meet all their system security needs.

Each agency will supplement these USDA standards, which apply to office environments as well as ADP facilities, with detailed security guidance for agency-specific terminal/microcomputer users.

For guidelines and additional material on the development of security measures, see the list of references in Section 20.

14 PHYSICAL SECURITY STANDARDS

Location.

All installations: Locate RDP sites out of highly visible, heavily-trafficked areas. Choose locations to take advantage of existing physical security.

Types I and II: Locate media libraries apart from ADP areas.

Provide off-site storage for critical data, software, and documentation.

Construction.

Type III: No construction requirements.

Types I and II: Fire-retardant construction is mandatory for Type I facilities and is recommended for Type II. Cover transparent windows with opaque material. Construction will conform to RP-1 standards.

Outside Equipment.

Type III: No requirements.

Types I and II: Assess the security of exposed electrical power, gas, water, and communications lines located outside the facilities. Facilities must coordinate with the appropriate utility company and/or GSA to assure adequate protection of these vital supports. Type I facilities must screen external air-conditioning and ventilating equipment with steel mesh or other protection which will prevent access by unauthorized persons.

Power.

Type III: Follow manufacturers' recommendations. In areas with intermittent power problems, consider using line-smoothing devices.

Types I and II: Eased on analysis of critical power requirements, provide for adequate power to guard against fluctuations and failures. Provide separate circuits to critical equipment; safeguards on switch gear (to prevent unauthorized manipulation) and warning instructions to maintenance personnel; emergency power-off control switches near emergency exits; automatic emergency exit lights in all staffed areas (fluorescent lights with

ballast recommended); and emergency power stand-by and power flow-smoothing devices for facilities processing critical applications.

Equipment.

All installations: All electronic data processing units and systems or similar electronic equipment shall conform to Underwriter Laboratory standards and be installed in conformance with RP-1 standards.

Fire Protection.

Type III: Furnish fire extinguishes of correct type; train employees in their use; practice good housekeeping.

Type II: Furnish all the above plus fire extinguishes in computer room; heat and smoke sensors; posted evacuation routes; periodic fire drills; labels on fire exit doors. Recommended features: Emergency cut-off switches; panic bars on exit doors; emergency lights.

Type I: Furnish all the above, plus installed central fire suppression system (Halon 1301 recommended); emergency cut-off switches; at least two exit doors; panic bars on exit doors; emergency lights; audible alarms; first-aid training. Recommended features: automatic notification of fire department.

Guidance covering fire protection is covered in RP-1.

Documentation and assistance are available from OIRM.

For guidance in fire extinguisher selection and maintenance, see NFPA No. 10, Portable Fire Extinguishes.

Access Control.

All installations: Limit entrances to the number essential for efficient operations. To the extent possible, shield ADP activities from casual observation. Escort visitors.

Type III: These facilities usually require no access controls except adequate locks on doors and windows and management of access to equipment and data. Lock all facilities when not in use, and store data in locked rooms or cabinets.

Types I and II: These facilities require formal access controls: key cards, magnetic card locks, remote controlled locks, security personnel, and closed-circuit television, used singly or in combination, to assure that only authorized personnel enter the facility.

If a facility employs more than 20 people, the facility should use badges for employee identification.

15 SOFTWARE AND DATA SECURITY STANDARDS

The standards in this section apply to the protection of operating systems, data communications routines, software security routines, application systems, and all other software and data files. They include controls for screening out unauthorized users.

ADP Data Control.

All installations:

a Establish controls to prevent unauthorized persons from reading from and, (or writing into programs and data files. Disseminate telephone numbers and remote access procedures, on a need-to-know basis. Protect systems access keys (logon IDs. passwords, etc.). Assign systems access keys to individuals only. Make periodic changes in access keys, and immediate change if a compromise has occurred or is thought to have occurred.

b Protect sensitive data by use of file level passwords, read/write locks, and/or encryption.

c Develop recovery procedures for data bases.

d Establish controls to monitor the movement of portable equipment. Arrangements for taking equipment off-site must be made with the security officer or the deputy responsible for site security.

e Protect user manuals containing explicit information, such as mnemonic codes for interpreting data.

f Establish controls to record and monitor the movement of sensitive information, documents, cards, tapes, and disk files within the ADP facility and data communications network.

ADP Operations.

All installations:

a Maintain logs to record the location of files and equipment which have been removed from the ADP facility.

b Store duplicate copies of critical data files, systems software, production programs, run instructions, and complete current documentation at a separate storage facility, remote from the primary site.

c Destroy all output showing any keys for access to USDA or non-USDA computer systems or handle as if the output were a file of sensitive data. If such output is not identifiable to a user, destroy it. This requirement applies to remote terminal output, as well as output generated in an ADP center.

d Protect all sensitive computer output.

Types I and II:

a Develop a program to train operators for various operating assignments and to provide adequate backup personnel when required.

b Make operations manuals covering all aspects of ADP operations available. Manuals will specify emergency procedures.

c Maintain operating logs, console logs, and logs for all off-line equipment. Console logs will explain any problems or interruptions of normal processing and list all affected programs, if known.

d For each major data base there will be available written procedures covering all aspects of restart and recovery. Operators will record all recovery actions taken on such data bases. When restart and recovery procedure is used, checkpoint memory dumps and related files will be treated as sensitive data and retained until clearance for their disposition is received from ADP control or other appropriate personnel. When clearance is received, they will be scratched.

e Under no circumstances allow a user to obtain a system memory dump; i.e., a dump of other than the user's assigned memory area.

f Establish controls to prevent unauthorized access to or loss of magnetic tapes or fixed or floppy disks.

g Maintain a tape and disk library system. Include a record of age, usage, cleaning, owner, and level of data security.

h Mark each tape with a permanent serial number.

i Identify all tape and portable disk files with external labels that conform to ADP facility conventions. The

label will not indicate the contents of the file(s). The label will indicate the presence of sensitive information.

j Furnish the means for sanitizing tape and disk devices containing sensitive data. The means include software for overwriting or equipment for degaussing.

k Provide secure bins for computer output. Computer center ADP security officers will furnish lock combinations or keys to agency ADP security officers, who are responsible for their control and for reporting to the center ADP security officer any need for lock changes.

16 INTERNAL CONTROLS STANDARDS

This section discusses controls which apply to the authorized user, once this user has gained access to the computer system. These controls must prevent inadvertent or intended harm to the user, other users, or this computer system.

Type III: Use controls available. Evaluate security features in operating systems and systems software packages and assure that security is adequate - before acquisition of WP or microcomputer equipment and software.

Types I and II: The operating systems and other systems software requirements which follow are mandatory for Types I and II and desirable for Type III. Provide controls which:

a Prevent a user program from executing privileged instructions;

b Isolate one user's programs and data areas from areas of other users and systems software;

c Assure error detection, memory bounds, parity, and hardware register checking on memory access;

d Maintain hardware and software error logs; and

e Maintain accounting and access logs sufficient to permit reconstruction of events in case of unauthorized data or program access or use, illegal use of privileged instructions or functions, unexplained program aborts, or questionable processing results.

Operating Systems.

The operating system must perform certain functions forbidden to users; it will contain controls which provide the user with all authorized access but no more. As a minimum, the operating system must control:

a All transfer of material between memory and on-line storage devices; between the central computer facility equipment and any remote device; or between on-line storage devices;

b All operations associated with allocating ADP systems resources (e.g., memory, peripheral devices, etc.), memory protection, system interrupt, and shifting between privileged and non-privileged protection modes;

c Access to programs and utilities which are authorized to perform the various categories of maintenance (e.g., as operations which effect authorized additions, deletions, or changes to data) on the operating system, including any of its elements and files. Such controls shall insure that access is limited to personnel authorized to perform particular categories of maintenance; and

d All other programs (user programs) so that access to material is made via an access control and identification system which associates the user with the material being accessed.

Other Systems Software.

Systems software will have built-in protection features to prevent unauthorized access to systems and files and will have the capability to record such accesses.

Systems software must:

a Monitor and record attempts by unauthorized users to access computer systems and files;

b Verify that the terminal and/or the terminal operator is approved for access to the programs and/or data requested and for the intended use of either the programs or data. Record unauthorized attempts; and

c Either obliterate or suppress the display of all keys for access to computer systems, programs, or data.

In addition, Types I and II operations must acquire or develop a software test package designed to test systems security rigorously; test temporary or permanent modifications of the operating system to assure that the security features of the ADP system are effective. Test the system at irregular intervals.

17 APPLICATION SYSTEM DEVELOPMENT

When application systems are being developed, converted, or modified, systems developers have a unique opportunity to address security. Retrofitting security into an operational system is difficult, expensive, and sometimes impossible. So developers

should seize this chance to achieve maximum results with minimum effort.

Developers should first ask these questions of agency management:

How critical is this systems to agency operations?

What would be the impact if this system couldn't run?

How long could processing be delayed without serious impact?

How sensitive is the data?

The answers to these questions will guide developers in determining how much security and what specific controls are needed. At this time, before the development work is begun, it should be possible to define the operating environment for the system, backup and contingency requirements, and controls which must be incorporated in application programs.

There are several guidelines which developers may find helpful.

FIPS PUBS 38 and 64 contain documentation requirements. FIPS PUB 73 provides guidance in building controls in application systems, and FIPS PUB 101 addresses lifecycle validation of computer software.

Appendix B discusses the evaluation and certification of sensitive application systems. OIRM recommends that any system, whether sensitive or not, be provided a reasonably secure operating environment.

The following standards apply to significant modifications or conversions of existing application systems, as well as to new systems. The standards are not dependent on facility type.

a Application Systems Controls.

(1) Build protective features in sensitive application programs to prevent unauthorized access to data files through the programs. These controls may include passwords, additional user validation, and procedural requirements. Unsuccessful attempts to access the programs or data must result in control being passed to systems software security routines for logging.

(2) Develop checkpoint and recovery routines and furnish documentation to computer operations.

(3) Do not program in assembly language unless it is necessary. A waiver from OIRM, is required for assembly language use.

(4) Design and write systems and applications to provide:

Comparison of input controls with data;

Generation of control totals during processing;

Correct selection of all files;
Validation of data;

Maintenance and adjustment of all files and totals; and

Protection of records associated with automated decision-making applications.

(5) Assure the development of adequate systems, program, operational, and user documentation. Protect development and maintenance of sensitive programs or data by restricting dissemination of information to those who need to know, locking up all material when not in use, and by giving work assignments only to those persons who have appropriate clearances.

(6) Assess and approve the adequacy of security safeguards in the initiation phase and monitor their incorporation at all stages of the development, conversion, or modification of a major system.

(7) Before any application is placed in production, test the new system, including file maintenance and run recovery, and run in parallel with the old system. Do not discontinue the old system until results are completely acceptable.

(8) Certify the adequacy of the application system's security, if the system is sensitive.

b Operational Security.

Once a system is placed in production the following procedures must be followed:

(1) Issue instructions to disallow by-passing beginning label checks for critical files.

(2) Establish procedures to monitor the periodic matching of production programs and critical software with current version programs which have been secured at a separate storage facility.

(3) Maintain a list of personnel authorized to make changes to operational programs, and make the list available to the facility manager.

(4) When tapes or disk files containing sensitive data are to be released, sanitize the storage media by degaussing or

overwriting the media in such a manner as to destroy the data.

(5) Perform regular evaluations and written certification/recertification of all systems and control functions dealing with financial, personnel, contracts, proprietary information, and other computer software handling sensitive data.

18 COMMUNICATIONS SECURITY STANDARDS

Telecommunications operations are vulnerable to errors. There are inherent possibilities for misrouting, garbling, or losing data processed in the communications environment. Protect, to the maximum extent possible, the security and integrity of all data transmitted. The following guidelines address this problem in a general way; apply more specific measures if security can be improved by their use.

All facilities: Use safeguards available, realizing that use of telecommunications increases vulnerability. Consider encrypting sensitive data.

If encryption/decryption techniques are employed, the following standards apply: Code books required for encryption and decryption will be locked up when not in use and protected from unauthorized use or possession at all times. Afford encryption keys maximum protection.

Encryption/decryption software is authorized only by a waiver; if used, protect it from unauthorized use or possession at all times.

Types I and II.

a Secure behind locked doors all crossbar switches, patch panels, or other such control points for communications lines, with access granted only to authorized personnel.

b If the system permits, use a resident program to interrogate and record the IDs of terminals logged on for extended periods of inactivity. Facility managers should consider automatic disconnection of terminals inactive for a specified period.

c Develop written restart procedures for use in the event of service interruptions and for restarting one line or the entire system; include procedures for immediate or delayed restart.

d Provide a software routine to log all transmission errors and retransmissions. Analyze the data for meaningful patterns. Report irregular conditions to the security

officer.

19 PERSONNEL SECURITY STANDARDS

The standards set forth in this section apply to ADP personnel selection and employment, security training, and personnel briefing and debriefing.

Federal regulations require clearance of all persons involved in the development, management, and operation of sensitive ADP systems and facilities. These requirements apply equally to Federal employees, contractors for the Federal Government, and nonfederal employees such as State and local government workers having access to sensitive Federal data. Appropriate agency authority will determine requisite clearance levels for positions in all cases.

Responsibility for the personnel clearance program rests with the Department Security Officer, Office of Personnel. Agencies should consult with the Office of Personnel to establish clearance requirements and obtain clearances.

Employee Briefing and Debriefing.

Brief new employees on the USDA security program and agency practices. Upon termination of employment, require personnel to turn in to the appropriate security officer all identification cards, keys, programs, data files, etc., in their possession. They will be interviewed by the appropriate security officer or management official, who will stress to such personnel their continuing responsibility to maintain the privacy and confidentiality of USDA data. Security clearances will be terminated, if not otherwise required. The agency will inform all appropriate employees of the termination and insure that data files-and programs used or maintained by the employee have been turned over to someone else. When supervisory personnel conduct a debriefing in the absence of the security officer, they must immediately notify the security officer of the employee's departure. Change all passwords or other means of accessing files or using computer resources known by the individual within 2 working days.

Contractor Personnel. Brief and debrief contractor personnel in a similar manner as employees.

Security Training. Agencies will furnish annual security training to all employees with ADP responsibilities. At a minimum, training will consist of a reminder of responsibilities.

Personnel Actions. Agencies should impose sanctions for willful disregard of security, violation of the Department's Employee

Responsibilities and Conduct regulations, or gross carelessness in handling equipment or information. Sanctions can range from a formal letter of reprimand to dismissal from Federal service.

Agencies should develop guidance for employees on proper and ethical behavior and define sanctions which may be invoked for violations.

20 REFERENCES

The Privacy Act of 1974 (PL 93-579, 5 U.S.C. 552a)

OMB Privacy Act Implementation Guidelines

OMB Privacy Act Implementation Supplemental Guidelines

OMB Transmittal Memorandum No. 1, Circular A-71.

FPM 732 Federal Personnel Manual

FIRMR 201-35.3, Security of Federal ADP and Telecommunication Systems (formerly FPMR 101-35.3)

FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management

FIPS PUB 38, Guidelines for Documentation of Computer Programs and Automated Data Systems

FIPS PUB 39, Glossary for Computer Systems Security

FIPS PUB 41, Computer Security Guidelines for Implementing of the Privacy Act of 1974

FIPS PUB 46, Data Encryption Standard

FIPS PUS 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase

FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis

FIPS PUB 73, Guidelines for Security of Computer Applications

FIPS PUB 83, Guideline on User Authentication Techniques for Computer Network Access Control

FIPS PUB 87, Guidelines for ADP Contingency Planning

FIPS PUB 101, Guideline for Lifecycle Validation, Verification, and Testing of Computer Software

FIPS PUB 102, Guideline for Computer Security Certification

and Accreditation

National Fire Protection Association, Protection of Electronic Computer Data Processing Equipment, NFPA No. 75

RP-1, Standard Practice for the Fire Protection of Essential Electronic Equipment Operations

Appendix I to USDA Employee Handbook, Employee Responsibilities and Conduct

USDA Records Security Regulations - Regulations for Classification, Declassification, and Safeguarding Classified Information

DR 3100-1, Telecommunications

DR 5020-2, Security and Privacy Act Requirements for ADP and WP Acquisitions

P&O Handbook No. 3, USDA Vital Operating Records

P&O Handbook No. 4, Procedures for Handling Material Designated "FOR OFFICIAL USE ONLY"

APPENDIX A

RISK ANALYSIS PROCEDURES

1 BACKGROUND

USDA regulations require inclusion of a risk analysis summary as part of the annual ADP security plan all user agencies, all major ADP facilities and some smaller facilities must prepare or update annually. Federal regulations require inclusion of a current risk analysis summary in all RFPs for facilities, equipment or services, when processing of systems of records covered by the Privacy Act is involved.

USDA regulations also require the development of contingency plans; these call for maintenance of off-site storage of tapes, disks, documentation, and other items required to transfer critical processing to an alternate site when the ADP facility is rendered inoperable. For contingency plans to be viable, this off-site material must be current and complete. A facility risk analysis, which evaluates the completeness and condition of present backup, is prerequisite to contingency plan development.

Risk analysis is an assessment of the vulnerability of a specific facility or organization and deals with a unique set of assets and conditions. "Assets", in the broad sense, includes data, software, equipment, buildings and furnishings, and the availability of the ADP facility's services. Physical surroundings, vulnerability to natural threats or subversion, effectiveness of protective measures in use, sensitivity of data processed, etc., must be considered.

For a risk analysis to fulfill its purpose, it must represent a considered judgment of threats to assets at a particular place at a specific time, with known and documented existing conditions. For example, a risk analysis study performed on an ADP facility when there was no off-site storage maintained and minimal processing took place would have little relevance after the facility has acquired off-site storage facilities and increased its work load.

There are many definitions of risk analysis, and a number of procedures for performing the analysis have been developed. The method detailed here is simplified but adequate. Much of the process requires use of subjective decisions and, sometimes, pure guesses. Experience shows, however, that if carefully done this process produces valid results.

In essence, a risk analysis is the development of answers to the following questions:

a How good is security now?

b How good does it need to be?

c What are the threats to assets in the ADP environment?

d What is the likelihood each of these threats will be realized?

e What would be the annual loss expectancy (ALE) if each threat is realized?

f What measures can be taken to minimize the chances of threat realization?

g What would each countermeasure cost (annualized amount)?

h What is the anticipated ALE reduction of each special threat for each countermeasure considered?

i What is the resultant cost/benefit value (in dollars) associated with each countermeasure? (Aggregation of all ALE reductions expected to result from use of the countermeasure vs., its annualized cost.)

2 SECURITY THREATS

Security threats can be of many types and of varying degrees of severity. They can produce a broad range of untoward results, if realized. For example, one real and constant threat is fire. It can be a holocaust that wipes out the facility and all service areas, a fire in the CPU, a smoldering chemical fire which produces corrosive materials, etc. Depending on the extent and type of damage and the time required for recovery, the facility could be down for hours - or weeks - or months.

We have neither the time nor resources to attempt to assess all threats nor to consider all permutations any one threat might pose.

Rather, in the interest of simplifying the task and cutting it down to a size we can cope with, we have arbitrarily defined two types of threats, major and minor, with the full knowledge that some "in between" threats will be excluded from consideration. Still, a risk analysis based upon only these two types of threats will produce a useful product.

They are defined:

a Major Threat. An event which threatens all the facility's assets. It can be an event of catastrophic proportions which destroys the ADP facility or renders it inoperable. Examples: fire, flood, earthquake, tornado, bombing, riot. Assumption is made that all attendant areas of the facility, such as the tape/disk library, are destroyed. Relocation to an alternate processing site is required. Only the material stored off-site is available for use. Or a major threat can be a plumbing leak which damages assets and delays processing, but does not destroy the facility.

b Minor Threat. This category includes all the deliberate or accidental failures, errors, and mishaps encountered daily. While each occurrence may result in relatively short processing delay or minor distortion or loss of data, the cumulative cost of many occurrences can be significant. Examples: CPU failure, wrong tape or pack mounted, listings lost, air conditioning failure.

It is necessary to define and evaluate threats according to the kind of adverse effects the threats pose. For example, the statement that fire potentially will cause a loss of $10,000 is incomplete. It is much more meaningful to state that fire will result in $5,000 loss from data destruction; $3,000 loss from delay in processing; and $2,000 loss from damage to ADP equipment. To devise countermeasures to threats, thereby improving Security (the purpose of the risk analysis), not only must we identify specific threats; we must also define the nature and scope of the potential harm. Use of the four categories listed below facilitates meaningful identification of the types of exposure each specific threat poses.

Security Exposure	Possible Results of Security Failure
Data Integrity	Destruction or unauthorized modification of data, unintentional or deliberate.
Data Confidentiality	Unauthorized disclosure of sensitive data.
Operational Reliability	Processing that is undependable, inadequate, delayed, or unavailable. (Processing should be accurate, dependable, and timely.)
Asset Integrity	Destruction or physical damage to buildings and equipment and supporting functions.

In general, the first three categories represent threats to data and processing. Asset integrity can most often be related to physical assets: equipment, supplies, furniture, storage media, etc.

The following list of threats is suggested for consideration. It is not intended to be all-inclusive. Conversely, many of the threats listed will be of little or no concern in specific situations.

External threats	Fire, flood, tornado, hurricane, earthquake, riot, bombing, water leakage on equipment
Environmental threats	Power or air-conditioning failure

Hardware error	CPU failure, memory fault, lock-out
	Peripheral device failure: disk, tape, etc.
	Device data transmission failure &r error
Software error	Operating system, sort, compiler, DBMS, etc.
Operations error	Mounting wrong version of system software, mounting wrong user data: disk, tape
	Accident during change of system software
	Accident during application program test or implementation
	Accidental destruction or modification of data by operations personnel
	Accidental disclosure of sensitive data
	Loss or misplacement of listings
	Misrouting of messages
	Misplacement of user data or program files
Subversive actions	Theft, arson, sabotage, "Slow down" tactics
	Unauthorized data, program, or systems software modification
	Unauthorized access to sensitive data

3 COSTS

It is necessary to establish ground rules before attempting to develop costs expected to be incurred because of security inadequacies. For instance, whether the facility is operating on a profit or non-profit basis has direct bearing on costing.

Decisions must be made on how to handle personnel salaries, rental vs. owned equipment, etc. These determinations must be made on an individual basis for each facility and its users and the details included in the risk analysis report.

When assigning costs to the various threats, it is necessary to consider carefully all peripheral expenses. Transportation of personnel and material, per diem costs, purchase of equipment, contractor support, replacement of storage media and paper stock: all are valid considerations.

For users, most of the costs will be associated with reconstructing data and rerunning jobs and with penalties or delays caused by loss, modification, or compromise of data. Loss of processing time also might result in monetary loss. And cost of moving personnel and materials to an alternate processing site must be included in assessing costs of recovery from a disaster.

The team or individual developing costs for facility assets must include costs to restore all equipment, buildings, etc., to operational condition, as well as costs associated with recovery of systems software and facility data. It is a large order.

4 USDA RISK ANALYSIS CONCEPT

To measure risks effectively, it is necessary to evaluate all functions which interact through common services, extending beyond organizational lines. Thus, all users of an ADP facility participate in the analysis of that facility. The risk analysis should be under the direction of the facility manager.

Procedures outlined here are intended primarily for use in assessing risk to a large Departmental Computer Center or other major ADP installation. However, with suitable modification the same method can be applied to risk analyses on smaller installations or agency ADP operations.

Essentially, the risk analysis consists of two parts, user tasks and facility tasks.

User Tasks:

a Identify sensitive and critical files and processes and give instructions for their protection.

b Develop total user costs to recover from realization of a major threat. (Threats are discussed in Section 2.)

c Develop ALE's to user files and processes from minor threats.

Facility Tasks:

a Evaluate present security.

b Identify major and minor threats.

c Develop costs to replace facility assets (including facility data) and recover from each major threat occurrence.

d Develop costs incurred from minor threat occurrences.

e Estimate the annual occurrence rate of realization of each major threat.

f Derive ALE's both for major and minor threats, incorporating data developed by users.

g Develop lists of remedial measures with potential to reduce losses. Perform cost/benefit analysis on these countermeasures. Submit list to facility management for approval.

h Prepare report. Include list of recommended countermeasures and all exhibits. Format for the report is included in this document.

As is evident, the larger number of tasks must be done by facility personnel. It should not be inferred, however, that theirs is the more important job. It can be argued that the only reason for the existence of an ADP facility lies in its function of service to users. User contribution is vital to the success of the undertaking.

We recommend that personnel familiar with broad agency programs, as well as computer programs and data, be assigned the task of assessing sensitivity and criticality of user data. If the number and size of systems render this a sizeable task, a team approach might be considered. We also recommend that agency management review all analysis results for reasonableness and completeness.

(Detailed instruction to users is found in Section 5.)

We further strongly recommend use of a team for the facility tasks.

On the premise that those best-equipped to deal with specific issues should do so, we suggest assignment of experts to the various sub-tasks. For example, auditors and safety experts can contribute materially, if requested. Seek out and use the diverse talents that can contribute to a successful risk analysis.

Risk analysis documentation may be prepared in any format that is meaningful and easy to use. OIRM, will provide suggested formats or assist in developing agency-specific formats, if requested.

5 USER TASKS

a Identify sensitive and critical files and processes.

(1) Identify to the ADP facility those files which are sensitive (as defined in Section 4, ADP Security Manual) or for which the user, for any reason, desires special handling, backup, or off-site storage. For example, a data file may be non-sensitive by any definition, but its cost of reconstruction may be prohibitive. In such a case, the user should carefully consider back-up and off-site storage needs.

(2) Critical files are those whose loss, unauthorized modification, or lack of availability would seriously affect the user's processing. Critical processes are those which, if unduly delayed or denied, would result in serious detriment to agency program operations. Critical files and processes should be considered sensitive.

(3) For each sensitive/critical file or system, give agency name; the ADP facility used for processing; the system and/or programs using sensitive files or the names of critical processes; and the current date.

Give common file or process name.

For file sensitivity indicate: "S" (Sensitive) or "N" (Non-sensitive).

For process criticality: Give requirements, such as time, accuracy, etc.

Specify mode of file transmission: mail, telecommunications, messenger, etc.

If the minimum standard for ADP facility security is not adequate to protect files or processes, state what protection is required.

Users should know or obtain a statement of the minimum security level maintained by their host facility. For DCCs the minimum standard is:

Security Exposure Category	Protection
DATA CONFIDENTIALITY	Protection adequate for the Privacy Act of 1974, including such items as logon identification, file level password protection, personnel clearances, administrative and procedural practices, and physical security.
OPERATIONAL RELIABILITY	Processing capability

	available to users 95 percent of scheduled time.
ASSET INTEGRITY	Weekly backup dumps of operating system and permanent on-line disk packs and backup as required for paper supplies (forms, checks, etc.).

b Develop total user costs for major threat recovery.

(1) This step is of vital importance. User costs to recover from serious disruption or loss of computing capability are crucial to the risk analysis study. As stated in Section 2, identification of threat categories associated with costs to recover furnishes guidance in selection of additional facility safeguards.

(2) For each major system develop costs to reconstruct data, transfer operations to new site, etc., in the event of disaster, using a data risk analysis worksheet and identifying the threats as "major". It is not necessary to identify specific threats unless there are differing loss expectancies!s associated with specific threats. For example, cost to recover from a major fire likely would be the same as the cost to recover from a destructive wind-storm. Consider present off-site backup in making these assessments. Do not include a cost in the Asset Integrity category; loss of physical items is included in the facility's risk analysis. The reason for this is that physical assets such as tapes, disks, etc., are usually in the custody of the ADP facility, and it is facility security we are evaluating.

c Estimate annual minor threat costs.

(1) Experience has shown that minor threat ALEs far exceed major threat ALES. For this reason, users should carefully estimate the total costs each system could be expected to incur because "something went wrong at the center." Users need not identify the specific associated threats; often they don't know the cause of problems. Rather, they should attribute anticipated costs to operational reliability, data integrity, etc. (See Section 2).

(2) Develop ALEs associated with minor threats, considering costs to reconstruct data and re-run jobs. Give a total value, in each appropriate security exposure category. Use data risk analysis worksheets to record the ALEs; identify types of threats evaluated as "minor." Remember that the only losses to be considered are those which occur while data is in the custody of the facility or is being processed. Do not include costs for which the user is responsible. No loss expectancy in the Asset Integrity

category is required. The best approach to this task is to use recent experience as a basis for protecting future losses.

d Review results.

(1) OIRM suggests that user management review the sensitivity assessment and data risk analysis results for reasonableness and completeness.

(2) Since performing a risk analysis entails a careful inspection of user files and processes, it seems an ideal time for users to go a step further and assess the quality, completeness, and currency of the backup material, including documentation, stored off-site. It is also a good time to weed out out-dated or unnecessary processing and files.

(3) Forward completed documentation to the risk analysis study leader. Retain all work papers.

6 FACILITY TEAM TASKS

a Organize team; develop action plan with milestones for significant events; assign specific duties.

b Meet with user representatives, both management and technical personnel, if possible, and explain the risk analysis procedure, identifying and describing user tasks.

c Evaluate present facility security; flag areas of weak security. Give immediate attention to potentially- serious deficiencies.

d Identify threats, using results of the evaluation as focus of attention. Categorize threats "major" and "minor." (A list of threats for consideration is in Section 2.) Note: the team may want to consider more than one degree of severity of a single threat, i.e., a catastrophic fire, one that destroys 10% of assets, etc.

e Estimate rates of occurrences of realization of these major threats.

f For major threats: develop costs for all threats to facility assets, data, and capabilities. Assign costs to the four exposure categories.

Remember that these figures represent costs to the facility, not users. This is also true of the minor threat costs discussed below.

g For minor threats: Use operational records, equipment failure reports, history of recent security breaches and problems, and informed judgement to estimate an annual cost for each minor threat. As for major threat costs, distribute over the

exposure categories.

h Develop ALEs for major threats, using facility- and user-generated costs and facility-generated occurrence rates. Enter values for "Cost per Occurrence" and facility ALEs for the four types of exposure on a risk analysis worksheet. Add user ALEs and total.

i Calculate facility minor threat ALEs and list on risk analysis worksheet. Apportion user ALEs among minor threats the facility team has identified. Add user values to the worksheet.

This process may be confusing. The intent is to assign a proper portion of the expected losses to both the facility and users to specific threats and threat categories. An example may illustrate.

The threat is operator error. The facility team has estimated that operator errors will cost the facility as follows:

DI 10,000, DC 1,000; OR 50,000; AI 5,000.

User A has furnished estimates that all minor threats combined will cost annually:

DI 100,000; DC 30,000; OR 500,000; AI 0.

The facility team has decided that 10% of user minor threat losses can be attributed to operator error. Applying this percentage to user data, user A's ALE for operator error is:

DI 10,000; DC 3,000; OR 50,000; AI 0.

So, if the facility had only one user, total operator error ALE would be the sum of facility and user losses:

DI 20,000; DC 4,000; OR 100,000; AI 5,000.

j Sum all values, for both major and minor threats, to obtain total ALEs in the four security categories. Sum all values for each threat. Add these values to obtain the one value representing loss expectancy from all threats, major and minor. Enter values on worksheet. Prepare risk analysis summary.

k At this point the risk analysis study is technically complete.

Now the team must use the study results to determine where and how security can best be improved. The team should consider various combinations of countermeasures which protect areas of greatest potential loss. Many times one countermeasure will address several problems. For example, installing a guard could be expected to reduce vulnerability to unauthorized access, theft, arson, bombing, fire, and water damage, particularly in an unattended facility. Guards, however, are expensive. The team must weigh the anticipated savings against

the costs of remedial measures, then recommend a list of those considered most cost-effective.

l List countermeasures with annualized costs. Develop relationships between these countermeasures and threats they are intended to counter. Give expected savings (reduction in potential loss) for each countermeasure.

m Review with facility management the risk analysis worksheets and summary and the cost/benefit analysis.

n After facility management has reviewed all work and selected those countermeasures which it recommends for implementation, prepare the Risk Analysis Summary Report, including Exhibits, in the suggested format.

o Submit the Report for facility management approval and action.

Retain all work papers.

7 RISK ANALYSIS SUMMARY REPORT FORMAT

TABLE OF CONTENTS

time and manpower considerations.

IV RISK ANALYSIS

A Reference to published guidelines used.

B Discussion of major threats considered, giving brief justification for their consideration.

C Risk analysis worksheets and summary, giving details to the level necessary for reader understanding. (Retain all background material).

V RECOMMENDATIONS

Prioritized list of recommended countermeasures with derived cost benefits.

VI SUMMARY

Discussion of difficulties encountered; techniques used (composition of the risk analysis team, for example); resources used (time, manpower); and any other details which might be helpful to the organization, or others, in performing studies in the future.

EXHIBIT 1 TABLE SHOWING RELATIONSHIP OF EXISTING SAFEGUARDS TO THREATS

EXHIBIT 2 TABLE SHOWING RELATIONSHIP OF SAFEGUARDS BEING IMPLEMENTED TO THREATS

EXHIBIT 3 DISCUSSION OF RECOMMENDED SAFEGUARDS

EXHIBIT 4 ANY ADDITIONAL DOCUMENTS PERTINENT TO THE STUDY

8 INSTRUCTIONS FOR PREPARING EXHIBITS

None of the exhibits is intended to be exhaustive; they are merely a capsulation of significant items. They will enable reviewing authorities, who may be totally unfamiliar with a facility's physical layout and operation, to see at a glance the overall security position now (Exhibit 1), in the near future (Exhibit 2), and, if recommended countermeasures are installed, in the more distant future (Exhibit 3).

Exhibit 1: List, in tabular form, major safeguards in effect vs. threats they counter or whose adverse effects they lessen.

Exhibit 2: List, in tabular form, safeguards presently being installed or for which money has been budgeted.

Exhibit 3: List safeguards recommended for adoption.

Include a brief discussion of reasons for

recommendation, together with a summary cost/benefit analysis, for each item.

These Exhibits should be prepared after final management review and adoption of recommendations.

APPENDIX B

CERTIFICATION/RECERTIFICATION OF APPLICATION SYSTEMS

1 CERTIFICATION METHODOLOGIES

There are many methods that can be used in implementing a certification process within an agency. No one method, however, is best suited for all situations; some methods require adaptation for the specific needs of the agency and application.

FIPS PUB 102, Guidelines for Computer Security Certification and Accreditation, outlines a detailed process. The procedure described here is an abbreviated ont which may meet agency needs individual circumstances will ultimately dictate the method used for each evaluation and certification.

A-71 requires that an evaluation be conducted by a group independent of the application developers. Ideally, this degree of independence helps to ensure objectivity and should be sought.

Nevertheless, often a fully-independent evaluation is not feasible or economical. In these cases, it may be reasonable and necessary to accept the technical assistance and judgement of application developers and users. The benefits of independence must be balanced against increased cost and resource limitations.

When considerations of money, time, and personnel restrict or discourage a fully-independent evaluation, an in-house approach utilizing available personnel must be developed.

Section 3 of this appendix contains an outline of the major tasks to be addressed when conducting an in-house certification effort.

Sections 4 through 8 outline the benefits of this process, the major functions performed by the various certification teams, and the review team report contents. The in-house approach outline is provided for consideration, adaptation, and possible use in developing an agency certification program.

2 DISCUSSION OF MAJOR CERTIFICATION TERMS

a Certification. Security certification is the signing of an official statement that approves the security of a computer application. Certification is based upon a security evaluation

process that assesses the extent to which an application satisfies Federal, Departmental, agency, and user computer security requirements.

b Certification Statement. The certification statement is an official document that records an explicit acceptance of responsibility for the security of a computer application system.

c Certification Boundaries. To present a complete picture, the certification boundaries of an application must be drawn to include all relevant factors of an application's environment, including the administrative, physical, and technical areas.

d Recertification. Certification is not permanent. As an application or its security environment changes, recertification is needed to verify that security protection remains acceptable. Any change or new finding that invalidates or calls into question a certification decision necessitates recertification. Situations that give rise to this include the following: changes to the application, changes in requirements, passage of time, occurrence of a significant violation, and audit or evaluation findings.

e Sensitive Application. A computer application which requires a degree of protection because it processes sensitive data or because of the magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application.

f The Certifying Official(s) is responsible for evaluating the certification evidence, deciding on the acceptability of application security safeguards, approving corrective actions, signing the Certification Statement, and ensuring that corrective actions are accomplished. Ideally, the individual appointed should be at a level such that he or she has sufficient authority over the entire application to allocate resources both to achieve acceptable security and to resolve any security deficiencies identified during the certification review.

g Management and General Controls are those controls that are part of the total environment in which all applications are processed. These controls comprise (1) the plan of organization and operation of the activity, (2) the procedures for documenting, reviewing, testing, and approving systems or programs and changes thereto, (3) use of controls built into the equipment and software by the manufacturer, (4) controls over access to equipment and data files, and (5) other data and procedure controls affecting overall ADP operations. Weakness in these controls can have an adverse impact on operational security.

h Application Controls are controls associated with a specific application. Their function is to provide reasonable assurance that the recording, processing, and reporting of data are properly performed. There is considerable choice in the

particular procedures and techniques which may be used. Application controls are often functionally classified as data origination controls, data input controls, data processing controls, and data output controls.

3 OUTLINE OF AN IN-HOUSE CERTIFICATION PROCESS

a Discussion. In the process outlined below, individuals familiar with the application system prepare and present information on the application to members of a review team. The review team then assesses the information, conducts its own investigation and verification of the presence and effectiveness of controls, and recommends certification/ non-certification to the Certifying Official.

b Major Tasks.

(1) Appointment of Certifying Official.

(2) Appointment of Review Team and Application Support Team members by the Certifying Official.

(3) Planning and training of the individual teams.

(4) Joint team preparation.

(5) Defining the application boundaries.

(6) Identifying critical processes within the application.

(7) Preparation of the application documentation.

(8) Preparation of threats and vulnerabilities assessments.

(9) Preparation of internal control listings.

(10) Briefings of Review Team by Application Support Team.

(a) General overview of the full application.

(b) Threats and vulnerabilities of the application.

(c) Management and general controls associated with the application.

(d) Detailed briefings of each portion of the application.

(e) Internal controls of each portion of the application.

(11) Assessment of controls by the Review Team.

(12) Investigation and verification of important items, areas, and controls of the application.

(13) Reporting of findings and recommendation for certification/non-certification.

(14) Certification or non-certification.

4 BENEFITS OF AN IN-HOUSE CERTIFICATION PROCESS

a Staff having knowledge of the application are used in the certification process.

(1) They understand, the application; they can contribute much to the effort.

(2) They are able to recognize weaknesses and to suggest corrections and improvements.

(3) Their involvement increases the likelihood of a more thorough examination of the entire application than spot checking by a review team would produce.

b Time required by the Review Team to examine an unfamiliar application is drastically reduced.

c The Review Team can do a better job because it is getting better information.

d Total time and effort expended are reduced.

5 THE REVIEW TEAM

a Purpose. Evaluate security controls in the application; present findings to the Certifying Official on the acceptability of controls and security measures; recommend certification, conditional certification, or non-certification.

b Tasks.

(1) Examine application documentation for completeness, adequacy, and omissions.

(2) Develop good understanding of internal application controls and management and general controls.

(3) Assemble and analyze information about the application provided through documentation, interviews, and briefings.

(4) Determine the relative importance of the management and general controls, and the application controls. (Critical

Task)

(5) Investigate and verify the most critical areas, items, and controls of the application.

(6) Determine the suitability and adequacy of claimed controls.

(7) Verify the existence of the critical controls. (Critical Task)

(8) Assess the effectiveness of the critical controls. (Critical Task)

(9) Prepare Review Team Report for the Certifying Official.

c Review Team Composition.

(1) 2 or 3 people.

(2) Team leader qualifications - manager or planner with knowledge of ADP and security.

(3) Team member qualifications - strong ADP program development background; analytical, interviewing, and writing skills.

(4) Individuals with specialized skills and backgrounds (e.g. an ADP security specialist) may be needed to assist as part-time team members.

6 THE APPLICATION SUPPORT TEAM

a Purpose. Serve as an aid to the review team in order to expedite the review process.

b Tasks.

(1) Assemble and update documentation on the application.

(2) Develop application flowcharts.

(3) Prepare list of known threats and vulnerabilities associated with the application.

(4) Develop detailed listing of the management and general controls and the application controls present in each portion of the application. (Cross referenced to the flowcharts.) (Critical Task)

(5) Develop briefing presentations.

(6) Present briefings to the Review Team.

(7) Correct problems uncovered by the Review Team.

c Application Support Team Composition.

(1) The size of the team will vary depending on the application and available resources.

(2) Team members will possess firsthand knowledge of the application.

(3) Individuals with specialized skills and backgrounds (e.g. an ADP security specialist) may be needed to assist as part time team members.

7 JOINT TEAM PREPARATION

Issues to be addressed by the combined teams:

a Defining the required security clearance of team members.

b Establishing agreement on the various controls to be evaluated and their purposes; deciding on the formats to be used to document controls for the briefings and the Review Team Report.

c Establishing the certification boundaries of the application.

d Identifying the working papers that must be collected or prepared and saved; designing working paper formats; assigning responsibility for preparation of the various working papers.

e Defining the sensitivity of the Various evaluation documents, the working papers, and the total certification package.

f Formulating the training needs of the various team members.

8 THE REVIEW TEAM REPORT

a Documents the certification review process, the findings and the recommendation(s,)

b Is prepared for and used by the certifying official as the basis for certification/non-certification of the application.

c Must be maintained as an official document of the agency.

d Is composed of three parts.

(1) The executive summary.

(a) Identifies significant findings.

(b) Recommends corrective actions needing immediate attention.

(c) Recommends certification/non-certification.

(2) The detailed findings.

(a) Furnishes direction to the applications staff.

(b) Provides any additional information on the major findings that may be useful in the correction of the problems identified.

(c) Identifies any additional problem areas needing correction if the opportunity arises.

(3) The report appendix.

(a) Contains a detailed listing of internal controls and security provisions.

(b) Contains a summary of the threat and vulnerability assessment of the application.

9 ADDITIONAL GUIDANCE

GAO Audit Guide, "Evaluating Internal Controls in Computer-Based Systems", June 1981, can be used throughout the certification process as general guidance and for determining specific requirements.

June 6, 1986 APPENDIX C Amendment 1

FACILITY TYPE DESIGNATION

1 PURPOSE

The purpose of this Appendix is to clarify and augment information contained within the body of this Manual.

2 SPECIAL INSTRUCTIONS

If facilities are judged to warrant Type I protection, as defined in DM 3140-1, or are clearly Type III facilities the requirements of DM 3140-1 apply without modification.

Difficulties arise in classifying those facilities which fall between minimal configuration and large-computer centers. In determining security requirements for these "in-between" ADP sites, the following guidance applies:

Provide basic Type III security for all sites.

Provide full Type II security for those sites that meet Type II criteria.

For sites not considered full Type II the following procedures are necessary:

Taking into consideration the sensitivity of processing and the importance of the site to agency program operations, determine the requirements for information protection and electronic access controls. Agencies which have many sites with similar or identical equipment and information processing requirements may want to treat the sites as a unit and define base protection for all.

Once this process is completed and fully documented, each site should be subjected to a thorough physical environment review. This review should identify physical security safeguards such as fire protection, off-site storage space, physical access controls, etc.

,

required to provide adequate security. This review must be done on each site separately because the need for these controls is dependent on local factors such as vulnerability to equipment theft, the construction of the building housing the facility, the number of employees or visitors having access to the facility, etc.

The review must also be well documented.

Annual facility security reviews, as defined in DM 3140-1, will assure the continued adequacy of security.

While it is impossible to state, in specific terms, what security measures are needed for each of the thousands of microcomputer, super-microcomputer, and word processing facilities the Department operates, it is even more difficult to assess the total security requirements of aggregates of equipment. It is possible, for example, that a combination of Type III equipments could result in a facility which should be classified Type II.

Those sites which solely support office automation most probably require only basic Type Ill protection. Those which support many users and are the custodians of large amounts of data (typically a super-microcomputer or minicomputer site) require all the Type II protection specified by DM 3140-1.

After careful analysis of the many considerations presented above, agency management must determine how much security is needed and define a program to assure that its requirements are met.

(###

USER ID/PASSWORD MANAGEMENT

1 PURPOSE

The purpose of this appendix is to clarify and augment information contained within the body of this Manual. This appendix is not intended to limit the use of technology but to manage the security of that technology.

2 SPECIAL INSTRUCTIONS/CANCELLATIONS

This Appendix D to DM 3140-1 replaces the Appendix D issued on December 14, 1987, which is rescinded.

3 BACKGROUND

The increasing use of microcomputers, distributed processing, local area networks, and cooperative processing results in greater vulnerability to misuse of Information Resources Management (IRM) resources. The protection of IRM systems and individual users requires unique User IDs and passwords for verification of the users authorized access to systems and information.

This appendix presents guidance in administering and monitoring the operation of access control systems. This appendix is applicable to all telecommunication facilities, including public/private networks and Local Area Networks (LANs). Refer to DR 3300-1, Telecommunications.

4 RESPONSIBILITIES

a Agencies will:

Appoint a qualified person to serve as ADP Security Officer and appoint as many deputies and assistants as necessary to assure that security duties are carried out in all locations in which IRM functions are performed. Such functions include data processing, telecommunications (data and voice), word processing, and office automation.

Assess the sensitivity of systems and data and develop adequate security for the operation of the systems. Use individual user IDs and passwords to control access to systems processing personal, financial, market-related, or other sensitive data. A key element in devising this protection is determining who should have access to what resources. The owner will notify the Security Officer who can have access to the data.

An agency may, if it wishes, designate program representatives as Deputy Security Officers, but all security activities must be under the purview of the agency ADP Security Officer. The

security staff, whatever its composition, is responsible for carrying out the instructions of program management staff in administering access control programs.

b Agency ADP Security Officers will:

Oversee and administer access control systems within their agencies. They must have ready access (electronic, if possible) to all files containing information on users. It is vital to the investigation of security breaches or other problems to have this information available immediately.

Implement access control according to the data owners decision. Further advise management on data security issues and practices. Mainframe Security Officers should control the installation, modification, and implementation of purchased or agency developed software used to control access to data and IRM resources.

c Central Computer Resource Centers will:

Deal only with designated security representatives in administering their access control programs. Central Computer Resource Centers include the National Finance Center, Departmental National Computer Centers, and agency computer resource centers.

5 REQUIREMENTS

Each facility which supports distributed processing shall use an ID/password control system. Vulnerability to errors and deliberate attempts to compromise data increases substantially when connected to a communication network. Tailor all access control packages to meet the protection needs of the agency.

If this capability is not available and significant vulnerability exists, develop or obtain control software or adopt another mode of operation.

For an access control system to be complete, there must be a software program which provides a record of each access, giving user ID, time of access, and depending on the sophistication of the system, details of operations for which access has been granted.

Unauthorized access (max. limit of three) attempts must also be recorded, and the connection dropped.

6 MANAGING USER IDs AND PASSWORDS

a Length and Composition.

Passwords must be at least 4 characters long; create longer ones if the systems permit. It has been noted that if

passwords are unusually long, users are tempted to write them in inappropriate places; a length of 6 to 8 characters is recommended. Random combinations of numeric, alpha, and special characters furnish a more complex therefore, more secure, password than will use of only one type of character. Passwords should never be composed of personal data such as birthday, street address, pet's name, etc. Agency, organization, or project acronyms must not be used.

b Password Life and Changes.

The maximum life of a password is 90 days for interactive applications and 180 days for batch applications. Passwords may be changed less than the above (90 or 180 days). Processing site requirements, data sensitivity and criticality, and other system considerations may dictate a lesser lifecycle for passwords. Frequently changed passwords reduce the level of vulnerability. Once changed, original passwords should not be reused for a period of at least four (4) days. Users must be able to make changes, and security staff should not know passwords after initial issuance. Users must change them immediately upon issuance. Users must also immediately change passwords they suspect may have been violated and report the incident to supervisors and security staff.

c Password Administration.

The use of default passwords is generally prohibited. Exceptions can be made for logon identifiers IDs which are created with a default password, but which are placed in a suspended or inactive state until their issuance by the security officer to the end user is effective. Agencies that have a need to use single logon IDs at multiple locations must request a waiver in writing from the Director of OIRM.

Security staff should remove employee user IDs and passwords when the employee is no longer with the agency. A formal procedure should be established for notification of the Security Officer by the agency personnel office of all retirements or other personnel separations. The Security Officer should be assured by the system administrator that all vendor supplied generic logon IDs and passwords have been removed from the system. The Security Officer should further assure that user automated logon procedures do not include IDs and passwords. When there is a change of a contractor that uses the system, all IDs and passwords on the system must be changed as soon as the contractor services are terminated. Security Officers will assign IDs and passwords to individual users. The IDs and passwords will be coordinated with the system administrator. Issuance of group logon IDs and passwords and the sharing of same is not permitted. Security staff must maintain files of users, including names, office addresses and telephone numbers. The security file, if automated, should not be stored on the system hard disk.

Immediately change all vendor-supplied passwords for access to any system components or software routine. These passwords are known to the hacker community who have detailed technical knowledge of many, if not all, computers in use. Make changing vendor passwords a mandatory task in new equipment and/or software installation.

System Administrators or Security Officers are not to create and provide user logon IDs without passwords. This appendix discourages the use of multiple user logon IDs and passwords for a single user.

d Application Developers

Application Developers are not permitted to:

1 Code in their program access to mainframe security files. These files are for the protection of the entire user community. Security is not enhanced by making security data files available to application programs.

In fact security could be compromised by the improper use or knowledge of security data.

2 Write routines that circumvent the security established by the center they are using;

Application Developers are encouraged to:

1 Code within their programs security protection to control the access and use of their programs and data, providing items 1 and 2 above are not violated.

e Awareness

Security Officers or supervisors must brief all new employees and contractors on security, stressing the need to protect passwords and change them frequently and to adhere to agency rules on the protection of information and equipment. Users must be made aware that passwords are used for their protection, as well as for safeguarding systems and data. Annual security reminders must be given to all employees and contractors. Reminders can take the form of informal discussion, more formal training, or documentation.

When an employee or contractor terminates association with an organization, Security Officers or supervisors must collect all access keys, badges, etc., and account for all equipment, software, and data which the individual has had in custody.

7 VULNERABILITY TO UNAUTHORIZED DISCLOSURE

Access administration must be handled to assure individual accountability and the least amount of access privileges to get the job done. Perhaps the most prevalent invitation to access-key misuse is user carelessness in creating, using, and changing

passwords. Password changes must not be effected by alternately using a couple of character strings, a practice which compromises good security. In security briefings and training, stress the importance of protecting these keys and remind users that the keys are in place for the-protection of users, as well as for the protection of information.

Many users, in the interest of simplicity, store job control language, user IDs, passwords, and telephone numbers for other computer facilities in their microcomputers. This practice should be discouraged. If it is deemed necessary, the computer should be made inaccessible to others. If data transfer from a microcomputer is necessary, the owner of the data should initiate all transactions. Similar information stored in mainframes or minicomputers must be protected from unauthorized access.

Users IDs for access to any computer system must not duplicate IDs used for access to other systems. Do not, for example, duplicate Departmental Computer Center or an agency computer center ID in assigning an ID for access to an agency computer, thus creating a vulnerability for both systems.

Another vulnerability arises through the use of line- monitoring equipment, which displays and often records all traffic passing down the line, including ID and password information.

Line-monitoring operations must be afforded maximum protection, and the equipment must be secured from unauthorized use.

8 SECURITY BREACHES

In the event of a suspected security breach, the agency Security Officers must be notified. The Security Officer must determine if the breach involves criminal action or significant loss. If the breach is of a criminal nature or involves significant loss, it must be reported to the Office of Information Resources Management, and the Office of the Inspector General at once. The Security Officer, if requested by investigating authorities, must work with the involved IRM facilities, the Office of Information Resources Management, and the Office of Inspector General to investigate the breach and solve the problem.

Procedures and reporting requirements for suspected security breaches on the Departmental Data Communications Network are outlined in DR 3300-1, Telecommunications.

9 REQUEST FOR WAIVER

USDA agencies requiring a waiver to allow single logon IDs at multiple locations must submit a request in writing. OIRM will consider providing a waiver on a case-by-case basis. At the end of

the waiver period the agency must determine if the waiver is still needed. The agency must determine whether having a single ID has caused a security problem that can not be managed. The following information must be explained in the request for waiver.

a The reason a waiver is being requested,
b How the agency will protect against misuse,
c How this will be managed by the agency, and
d The length of time a waiver is being requested.

5/23/91)

SMALL SYSTEMS SECURITY

1 PURPOSE

The purpose of this appendix is to provide guidance for devising and maintaining security programs for small ADP systems, typically consisting of microcomputers, and for incorporating these programs in comprehensive agency programs.

2 BACKGROUND

The body of this manual contains standards for security of all types of ADP operations conducted by or on behalf of USDA. These standards must be applied. As use of distributed processing expands, it becomes increasingly more difficult for and users--typically microcomputer users--to determine, within the framework of the standards, exactly what protective features and procedures should be adopted. This appendix provides guidance in making that determination.

3 RESPONSIBILITIES

Agency management must assure that all ADP operations are conducted in protected environments and that IRM resources are afforded adequate protection at all times.

Agency management will:

Establish that ADP security is important and must be provided for all the agency's ADP operations.

Determine the sensitivity of all information and systems.

Incorporate security in ADP training.

Assign responsibility for all microcomputer functions, including

all micro-to-mainframe links; establish a procedure for authorizing such links; and maintain current records that list persons authorized to access mainframes, types of access authorized, etc.

Develop and issue guidance on equipment maintenance.

Develop and issue policies related to use of Government equipment in the home and use of mainframes for training purposes.

Define the level of data uploading and downloading permitted, the extent and type of processing allowed against downloaded files or files to be uploaded, file transfer limitations, and audit trails and accountability controls required.

Define which version of each data base is the official version.

Assure that all agency ADP facilities develop security plans, an outlined below.

4 SECURITY PLAN REQUIREMENTS

This manual requires development of formal security plans for all Type I and II facilities and specifies the minimum security which must be provided for Type III facilities written plans for Type III facilities have not previously been required, but the Computer Security Act of 1987, PL 100-235, enacted in December 1987, specifies that each ADP facility must develop a plan for providing at least minimum protection to equipment and information.

Security plans for small sites need not be lengthy, formal documents requiring extensive effort. They should document the site's compliance with the requirements listed for management attention, the site's current security status, and plans for security improvement. For the purpose of security plan development, a "site" can consist of all computers and related peripherals and telecommunications equipment located in a logical area, such, as contiguous offices performing similar functions. Security reviews of all individual components can be summarized, with significant details highlighted for action. Agencies will provide additional guidance, as required, to assure conformity with agency reporting requirements or other needs.

Agencies will monitor site security plan development and will incorporate information thus gained into agency security plans in addressing the agency's overall security posture.

5 MINIMUM SECURITY REQUIREMENTS

The minimum requirements listed below address the level of protection required for all processing. The means of achieving and maintaining this level are addressed in detail in the body of this manual but are not included in this briefer document. If additional guidance is required, agency or Departmental security staff can advise.

It should be understood that exceptional conditions, such as the presence of sensitive information, may mandate more than animal protection. The value and sensitivity of the information or critical nature of processing should determine the type of protection needed.

Physical Security. Protect equipment and information from theft and misuse. Access control can be accomplished by many means, ranging from armed guards and alarmed entrances to simply locking doors and windows. Depending on the vulnerability of the site to unauthorized access, consider such additional deterrents as protective cabling.

Do not leave equipment unattended and accessible for lengthy periods during office hours. Log off properly and secure data and equipment at the end of the day.

Escort visitors and challenge anyone purporting to be a repairman authorized to pick up equipment before releasing equipment.
In
offices having open access, such as field offices providing services to the public, particular care must be exercised.

Protect equipment and information from damage or destruction from ill-treatment, dust, fire, or other hazards. Assure that equipment is properly maintained, that work areas are clean and hazard-free, and that fire extinguishes designed to counter electrical fires are available.

Information Security. Protect information against unauthorized access or disclosure, unauthorized modification, and intentional or accidental destruction. If the systems used to process sensitive information provide the capability to restrict access to computers or data by use of passwords, use this feature. Be sure that security software has been properly installed and that all vendor-supplied passwords have been changed.

Protect passwords, changing them frequently and disabling them immediately upon the departure of personnel.

Restrict access to sensitive information to those with a need to have the access. In offices which process or store information subject to the Privacy Act, market-sensitive data, or data vulnerable to manipulation, fraud, or other misuse, additional

controls say be necessary. It is important to protect sensitive information in any form.

Users are cautioned that word processing, electronic mail, and output document handling warrant assessment when reviewing site security.

One of the best protections against catastrophic data loss is in regular, scheduled data backup, with interim backup as indicated.

Provide off-site storage for information that is critical to program operations, that would be difficult to reconstitute, or that is required by law or custom to by current.

Administrative Controls. Monitor compliance with agency requirements for personnel security clearances, as well as compliance with other policies such as equipment maintenance, training, use of equipment in the home, etc.

To the extent possible, practice separation of duties. Cross-train employees in the various aspects of program operation. Above all, do not permit "one man shows" to flourish.

Assure that all employees are aware of the sensitivity of information they are handling and that they have knowledge of processing results to be expected. Remind them to report anomalies in results to supervisors.

Monitor the use of telecommunications.

Stress to all users that maintaining good security requires participation by all. In annual briefings, required by this manual, inform users of their responsibility to assume personal responsibility for maintaining security and reporting violations.

SECURITY PROBLEM IDENTIFICATION AND RESOLUTION

1 PURPOSE

The purpose of this appendix is to clarify and augment information contained within the body of this Manual.

2 BACKGROUND

Widespread use of microcomputers, local and wide area networks, distributed processing, and cooperative processing have increased the vulnerability to misuse of ADP resources. The growing threat of computer virus infections and increased sophistication of hackers has further increased the need for speed in the identification and resolution of computer security problems.

This appendix presents guidance for determining the extent and severity of computer security problems and for notifying other USDA security personnel about the problem.

3 RESPONSIBILITIES

Agency and facility security personnel will immediately report Departmental telecommunication or computer system security problems to the OIRM Security Office by telephone or by Departmental electronic mail. The SO will take immediate action to determine the extent of the problem -- its severity and its threat to systems and data integrity. The So will:

a Use the Departmental electronic mail system to inform agencies' security staffs about the security problem. So will use the "urgent" and "receipt" functions to bring maximum attention to the problem. The "urgent" function posts the message for immediate delivery. The message goes to the top of the recipient's sign-on scan table, with an "URGENT" flag.

The "receipt" function issues a return receipt to the sender when the message has been accessed by the recipient. The return notification includes the date and time the recipient accessed the message.

b Send memorandums to all persons who will be involved in discussions related to the problem.

c Use all available and appropriate resources for correcting the problem.

d Change Departmental security regulations if a problem warrants such action for the long term.

e If requested by investigating authorities, work with involved ADP facilities and the Office of Inspector General to

investigate suspected security breaches and implement solutions.

f Use the reporting requirements outlined in applicable Departmental regulations for handling suspected security breaches (for example DM 3140-1, section 8b, and DR 3300-1, appendix E).

g Report immediately to the Office of Inspector General all security problems or significant losses.

BULLETIN BOARDS

1 PURPOSE

The purpose of this appendix is to clarify and augment information contained within the body of this manual, DM 3140-1. This appendix is not intended to limit the use of technology but to manage the security of that technology.

2 BACKGROUND

Use of bulletin boards has resulted in greater vulnerability and misuse of ADP and telecommunications resources. Proprietary software has been placed on a bulletin board allowing unauthorized distribution. Access controls placed on systems have not adequately prevented unauthorized users access to data base systems. The protection of IRM systems and individual users requires unique User Identifiers (IDs) and passwords for verification of users authorized access to systems and information.

The need for bulletin boards plays a vital role in the electronic sharing of information. The main objective of this appendix is the management of USDA created bulletin boards, their use and the use of private sector bulletin boards For Telecommunications guidance refer to Departmental Regulation (DR) 3300-1.

3 RESPONSIBILITIES

a Agencies will:

1 Direct the control and use of bulletin boards.

2 Prohibit the imbedding of logon IDs and passwords in logon procedures.

3 Control the use of accounting codes and protect them by masking at all times.

4 Prohibit the transmission of proprietary software to bulletin boards (see DR 3130-2, section 10d).

5 Test all software and data obtained from bulletin boards, government or private sector, and other free "shareware" for viruses before placing into the government computing environment. Do not install shareware software on a computer system that is a part of a network.

6 Designate responsible agency security officers who will monitor usage of bulletin boards on a regular basis and delete any inappropriate data.

7 Archive all data after seven (7) days of non-use.

8 Once data has been archived, and is not recalled for use, delete from archive after 30 days.

b SECURITY OFFICER RESPONSIBILITIES

1 The Security Officer will be responsible for approving bulletin board creation. Approval will include assuring that proper access control is part of the bulletin board system. Give particular care to compliance with DM 3140-1 and other Departmental and other relevant security regulations when overseeing the installation of the bulletin board.

2 For an access control system to be complete, there must be a software program which provides a record of each access, providing: User ID's, time of access, and, depending on the sophistication of the system, details of operations for which access has been granted. Record unauthorized access attempts.

3 The Security Officer will be responsible for monitoring bulletin board use on a regular basis. Particular care will be given to locating unauthorized access, misuse of data, and storage of inappropriate information. When inappropriate data is located, it is the Security Officer's responsibility to see that it is removed.

4 Vulnerability to errors and deliberate attempts to compromise data increases substantially when operating in telecommunications mode. If a system has an access control package, use all features. If this capability is not furnished and significant vulnerability exists, develop or obtain control software or adopt another access control system.

4 REQUIREMENTS

Bulletin boards fulfill a requirement for wide distribution of time-sensitive information. They are not to be used to store mission-critical data or information with long-term retention requirements. Bulletin boards are to be monitored for adherence to these guidelines.

USDA AUTOMATED DATA PROCESSING (ADP) EMERGENCY MANAGER

1 PURPOSE

The purpose of this appendix is to create and maintain within each USDA agency an ADP Emergency Manager (EM). This appendix further recommends the creation of an internal agency emergency network team.

2 SPECIAL INSTRUCTIONS/CANCELLATIONS

This Appendix H to DM 3140-1 replaces the Departmental Notice issued on April 22, 1991 which is rescinded.

3 BACKGROUND

In a continuing effort to safeguard the integrity of USDA automated data processed and stored at the Departmental National Computer Center (NCC), an emergency point of contact is required. In February 1991 the NCC at Kansas City experienced an emergency requiring the recovery of data files over a weekend. The NCC staff was unable to contact the appropriate management and technical personnel in some agencies. This prolonged the recovery process.

4 POLICY

USDA agencies that use an NCC facility will establish and maintain an ADP Emergency Manager and a Emergency Manager alternate.

5 DUTIES

The persons identified as the EM and EM alternate serves as the central point of contact in emergency situations. The EM must be aware of the agency emergency procedures and participates in any updating of those procedures. The EM should have contacts with is personnel from various operational areas that own the automated data files within the agency. These internal agency contact points should make up the internal agency emergency network team. The internal network team will provide support to the EM. The EM must be prepared to receive calls during operational hours of the computer center (nights, weekends, and holidays).

6 RESPONSIBILITY

a OIRM will maintain a list of the EM's. In an emergency situation involving NCC and USDA agencies, OIRM will contact the Agency EM's to inform them of the situation. The NCC will work with the EM to resolve the emergency.

b USDA agencies will designate a lead EM, and an alternate. The EM and the alternate should be technical persons with knowledge of the agency, agency automated data, automated data file structure, and where the automated data is located. The agency should maintain an off duty telephone number for both the EM and the alternate. It is suggested that the agency create a network of persons familiar with the agency automated data in the various operational areas. When an emergency occurs, the EM must have access to responsible persons in the various operational areas Initially, each agency should provide the following information for both the lead EM and alternate to OIRM:

1 The Agency name, and the EM mailing address,
2 EM name,
3 EM daytime telephone number,
4 EM nighttime telephone number.

c Agencies must notify the National Computer Center of any change in personnel assigned as the EM or the alternate. The information required in section 5(b) must be provided within five working days of a change.

All updates should be submitted to:
U. S. Department of Agriculture
National Computer Center
Attn: ADP Emergency Manager
8939 Ward Parkway
Kansas City, Mo. 64141-0205

March 27, 1992 Amendment 8
(###

APPENDIX I

GUIDELINES FOR CONTROLLING COMPUTER VIRUSES

1 PURPOSE

This appendix establishes policy to minimize the risk of introducing and spreading virus infected or malicious software into the USDA computer environment. It also provides guidelines for the detection and removal of malicious software from computer systems.

2 BACKGROUND

Virus infected software presents an increasingly serious security problem for computer systems and networks. Malicious software harbors viruses and other destructive programs that are often written as independent programs which appear to provide useful functions. These programs are spread through software bulletin boards, shareware, and users who unknowingly copy and share virus infected programs. Networks are particularly vulnerable as they

allow a very rapid spread of viruses to all systems connected to the network. A virus can destroy programs and data by erasing files or adding unwanted code to executable programs. Once a program has been infected it serves as a host and the user serves as a carrier.

USDA's dependence on networked computer systems, personal computers, and office automation makes us susceptible to virus "attacks." Many USDA agencies are losing staff time to virus origin research and to isolating and eliminating viruses. In most instances the damage is minimal and easily corrected. Preventive measures reduce the chances of virus infected software invading our systems.

Malicious programs such as Trojan horses and trap doors were originally written for mainframe computer systems. Larger systems without adequate controls are prime candidates for the introduction of malicious programs. Authorized users making unauthorized use of the system may also introduce malicious software to the system.

Sound security procedures will help detect and prevent computer viruses and other malicious programs from entering and spreading damage to networked computer systems or personal computers. The guidelines contained in this appendix are adaptable for any type of computer system.

3 POLICY

USDA agencies that distribute or receive computer diskettes must use antivirus detecting software on those diskettes.

All information or programs obtained from bulletin boards and stored on hard disk, or diskette must be scanned with antivirus detecting software.

4 DEFINITIONS

Through the introduction of viruses and other malicious software, computer hackers have generated a set of new terms. The following list of definitions is provided to familiarize personnel with some of these terms.

a Bacterium - A late bloomer in the infectious terminology jargon is a "bacterium." It is a program that replicates itself and becomes a parasite on the host system by preempting processor and memory capacity.

b Computer Hacker - A person or group of persons using computers to illegally break into other computers. These persons

normally have interest only in the ability to break into another system. This term also describes computer "whiz kids" who push their knowledge of computers and programming to its limits. The unauthorized access of computers by the computer hacker is a criminal act by law.

c Computer Virus - A program designed to infect computer systems in much the same way as a biological virus infects humans. The typical virus reproduces by making copies of itself when inserted into other programs. Computer viruses normally infect either systems software or application programs.

d Flying Dutchman - A feature of the Trojan horse malicious program. It erases all traces of the programming codes from the computer's memory and eludes any detection.

e Freeware - Software that has been developed and placed in public domain for general public use. This software do not have a fee for use or updates.

f Logic Bomb - A computer code that is preset to cause a malfunction when a specified set of logical conditions occur. For example, when a specific social security number in a payroll system is processed, the logic bomb is activated. The logic bomb will then cause an improper amount of money to be printed on the check.

g Machine-Readable Media - Media that can convey data to a given sensing device (for example: diskettes, hard disks, and tapes).

h Malicious Software - Any of a family of computer programs developed with the sole purpose of doing harm. Malicious code is usually embedded in software programs and appears to provide useful functions. When activated by a user, it causes undesirable results.

i Scan - To examine computer coding/programs sequentially, part by part. Scans are made for virus signatures or potentially unsafe practices. (For example: scan for changes made to an executable file, or search for direct writes to specific disk sectors, etc.)

j Shareware - Software that has been developed and placed in public domain or in general circulation for general public use. The developer of this software request a small fee ($10.00 - $20.00) for use and future updates.

k Time Bomb - A computer code that is preset to cause a malfunction after a specific date, time, or number of operations. The "Friday the 13th" computer virus is an example. The system is infected for several days, or even months, and the virus lies dormant until the date reaches "Friday the 13th."

l Trap Door - A set of instruction codes embedded in a computer operating system that permits access while bypassing security

controls.

m Trojan Horse - A set of unwanted embedded computer instructions inside a program. The instructions cause unexpected results when the program is executed. It may create logon ID's and passwords for later intrusion by hackers. Further, Trojan horses allow persons to create or gain access to the source code of common or frequently used programs. These programs may be modified to perform a harmful function in addition to its normal function. A Trojan horse can alter, destroy, disclose data, or delete files.

n Virus Detection Software - Software written to scan machine readable media on computer systems. There are a growing number of reputable software packages available that are designed to detect and/or remove viruses. In addition, many utility programs can search text files for virus signatures or potentially unsafe practices.

o Virus Signature - A unique set of characters which identify a particular virus. This may also be referred to as a virus marker.

p Worm - A worm is a complete program that propagates itself from system to system, usually through a network or other communication facility. A worm is similar to a virus and can infect other systems and programs. A worm differs from a virus in that a virus replicates itself, and a worm does not. A worm copies itself to a person's workstation over a network or through a host computer and then spreads to other workstations. It can easily take over a network as the "Internet" worm did. Unlike a Trojan horse a worm enters a system uninvited.

5 RESPONSIBILITIES

The Office of Information Resources Management is responsible for coordinating the Department's IRM security program (ADP and Telecommunications). This includes establishing information security policies and procedures for safeguarding Departmental information resources. The Departmental IRM Security Officer shall serve as the focal point for all matters relating to ADP and Telecommunications security. The Departmental IRM Security Officer will further be responsible for developing and disseminating information concerning the potential dangers from malicious software and guidelines for its control.

Agency Security Officers are responsible for:

a Promptly notifying the Departmental IRM Security Officer of computer security incidents including malicious software;

b Developing appropriate procedures and issuing instructions for the detection and removal of malicious software consistent with the guidelines contained in this appendix;

c Ensuring all personnel within their agency are made aware of this policy and incorporating it into computer security briefings and training programs;

d Identifying and recommending software packages for the detection and removal of malicious software;

e Developing a system for users to report computer viruses and other incidents, which includes notifying potentially affected parties of the possible threat;

f Providing assistance in determining the source of malicious software and the extent of contamination; and

g Conducting periodic reviews to ensure that proper security procedures are followed, including those designed to protect against malicious software.

Managers must ensure that employees and contractors follow agency procedures which comply with this policy. Personnel from other organizations using USDA systems, contractors, and vendors are responsible for following agency procedures for the protection of information resources to which they have access. This includes reporting computer security incidents, including viruses and other malicious software, to the agency Security Officer.

6 REQUIREMENTS

The requirements defined in this section, when implemented, will minimize the risk of introducing viruses and other malicious software. Not all requirements listed will apply to every computer system or network. Agencies must conscientiously evaluate the appropriateness of each of the following procedures and implement those that apply to their particular system.

a All USDA agencies must acquire and use virus checking software.

b This appendix covers all computer systems that are used to process USDA data, including contractor-owned and/or contractor-operated systems. This appendix applies to new contracts and is not retroactive.

c This appendix applies to all USDA and non-USDA personnel from other organizations, contractor personnel, and vendors using USDA systems. This appendix further applies to USDA-sponsored software development, software demonstrations, and the operation and maintenance of computer systems.

d This appendix is intended to supplement "ADP Security Policy." Specifically, this appendix delineates policy to:

(1) Minimize the risk of introducing and spreading viruses

and other malicious software;

(2) Ensure timely detection of virus infections;

(3) Provide procedures for eliminating virus infections from the Department's inventory of microcomputers (PCs); and

(4) Provide procedures to minimize the risk from malicious programs to larger systems, or systems where virus detection software is not yet available.

e All USDA agencies that distribute diskettes must check the diskettes for viruses prior to disbursement. A statement certifying the distributing agency checked the diskette with an antivirus software package prior to disbursement should be included with the diskette. The certification should include the name of the antivirus software and the version number. The certification should not include a statement claiming the distributed diskette is virus free. The distributed diskette is only virus free of the known viruses that the antivirus program checked for.

f All USDA agencies receiving diskettes from external sources must test the incoming diskette.

g All software and data obtained from bulletin boards, or other free "shareware", must be tested before placing into the Government's computing environment. It is recommended that shareware software should not be installed on a computer system that is a part of a network.

h All diskettes brought from home or other non-Government sources must be tested for viruses.

i Each agency will establish appropriate procedures for adherence to this policy based on:

(1) Criticality,

(2) Sensitivity, and

(3) Risks to their computer systems.

j Employees should back up new software immediately, retaining the original distribution diskettes in a safe and secure location. Write-protect original diskettes prior to making backup copies. If a virus destroys the working copy, the original software is still available. Copying copyrighted software material without the vendor's consent is illegal. If a vendor has not provided preapproval of backup copies, employees must have vendor approval to create additional copies. Use only newly formatted diskettes for copying software for backup. Used disks may already contain malicious programs which would contaminate the backup copies. Data files should be backed up frequently and stored off-site or in a secured environment.

Keep fresh backup copies of original diskettes. Restore damaged software programs from the original backup diskettes, not from regular backups. A virus may have been introduced prior to backing up from hard disk.

k A serious impact on the credibility of the Department would result from being identified as the source of a virus. Therefore, all software and data leaving the Department must be checked for viruses or other malicious coding.

Use only new media for making copies for distribution. Where possible, use a stand-alone computer system when preparing copies for distribution. Personal computer systems to which access is somewhat open (i.e., training rooms, user laboratories, etc.), should never be used as a source of software or files to be transmitted. These files or software should not be copied for distribution without first taking steps to ensure that the system is free from viruses or other malicious software.

l Personal computer machine-readable media will be scanned for malicious software before initial use. Follow all vendor instructions carefully and write-protect virus scanning software prior to use. Scanning software can become contaminated in the same way as other software. Although software sealed in "shrink-wrapped" plastic is usually checked by vendors, it is still advisable to scan this software since there have been reported cases of software contamination. Write-protect software prior to scanning to prevent possible contamination from system and scanning software. Requirements to scan for malicious software are to be implemented as soon as the tools become available for a particular combination of hardware and software.

Establish controls for local area networks that prevent anyone except the system administrator or other authorized staff from loading software on file servers. Ensure that operating system files and other executable files are read-only. If possible, disable the network mail facility from transferring executable files. This will help prevent network worm programs from spreading through the network.

Trojan horses and other similar malicious software programs are often introduced by insiders. It is not unusual for larger systems to be the target of this type of malicious software. The best protection against attacks of this type is to establish good management procedures. Effective controls include:

(1) Separation of duties,

(2) Limiting individual access,

(3) Formal change control and configuration management procedures,

(4) Separation and testing of development versus production

software,

(5) Control of installation of new software versions, and

(6) Frequent backups of the system and data for recovery should an incident occur.

m It is imperative that machine-readable software and data files be obtained from reliable sources. Viruses are often spread through free or shared programs, games, demonstration programs, and programs downloaded from bulletin boards. Commercial software must be obtained through properly defined procurement channels. Software development must be done in accordance with established Departmental Software Management policy (DR 3220-3 Software Management) and have prior management approval.

Shareware and freeware software must be obtained only with prior management approval. Software obtained electronically from bulletin boards should be downloaded to newly formatted diskettes and not directly to the computer hard disk. All newly acquired software, regardless of source, is subject to the policy of this document.

n When possible, employees demonstrating USDA products must be certain that the hardware and software they are using are free of viruses. Use hardware write-protection mechanisms (i.e., read-only diskettes with write tabs; write-protect rings for tapes; knock-out rings on cassettes, etc.) to prevent any virus from infecting the media. If possible, check the hardware for viruses before loading the demonstration software. Do not allow other software to be used until the demonstration is completed.

o For larger systems and networks, user identification and passwords are the primary protection mechanisms against malicious software. If the would-be perpetrators cannot get into the system, they cannot put malicious software on the system. When possible, all computer systems that are shared resources, including local area networks and multi-user stand-alone systems, shall implement a user identification and verification system such as a USERID and password. Conformance to the requirements of the USDA "ADP Security Manual" DM 3140-1 in establishment, structure, individual accountability, periodic changing and removal are required.

System managers should change all vendor-supplied passwords, including those for software packages and maintenance accounts, as soon as the system has been installed. Vendor supplied passwords are usually the same on every computer system of the same make and model. It is a very common method used by hackers for gaining access to a computer system to try known vendor supplied passwords. Procedures must be established for vendors to identify in writing and for USDA or vendor to remove such USERID's and passwords. Procedures must be set up to remove USERID's and passwords when an authorized

user no longer needs access to the system for official reasons. Log files should be reviewed periodically to detect unusual activity. Terminals, workstations, and networked PCs should never be left unattended when logged on.

p Vendors when demonstrating their software on USDA hardware must use stand-alone hardware, where possible. USDA employees must scan the hardware before it is used by the vendor to verify that the computer does not contain a virus. This will demonstrate that the Department acted in good faith in attempting to prevent infection of the vendor's software.

USDA employees will scan the hardware when the demonstration is completed to determine if the vendor software contains a virus and remove it from the system. The vendor should be notified immediately, if one is found, to prevent further infections.

In the case of network software demonstrations, the system administrator must approve and coordinate the demonstrations. Written certification from the vendor that the demonstration software has been checked and is free from viruses, should be obtained prior to loading any vendor software.

q Personal computer hard disk drives, network file servers, and other media which will be used to handle departmental information will be formatted between the time they are received and put into use.

There have been cases of formatted hard disk drives being received that contained viruses. This requirement also applies to replacement parts resulting from repair and maintenance of equipment. This requirement may be waived only if the vendor installing the software provides a written certification that the system and software have been checked and are virus free. Never start up (boot) your computer from a diskette unless it is the original write-protected system master or a reliable copy. Portable computer systems that leave USDA controlled areas must be scanned when returning to the USDA environment.

r All procurement for computer software and hardware will contain a requirement that the vendor has antiviral procedures in place to ensure that the media supplied are uncontaminated by malicious software. When using off- the-shelf software procurements, where it is not possible to write antiviral clauses, the software will be scanned with virus detection software prior to use. Procurement for personal computer system maintenance should also require antiviral procedures on the part of the contractor.

Vendors depend on the reputation of their products to ensure future sales. Reputable vendors are concerned about correcting any flaws in their systems or products that would make them vulnerable to attack from viruses or other malicious software, and on occasion issue recommended changes to improve security of their products. System administrators and managers are to

implement any vendor recommended changes or security fixes as soon as possible after official receipt.

7 MALICIOUS SOFTWARE INDICATORS

If your computer system seems to be acting differently than usual, a malicious software incident may have occurred. Most of the time (90%) the problem my be an error in the software. Below are a few signs that may indicate that a system has been infected.

a Any unexplained messages or graphics on the screen,

b An increase in the time required to load or execute programs,

c An increase in the time required for disk accesses or processing from disk,

d Unusual error messages,

e Programs or files mysteriously disappearing,

f Less memory available than usual,

g Executable files changing size for no apparent reason,

h Accesses made to non-referenced devices,

i Data consistently out of balance,

j File date and time stamps changing for no apparent reason,

k Obsolete user accounts in use,

l The presence of unexplained hidden files,

m Unusual network activity, and

n System crashes.

If your system demonstrates any of the above, it could indicate that malicious software is present.

8 ELIMINATION AND RECOVERY

If you suspect that your computer system or network has been attacked by a virus or other malicious software program, contact your agency Security Officer. Report the problem and obtain assistance before any corrective action is taken.

It is important that the particular virus, source, and spreading potential be identified and controlled. The process of cleaning

and restoring the system require that O EXECUTABLE FILES FROM BACKED UP DISKETTES ARE RESTORED TO THE CLEAN SYSTEM. You must ALERT all persons who have received a diskette created by or used on the infected system.

If your agency has copies of antivirus software, the following steps should be taken once a system has been identified to contain a virus infection:

a Obtain a copy of the antivirus software. Write-protect the antivirus diskette.

b Scan the hard disk (C, D, E, etc.) using antivirus software.

c If a virus is found, use repair or clean option of the antivirus software.

d Once the hard drive has been cleaned, start the scanning process on all floppy diskettes used on the system.

e Do not restore executable files from backup diskettes to the clean system environment.

f Notify all persons that used the infected system or received diskettes created on the system.

If your agency does not have antivirus software:

a Turn the power off to the infected system, write-protect all diskettes.

b Obtain copies of the systems data file backup diskette.

c Obtain a copy of the original operating system diskette, and write-protect the diskette.

d Obtain copies of the original systems software diskette.

(write-protect these diskettes)

e Restore power to the infected system with the original operating system diskette in the 'A' drive. (Do not forget to write-protect the system diskette)

f Perform a low-level format of the infested disk.

g Restore the operating system from the original diskettes to the hard disk.

h Create all directories that are needed.

i Restore all system software to the proper directory using the

original distribution diskettes.

j Do not restore executable files from backed up diskettes to the clean system environment.

k Restore all backed up data files.

l Identify all diskettes used on the infected system.

m Format a new set of diskettes to be used as data file backups.

n Copy desired data files to the newly formatted diskettes.

o You may wish to reformat the old diskettes or you may desire to destroy them.

Provide the following information to OIRM in writing or by Electronic Mail:

a Name of the particular virus,

b Source,

c Where was it spread,

d Damaged caused,

e Time lost due to virus:

(1) Total time Program delivery staff,

(2) Total time IRM support staff,

(3) Total time Security Officer and virus cleanup staff,

f Number of persons used in virus cleanup,

g Number of systems scanned during detecting process,

h Number of systems containing virus, and

i Procedures used to recover.

9 VIRUS SOURCE OF INFORMATION

Computer Viruses by National Computer Security Association $44.00.

Computer Virus Handbook by Harold J. Highland, Elsevier Science Publishers Ltd, 1990. $153.

Computer Viruses: A High Tech Disease, by Ralf Burger, Abacus Software, 1988. $29.95.

Computer Viruses: What They Are, How They Work, and How to Avoid Them, by Jonathan L. Mayo 1989, Windcrest, $29.95.

Computer Viruses, Worms, Data Diddlers, Killer Programs, and other Threats to your System by John McAfee and Colin Haynes, 1989, St. Martin's Press, 1989. $16.95. 235 pages.

Computer Virus Survival Guide by National Computer Security Association $5.00.

Virus Scanners: An Evaluation by National Computer Security Association $44.00.

Virus Removal Tools: An Evaluation by National Computer Security Association $44.00.