

AUTOMATED INFORMATION SYSTEMS SECURITY

1. REASON FOR ISSUE: To revise Department of Veterans Affairs (VA) automated information systems (AIS) security policy, formerly contained in VA Manual MP-6, Part I, Chapter 2. This directive implements recommendations of VA's Security Working Group (SWG).

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This directive sets forth policies and responsibilities for protecting AIS and telecommunications resources from unauthorized access, disclosure, modification, destruction or misuse. The directive contains:

a. Identification of eight primary elements applicable throughout the Department and to the security of all automated information collected, transmitted, used, processed, stored, or disposed of, by or under the direction of VA or its contractors, or other government agencies under computer matching.

b. Responsibilities for implementing and managing the AIS security program.

c. References related to AIS security.

3. RESPONSIBLE OFFICE: The Associate Deputy Assistant Secretary for Information Resources Management Policy & Program Assistance (045A), Office of the Deputy Assistant Secretary for Information Resources Management.

4. RELATED HANDBOOK: VA Handbook 6210, Automated Information Systems Security Procedures.

5. RESCISSIONS: MP-6, Part I, Chapter 2, Change 18, dated February 24, 1992.

CERTIFIED BY:

**BY DIRECTION OF THE SECRETARY
OF VETERANS AFFAIRS:**


Nada D. Harris
Deputy Assistant Secretary for
Information Resources Management


DC Mark Catlett
Assistant Secretary for
Management

Distribution: RPC: 6500
FD

AUTOMATED INFORMATION SYSTEMS SECURITY

1. PURPOSE

a. This directive establishes policy and responsibilities for the security of automated information systems (AIS) within the Department of Veterans Affairs (VA). The Department-wide program is designed to protect all AIS and telecommunications resources from unauthorized access, disclosure, modification, destruction, or misuse. These provisions comply with Federal AIS security laws and regulations, including the Computer Security Act of 1987 (PL 100-235), and the requirements of Office of Management and Budget (OMB) Circular A-130 and its appendices.

b. The provisions of this directive are applicable throughout the Department, and to the security of all automated information collected, transmitted, used, processed, stored, or disposed of, by or under the direction of VA or its contractors, or other government agencies under computer matching. Computer matching is defined in 5 U.S.C. Section 552a (a) (8).

2. POLICY

a. VA shall establish, maintain, and enforce a comprehensive security program to assure an adequate level of security protection for all AIS, whether maintained in-house or by a contractor on behalf of, or for the benefit of the Department. Specifically, VA shall assure that AIS operate effectively and accurately, using appropriate technical, personnel, administrative, environmental, and telecommunications safeguards. VA will maintain the continuity of operations of AIS supporting critical Department functions.

b. Administration heads, Assistant Secretaries, and other key officials shall develop, implement, maintain, and enforce a structured program to safeguard all AIS assets for which they are responsible. The AIS security program will be designed to ensure the continued operation of mission-critical activities and will implement measures to prevent unauthorized access to and use of automation and telecommunications resources.

c. Responsible program offices will perform reviews and certifications of AIS at least every three years. They shall evaluate the adequacy and proper functioning of security safeguards and shall identify vulnerabilities that could heighten threats to sensitive data or valuable resources. Security or other control weaknesses shall be included in the Federal Managers Financial Integrity Act Report, an annual internal control report, required by OMB Circular A-123.

d. The VA AIS security program shall, at a minimum, include the following components:

(1) Computer Systems Security

(a) A management control process shall be established to assure that appropriate safeguards are incorporated into new or redesigned AIS applications. Principal users of AIS applications shall evaluate and determine the data protection requirements for new applications and for existing AIS applications that are undergoing substantial modifications. For those applications considered sensitive, the management control process shall, at a minimum, include sensitive systems security plans, security specifications, design reviews, and systems tests. These requirements are detailed in OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, and in OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information. The life cycle documentation requirements of the sensitive system shall be consistent with the requirements outlined in the document "Model Framework for Management Control over AIS."

(b) Department components shall comply with VA Directive 0710, Security, for the determination of position sensitivity designations, risk levels and necessary screening of both Federal and contractor personnel.

(c) Responsibility for the security of each office or facility and its computer systems (personal computers, local area networks, mini and mainframe computers, associated equipment, and the automated information) shall be assigned. The responsible official shall assign information security duties to personnel who do not have management or operational responsibility for the AIS, but who do possess expertise in information resources management and security matters.

(d) Sensitivity analysis of the data in VA records and information systems is the responsibility of the organizational element that develops the data, system of records, or other information to accomplish its mission or purpose. The information owner determines the sensitivity of information and the appropriate protection to be afforded, as well as who is authorized access and what functions persons granted access are permitted to perform. The owner of information requiring protection authorizes its release to users, establishes requirements for protection, and endorses the level of protection provided by information custodians. In determining the appropriate level of sensitivity and the degree of protection required, information owners should consider the specific criteria presented below and the systems of which the information is a part. Some information is not sensitive by itself, but becomes sensitive when combined with other information. Therefore, sensitivity determinations should be made on the basis of judgment that weighs various factors including, but not limited to, the following:

1. The nature of the information being processed or transmitted.
2. The degree of access control and physical protection in effect.
3. The degree to which information is accessible by remote terminals, other systems or networks.
4. The extent to which violations or attempted violations are detectable.
5. The extent to which backup is available.

(e) Each responsible security official shall oversee the general assessment of risks and take actions to manage them to ensure that safeguards are incorporated into existing facilities, new facilities and their computer systems. These analyses should be risk-based and take into account the size and sensitivity of the system or facility. The results of these analyses shall be maintained in a report at the facility. The assessment results will be considered when certifying applications processed at the facility and on these systems according to the standards recommended in FIPS PUB 102, Guideline for Computer Security Certification and Accreditation, and when evaluating controls over facility and system management in accordance with OMB Circular A-123, Internal Control Systems. The major factors in this risk management determination are: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Risk assessments should be performed:

1. Prior to the approval of design specifications for new facilities or the acquisition of new computer systems.
2. Whenever there is a significant change to the facility or its computer systems.
2. A minimum frequency of once every three years

(f) Disaster recovery and continuity of operations plans shall be maintained for each facility and computer system. These plans are required to be documented for

computer systems which support essential Department functions and must be fully documented and operationally tested periodically.

(g) Appropriate technical, administrative, physical, and personnel security requirements shall be included in all specifications for the acquisition, operation or maintenance of facilities, equipment, software, and related services, whether procured through VA, General Services Administration (GSA), or another agency. The management official responsible for security at the facility making the acquisition will review and approve these security requirements.

(h) Removal of sensitive information on automatic data processing equipment (ADPE) storage media shall be conducted prior to disposal of the equipment. VA shall ensure that all offices and facilities include policy and procedures in their computer security programs for the protection of sensitive information during the disposal of ADPE storage media. Procedures for implementing the policies in this section are found in VA Handbook 6210, Chapter 6.

(i) Computer virus and malicious computer program code prevention, detection and elimination policies and procedures shall be developed and implemented by VA program and staff offices. Procedures for implementing the policies in this section are found in VA Handbook 6210, Chapter 4.

(j) Electronic mail and information messaging applications and systems shall only be used for authorized government purposes and shall contain only non-sensitive information unless the data, and accompanying passwords or other authentication mechanisms, are protected with an approved encryption algorithm. Electronic mail systems provide the means for communicating information (excluding voice) by sending, storing, processing, and retrieving the information. This allows users to communicate under specified conditions. Electronic message systems (e.g., Personal Computer Telecommunications System) are electronic mail systems that incorporate the additional feature where the central facility assumes active responsibility for delivering the message to the intended addressee rather than the passive role an electronic mail system, which delivers messages in response to a request by an addressee. This policy does not cover privacy and confidentiality issues of records in automated information systems; refer to Records and Information Management Handbook 6300.1 for records management policy and procedures. VA Directive 6301, Electronic Mail Records, establishes the policies and responsibilities for managing the creation, maintenance, use, and disposition of federal records created or received in electronic mail applications.

(2) Network Security. Proper safeguards shall be implemented on VA communication networks that transport or provide access to sensitive information. VA security requirements must be satisfied before full access to the Internet system is granted through VA ADPE. VA Directive 6102, VA Internet Policy, and Appendix A, governs VA access to the Internet system and specifies the minimum security requirements for establishing Internet gateway connections. Sensitive information transported over VA wide area data communications networks shall be protected by a NIST-approved (National Institute of Standards and Technology) encryption method. Procedures necessary to comply with the policies in this section, including mandatory features to be implemented in VA networks or interfaces to VA networks, are found in VA Directive 6100, Telecommunications and related handbook. Required security procedures for establishing, operating, or connecting to a local area network (LAN) are found in VA Handbook 6210, Chapter 7.

(3) Security Awareness and Training. A program shall be established to assure that Department and contractor personnel are aware of their security responsibilities and know how to fulfill them. Users of information technology systems should be apprised of the vulnerabilities of such systems and trained in techniques to enhance security. Each employee shall attend an initial AIS security awareness training before accessing VA systems and receive other AIS security training on an annual basis; this attendance shall be documented and placed in their official personnel file. As part of an initial security training course or instruction, rules of behavior for systems shall be included that specify limits on interconnections to other systems, consequences of behavior not consistent with

system rules and basic computer security principles. Specific security training as prescribed in FPM Bulletin No. 410-131, Training Requirement for the Computer Security Act, dated January 1, 1992 shall be conducted for all VA employees and contractors as described in VA Handbook 6210, Chapter 2. The Department Information Resources Security Officer (IRSO) shall develop and issue basic computer security principles to each VA organization to include in their security awareness and training.

(4) Security Incident Reporting. VA shall establish, maintain, and enforce an AIS security incident reporting and response capability to ensure that computer security incidents are detected, reported, and corrected at the earliest possible time. The incident reporting and response process shall be designed to detect and respond to AIS security incidents as they occur, assist in preventing future incidents from occurring through awareness, contain necessary response mechanisms to deal with incidents, and support security controls and procedures. Procedures for implementing the policies in this section are found in VA Handbook 6210, Chapter 3.

(5) Copyright. All VA employees shall ensure that government-acquired commercial software is used only in accordance with licensing agreements. It is the responsibility of management and individual employees to ensure that proprietary software is properly licensed before being installed on VA equipment. VA facilities and organizations should consider acquiring special purpose software to perform software audits on each PC in the facility or organization. This policy does not apply to software developed by or specifically for the use of the Department. Procedures for implementing the policies in this section are found in VA Handbook 6210, Chapter 5.

(6) Contingency Planning. AIS contingency plans shall be the responsibility of end users, where applications computing is performed or directly used by the users. The plans shall be developed and maintained by the end user or a designated vendor or contractor approved by the end user. This responsibility extends to individual personal computer (PC) usage by or on behalf of VA. Contingency plans are an integral part of business resumption planning which is the facility's or organization's plan to resume business or services. Contingency plans for applications and systems, when maintained at a VA automation center, are the joint responsibility of the VA program office responsible for the system, or a designated group within the responsible program office, and the VA facility. Such plans shall be consistent with disaster recovery and continuity of operations plans maintained by the facility at which the application is processed. Procedures for implementing the policies in this directive are found in VA Handbook 6210, Chapter 1.

(7) Physical Security. Policies and procedures shall be developed and implemented by VA program and staff offices which require the application of physical devices and control measures to safeguard information assets and sensitive information. Federal Information Processing Standards (FIPS) Publication 31, establishes guidelines for automated data processing physical security and risk management.

(8) Access Control to Employee Records. Employee records, in hard copy or automated forms, are sensitive records and must be afforded the same protection as veterans' records. VA employees are entitled to review the information contained in their own medical, benefits, or other records maintained in VA automated systems. In accordance with the Privacy Act of 1974, this access request must be authorized and follow a "reasonable" procedure for disclosure of employee record information. This process shall include a requirement that the employee seeking access to his/her record notify, in writing, the organizational official responsible for release of Privacy Act-covered information prior to accessing the record. This authorization process shall be supplemented by the requirement for the creation of an audit trail of access to sensitive records. This prior notification requirement does not pertain to applications such as IFCAP, Leave Balance and Service Record Screen options, where the record owner (an employee) is the primary source of input to the

application. Except for these "self-service" input systems, employees shall be granted "read-only" access.

3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs.** The Secretary has designated the Chief Information Officer (CIO) as the senior agency official responsible for the Department's IRM program.

b. **Chief Information Officer.** The VA CIO will, through the Deputy Assistant Secretary for Information Resources Management (DAS/IRM):

(1) Implement the Computer Security Act of 1987, OMB Bulletins related to that Act, OMB Circulars A-123 and A-130, and their appendices, and other directives issued by the National Institute of Standards and Technology, General Services Administration, or the National Telecommunications and Information Security Committee.

(2) Develop and issue VA AIS security policies and regulations.

(3) Ensure that appropriate criticality and sensitivity levels and controls for selection and protection of information processed or handled by the Department are identified.

(4) Periodically review new and ongoing IRM projects and computer information systems throughout the Department to assess their compliance with the provisions of this directive, and ensure that AIS security requirements are incorporated in VA-developed or acquired hardware, system; and applications software, and VA-wide telecommunications networks.

(5) Designate an Information Resources Security Officer (IRSO) for the Department.

c. **The Inspector General.** This Office is responsible for:

(1) Conducting and supervising information security audits and providing follow-up regarding progress in implementing security enhancement and corrective actions.

(2) Conducting or providing oversight for criminal investigations as appropriate.

(3) Developing composite analyses of risk assessments conducted as part of the Department security program, identifying patterns of weaknesses, and recommending preventive measures and improvements.

d. **The Deputy Assistant Secretary for Security and Law Enforcement.** This Office is responsible for:

(1) Developing and implementing Department-wide policy regarding position sensitivity and its applicability to all national security/public trust positions

(2) Processing requests for security clearances for personnel designated to national security/public trust positions.

(3) Implementing the Department Personnel Security Program.

(4) Providing/issuing policy, operating procedures, and technical standards for the protection of classified national security information.

(5) VA Emergency Preparedness Program as it involves VA's Information Security Programs.

(6) Developing and implementing Department-wide policy regarding physical security at all VA facilities.

e. The General Counsel. This Office is responsible for:

(1) Interpreting laws, regulations, and directives applicable to VA AIS security activities.

(2) Rendering legal advice and services in the area of AIS security upon request of Administration Heads, Assistant Secretaries, and other key officials.

f. Deputy Assistant Secretary for Human Resources Management. This Office is responsible for:

(1) Developing and recommending VA-wide policy related to personnel suitability.

(2) Interpreting Federal suitability policy.

(3) Recommending and advising on retention, reassignment, adverse or other actions against individuals for violation of security policies, including coordination with the Office of the Inspector General.

g. Administration Heads, Assistant Secretaries, and Other Key Officials. These Offices are responsible for:

(1) Safeguarding AIS assets under their control, including those shared with or operated by other VA organizations, other Federal agencies, contractors, or State or local governments.

(2) Appointing an Information Security Officer (ISO) and alternate for their organization.

(3) Allocating sufficient funds, personnel, and management support to implement the provisions of this directive, and assure compliance with Federal and VA AIS security requirements.

(4) Ensuring that the designated ISO reports major violations of AIS security policies, procedures, and practices to the VA IRSO.

(5) Ensuring that personnel within their organizations attend AIS security orientation and functional training, in accordance with Department policy and OPM regulation. Ensuring that all personnel within their organizations attend initial security training before they are granted access to VA systems, and at least once each year thereafter.

(6) Implementing security plans for general support systems and major applications as required by OMB Circular A-130, Appendix III.

(7) Ensuring that AIS security policies and procedures are developed and periodically updated, and that contingency plans are developed, tested, and periodically certified as accurate and current.

(8) Ensuring that a security certification review is made of operational sensitive systems, or those under development to determine adequacy of controls and security safeguards. The review should follow provisions of OMB Circular A-130, Appendix III.

(9) Ensuring that risk analyses are performed and security plans developed for projects involving development of new systems, acquisitions of equipment or services, and preparation of Requests for Proposals (RFPs) and other procurement documents which must specify AIS security requirements, activities and related deliverables.

4. REFERENCES

- a. Computer Security Act of 1987, PL 100-235, 101 Stat. 1724.
- b. Electronic Communications Privacy Act of 1986, Public Law 99-08. 100 Stat. 1848.
- c. Executive Order 10450 Security Requirements for Government Employment.
- d. FIPS PUB (Federal Information Processing Standards Publication) 1-1-3 Guideline: American National Dictionary For Information Systems.
- e. FIPS PUB 31, Guidelines for Automated Data Processing Physical Security and Risk Management.
- f. FIPS PUB 39, Glossary for Computer Systems Security.
FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 197::
- h. FIPS PUB 46-1, Data Encryption Standard (DES).
1. FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification
- j. FIPS PUB 65, Guidelines for Automated Data Processing Risk Analysis.
- k. FIPS PUB 73, Guidelines for Security of Computer Applications, dated June 30, 1980.
 1. FIPS PUB 81, DES Modes of Operation.
- m. FIPS PUB 83, Guidelines on User Authentication Techniques for Computer Network Access Control, dated September 29, 1980.
- n. FIPS PUB 87, Guidelines for ADP Contingency Planning.
- o. FIPS PUB 88, Guidelines on Integrity Assurance and Control in Database Administration, dated August 4, 1981.
- p. FIPS PUB 102, Guidelines for Computer Security Certification and Accreditation, dated September 27, 1983.
- g. FIPS PUB 112, Password Usage, dated May 30, 1985.
- r. FIPS PUB 113, Computer Data Authentication, dated May 30, 1985.
- s. Model Framework for Management Control over Automated Information Systems, January 1988; President's Council on Integrity and Efficiency and President's Council on Management Improvement.
- t. MP-I, Part II, Chapter 13, Emergency Preparedness Planning (VA Directive 0320).
- u. NISTIR 4659, Glossary of Computer Security Technology
- v. NISTIR 5153, Minimum Security Requirements for Multi-User Operating Systems.
- w. OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, July 9, 1990.

- x. OMB Circular A-130, Management of Federal Information Resources, particularly Appendix III, Security of Federal Automated Information Systems, February 8, 1996.
- y* OMB Circular A-123 Revised, Internal Control Systems, August 4, 1986.
- z. OMB Privacy Act Implementation Guidelines, and Responsibilities published at Federal Register Vol. 40, Pages 28948-28978, **July 9, 1975.**
- aa. OMB 1975 Privacy Act Supplementary Guidance published at Federal Register Vol. 40, pages 56741-56743, December 4, 1975.
- bb. VA Directive and Handbook 0710, Security.
- cc. VA Directive 6301, Electronic Mail Records.
- dd. 5 CFR Parts 731, 732, and 736.
- ee. 36 CFR Part 1234, Electronic Records Management, 60 Fed. Reg. 44634 (1995).
- ff. 41 CFR (Code of Federal Regulations) Chapter 201, Federal Information Resources Management Regulation (FIRMLI).
- gg* 5 U.S.C. 552, Freedom of Information Act.
- hh. 5 U.S.C. 552a, Privacy Act of 1974.
- ii. 18 U.S.C. 1029-1030, Fraud and Related Activity in Connection with Access Devices and Computers.
- jj. 38 U.S.C. 5701, Confidential Nature of Claims.
- kk. 38 U.S.C. 5705, Confidentiality of Medical Assurance Records.
- ll. 38 U.S.C. 7332, Confidentiality of Certain Medical Records.