U.S. Department of Energy

Washington, D.C.

ORDER

HQ 5636.1

7-10-85

SUBJECT: SECURITY REQUIREMENTS FOR CLASSIFIED AUTOMATIC DATA PROCESSING SYSTEMS

1. PURPOSE. To establish and describe the computer security program for classified automatic data processing (ADP) systems at the Department of Energy (DOE) Headquarters.

2. SCOPE. The provisions of this Order apply to all Headquarters Elements, and to Headquarters contractors and subcontractors who process, store, or produce classified data on Headquarters ADP systems, as provided by law and/or contract and as implemented by the appropriate contracting officer.

3. EXCLUSION. The provisions of this Order do not apply to the Energy Information Administration. The Energy Information Administration is subject to the provisions of DOE 5636.2.

4. REFERENCES.

a. Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1, "Security of. Federal Automated Information Systems," of 7-27-78, which promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies.

b. Executive order 12356, "National Security Information," of 4-2-82, 3 C.F.R. 166 (1983), which authorizes classification of information pertaining to national security.

c. Public Law, Sections 141-146, 42 U.S.C 2161-2166, The Atomic Energy Act of 1954, as amended (hereinafter referred to as the Atomic Energy Act), which provides the policy to control the dissemination and declassification of Restricted Data in such a manner as to ensure the common defense and security.

d. DOE 1360.2, COMPUTER SECURITY PROGRAM FOR UNCLASSIFIED COMPUTER SYSTEMS, of 3-9-79, which establishes DOE-wide policies and procedures for developing, implementing, and administering a program for safeguarding DOE computer systems, and in particular, DOE sensitive unclassified information.

e. DOE 5636.2, SECURITY REQUIREMENTS FOR CLASSIFIED AUTOMATIC DATA PROCESSING SYSTEMS, of 1-10-80, which establishes uniform requirements, policies, and

DISTRIBUTION:
All Headquarters Elements

INITIATED BY:
Office of Computer Services and Telecommunications Management

responsibilities for the development and implementation of a DOE program to ensure the security of information stored in classified ADP systems.

f. DOE 5636.4, SECURITY MANUAL FOR CLASSIFIED AUTOMATED DATA PROCESSING SYSTEMS, of 7-13-83, which establishes uniform procedures for techniques to be used when applying computer security measures for the protection of classified information being processed, stored, or produced on ADP systems.

g. DOE 5631.2, PERSONNEL SECURITY PROGRAM, of 11-13-80, which implements the provisions of the Atomic Energy Act and Executive Orders 10450, 10865, and 12065.

h, Federal Information Processing Standards Publication 73, "Guidelines for Security of Computer Applications," of 6-80, which describes the technical and managerial decisions that should be made in order to ensure that adequate controls are included in new and existing computer applications to protect them from natural and man-made hazards and to assure that critical functions are performed correctly.

5. DEFINITIONS.

a. Accreditation is the authorization and approval granted to an ADP system or network to process classified data. It is based on the certification made by designated technical personnel confirming that the design and implementation of the system satisfies previously specified technical requirements for adequate security.

b. Administrative Security is operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for classified information.

c. ADP System Security is all physical, procedural, and technological safeguards and controls established and applied to computer hardware, software, facilities, and data to ensure the security, reliability, integrity, and availability of classified information.

d. Authentication is the act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

e. Certification is the technical evaluation, made as part of the accreditation process, that establishes the extent a particular computer system or network design and implementation meet a specified set of security requirements.

f. Classified ADP System is any system that processes, stores, or produces classified information. This system may include any large resource-sharing computer system or smaller automated office support system regardless of complexity, functional use, or configuration. An automated office support system can include word processors, microprocessors, controllers, or other special type systems, connected via local area networks or other means, or operated in the stand-alone mode.

g. Classified Information is Restricted Data and Formerly Restricted Data, pursuant to the Atomic Energy Act, and National Security Information that has been classified in accordance with Executive Order 12356 or other pertinent Executive orders to require protection against unauthorized disclosure.

h. Degauss is to apply an electrical or permanent magnetic field for the purpose of erasing magnetic recording media.

i. Overwrite is to record into an area of computer memory so as to completely replace the data that was previously stored there.

j. Physical Security is the use of locks, guards, badges, alarms, and similar measures to control access to the computer and related equipment. It also includes the measures required for the protection of the-structures housing the computer, related equipment, and their contents from espionage, theft, or damage due to-accident, fire, and environmental hazards.

k. Risk Analysis is an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on the estimated probabilities of the occurrence of those events.

l. System Owner is a DOE employee who has responsibility for creating, maintaining, and updating a data file application system and who is the approving authority for information to be processed and for access permission.

m. System User is an individual with a bona fide need to access data within Headquarters computer systems or use the products and components of these systems and who, consequently, has been granted access rights to the data and products.

6. OBJECTIVES. To ensure the security of information stored in Headquarters classified ADP systems; and to implement DOE 5636.2 and DOE 5636.4.

7. RESPONSIBILITIES,

a. Director of Administration through the Director of Computer Services and Telecommunications Management (MA-25).

(1) Establishes, manages, and provides overall direction and control for the Headquarters classified computer security program.

(2) Develops and maintains policies, directives, and procedures necessary to implement the Headquarters classified computer security program in accordance with the procedures specified in this Order.

(3) Appoints a computer security operations manager from MA-25 and notifies the computer security program manager in the Office of Safeguards and Security (DP-34) of the appointment.

b. Heads of Headquarters Elements Having Responsibility for Classified ADP Systems or Installations at Headquarters.

(1) Appoint a computer systems security officer for each system and notify the computer security operations manager in writing of the appointment. A computer systems security officer may be given the responsibility for one or more systems.

(2) Ensure compliance with the procedures specified in this Order.

(3) Include in the scope of work of those contracts under their cognizance a requirement to comply with the provisions of this Order.

c. Computer Security Operations Manager (MA-25).

(1) Is directly responsible for the establishment and management of the Headquarters classified ADP security program.

(2) Coordinates all Headquarters classified ADP security activity to ensure compliance with DOE 5636.2, DOE 5636.4, and other applicable Federal directives on classified computer security.

(3) Ensures that Heads of Headquarters Elements who have responsibility for a classified ADP system or facility appoint a computer systems" security officer for each classified system or facility and evaluate the performance of these officers in regard to their duties as computer system security officers.

(4) Evaluates and approves each classified ADP protection plan before computer security measures detailed in the plan are implemented.

(5) Approves the selection, acquisition, distribution, implementation, and safeguarding of ADP security measures for Headquarters classified ADP systems.

(6) Ensures that each Headquarters Element having responsibility for a classified ADP system periodically conducts a security test to determine the adequacy of safeguards provided for each classified ADP system under their control and determines the frequency of security tests for each classified system.

(7) Evaluates security tests conducted on classified ADP systems and ensures that appropriate modifications are made to make the system comply with DOE-wide policies, standards, and procedures for classified ADP systems.

(8) Accredits Headquarters classified ADP systems after the computer systems security officer has certified that the design and implementation of the computer security measures applied to a classified ADP system meet security requirements as set forth in DOE 5636.4 and specified by the computer security operations manager.

(9) Concurs in the emanations security measures approved by the computer systems security officer for a classified ADP system or facility.

(10) Conducts annual security evaluations of each classified ADP system or facility to ensure that uniform computer security standards are being applied and utilized properly.

(11) Coordinates the classified ADP security .program with the unclassified computer protection program.

d. Computer Systems Security Officer.

(1) Ensures that adequate security measures are applied to safeguard classified ADP systems, and the applied measures are cost effective.

(2) Certifies to the Headquarters computer security operations manager that the ADP system has been given the required security protection.

(3) Analyzes the security requirements for the protection of classified data in the ADP system and prepares the ADP protection plan, which includes the following information:

(a) The manufacturer and model identity of all computer systems that process sensitive data, plus name and brief description of sensitive application software addressed by DOE 1360.2 and DOE 5636.2.

(b) A summary of the management control process describing the attendant administrative, technical, physical, and personnel safeguards employed within the site. If special provisions apply to selected systems or applications, this information may be appended and appropriately identified.

(c) A summary of the contingency and post-disaster recovery procedures.

(d) A summary of the result of the latest risk analysis and audit reviews.

(e) A summary of training provided to both computer facility and user organization personnel regarding this program.

(f) The identity of any internally developed or proprietary software to be required partially or totally to improve the computer protection program.

(g) Copies of certification/recertification documents or summaries thereof.

(h) Name of the responsible program official and assistants, and emergency notification procedures.

(i) Percentage and level of classification and type of information being handled.

(j) Description of the communications network for the system, both internal and external.

(k) A statement of the threat to the system or facility.

(4) Approves and controls personnel and physical access to the computer operations area and to remote terminals.

(5) Prescribes, implements, and approves methods to control remote terminal access and techniques to disconnect remote terminals.

(6) Approves and implements authentication methods for the ADP facility, including the distribution and control of passwords within the ADP system.

(7) Approves emanations security measures for the ADP system or facility.

(3) Provides a system for monitoring and auditing use of the ADP system to prevent or detect security violations.

(9) Ensures that established administrative procedures are being used properly. These include procedures governing marking, handling, and destruction of classified ADP system output and removal of computer equipment from the security area.

(10) Approves software controlled overwriting techniques used to declassify computer memory or online disk storage. Approves degaussing equipment used to erase and declassify offline magnetic tapes and disks.

8. PROCEDURES.

a. Heads of all Headquarters Elements having responsibility for classified ADP systems or facilities will notify the computer security operations manager when they appoint a computer systems security officer for one or more of their classified systems or facilities.

b. Computer systems security officers will prepare an ADP protection plan for each classified system or facility for which they are responsible. The ADP protection plan shall include the information specified on page 5, paragraph 7d(3).

c. Each computer systems security officer shall forward each ADP protection plan to the computer security operations manager for review and approval.

d. The computer security operations manager shall review all ADP protection plans prepared by system or facility computer systems security officers to ensure that adequate security measures have been applied. Inadequate protection plans shall be returned to the originating office for revision. When a plan is approved, the computer security operations manager shall notify the originator of the approval.

e. Computer systems security officers shall arrange for accreditation process ADP security tests. ADP security tests shall be conducted on classified systems described in ADP protection plans approved by the computer security operations manager. ADP security tests shall consist of the preparation of a test plan by the system owner, conduct of the test by a security test team independent of the system owner's organization, and preparation of a security test analysis report by the test team. The test for each classified system shall be performed to verify the adequacy of the security controls applied to the system and to ascertain that the

controls function as intended. The security test analysis report on each test shall be forwarded to the appropriate computer systems security officer for evaluation.

f. Computer systems security officers shall review security test analysis reports prepared by security test teams to ensure that system security controls function as intended, and that all applicable security requirements are met. Systems failing the security test shall be modified and retested.

g* Computer systems security officers shall certify to the computer security operations manager that systems meet all applicable security requirements and that system security measures are adequate to protect the information contained in the systems, once the security test for each system is completed and approved.

h. The computer security operations manager shall review all relevant protection plans, documentation, and test results once each computer system security officer has certified that a system meets all applicable security requirements. If the system contains intelligence data, the computer security operations manager shall forward the appropriate system documentation, protection plans, and test reports to the senior intelligence officer, Deputy Assistant Secretary for Intelligence (DP-40), for concurrence in the accreditation process. If the senior intelligence officer concurs, the appropriate system documentation, protection plans, and test reports are returned to the computer security operations manager. If the senior intelligence officer does not concur, the computer security operations manager shall notify the computer systems security officer of the system to that effect and the computer systems security officer shall ensure that any security deficiencies are corrected.

i. The computer security operations manager shall accredit each classified ADP system or facility following certification by the computer systems security officer of that system or facility and, if the system contains intelligence data, concurrence by the senior intelligence officer. The computer security operations manager shall notify the computer systems security officer of that system or facility, the senior intelligence officer if appropriate, and the system owner, of the accreditation.

j. The computer security operations manager shall review each classified ADP system or facility annually in order to ensure that classified systems and facilities maintain adequate security controls and meet all applicable security requirements. If security measures are adequate for each system or facility, the computer security operations manager shall reaccredit the system or facility; if controls are inadequate for any of the systems or facilities, the computer systems security officer of the inadequate system or facility shall be notified of the Deficiencies and be required to arrange for them to be corrected.

HARRY L. PEEBLES
Deputy Director of Administration