U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5639.6

9-15-92

SUBJECT: CLASSIFIED COMPUTER SECURITY PROGRAM

1. PURPOSE. To establish uniform requirements, policies, responsibilities, and procedures for the development and implementation of a Department of Energy (DOE) Classified Computer Security Program to ensure the security of classified information in automated data processing (ADP) systems.

2. CANCELLATION. DOE 5637.1, CLASSIFIED COMPUTER SECURITY PROGRAM, of 1-29-88.

3. SCOPE. The provisions of this Order apply to all Departmental Elements and contractors who process, store, transfer, or provide access to classified information on an ADP system, as provided by law and/or contract and as implemented by the appropriate contracting officer.

4. POLICY

   a. It is the policy of DOE that classified information and classified ADP systems shall be protected from unauthorized access (including the enforcement of need-to-know protections), alteration, disclosure, destruction, penetration, denial of service, subversion of security measures, or improper use as a result of espionage, criminal, fraudulent, negligent, abusive, or other improper actions. The DOE shall use all reasonable measures to protect ADP systems that process, store, transfer, or provide access to classified information or Protect as Restricted Data (PARD) to include, but not limited to, the following: physical security; personnel security; telecommunications security; administrative security; and hardware and software security measures. This Order establishes this policy and defines responsibilities for the development, implementation, and periodic evaluation of DOE's Classified Computer Security Program.

   b. The Classified Computer Security Program shall be consistent with Federal policies, procedures, and standards and shall progress toward parity with the criteria for protection of ADP systems as specified in Department of Defense (DOD) 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria."

5. BACKGROUND.

   a. For the purpose of this Order, classified information includes intelligence information, such as Sensitive Compartmented Information (SCI), when this information is processed, stored, transferred, or accessed on ADP systems. The requirements of

this Order also apply to information which is designated as PARD. This Order implements the appropriate requirements of the following statutes and directives:

(1) Atomic Energy Act of 1954, as amended.

(2) Executive Order 12356 National Security Information, of 4-2-83.

(3) National Security Directive 42, National Policy for Security of National Security Telecommunications and Information Systems, of 7-5-90.

(4) Director of Central Intelligence Directive 1/16 (DCID 1/16), Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks, of 7-19-88.

(5) Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," of 12-12-85.

b. This Order establishes the baseline security requirements for the protection of classified ADP systems. This Order is to be used in conjunction with DOE 6430.1A, GENERAL DESIGN CRITERIA, to provide a comprehensive protection program for ADP systems. It also provides the security considerations for the acquisition of new ADP systems. As such, the requirements are minimum standards for the design, procurement, and implementation of ADP systems processing, storing, transferring, or providing access to classified information.

c. This Order is to be used in conjunction with DOE 1360.1A, ACQUISITION AND MANAGEMENT OF COMPUTING RESOURCES and DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, to provide a DOE program for computer security.

d. Unclassified Controlled Nuclear Information (UCNI) is to be protected as specified in DOE 1360.2B.

e. At a minimum, protection of a classified ADP System with multiple users, and no common need-to-know, shall meet the protection level prescribed in National Telecommunications and Information Systems Security Policy (NTISSP) 200.

f. The requirements of this Order apply to ADP systems that process intelligence information. However, they may not fully represent the protection requirements for processing intelligence information. Further requirements may be established by directives of the intelligence community or DOE Orders established by the Senior Intelligence Officer within the Department.

6. APPLICABILITY. This Order is applicable to all ADP systems, including word processors, microprocessors, personal computers, controllers, Automated Office Support Systems (AOSS), memory typewriters, and other stand-alone or special systems that process, store, transfer, or provide access to classified information. This Order also applies to sensitive, mission essential, and other unclassified information processed on classified ADP systems.

a. The term ADP system is used throughout this Order to mean the computer hardware, firmware, telecommunications, interconnections with other ADP equipment (e.g., networks), and the entire collection of software that is executed on that hardware. While the term "system" is occasionally used to refer to a set of programs that implement some function (e.g., a financial management package), computer security must be applied to the complete ADP system.

b. The terms "data," "information," "material, " "documents," and "matter" are considered synonymous and used interchangeably in this Order. They refer to all data regardless of its physical form (e.g., data on paper printouts, on tapes, on disks or disk packs, in memory chips, in Random Access Memory (RAM), in Read Only Memory (ROM), on microfilm or microfiche, on communication lines, and on display terminals).

7. REFERENCES. See Attachment 1.

8. DEFINITIONS. See Attachment 2.

BY ORDER OF THE SECRETARY OF ENERGY:

DOLORES L. ROZZI
Director of Administration
and Human Resource Management

THIS PAGE MUST BE KEPT WITH DOE 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM.

DOE 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM, HAS REVISED DOE 5637.1 TO REFLECT ORGANIZATIONAL TITLE, ROUTING SYMBOL, AND OTHER EDITORIAL REVISIONS REQUIRED BY SEN-6. SOME SPECIFIC AREAS WHICH HAVE BEEN REVISED ARE THE FOLLOWING: DEFINITIONS TO COINCIDE WITH THE SAFEGUARDS AND SECURITY DEFINITIONS GUIDE; CHAPTER I, PARAGRAPHS 1 THROUGH 4; ATTACHMENT I-1 HAS BEEN DELETED; CHAPTER III, PAGE III-4, PARAGRAPH 3c HAS BEEN ADDED AND PAGE 111-10, SUBPARAGRAPH h. DUE TO THE NUMBER OF PAGES AFFECTED BY THESE REVISIONS, THE ORDER HAS BEEN ISSUED AS A REVISION. THE NUMBER HAS BEEN CHANGED TO DOE 5639.6 TO REFLECT ITS PROPER DESIGNATION WITHIN THE INFORMATION SECURITY SERIES OF ORDERS. ANY QUESTIONS OR CONCERNS RELATING TO THE ISSUANCE OF THIS REVISED ORDER SHOULD BE DIRECTED TO THE OFFICE OF SECURITY AFFAIRS.

REFERENCES

1. Atomic Energy Act of 1954, as amended, which provides the policy to control the dissemination and declassification of Restricted Data (RD) in such a manner as to assure the common defense and security.

2. Executive Order 12356, "National Security Information," of 4-6-82, which prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

3. National Telecommunications and Information System Security Publication (NTISSP) 200, National Policy on Controlled Access Protection, of 7-15-87, which establishes the requirement that all multi-user classified AIS systems, without a common need-to-know be protected at the C2 level, as defined in the DoD 5200.28 STD, TCSEC, by 7-92.

4. National Security Directive 42, "National Policy for Security of National Information Telecommunications and Information Systems", of 7-5-90, which provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which possess or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns responsibilities for implementation.

5. OMB Circular A-130, "Management of Federal Information Resources," of 12-12-85, which promulgates policy and responsibilities for the development and implementation of computer security programs by Executive Branch departments and agencies.

6. DOE 1324.2A, RECORDS DISPOSITION, of 9-13-88, which assigns responsibilities and authorities and prescribes policies, procedures, standards, and guidelines for the orderly disposition of the records of the Department of Energy.

7. DOE 1360.1A, ACQUISITION AND MANAGEMENT OF COMPUTING RESOURCES, of 5-30-86, which establishes Department of Energy policies and procedures for the acquisition and management of ADP systems.

8. DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, of 5-18-92, which establishes policy for safeguarding DOE ADP systems and, in particular, DOE sensitive unclassified information.

9. DOE 5300.1C, TELECOMMUNICATIONS, of 6-12-92, which establishes policy and general guidance for the use, review, coordination, and provision of telecommunications services for the Department of Energy.

10. DOE 5300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST) , of 5-18-92, which establishes the Department of Energy telecommunications program for emission security.

11. DOE 5300.3C TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, of 5-18-92, which establishes policy, responsibilities, and guidance concerning the communications security (COMSEC) aspects of telecommunications services of the Department of Energy, and implements the national telecommunications protection policy.

12. DOE 5300.4C, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS, of 5-18-92, which establishes policy for the Department of Energy concerning protected distribution systems used for the transmission of unencrypted classified or sensitive unclassified information related to national security.

13. DOE 5631.2C, PERSONNEL SECURITY PROGRAM, of 9-15-92, which establishes the policies, responsibilities, and authorities for implementing the Department of Energy personnel security program.

14. DOE 5632.1B, PROTECTION PROGRAM OPERATIONS, of 9-8-92, which prescribes policies for the physical protection of security interests and baseline physical protection standards.

15. DOE 5639.3, VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 9-15-92, which assures timely and effective investigation and other follow-up actions relating to violations of Federal laws and to certain losses of security interests.

16. DOE 5635.1A, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION, of 2-12-88, which provides guidance for the safeguarding and control of classified documents and information.

17. DOE 5639.5, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 8-3-92, which establishes the Department of Energy Technical Surveillance Countermeasures (TSCM) Program.

18. DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, of 12-31-91, which provides specific responsibilities, standards, policy, and procedures for the management of the Department of Energy classification system.

19. DOE 5670.1A, MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE, of 1-15-92, which provides for the management of, and assigns responsibilities for, the foreign intelligence activities of the Department of Energy.

20. DOE 6430.1A, GENERAL DESIGN CRITERIA, of 4-06-89, which establishes the general design criteria (GDC) for use in acquisition of the Department's facilities.

21. Director of Central Intelligence Directive 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks, of 7-19-88, which establishes policy for safeguarding intelligence information in ADP systems.

22. CSC-STD-002-85, "Department of Defense Password Management Guideline," of 4-12-85, which provides guidance related to the design, implementation, and use of password-based user authentication mechanisms.

23. NCSC TG 025, Version 2, "A Guide to Understanding Data Remanence in Automated Information Systems," of 9-91, which provides guidance and procedures for sanitizing magnetic storage media and for downgrading the security classification levels of such media.

24. DOD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," of 12-26-85, which defines the classes of computer security protection and provides a basis for the evaluation of effectiveness of security controls built into ADP systems.

DEFINITIONS

1. ACCESS CONTROL. The process of limiting access to information or to resources of an ADP System to only authorized users.

2. ACCESS CONYTROL MEASURES. Hardware and software features, physical controls, operating procedures, administrative procedures, and various combinations of these designed to detect or prevent unauthorized access to classified information, special nuclear materials, government property, ADP systems, facilities, or materials, and to enforce utilization of these means to protect DOE security interests.

3. ACCOUNTABILITY. The property which enables activities on an ADP System to be traced to individuals who can then be held responsible for their activities.

4. ACCOUNTABILI TY INFORMATION. A set of records, often referred to as an audit trail, that collectively provide documentary evidence of the processing or other actions related to the security of an ADP System.

5. ACCREDITATION. Accreditation is the formal declaration by a designated official that an automated information system or network is approved to operate: in a particular security mode; with a prescribed set of technical and nontechnical security safeguards; against a defined threat; in a given operational environment; under a stated operational concept; with stated interconnections to other automatic information systems or networks; and at an acceptable level of risk for which the accrediting official has formally assumed responsibility. The accreditation statement affixes security responsibility with the accrediting official and shows that due care has been taken for security.

6. ADMINISTRATIVE SECURITY The management procedures and constraints, operational procedures, accountability procedures, and supplemental controls established *to* provide an acceptable level of protection for classified information.

7, ADP FACILITY One or more rooms, generally contiguous, containing the elements of an ADP System.

8. ADP SYSTEM. An assembly of components of computer hardware, telecommunications, interconnections with other ADP equipment (e.g., networks), and the entire collection of software that is executed on that hardware. Included in this definition are word processors, microprocessors, personal computers, controllers, Automated Office Support Systems (AOSS), memory typewriters, and other stand-alone or special computer systems.

9. AUTOMATED OFFICE SUPPORT SYSTEMS (AOSS). Automated Office Support Systems, which include stand-alone microprocessors; word processors; memory typewriters; and terminals connected to mainframes.

10. ASSURANCE TESTING. A process used to determine that the safeguards and security features of a system are implemented and functioning as designed and that they are adequate for the proposed environment. This process may include hands-on functional testing, penetration testing and/or verification.

11. AUTHENTICATION. The act of verifying the claimed identity of an individual, station or originator.

12. AUTHORIZATION. Access rights granted to a user, program, or process.

13. CATEGORY. A grouping of information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have appropriate authorization (e.g., Restricted Data [RD]).

14. CERTIFICATION. Formal written assurance that, based on evaluation of security tests, the classified ADP System and its environment meet the security specifications outlined by the approved ADP Security Plan.

15. CLASSIFIED COMPUTER SECURITY PROGRAM All of the technological safeguards and managerial procedures established and applied to ADP Facilities and ADP systems (including computer hardware, software, and data) in order to ensure the protection of classified information.

16. CLASSIFIED INFORMATION. Certain information requiring protection against unauthorized disclosure in the interests of national defense and security or foreign relations of the United States pursuant to Federal statute or executive order. The Term includes Restricted Data, Formerly Restricted Data, and National Security Information. The potential damage to the national security of each is denoted by the classification levels Top Secret, Secret, or Confidential.

17. CLEARING. The overwriting of classified information on magnetic media such that the media may be reused. (This does not lower the classification level of the media.) Note: Volatile memory can be cleared by removing power to the unit for a minimum of one minute.

18. COMMUNICATION SECURITY (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the Possession and study of telecommunications. or to-mislead unauthorized persons in their interpretation of the results of such possession and study.

19. COMPROMISE. The disclosure of classified data to persons who are not authorized to receive such data.

20, COMPPROMISING EMANATIONS (TEMPEST). Unintentional signals that, if intercepted and analyzed, would disclose classified information being transmitted, received, handled, or otherwise processed by any information processing equipment.

21. COMPUTER SECURITY INCIDENT. An adverse event associated with an ADP System(s): (a) that is a failure to comply with security regulations or directives; (b) that results in attempted, suspected, or actual compromise of classified information; or (c) that results in the waste, fraud, abuse, loss, or damage of government property or information.

22. CONFIGURATION MANAGEMENT. Control of changes made to an ADP System's hardware, software, and documentation (including an inventory of the system elements) throughout the development and operational life of the ADP System.

23. CONTINGENCY MANAGEMENT. Management of the potential options or actions which may be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures that, if followed, will ensure the availability of critical ADP systems and which will facilitate maintaining the continuity of operations in an emergency condition.

24. CRITICAL RESOURCES. Those physical and information assets required for the performance of the site mission.

25. DESTRUCTION The physical alteration of ADP System media or of ADP System components such that they can no longer be used for storage or retrieval of information.

26. EXCLUSION AREA. A type of DOE security area where mere presence in the area would normally result in access to classified information. An Exclusion Area has barriers identifying its boundaries and encompassing the designated space, as well as access controls to ensure that only authorized personnel are allowed to enter and exit the security area.

27. INFORMATION. The terms "data," "information," "material, " "documents," and "matter" are considered synonymous and used interchangeably in this Order, They refer to all data regardless of its physical form (e.g., data on paper printouts, tapes, disks or disk packs, in memory chips, in Random Access Memory (RAM), in Read Only Memory (ROM), on microfilm or microfiche, on communication lines, and on display terminals).

28. INTELLIGENCE INFORMATION . Classified information defined as intelligence information by Director of Central Intelligence Directive 1/16.

29. LABEL. The marking of an item of information to reflect its classification level and category that represent the highest sensitivity of the information.

    a. INTERNAL LABEL. The marking of an item of information, to reflect the classification level and category of the information, within the confines of the medium containing the information.

b. EXTERNAL LABEL. The visible and readable marking on the outside of the medium or the cover of the medium that reflects the classification and sensitivity of the information resident within the medium.

30. LIMITED AREA. A type of DOE security area having boundaries identified with barriers for the protection of classified information where guards, security inspectors, or other internal security measures provides means to control access to the security area, and thus to prevent inadvertent or deliberate access to the security area by unauthorized persons.

31. LONG RANGE PLAN. A written description of the strategy for implementing the Classified Computer Security Program that covers the 5 years beginning at the date of the plan.

32. MULTILEVEL SYSTEMS. Systems/networks that incorporate the mode of operation that allows two or more classification levels (including unclassified) of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present.

33. NETWORK. A communications medium and all components attached to that medium that are responsible for the transfer of information. Such components may include ADP systems, packet switches, telecommunications controllers, key distribution centers, technical control devices, and other networks.

34. PASSWORD. A protected word, phrase or a string of symbols that is used to authenticate the identity of a user.

35. PASSWORD SPACE. The total number of possible passwords that can be created by a given password generation scheme.

36. PERSONNEL SECURITY. The procedures established to ensure that all personnel who have access to any classified information or special nuclear material have the required authorizations.

37. PHYSICAL SECURITY.

a. The use of locks, guards, badges, alarms, procedures, and similar measures (alone or in combination) to control access to the classified ADP system and related equipment.

b. The measures required for the protection of the structures housing the classified ADP system, related equipment, and their contents from espionage, theft, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

38. PROPERTY PROTECTION AREA. A type of security area having boundaries Identified with barriers and access controls for the protection of DOE property.

39. PROTECT AS RESTRICTED DATA (PARD) . A handling method for computer-generated numerical data, or related information, which is not readily recognized as classified or unclassified because of the high volume of output and low density of potentially classified data. The above information is designated as PARD because it has not had a sensitivity (classification) review and must be protected under a different set of security rules.

40. PROTECTED DISTRIBUTION SYSTEM (PDS). Wireline or fiber-optic telecommunications system which includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

41. PROTECTION INDEX. A measure of perceived risk determined from the combination of the clearance level of users and the classification of the data on the classified ADP system. The determination of this index is described on page III-14, paragraph 5.

42. RISK ASSESSMENT. An identification of a specific ADP Facility's assets, the threats to these assets, and the ADP Facility's vulnerability to those threats.

43. SANITIZATION . The elimination of classified information from an ADP system or media associated with an ADP system to permit the reuse of the ADP system or media at a lower classification level or to permit the release to uncleared personnel or personnel without the proper information access authorizations.

44. SECURITY AREA. A physical space which has been designated as an area containing safeguards and security interests which dictate the need for the imposition of physical protection measures, as a minimum, entailing control of access to and from the designated area, in order to protect Department of Energy interests. The types of security areas used within DOE include: Property Protection Areas, Limited Areas, Exclusion Areas, Protected Areas, Material Access Areas, and functionally specialized security areas such as SCIFs, Classified Computer Facilities, and Secured Communications Centers. Safeguards and security measures applicable to each type of security area are tailored to the protection needs of the security interests contained therein.

45. SHORT RANGE PLAN. A documented, tactical (1 year) plan describing the implementation of the Classified Computer Security Program.

46. SITE. One or more operational facilities, usually geographically contiguous, operated by or for the DOE under the management and administrative direction of a DOE or DOE contractor organization.

47. TEMPEST. Short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information processing systems.

48. USER. Any individual who is able to operate any equipment or implement a procedure that can access the ADP system or input commands to the ADP system or receive output from the ADP system without intervention of an authorized reviewing official. Note that a user may not necessarily be an authorized user of the ADP system.

49. VERIFIABLE IDENTIFICATION FORWARDING. An identification method used in networks where the sending host can verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user.

TABLE OF CONTENTS

CHAPTER III - REQUIREMENTS FOR ADP SECURITY

CHAPTER I

RESPONSIBILITIES AND AUTHORITIES

1. SECRETARIAL OFFICERS shall:

   a. Ensure that this Order and other related directives are followed within their respective programs and facilities.

   b. Ensure that all managers and supervisors are aware of and fulfill their responsibilities for security of classified ADP systems.

   c. Ensure that ADP acquisitions intended for classified use meet the requirements for the protection of classified information.

   d. Through their Headquarters Security Officer (HSO), assure the implementation of the provisions of this Order in the, Headquarters facilities.

   e. Implement this Order for classified ADP systems under their management and control including those of DOE contractors.

   f. Provide, establish, and document the assignment of responsibility for the management and control of classified ADP systems under their cognizance.

   g. Through the Managers of DOE Field Offices:

      (1) Appoint a Computer Security Operations Manager (CSOM), as appropriate, who is a DOE employee knowledgeable in ADP systems and ADP security, to manage the classified computer security program.

      (2) Approve the interim operation of an ADP system where the accrediting official is not able to complete accreditation in a reasonable time. This authority may not be redelegate.

2. DIRECTOR OF SECURITY AFFAIRS (SA-1) shall approve and promulgate the DOE Classified Computer Security Program policy and through the:

   a. Director of Safeguards and Security (SA-10):

      (1) Develop DOE policy and establish the DOE Classified Computer Security Program to assure an adequate level of security for all ADP hardware and software and for the classified information that is processed, stored, transferred, or accessed.

(2) Appoint, in writing, the Classified Computer Security Program Manager (CSPM) who is a DOE employee knowledgeable in computer security, to manage the DOE Classified Computer Security Program.

b. Director of Headquarters Operations (SA-14):

(1) Appoint, in writing, a DOE employee as the Computer Security Operations Manager (CSOM) for applicable classified ADP systems operated by:

(a) Headquarters Elements; and

(b) DOE and DOE contractor organizations not under the jurisdiction of a DOE Field Office for security administration.

(2) Appoint, in writing, a DOE employee as the Computer Security Site Manager (CSSM) to implement the site Classified Computer Security Program for the DOE contractor organizations under contract to Headquarters Elements.

3. DIRECTOR, NAVAL NUCLEAR PROPULSION PROGRAM (NE-60), shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by Public Law 98-525 (42 United States Code (U.S.C.) 7158, note)) and to ensure consistency throughout the joint Navy/DOE organization of the Naval Nuclear Propulsion Program, implement and oversee all policy and practices pertaining to this DOE Order for activities under the Director's cognizance.

4. CLASSIFIED COMPUTER SECURITY PROGRAM MANAGER (CSPM) shall:

a. Develop and establish policies, standards, and procedures for the protection of ADP systems that process, store, transfer, or provide access to classified information.

b. Review and evaluate the Classified Computer Security Program, at least every 3 years, and provide a written report to management on the effectiveness of its coordination. Recommend actions to correct any identified deficiencies. Oversee the resolution of the identified deficiencies.

c. Review selected ADP security plans and coordinate periodic, documented ADP facility compliance reviews with the responsible Computer Security Operations Manager (CSOM).

d. Represent DOE before Government, private, and public organizations concerned with the protection of classified ADP systems.

e. Coordinate the Classified Computer Security Program with the Unclassified Computer Security Program as described in DOE 1360.2B.

f. Develop, implement, and review Departmental short and long range plans for the Classified Computer Security Program.

g. Ensure the application of the Technical Surveillance Countermeasures Program, specified in DOE 5639.5, as it applies to classified ADP facilities.

h. Assure compliance with Communications Security (COMSEC), Protected Distribution Systems (PDS), and TEMPEST requirements, as they apply to classified ADP systems, in coordination with the Office of Information Resources Management.

i. Publish computer security manuals and guidelines for classified ADP systems.

j. Develop, acquire, and establish methods, techniques, standards, and procedures for the design, analysis, testing, evaluation, and approval of computer security measures for ADP systems that process, store, transfer, or provide access to classified information.

k. Accredit and provide accreditation documentation for classified ADP systems for which he or she is the designated accrediting official.

1. Review and approve the ADP security plan, the certification, and recommend accreditation to the appropriate official as specified in Director of Central Intelligence Directive (DCID) 1/16, for ADP systems which process, store, transfer, or provide access to intelligence information.

m. Coordinate the protection of intelligence information with the appropriate official as specified in DCID 1/16.

n. Provide advice and guidance to CSOMs in applying computer security measures to classified ADP systems.

o. Provide overall guidance and direction for an education and awareness program for the Classified Computer Security Program.

p. Ensure that a computer security training program for CSOMs and Computer Security Site Managers (CSSMs) is developed, presented, and documented.

q. Provide for the collection and dissemination of information pertinent to the Classified Computer Security Program.

r. Provide overall guidance and direction for the field assistance, research and development, and training activities.

s. Issue the DOE Statement of Threat for Classified Computers.

5. Each COMPUTER SECURITY OPERATIONS MANAGER (CSOM) shall:

a. Assure that each classified ADP system under his or her responsibility has been accredited or reaccredited at least every 3 years, in accordance with this Order and OMB Circular A-130. This accreditation shall be documented.

b. Review and appraise the Classified Computer Security Program at each site at least annually. This review shall be documented.

c. Coordinate the Classified Computer Security Program with the Unclassified Computer Security Program described in DOE 1360.2B at their site.

d. Assure compliance with appropriate COMSEC, PDS, and TEMPEST requirements in coordination with the Office of Information Resources Management.

e. Develop and implement short and long range plans for the implementation of the Classified Computer Security Program. These plans are to be forwarded to the CSPM for review.

f. Certify that classified ADP system procurements (hardware, software, and services) meet security requirements in compliance with DOE 1360.1A.

g. Establish an incident reporting system for the site(s) over which the CSOM has cognizance.

h. Coordinate with the Technical Surveillance Countermeasures Program, as appropriate.

i. Assure that a Computer Security Site Manager (CSSM), either a DOE or DOE contractor employee, with ADP systems and ADP security experience, is appointed for each site and that these appointees are properly trained to perform their duties effectively. This individual will act as the primary interface between the site and the CSOM.

j. Evaluate. accredit. and provide accreditation documentation for classified ADP systems for which he or she is the accrediting official.

k. Approve the selection, acquisition, distribution, and implementation of security measures for classified ADP systems, as appropriate.

6. Each COMPUTER SECURITY SITE MANAGER (CSSM) shall:

a. Establish, document, implement, and monitor the classified computer security program for the site and assure site compliance with DOE policies, standards, and procedures for classified ADP systems.

b. Develop and document the site Statement of Threat for Classified Computers and forward to the CSOM for approval.

c. Develop and implement short and long range plans for the implementation of the site classified computer security program. These plans are to be forwarded to the CSOM for approval.

d. Certify to the CSOM that the classified ADP system has been implemented as described in the ADP security plan and that the specified security controls are in place and operating.

e. Implement, document, and maintain a classified computer security incident reporting system for the site.

f. Certify, in those cases where an approved ADP security plan exists, that classified ADP system (hardware, software, and services) site procurements meet security requirements in compliance with DOE 1360.1A.

g. Assure that a Computer System Security Officer (CSSO), either a DOE or DOE contractor employee, is appointed for each classified ADP system at. a site. An individual may serve as CSSO for one or more ADP systems.

h. Ensure that a computer security training program for CSSOs and users is developed, presented, and documented.

i. Ensure that a training program for computer-security-trained escorts is developed, presented, and documented.

j. Ensure that a computer security awareness program for users of classified ADP systems is developed, presented, and documented.

k. Assist the CSSO in the development of ADP security plans for each classified ADP system.

l. Approve the documented site physical access methods to classified ADP systems operations areas, including areas containing peripheral equipment.

m. Assure compliance with COMSEC, PDS, and TEMPEST requirements, as they apply-to classified ADP systems.

n. Establish procedures to ensure that classified ADP systems are continuously monitored and periodically evaluated to prevent or detect security infractions and instances of waste, fraud, or abuse.

o. Establish site procedures governing marking, handling, destruction of output, and removal of ADP media or equipment containing classified information, from the security areas of the DOE site.

p. Establish procedures for clearing and sanitizing ADP media and assure the use of approved degaussing equipment.

q. Approve the selection, acquisition, distribution, and implementation of security measures for classified ADP systems, as appropriate.

r. Coordinate the classified computer security program with other site functional areas that may impact the program.

s. Develop and document a procedure for validation/revalidation of user identification (user ID) and for prompt notification when a user identification is no longer needed.

t. Assure that the site Master Safeguards and Security Agreement (MSSA), where one exists, is consistent with the site classified computer security program.

7. Each COMPUTER SYSTEM SECURITY OFFICER (CSSO) shall:

a. Prepare the ADP security plan consistent with an analysis of the security requirements for the protection of classified information in the classified ADP system and in the ADP facility.

b. Advise the CSSM that the classified ADP system has been implemented as described in the ADP security plan and that the specified security controls are in place and operating.

c. Develop, implement, maintain, and document security measures for each classified ADP system to assure that the classified ADP system is in compliance with DOE and site policies, standards, and procedures and that the classified ADP system implements the Classified Computer Security Program.

d. Develop a contingency plan to ensure the availability of critical ADP systems and to facilitate the continuity of operations in an emergency situation.

e. Perform a risk assessment to identify and document the specific ADP facility's assets, the threats to these assets, and the ADP facility's vulnerability to those threats.

f. Implement DOE and site policy, standards. and procedures governing marking, handling, and destruction of classifi ed ADP system output and the removal of ADP media or ADP equipment containing classified information from the security area(s) of the DOE site.

g. Identify ADP security training needs and designate appropriate personnel to attend training programs.

h. Develop, implement, and document a continuing audit and review process for the classified ADP system to prevent or detect security infractions and the occurrence of waste, fraud, or abuse.

i. Assure that the proper level of protection of data is determined prior to use on the ADP system and that the proper security measures are afforded this data.

8. Each DATA OWNER shall:

a. Determine and declare the required protection level of the information prior to the information being processed, stored, transferred, or accessed on the classified ADP system.

b. Provide the ADP system CSSO with any special security requirements for the information to be processed on the classified ADP system.

c. Determine the criticality of the information for which he or she is custodian and inform the ADP system CSSO.

9. Each USER OF THE CLASSIFIED ADP SYSTEM shall:

a. Comply with the ADP system security requirements.

b. Remain aware of and knowledgeable about his or her responsibilities in regard to classified ADP system security.

c. Be accountable for his or her actions on classified ADP systems.

CHAPTER II

CLASSIFIED COMPUTER SECURITY PROGRAM MANAGEMENT

1. MANAGEMENT RESPONSIBILITIES.

   a. Director of Safeguards and Security (SA-10). The Director of Safeguards and Security is responsible for establishing procedures for the management of the Classified Computer Security Program and for enforcing these procedures through oversight of the program. The Director shall appoint a Computer Security Program Manager (CSPM) to direct and manage the Classified Computer Security Program.

   b. Organization Responsibilities. Secretarial Officers, Managers of DOE Field Offices, and the Director of Headquarters Operations (SA-14) having responsibility for classified ADP systems shall be responsible for establishing internal Classified Computer Security Programs, and for assuring that solicitations and contracts for the acquisition of components of classified ADP systems are subject to the requirements of this Order. These managers shall each appoint a Computer Security Operations Manager (CSOM), as appropriate, who shall direct and manage the Classified Computer Security Program for all classified ADP systems and ADP facilities under the cognizance of their organizational element.

   c. Sire Responsibilities. At each DOE or DOE contractor site a DOE or DOE contractor employee shall be designated as Computer Security Site Manager (CSSM) to manage the Classified Computer Security Program for the site. The CSSM shall ensure the designation of a Computer Systems Security Officer (CSSO) for each ADP system to plan, implement, and maintain security for that ADP system.

   d. Network Responsibilities For ADP systems that span multiple ADP sites (e.g., networks), the accrediting official shall assure the designation of responsible officials (e.g., CSSM, CSSO) for the entire ADP system, and a responsible official shall be designated to assist in local implementation at each ADP facility.

2. MANAGEMENT PROCEDURES.

   a. Statement of Threats.

      (1) There shall be a written site Statement of Threat for classified computers referenced in each ADP security plan. This statement relates to various Headquarters generic threat statements and the site Statement of Threat and specifically addresses computer related threats to the site.

(2) There shall be a written Statement of Threat for each classified ADP system. This statement shall identify threats unique to the ADP system (if any) not covered in the site Statement of Threat for Classified Computers. The statement shall be included or referenced in the ADP security plan. If there are no unique threats to the ADP system, a statement to this effect is required.

b. Risk Management. DOE and DOE contractor organizations shall establish a risk management program. This risk management program shall be correlated with the DOE and site Classified Computer Security Statements of Threats. Periodic risk assessments shall be performed at each site to ensure that appropriate, cost effective safeguards are incorporated into existing and new classified ADP systems.

(1) The objective of a risk assessment is to provide an evaluation of the assets of the classified ADP system and of the relative vulnerabilities, hazards, and threats to the classified ADP system so that security resources may be effectively distributed to minimize potential loss.

(2) A risk assessment may vary from an informal qualitative review of a personal computer to a formal, fully quantified risk analysis of a large scale ADP system. The results of these assessments shall be documented, reported, and considered by management when planning security upgrades and by the CSSM when certifying an ADP system. A qualitative risk assessment technique may be used since most DOE ADP systems have intangible or non-monetary assets, such as public confidence, good will, irreplaceable information, or classified information.

(3) A risk assessment shall be performed as a part of the accreditation process of a classified ADP system, or whenever a significant change occurs to an accredited ADP system, and at periodic intervals commensurate with the sensitivity of the data processed, but at least every 3 years.

c. Computer Security Planning.

(1) In response to a call issued by the CSPM, each DOE and DOE contractor organization shall develop annually a long range plan which forecasts the requirements and costs in dollars and manpower of the site classified computer security program. The call document will describe the format and content of the plan. As a minimum, this plan shall address the actions and resources (e.g., hardware, personnel, etc.) necessary to comply with the requirements of the Classified Computer Security Program and to reduce the impact of any

vulnerabilities in the operational environment of the site's classified ADP systems. This plan shall be forwarded to the CSOM for review, approval, and transmittal to the CSPM.

(2) As a part of the long range plan, each site shall prepare an overview configuration diagram that describes the various classified ADP systems at the site and how they are related. This diagram presents the ADP system plans and ADP system interconnection (network) plans. This document should provide a listing of all classified ADP systems at the site and information about connecting ADP systems.

(3) The long range plan shall also address any proposed changes in the operational environment of the classified ADP systems at the site.

(4) Each DOE and DOE contractor organization shall also prepare a short range plan annually which addresses the current implementation of the long range plan. This plan shall be forwarded to the CSOM for review, approval, and transmittal to the CSPM.

d. ADP System Reaccreditation. Following the intent of OMB Circular A-130, "Management of Federal Information Resources," each ADP system shall be reaccredited by the accrediting official at least every 3 years to ensure that the ADP system continues to be in compliance with the applicable Federal and DOE policies, procedures, and directives and the ADP security plan; that it meets any applicable new requirements; and that the protective features and assurances continue to be effective.

e. Computer Security Program Evaluations.

(1) Program evaluations ensure that the Classified Computer Security Program management process continues to meet the requirements of the policies and procedures of DOE. At least once every 3 years, the CSPM shall review, and document the review of, the Classified Computer Security Program that has been implemented by each CSOM.

(2) Each CSOM shall review annually, and document the review of, the Classified Computer Security Program implemented by each site.

(3) Each CSSM or his or her designee shall review annually, and document the review of, compliance with the site Classified Computer Security Program by each CSSO.

(4) For sites that have many small classified ADP systems (e.g., personal computers, process control computers) or have many similar systems such as distributed processors, this review

may be performed on a random basis so that each such classified ADP system is reviewed by the CSSM at least once every three years.

(5) The results of the CSPM and CSOM evaluations shall be submitted through the management and accreditation chain for retention by the CSSM and the CSSO.

f. Acquisition Specifications. DOE and DOE contractor organizations shall assure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition of ADP equipment, software, or related services to be utilized in the classified computer environment. These security requirements shall be reviewed and approved by the accrediting official or, in cases where an approved ADP security plan exists, by the CSSM. This approval shall be documented prior to issuance and included as part of ADP procurement documents.

g. Contingency Planning.

(1) The CSSO shall assure that appropriate contingency plans are developed, documented, and maintained for each classified ADP system. The plans shall be consistent with disaster recovery, known threats, and continuity of operations required for the classified ADP system. These requirements shall be identified in the ADP security plan. Procedures shall be established to identify critical resources related to classified ADP systems, key response and recovery personnel, and alternate site processing requirements. The intent of such plans is to assure that users can continue to perform essential functions in the event the classified ADP system cannot continue to perform its functions.

(2) For critical resources related to classified ADP systems, these plans shall be operationally tested periodically (and the tests documented). These tests shall be exercised at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of service but no less frequently than annually.

h. Critical Software and Data Backup. Procedures shall be established to assure as a minimum, that current backup copies of critical software, data, and documentation must be included in the configuration management scheme for the ADP system being supported.

i. Protection of ADP Systems from Waste, Fraud, and Abuse. The ADP security plan shall describe and document the management controls established to prevent waste, fraud, and abuse.

j. Configuration Management. The software and hardware, and the security mechanisms and procedures, of each classified ADP system shall be under configuration management. The CSSO, for each ADP system, shall have a current list of all the components of the system. The CSSM shall ensure that a current site inventory of all classified ADP systems is maintained. This inventory will assist in accountability and will provide information for the management of the Classified Computer Security Program. Modifications (software or hardware) that relate to the security of the ADP system shall be documented. These modifications shall be reviewed and approved by the accrediting official prior to implementation. As a minimum, the site inventory shall include the information specified in Table II-1.

k. Computer Security Incident Reporting.

(1) Procedures for the recording, reporting, investigating, documenting and responding to computer security incidents shall be established by the CSSM and approved by the cognizant CSOM for all ADP systems that process, store, transfer, or provide access to classified information. These procedures must be defined in such a way that they will provide a vehicle for reporting, documenting, and investigating the violation of laws and infractions of procedures (see DOE 5639.3, VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY INTERESTS, and DOE 5635.1A, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION) . Incident reporting shall be the responsibility of all DOE and DOE contractor employees, including classified ADP system users, operators, security personnel, and management.

(2) Any discovery of a hardware or software vulnerability shall be ranked and reported as if it were an incident. This will facilitate communication to the community of a newly discovered vulnerability.

(3) Important and routine incidents, as defined in Table II-3, will be summarized and forwarded through the CSOM quarterly to the CSPM.

(4) The CSSM of each site shall be responsible for the ranking of incidents as outlined in Table II-3, and for the timely initial notification of incidents as specified in Table II-4. The CSSM shall also maintain complete historical record of the reports of all classified ADP system incidents for ADP systems under his/her cognizance. The written report of each incident shall include, as a minimum, the information contained in Table II-2. (The CSOM or the CSSM may require additional information to meet local procedures or requirements.)

TABLE II-1

HARDWARE AND SOFTWARE ACCOUNTABILITY INFORMATION

System Name:
Location:
- Area, Building, Room
- Responsible organization, official

Hardware:
- Manufacturer
- Model
- Serial Number
- Hardware Special Security Features (boards, etc)
- TEMPEST Characteristics

Operating System Software:
- Developer
- Name or Other Identifier
- Version Number

Security Related Software:
- Developer
- Name or Other Identifier
- Version Number

- **This represents the minimum amount of information necessary to support the configuration management inventory requirement**

Table II-1
Hardware and Software
Accountability Information

TABLE II-2
MINIMUM CONTENTS OF INCIDENT REPORTS

Organization:
Author of Report (including author's tide and location)
Date, Time, and Place of Incident
Ranking of Incident
Nature of Incident (including names of personnel involved)
ADP System Name and Description:
Classification or Sensitivity Level of Information Involved:
Name of CSSM:
Name of CSSO:
Hardware and Software involved:
To Whom was the Incident Reported:
Date and Time of Report:
Action Taken to Contain Incident
Statement of Corrective Action Taken:

Table II-2
Minimum Contents of Incident Reports

TABLE II-3
INCIDENT RANKING TABLE

Ranking	Severity of Incident
Significant	**Such as: complete penetration of a classified ADP System; penetration of a classified ADP System that exposes a security vulnerability in hardware or software that may be in use at other sites within DOE; physical loss sufficient to cause mission or programmatic impact; known loss or compromise of classified information; use of a classified ADP System in support of a criminal activity; any incident that may result in: loss, harm or embarrassmont to the DOE, or the occurrence of similar incidents at other DOE sites.**
Important	**Such as: loss or compromise of one or more authentication mechanisms that results in suspected compromise of classified information; penetration of a classified ADP System that does not allow control of the classified ADP System or access to all data; major misuse of a system by an authorized user (e.g. using the system to support a personal business); suspected loss or compromise of classified information or security software features; an incident that could be embarrassing to the site.**
Routine	**Such as: an external attempt to access a system with little potential for success; minor abuse of a system by authorized users (e.g., using the system for personal entertainment).**

Table II-3
Incident Ranking Table

TABLE II-4
INITIAL INCIDENT REPORTING PROCEDURES

Ranking	Reporting Time	Final Reporting Level*
Significant	Within 12 hours	To CSPM
Important	Within 3 working days	To CSOM
Routine	Discretionary, but within 30 days	To CSSM

***Reporting path is through the accreditation chain. These reports are in addition to those required by other DOE orders.**

3. ADP SYSTEM ACCREDITATION.

a. Overview of Accreditation. Accreditation is the written formal decision to approve and authorize an organization to operate an ADP system to process, store, transfer, or provide access to classified information. The decision to accredit takes into account any risk of operating the ADP system, the security protections of the ADP system as documented in the ADP security plan, the results of the security tests, and the certification by the CSSM. Certification documents that the ADP system and its environment comply with DOE's Classified Computer Security Program provisions as specified in the ADP security plan. The CSSM certifies the ADP system and provides the results of the security tests to the accrediting official as an aid in the accreditation decision. The accrediting official reviews the ADP security plan and the certification of the system and issues the formal written accreditation of the ADP system.

b. Determination of the Accrediting Official. The determination of the accrediting official is based on factors described below. The accrediting official and the certifying official shall not be the same person. For all classified ADP systems the accrediting official shall be a DOE employee. (At al 1 times, the approvals and recommendations shall proceed through the stated accreditation channels.)

(1) For classified ADP systems that do not process, store, transfer, or provide access to intelligence information and are to be operated with a Protection Index (see page III-14, paragraph 5b) of zero or one, the CSOM shall be the accrediting official.

(2) For classified ADP systems that do not process, store, transfer or provide access to intelligence information and are to be operated at a Protection Index of two or more, the CSPM shall be the accrediting official.

(3) For classified ADP systems that do not process, store, transfer or provide access to intelligence information but that have external connections (an arrangement commonly referred to as a network) with components not under the jurisdiction of the same CSOM, the CSPM shall be the accrediting official for the ADP system and, as necessary, for all the interconnected components.

(4) For classified ADP systems that process, store, transfer or provide access to intelligence information, the CSPM shall review the ADP security plan and the certification of the ADP system and, if acceptable, forward it with a recommen-

dation for accreditation to the appropriate official as specified in DCID 1/16.

(5) For classified ADP Systems that are solely within the jurisdiction of Naval Reactors and whose external components extend into the jurisdiction of different Naval Reactor CSOMs, NE-60 will designate one of the CSOMs to be the accrediting official. Copies of the approved network ADP security plan, certification, and accreditation documentation will be furnished to the CSPM for information.

c. ADP Security Plan.

(1) An ADP security plan shall be developed by the CSSO following the requirements in Attachment III-1, page 111-21. The ADP security plan shall describe the complete classified ADP system, its interconnections, and the security protections that will be used. It will discuss the manner in which the requirements of this Order are to be implemented for the ADP system. If all of these requirements cannot be implemented, then the plan must present alternative protection mechanisms and justify their effectiveness. Prior to implementation and certification by the CSSM, each ADP security plan shall be reviewed and approved by the accrediting official of the classified ADP system. (If the CSPM is the accrediting official, the CSOM shall review, approve, and forward the ADP security plan to the CSPM for approval.)

(2) Where many similar classified ADP systems (e. g., stand-alone micro-processors or word processors) are to be operated in the same environment, a master ADP security plan may be written and approved to cover all such classified ADP systems. Each such system shall be individually certified by the CSSM as meeting the conditions of the master security plan.

d. ADP Security Plan for a Network.

(1) Requirements. Network ADP security plans shall be developed following the guidelines contained in Attachment III-1 for an ADP security plan. Some components of a network may have separate ADP security plans. The network ADP security plan may consist of the ADP security plans for its components plus an overall network ADP security plan. In addition, the network ADP security plan shall clearly delineate the respective responsibilities and management jurisdiction for network and component CSSOs. The network ADP security plan shall show how the network implements the mechanisms necessary to satisfy requirements of the Classified Computer Security Program. Each ADP security plan for individual components shall take into account the total environment in

which each is operated. The network ADP security plan shall provide details-on network security management as it pertains to the unique configuration of the network.

(2) Access Control. In forming a network of components, it is important to analyze the secure operating assumptions each component depends upon. This analysis is necessary to ensure that access decisions throughout the network will consistently implement the Classified Computer Security Program. It will also ensure compliance with the network ADP security plan and ensure that secure operation is maintained as the components are incorporated into a network. The network ADP security plan shall show how the various components implement and enforce these mechanisms.

(3) Remote User Identification. It is recommended that some form of verifiable identification forwarding be used between ADP systems when users are connecting through a network. When verifiable identification forwarding is not used, a remote ADP system shall require the user's ID and authentication before permitting access to the system.

(4) Configuration Control. It is the nature of a network that the network configuration changes frequently; therefore, it is important for the ADP security plan to specify the means of configuration control and the methods for assuring continuing security as the changes occur.

e. ADP System Security Tests.

(1) After the ADP security plan has been approved by the accrediting official, the CSSO shall begin testing the security features of the system. The tests necessary for certification shall be designated by the CSSM. After certification, the accrediting official may designate any further security tests that must be performed prior to accreditation. It may be required that these tests be conducted by a group independent from the user/developer and the CSSO.

(2) Should any vulnerabilities be revealed during the security tests, the CSSM shall ensure that the necessary steps are taken to eliminate or minimize their impact. Any modifications, changes, or additions to the system security measures shall be included in a revised ADP security plan and the revised plan shall be re-approved.

(3) The results of the tests performed and an overall evaluation of the security protection provided the ADP system shall be documented.

(4) Network security testing shall be conducted to demonstrate that the implementation of the network meets the requirements specified in the network ADP security plan. The tests to be performed shall be specified by the CSSM responsible for the network.

f. Certification.

(1) The CSSM will evaluate the ADP system and the results of the security tests to verify that the ADP system has been implemented as described in the ADP security plan and that the specified security controls are in place and operating properly.

(2) Certification of a network by the CSSM responsible for the network includes both network security tests and an analysis to provide the necessary evidence to assure that a consistent implementation has been achieved.

(3) The CSSM shall issue a written certification that assures the accrediting official that all requirements of the ADP security plan have been met and that the ADP system is ready for accreditation.

(4) The CSSM shall compile a certification report as supporting evidence for the certification statement. This report will be-forwarded through the accreditation chain. The-report shall, at a minimum, be composed of the approved ADP security plan, the security test results and any other supporting material.

g. Accreditation Procedures.

(1) The accreditation process (see Attachment 11-1) begins with the responsible CSSO developing the ADP security plan to define the manner in which the ADP system and its information will be protected.

(2) The completed ADP security plan is reviewed by the CSSM and, if it is acceptable, approved and forwarded to the CSOM.

(3) The CSOM reviews the ADP security plan and, as appropriate, approves it or returns it to the CSSM for modification. If the CSPM is the accrediting official and if the ADP security plan is acceptable, the CSOM forwards it with a recommendation to the CSPM. The CSPM then reviews the ADP security plan and either approves it or returns it to the CSOM for modification. The written approval is forwarded through the accreditation chain for retention by the CSSM and the CSSO. For ADP systems processing intelligence information (see page II-10, paragraph 3b(4)).

(4) After the ADP security plan is approved, security testing is performed as required by the CSSM. The CSSM evaluates and certifies the implementation of the security features for the ADP system and verifies that the ADP system operates in accordance with the approved ADP security plan. The security test results and the certification are forwarded through the CSOM to the accrediting official.

(5) The accrediting official reviews the certification and test results and formally issues a written accreditation accepting the risk of operating the ADP system and authorizing its use as documented in the ADP security plan. The written accreditation shall be forwarded through the accreditation chain for retention by the CSSM and the CSSO.

(6) With the exception of ADP systems" processing intelligence information, in the event that a system has been certified and it appears that a delay (of more than 30 working days) in accreditation may take place, the Manager of the DOE Field Office may grant an interim approval to operate the ADP system in accordance with the written, approved ADP security plan. Notification of this approval, with full explanations, shall be sent to the accrediting official within 5 working days. If the ADP system is not accredited within 90 days of the issuance of the interim approval to operate, the Manager of the DOE Field Office may extend the approval for another 90 days. If the ADP system has not been accredited at the end of this period, the ADP system shall not be operated in the classified mode until formal accreditation is received.

(7) The accreditation of a classified ADP system shall be valid until there are modifications that impact the ADP system's security or environment, the applicable security requirements change, or for a maximum of 3 years. In these cases, a revised ADP security plan shall be prepared by the CSSO and approved prior to implementation of the changes. These ADP systems shall be certified and processed for reaccreditation.

(8) A network shall be formally accredited prior to its operational use. The accrediting official shall, on an annual basis, review the network implementation to verify that no changes have been made to the network which might degrade its overall security. The CSSM responsible for the network and the accrediting official shall be advised of any alterations to the network design which might impact upon network security. The CSSM is responsible for ensuring compatibility between the overall network ADP security plan and the individual ADP security plans of each network component.

h. Reaccreditation Procedures.

(1) Reaccreditation must occur if there are modifications to an ADP system that impact its security, or that impact the security aspects of its environment; or if the applicable security requirements change; but, as a minimum, at least every three years.

(2) The CSSO prepares an update to the ADP security plan and forwards it to the CSSM. This updated ADP security plan shall include the procedures and methods of operation to be used during the period between the approval of the plan and the final accreditation of the updated ADP system.

(3) The completed ADP security plan is reviewed by the CSSM and, if it is acceptable, approved and forwarded to the CSOM.

(4) The CSOM reviews the ADP security plan and, as appropriate, approves it or returns it to the CSSM for modification. If the CSPM is the accrediting official and if the ADP security plan is acceptable, the CSOM forwards it with a recommendation to the CSPM. The CSPM then reviews the ADP security plan and either approves it or returns it to the CSOM for modification. The written approval is forwarded through the accreditation chain for retention by the CSSM and the CSSO.

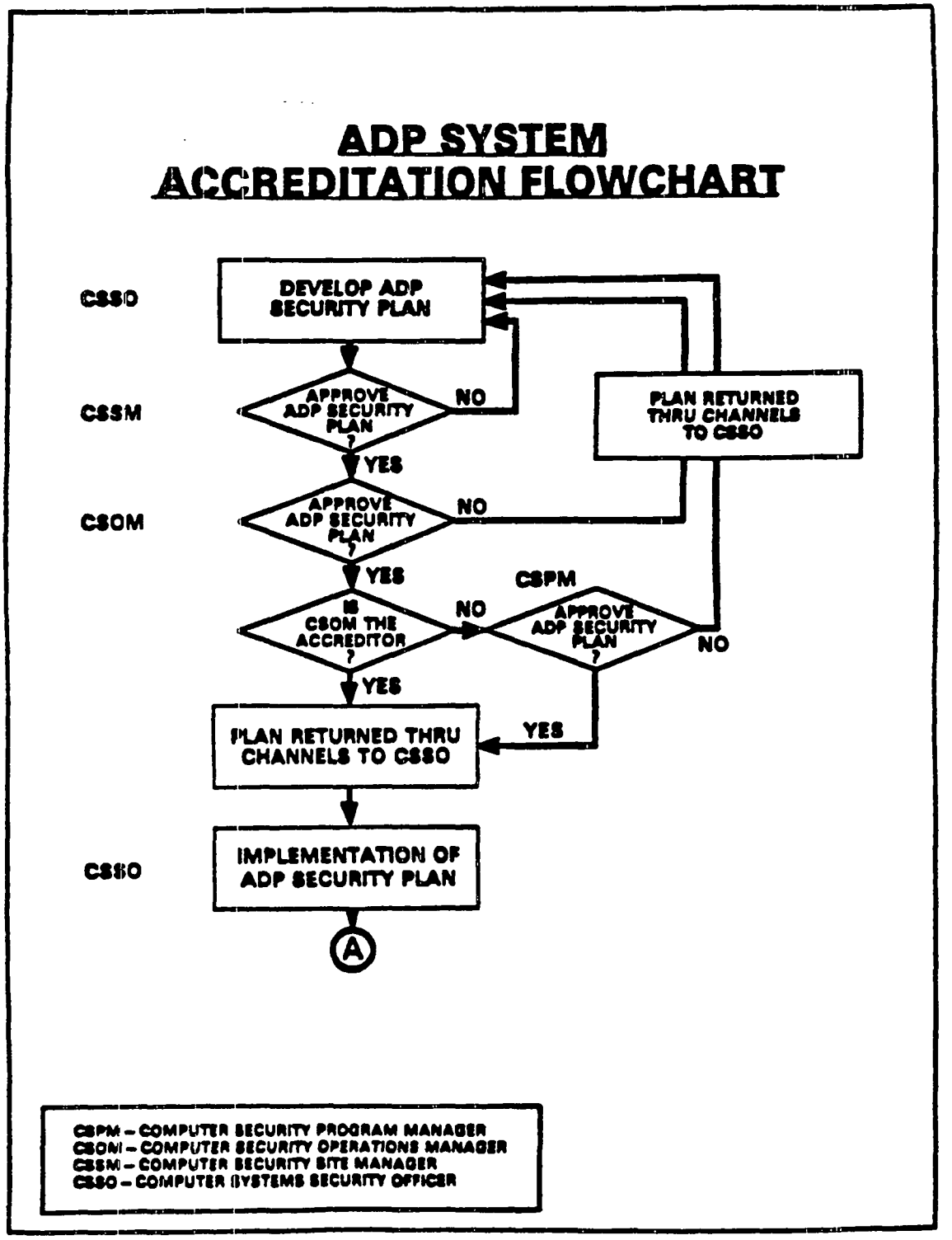
(5) After the updated ADP security plan is approved by the accrediting official, the designated changes to the system are installed.

(6) Security testing is performed as required and the CSSM evaluates the system implementation to verify that it is in accordance with the approved ADP security plan. During this period, the ADP system is operated under interim procedures as designated in the updated ADP security plan and is still considered to be accredited.

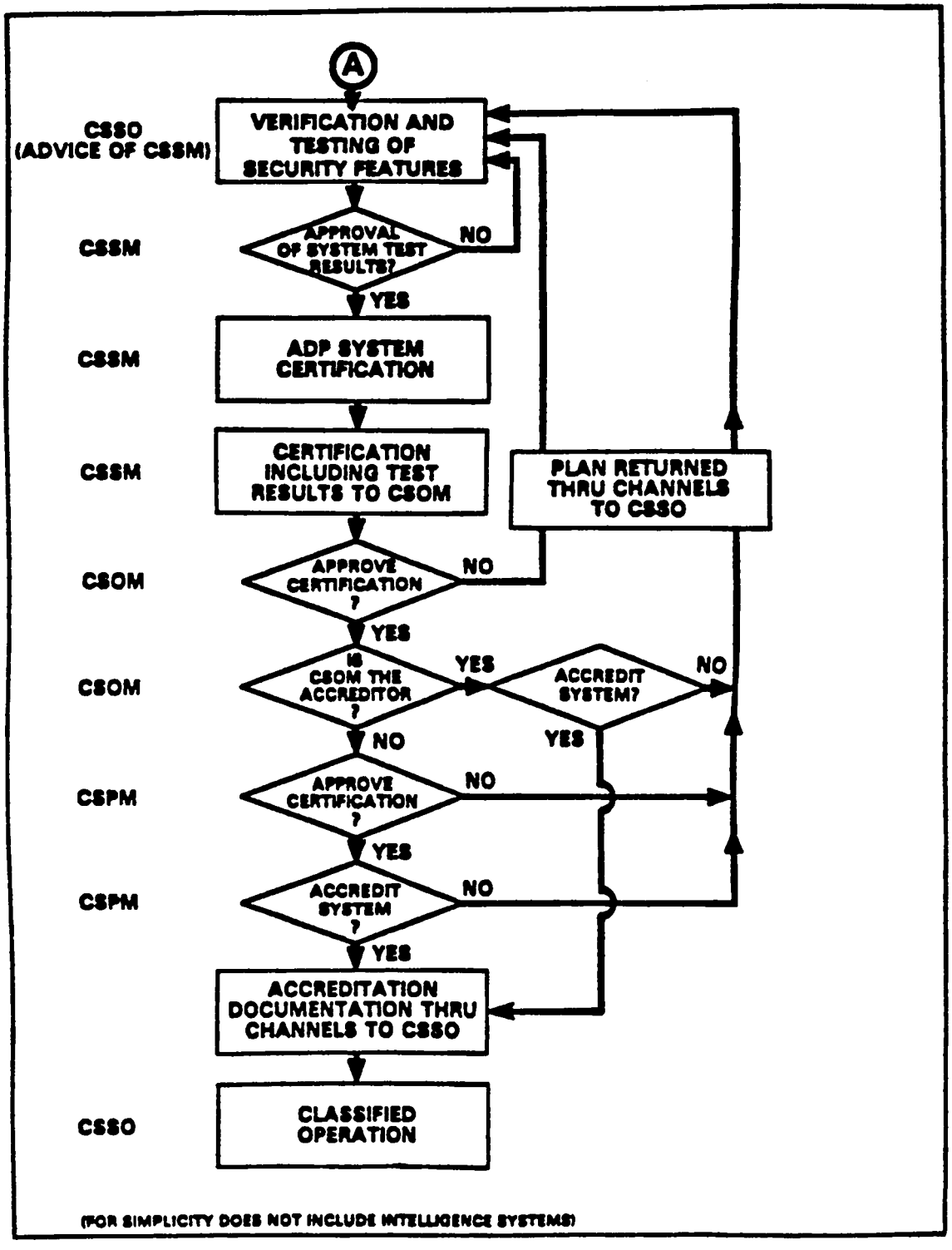
(7) The security test results and the certification are reviewed, approved (if appropriate), and forwarded through the CSOM to the accrediting official. The accrediting official reviews the certification and test results and formally issues a written accreditation for operating the updated ADP system and authorizing its use as documented in the updated ADP security plan. This written accreditation is forwarded through the accreditation chain for retention by the CSSM and the CSSO.

(8) Reaccreditation is required prior to the activation of a network whose components or ADP systems have undergone security-relevant changes which may affect the security integrity of any one component or of the network as a whole.

ADP SYSTEM ACCREDITATION FLOWCHART



ADP SYSTEM ACCREDITATION FLOWCHART
(continued)



CHAPTER III

REQUIREMENTS FOR ADP SECURITY

The Classified Computer Security Program combines requirements in the areas of personnel security, physical security, telecommunications security, hardware and software security, and administrative security to provide the required protection for classified data processed, stored, transferred, or accessed by the ADP system. These measures are necessary to provide the protection of hardware and of classified data against accidental or intentional destruction, disclosure, or modification. The provisions hereinafter set forth are intended to satisfy the basic requirements that classified information must be under the positive control of an individual at all times and not passed to another individual's control unless the identity of the receiving individual has been positively established and authenticated, accountability has been accepted by the receiving individual, and an audit trail has been established. All of these requirements must be met to comply with this Order.

1. PERSONNEL SECURITY. The requirements of DOE 5631.2C, PERSONNEL SECURITY PROGRAM, shall be met. All classified ADP systems shall have adequate controls to ensure that personnel having access to the equipment, software, and data have the proper clearance and "need-to-know."

   a. Operations. Maintenance, and Operating Systems Personnel. DOE and DOE contractor personnel who (1) operate the classified ADP system, (2) control access, or (3) design, develop, install, modify, service, or maintain the security features that control user access or program access to the ADP system or to the operating system shall be cleared for access to the highest level of classification and most restrictive category of information for which the ADP system or any connected ADP system is accredited. If it is necessary for maintenance or other personnel who are not cleared to the highest level and most restrictive category to have temporary access to the classified ADP system, they shall be escorted by a computer-security-trained escort authorized by the CSSO.

   b. Users of Classified ADP Systems. All users (including application programmers) who have access to-the classified ADP system shall be cleared for access to the highest level of classification and most restrictive category of information in the classified ADP system. This requirement may be relaxed if adequate security features and assurances, including access controls which would allow for multilevel processing are installed. These controls shall be documented in the ADP security plan, implemented in the ADP system, and approved by the accrediting official.

2. PHYSICAL SECURITY. Each ADP system including remote terminals, printers or other output devices, communications paths, memory, and other interconnected devices shall be afforded physical security commensurate-with the highest level and most restrictive-category of classified informa-

tion for which the system is accredited. Security controls to safeguard the physical equipment apply not only to the computer equipment and its peripheral equipment but also to all removable media such as magnetic tapes, magnetic disk packs, and spare or replacement parts once they are associated with a classified system. An exception may be made for multilevel ADP systems (those with a Protection Index of two or three) where selected components of the system provide service to users with security requirements less than the highest level of classification and most restrictive category of information accredited on the ADP system. In this case, the physical security controls over those components and their associated communications channels shall be commensurate with the highest classification level and most restrictive category of information processed by that component.

a. Protection Requirements for Single Level ADP Systems. Any ADP system with a Protection Index of zero or one (see page III-14, paragraph 5b) accredited to process, store, transfer, or provide access to classified information shall be located within a DOE Exclusion Area such that access is controlled as required by Chapter III, page III-3, subparagraph c. The following protection requirements also apply:

(1) The classified ADP system or system components can be left unattended if the Exclusion Area is securable as a vault type room or is authorized for open storage of classified information at a level commensurate with the classified ADP system accreditation.

(2) If the classified ADP system or system components is to be left unattended and the Exclusion Area is not securable, then:

(a) The classified ADP system or component shall have all classified information removed and stored in DOE approved security containers;

(b) The ADP system or component shall be sanitized as described on page 111-10, subparagraph h(2); and

(c) All interfaces to protected wirelines shall be disconnected and the protected wireline interface secured (both the disconnection and securing of the Interface can be accomplished with a CSOM approved locking mechanism) to prevent access to the classified information which may be available to the protected wireline.

b. Protection Requirements of Multilevel ADP Systems. Any multilevel classified ADP system with a Protection Index of two or more (see page III-14, paragraph 5b) accredited to process, store, transfer,

or provide access to classified information shall be located in a DOE security area. The following protection requirements apply to these systems:

(1) Those ADP systems or system components which process, transfer, or provide access to classified information shall adhere to the physical protection requirements described for systems with a Protection Index of zero or one.

(2) Those ADP systems or system components which are exclusively in the unclassified partition of a multilevel system or network may be located within a DOE Property Protection Area or alternative physical protection requirements shall be described in the ADP system security plan and approved by the accrediting official.

c. Access t'o the Classified ADP System. Routine unescorted access to the classified ADP system shall be controlled and limited to personnel who are cleared for access to the highest level and most restrictive category of information processed, stored, transferred, or accessible and whose "need-to-know" has been verified by the CSSO. If it is necessary for personnel who are not cleared to the highest level and most restrictive category to have temporary access to the computer equipment area, they shall be escorted by a computer-security-trained escort authorized by the CSSO.

d. Protection of ADP Storage Media.

(1) Whenever ADP storage media are removed from the physical protection provided the classified ADP system, any ADP storage medium (including system or data backups, paper), shall be afforded security protection commensurate with the highest classification of data or information processed by the ADP system until the information stored on the media has been reviewed and the level of classification of the media determined.

(2) All storage media containing classified material, such as tapes and disks, shall be protected and stored as appropriate for the highest level of classification and most restrictive category of information ever stored thereon until the medium is destroyed or sanitized. DOE 1324.2A, RECORDS DISPOSITION, shall be consulted prior to destroying any records.

(3) Procedures shall be implemented to protect and control all classified ADP media at a site. If the media is at a level of classification that requires accountability, these procedures shall include accountability controls.

(4) All ADP storage media must be protected with an adequate level of environmental protection.

e. Electronic Protection Requirements. Each classified ADP system shall be electronically and logically separated from all other ADP systems unless they are managed under the same ADP security plan.

f. Visual Access Requirements. Each classified ADP system shall be protected in a manner which prevents unauthorized personnel 'from having visual access to the information being processed.

3. TELECOMMUNICATIONS SECURITY. Each communication link which supports a classified ADP system with a Protection Index of one or zero shall be protected commensurate with the level of classification and category for which the system is accredited. Communication links supporting classified ADP systems with a Protection Index of two or three shall be protected according to the highest level and most restrictive category of information carried by that link (see DOE 5300.3 C).

a. Transmissions Security. Only Protected Distribution Systems (PDS) or National Security Agency (NSA) approved cryptographic devices shall be used to protect classified information on communication lines that pass outside the security area of an ADP system or ADP Facility (see DOE 5300.4 C). The specific security area of an ADP Facility and the cryptographic devices or PDS to be used shall be defined in the ADP security plan (see Attachment III-1).

b. Emission Security. Measures shall be implemented to control compromising emanations from crypto-equipment, telecommunications, and ADP systems in accordance with DOE 5300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST). These measures shall prevent compromising emanations from being exploitable beyond the limits of effective physical control (TEMPEST Control Zone). The emanations security measures and the installation of the ADP equipment and cabling shall be reviewed and approved as a part of the accreditation process.

c. Use of STU-III as an Encryption Device.

(1) The use of STU-III instruments to transmit and receive classified information as a scheduled, integrated part of a classified ADP application constitutes the establishment of a network. In this case, all requirements for the accreditation of a network are applicable.

(2) When STU-III instruments are used as an encryption device for the transmission or reception of classified information for unscheduled sessions, the following requirements apply:

(a) The classified ADP security plan for both the ending and receiving systems must reflect the classification level, and conditions under which the STU-III usage is authorized.

(b) Sending and receiving users must accept responsibility for providing access to their data, authenticating the classification level of both the transmitted and received data.

(c) The use of the STU-III as an encryption device is authorized only when the "Clear Data Function" is disabled.

(d) Properly cleared personnel must be present at both terminals during the entire period of interconnection or the terminal must be located in an area approved for the open storage of classified material.

4. ADMINISTRATIVE SECURITY. Procedures shall be established to ensure that all classified ADP systems and classified ADP facilities have adequate administrative controls for the controlled access to and appropriate handling of classified information. These procedures shall be documented in each ADP security plan. The CSSO is responsible for ensuring that these security procedures are enforced. DOE 5635.1A applies to all material removed from the control of the ADP system.

a. Single-User ADP System Procedures. A single-user ADP system is a system in which only one user controls all system resources at any specific time. For a single-user ADP system that is not connected to another ADP system, accountability and physical controls appropriate to the classification of the data being processed are sufficient. If two or more users have sequential access to an ADP system or more than one level of classification is processed sequentially (i.e., periods processing on an otherwise single-user system), the ADP security plan must specify the sanitization procedures to be employed by each user at the end of each session of use of the ADP system.

b. Multiuser ADP System Procedures. A multiuser ADP system is one where two or more users simultaneously share system resources, or two or more users sequentially use system resources without assurance of complete sanitization of all shared resources between each user and all other users. Access controls in multiuser ADP systems will be assigned by the CSSO and will include user identification, authentication, authorization, and accountability.

(1) User IDs Each user ID shall be assigned to only one person. "No two persons may ever have the same user ID at the same time. Prior to reuse of a user ID, all previous access authorizations must be removed from the ADP system.

A record of the user ID assignment shall be kept available for a minimum of 3 years after the user access has been terminated. It shall be considered a security infraction when two or more people have access to the authentication for a user ID (except in the unavoidable case involving the CSSO). Note: There is no intention of prohibiting alternate forms of user identification (e.g., group IDs, functional titles) for non-authentication purposes (e.g., data base access control, mail). If alternate methods are used, they must be based on user IDs.

(2) User ID Revalidation.

(a) The CSSM shall be responsible for the development implementation of a procedure whereby prompt notification given to the CSSO when a user ID and its authentication must be removed from the ADP system (e.g., when an employee leaves the sponsoring organization).

(b) In addition, the CSSO shall ensure that all user IDs are revalidated at least annually, and information such as sponsor and means of offline contact (e.g., phone number, mailing address) updated as necessary.

(3) Authentication. Authentication is the act of verifying a person's claimed identity as he attempts to log on to an ADP system. Each user of a multiuser ADP system shall be identified and authenticated before access is permitted. This verification can be based on three types of information: something the person knows (e.g., a password); something the person possesses (e.g., a card or key); something about the person (e.g., fingerprints or voiceprints); or some combination of these three. Authenticators that are passwords shall be developed in accordance with Attachment III-2.

(a) Logon. Users shall be required to authenticate their identities at "logon" time by supplying their authenticator (e.g., password or fingerprints) in conjunction with their user ID.

(b) Protection of Authenticator. The authenticator (password or other mechanism) shall be protected at a level commensurate with the classification level and category of the information to which it allows access. The authenticator shall not be shared with anyone.

(c) Logon Attempt Rate. Successive logon attempts shall be controlled where possible by denying access after multiple (maximum of five) unsuccessful attempts to the same user ID, by limiting the number of access

attempts in a specified time period, or by a time delay control system, or other such methods, subject to approval by the accrediting official.

(d) Notification to System Personnel. Each accumulation of not more than five consecutive unsuccessful logon attempts, from a single access port or against a single user ID, shall result in immediate notification of the event to the ADP System Operator or the CSSO. (While there is no requirement for the CSSO or Operator to take any action upon receiving the notification, frequent notifications may indicate that a penetration attempt is in progress and should warrant investigation and possible corrective action).

(e) Notification to the User. Upon successful logon, it is recommended that the user be notified of: the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and each unsuccessful logon attempt using this user ID since the last successful logon. This allows the user to determine if someone else is using *or* attempting to use or guess this user ID and password.

(4) Authorization. Each file or collection of data shall have an identifiable owner. Authorization must be granted by the data owner for accessibility, maintenance, movement, and/or disposition of data based on the user's *need-to-know." This authorization may be in the form of a permission password for each type of permission on files and giving the permission password only to authorized users, or creating a file access list of users who are allowed to use the files and the permission type (read, write, change, delete) of each user.

(5) Accountability.

(a) Identification and Authentication. ADP systems must assure individual accountability. Each user of the system shall have the proper credentials and be Identified and authenticated before access is permitted. The identification and authentication methods used shall be specified and approved in the ADP security pan.

(b) Accountability Records. Where the ADP system provides the capability, accountability records shall be generated automatically by the ADP system. Manual records such as log books may be used if the automated capability does not exist. To ensure accountability, the accountability records must be protected from access

by unauthorized users (i.e., only the CSSO or other designated person should have access to these records).

(c) Audit Trail. As an accountability record for ADP systems that implement access controls, the ADP system shall create an audit trail of user IDs, authentication records, and subsequent changes to these. The events causing an entry in the audit trail shall include at least the following: successful logons; unsuccessful logon attempts; use of an authentication changing procedure; the blocking of a user ID; the reason for the blocking (e.g., due to its password reaching the end of its lifetime); and a change to the classification or protection level of information.

(d) Audit Trail Entry. For each recorded event, the audit trail record shall include at least the following: date and time of the event; type of event; offered user ID for unsuccessful logons or actual user ID for other events; and origin of the event (e.g., terminal or access port ID). Such an audit trail should not contain actual passwords.

c. Training. A training program shall be established, documented, and periodically reviewed for updating to keep ADP and user organization personnel aware of and familiar with the Classified Computer Security Program and the security aspects of the classified ADP system and the contents of associated DOE Orders.

(1) The CSPM shall ensure that a training program for CSOMs and CSSMs is developed, periodically presented, and documented. This training program shall be a preparation for the role of managing the Classified Computer Security Program.

(2) Each CSOM shall ensure that CSSMs under his or her cognizance participate in this training.

(3) Each CSSM shall ensure that a training program for CSSOs and users under his or her cognizance is developed, presented, and documented.

(4) Each CSSM shall ensure the development, documentation, and presentation of a site training program to train computer-security-escorts in their responsibilities and in the proper techniques for monitoring the actions of visitors and maintenance personnel to avoid unauthorized access or modification of equipment or data.

(5) The CSSO identifies ADP security training needs and designates appropriate operations and user personnel to attend training programs.

d. User Guidelines.

(1) Each site shall have a site-specific guideline on computer security available to all users. The purpose of this guideline is to provide all users with a basic understanding of their responsibilities and local ADP security procedures. The information in this guideline shall be included in user training. The CSSM shall establish a formal mechanism to ensure that each user acknowledges his or her responsibilities, prior to accessing a classified ADP system,

(2) In addition, each site shall have a site-specific guideline on computer security for microprocessors and word processors to be made available to all users. The purpose of this guideline is to provide all users of such ADP systems a basic understanding of their responsibilities and local ADP security procedures.

e. Marking of Classified Information. The CSSM shall ensure the development and establishment of procedures to ensure that the security classification and categories of information are clearly identified. The CSSO shall ensure that personnel handling classified information, or PARD, apply the appropriate markings to output.

(1) The appropriate classification and category of information shall be marked on all hard-copy output or recorded data that is retained in, or distributed from, the ADP facility. Appropriate security measures shall be applied to protect the information after it has been marked, such as an approved security container or vault for storage of classified information.

(2) All input/output devices, terminals, stand-alone microprocessors, or word processors used as terminals to an ADP system shall bear a conspicuous, external label which states either the highest classification and most restrictive category of the information in the ADP system or of the information being processed or displayed. This labeling may be accomplished using permanent markings on the terminal; a sign placed on the terminal (e.g., DOE/DP-0018, DOE Computer/Terminal Sensitive Data Warning Signs); or labels generated by the ADP system and displayed on the screen.

(3) Media containing classified information shall be visibly marked with the highest level of classification and most restrictive category of information contained thereon.

(4) The classification markings shall be readable and obvious to personnel handling the medium.

(5) Additional markings, documentation, and accountability control shall be applied, as appropriate, to all material in accordance with DOE 5635.1A or DCID 1/16.

(6) Procedures shall be implemented to perform a classification review of information before the information is marked at a lower classification and/or protection level unless other procedures have been approved in the ADP security plan.

(7) Procedures shall be implemented to insure that output media that are to be reused by the ADP system (magnetic tape, magnetic disks, etc.) shall have both internal and external marking indicating classification, to the extent possible.

f. Accountability. Accountability for documents produced by ADP systems shall be in accordance with DOE 5635.1A. For systems accredited at the confidential level or lower, accountability of information is not required. For systems accredited at the secret level or higher, accountability for all information is required. Accountability for information that is accessed electronically may be via the ADP system accountability records.

g. Protection of Media Containing Software. All media containing program software (operating system, security systems, utilities) which has been accepted to run on the classified ADP system shall be protected at the highest level of classification and most restrictive category of information authorized in the ADP system or any connected ADP system.

h. Clearing and Sanitization. When a classified ADP resource has been used to process classified information, all residual data must be removed before reallocation of the resource. More detailed guidance on the procedures required can be found in "A Guide to Understanding Data Remanence in Automated Information Systems, " NCSC TG 025, Version 2, (Green Book).

(1) Clearing permits the reuse of the media within the same environment (i.e., the same mode of operation and classification level), Clearing does not lower the classification level of the media.

(2) Sanitization permits the reuse of the media on a classified ADP system operating at another classification level or at an unclassified level.

(3) To complete sanitization of a classified ADP system, any classified media such as diskettes, disk cartridges, disks, tapes, printer ribbons, and hardcopy output shall be phYsically removed and protected commensurate with the highest classification of information stored on or processed by the component of the classified ADP system unless shown to be at a lower level by an approved, tested program or reviewed by an appropriately authorized person.

i. Release of ADP Equipment or Media. The CSSM shall establish procedures to assure that ADP equipment or media contain no classified information before they are released to uncleared personnel or to personnel without the proper information access authorizations. The CSSO shall assure compliance with procedures to eliminate classified information from ADP equipment or media.

j. Destruction Procedures.

(1) Destruction of Media. Procedures shall be established by the CSSM to destroy media such that the media are no longer usable and can be released without classification or other sensitivity labels. Before releasing for destruction, it is recommended that media be subjected to an approved degaussing procedure. All markings and labels which indicate previous use or classification shall be removed before releasing for destruction. Destruction shall be done in a DOE approved destruction facility.

(2) Destruction of Output. Classified printed data shall be destroyed in accordance with procedures approved by the CSSM, and according to DOE 5635.1A.

k. Remote Diagnostic Services.

(1) Remote diagnostic services for an ADP system are typically provided via a telephone line to a vendor's diagnostic service facility. The use of a remote diagnostic service in a classified ADP system will be specified in the ADP security plan. During normal operation of the classified ADP system, this communication line shall be physically disconnected from the classified ADP system by means of some positive control measure such as a lock box with a controlled key. If the diagnostic services are required, the classified ADP system shall be sanitized prior to the connection of any nonsecured communication line. The CSSM shall establish site procedures for the use of the remote diagnostic service.

(2) If a secure remote diagnostic facility can be established, such that all the diagnostic facility personnel have the appropriate clearances, and, such that secure communications

are used, then the accrediting official may approve the connection of the communication line without previous sanitization of the classified ADP system.

l. Handling and Control of Protect as Restricted Data Information
Before the designation of PARD may be used at any site, approval by the Office of Safeguards and Security is required. The security measures contained herein apply only to PARD as it appears on output media. Within the ADP system (including communication lines) PARD information will be protected consistent with the highest level of the information in the ADP system, or, at a minimum, at the Secret level. To insure against the abuse of the policy, the CSSM shall periodically and selectively review the material marked by the users as PARD.

(1) The user shall determine the use of the PARD marking for his or her information. The PARD marking shall be used if all the following criteria are met:

(a) An ADP document that may contain classified information that is not readily recognized as classified or unclassified.

(b) Operational conditions resulting from large volumes of the documents preclude utilization of certain security measures applicable to classified information.

(c) The ADP document contains a low density of potentially classified information.

(2) Examples of ADP documents that may be committed to PARD security measures are:

(a) Numerical output from weapon code calculations.

(b) Weapon code programming statements excluding documentation of the program, explanatory notes, and similar clear text material associated with a weapons code.

(3) PARD documents shall be marked as follows:

(a) The ADP documents shall be conspicuously marked on each page or sheet with the words “PROTECT AS RESTRICTED DATA.”

(b) On other output media where space does not allow, the letters “PARD” may be used.

(c) This marking shall be applied at the time of origination of the documents (e.g., printouts, microfiche, film, disk packs, and tapes).

(d) When the "PROTECT AS RESTRICTED DATA" marking cannot be included in a CRT display, the marking shall be affixed to the CRT.

(e) All PARD documents shall show the date of origination.

(4) PARD documents shall be generated and used only in a DOE security area wherein all assigned personnel have been cleared to the highest level and most restrictive category of information approved for the ADP system.

(5) PARD documents when not in use shall be stored within a security area in a manner consistent with at least one of the following:

(a) In a manner authorized for Secret documents (see DOE 5635.1A);

(b) In a security container or filing cabinet equipped with a locking device; or

(c) When the volume is so large it becomes operationally necessary, PARD matter may be stored, as a minimum, within a security area where it is administratively controlled during work hours and maintained under locked conditions during non-work hours.

(6) PARD documents shall be destroyed in the same manner as classified documents. Physical destruction shall be accomplished in compliance with DOE 5635.1A.

(7) PARD data/information shall be transferred as follows:

(a) The PARD document(s) to be transferred from the site in which it was originated to another site shall be reviewed for classification (see DOE 5650.2B), marked accordingly, and if classified, marked, handled, safeguarded, and transferred as other classified documents (see DOE 5635.1A). PARD documents may be transferred between sites authorized to originate and use PARD without such classification review.

(b) The transfer of PARD documents between points within a security or controlled area shall be made in the personal custody of "Q" cleared personnel or other appropriately cleared person approved by the accrediting official.

(c) PARD documents transferred between security or controlled areas located at the same site shall be in the personal custody of a "Q" cleared person or other appropriately cleared person approved by the accrediting official. The PARD documents shall be double wrapped with only the inner wrap marked with "PROTECT AS RESTRICTED DATA" marking. Both the inner wrapping and the outer wrapping shall contain the address label of the person to whom the matter is to be delivered. Large quantities of PARD documents may be transferred in locked substantial containers, such as a brief case, in lieu of the outer wrapper. The case or container must bear the dispatcher's or recipient's name and address.

(8) The CSSM, at each site approved for the use of PARD documents, shall ensure proper control and use of PARD documents by ensuring that each user is thoroughly aware of the special security measures necessary for the handling of PARD information. The CSSM shall ensure that an annual review is conducted to assure that accumulations of PARD documents are kept to a minimum. The CSSM shall ensure that unnecessary documents shall be destroyed without delay.

5. HARDWARE AND SOFTWARE SECURITY.

a. Protection Requirements. A combination of hardware and software security features and assurances shall be implemented (in addition to other measures such as physical and personnel security) to provide the required protection for classified data processed, stored, transferred, or accessed via the ADP system. This section defines the objectives for these hardware and software security features and assurances.

b. Determination of the Protection Requirements. The particular measures to be used are a function of the processing situation for the system. For the following specifications, the term "level of data" means the highest classification and most restrictive category of data on the ADP system. The term "user clearance" means the highest clearance level of the least cleared user. A detailed description of each requirement is in this section.

(1) Protection Index O. If the "user clearance" meets or exceeds the "level of data" on the ADP system, and all users have a need-to-know all data on the ADP system, the security program must provide for identification and authentication plus the physical, personnel, telecommunication, and administrative controls appropriate to the level of data.

(2) Protection Index 1. If the "user clearance" meets or exceeds the "level of data", but, not all users have a need-to-know all data on the ADP system, the security program must provide for access control, audit trail, and the requirements of subparagraph b(l), above.

(3) Protection Index 2. If the "user clearance" meets the classification level one level below the "level of data", the security program must provide for internal labels plus the requirements of subparagraphs b(2) and (1), above.

(4) Protection Index 3. If the "user clearance" meets the classification level two levels below the "level of data", the security program must provide for assurance testing, plus the requirements of subparagraph b(3), (2), and (1), above.

(5) Protection Index X. If the "user clearance" meets the classification level at more than two levels below the "level of data", the security program cannot at present adequately protect the data. The ADP system shall not be accredited.

(6) Protection Index Tables.

(a) A tabular form of the specification of these requirements is in Tables III-1 and III-2. The applicability of the specific hardware and software requirements is specified in Table III-2; i.e., the appropriate row of Table III-2 is chosen based on the protection index specified in Table III-1. For example: an ADP system processing Confidential and Secret Restricted Data, but, which has at least one user with only an L-clearance, (i.e., Protection Index = 2) would require accountability, access controls, internal labeling, and assurance testing. users of the ADP system had, as a minimum, a Q-clearance or a DOD Top Secret with CNWDI access, (i.e., Protection Index = O), the ADP system would require only accountability and the physical security controls necessary for the sensitivity of the data.

(b) For any classified ADP system where it is not clear what the Protection Index should be, the accrediting official shall make the determination of the required protections.

c. Features and Assurances. The following features shall be considered for use, as appropriate, to implement the security aspects of a classified ADP system. The determination of the particular measures to be used are a function of the processing

situation of the system as described above. Where it is impossible or impracticable to implement these features in the hardware or software of the ADP system, equivalent protection methods, such as increased or expanded physical or administrative security measures, may be approved by the accrediting official. If the ADP system to be used is chosen from those listed on the Evaluated Products List (EPL), as published by the National Computer Security Center as specified in DOD 5200.28-STD, the features and assurances provided at the EPL level, when properly implemented, will be accepted as proof of the systems security capabilities. For other ADP systems, adequate proof of protection features and assurances is required.

(1) Access Controls. For classified ADP systems requiring access controls, the ADP system shall control and limit access based on identification of the user and the determination of the need-to-know for the information and the appropriate clearances and authorizations.

(2) Internal Labels. Classified ADP systems requiring internal labels (those with a Protection Index of two or more) must store and preserve the integrity of the classification and other sensitivity of all information internal to the ADP system. These markings shall be an integral part of the media. These internal labels shall be used in the comparison of the individual's clearance or authorization for the information and the classification or sensitivity designation of the information being sought. Internal labels exported from the ADP system must be accurate representations of the corresponding internal labels on the information in the originating ADP system.

TABLE III-1
DETERMINING THE PROTECTION INDEX[1, 2]

Level of Data \ DOE Clearance Level[3]	None	Secret "S"	L "S"	TS "4"	QN "3"	QS "2, 1"
Sensitive Unclassified	0/1	0/1	0/1	0/1	0/1	0/1
Confidential NSI	2	0/1	0/1	0/1	0/1	0/1
Confidential RD	2	2	0/1	2	0/1	0/1
Secret NSI	3	0/1	0/1	0/1	0/1	0/1
Secret RD	3	2	2	2	0/1	0/1
Top Secret NSI	X	3	3	0/1	0/1	0/1
Top Secret RD	X	3	3	3	2	0/1
Intelligence Information[4]						

[1] For multilevel ADP Systems processing multiple levels of information, the highest value derivable from this table shall be used.

[2] ADP Systems with multiple users where all users do not have the same "need-to-know" require a minimum protection index of 1.

[3] This is the highest DOE clearance level of the least cleared user.

[4] For ADP Systems processing intelligence information, the particular processing situation and access authorizations of the users shall be addressed by the accrediting authority to determine the appropriate Protection Index.

Table III-1
Determining the Protection Index

TABLE III-2
DETERMINATION OF REQUIRED PROTECTIONS AND ASSURANCES[1]

Protection Index	Example Processing Situation	System Protection Features and Assurances	Min[2] EPL Level
0	Single user/stand alone, single level — single user personal computers — Multi user, common need-to-know (dedicated system)	Identification and authentication plus physical and administrative controls appropriate to level of data.	C1
1	Multi-user, not all same need-to-know.	Index 0 plus access control and audit trail.	C2
2	Partitioned networks, (each partition as a single level) with multi-level processing.	Index 0 and Index 1 plus internal labelling and appropriate ADP System assurance testing.	B1
3	Multi-partition networks, multi-site networks	Indexes 0 and 1 and 2 plus appropriate ADP System assurance testing.	B2
X	Not allowed	Impractical at this time.	

[1] ADP Systems with multiple users where all users do not have the same "need-to-know" require a minimum protection index of 1.

[2] If the ADP System to be used is chosen from those listed on the Evaluated Products List (EPL), as published by the National Computer Security Center and specified in DoD 5200.28-STD, the features and assurances provided by the EPL will be accepted as proof of the ADP Systems security capabilities. For other ADP Systems, adequate proof of protection features and assurances is required.

Table III-2
Determination of Required Protections
and Assurances

(3) Assurance Testing.

(a) The ADP security plan must provide a basis for determining that the ADP system correctly implements the Classified Computer Security Program. If the security features of the ADP system, as specified in the ADP security plan, are expected to restrict user access, these features must be tested to ensure that they are implementing the specified security requirements.

(b) ADP hardware and software developed by uncleared personnel shall be appropriately examined before being placed into use. The purpose of this examination is to attempt to detect features that are detrimental to ADP system security, such as hidden software that circumvents the security protections of an ADP system.

(4) Applications Software. The following requirements shall be met for new or significantly changed classified computer applications software:

(a) Security requirements shall be defined by the application owner.

(b) Security requirements shall be reviewed and approved by the CSSO prior to acquisition or formal development.

(c) Classified computer applications shall be design reviewed and system tested by the CSSO prior to operational use.

(d) The certification by the CSSO shall specify that the system meets all of the following:

1 The documented and approved security requirements;

2 Related applicable Federal and Departmental policies; and,

3 Adequate and functioning safeguarding provisions as demonstrated by the results of systems test.

(5) Data Base Management System Access Controls. Where data base management systems are used, the access controls specified in this Order for single and multi-user systems will be enforced.

ADP SECURITY PLAN

The ADP security plan is prepared by the CSSO as the basic ADP system security document and as evidence that the proposed classified ADP system, or update to an existing classified ADP system, meets the appropriate Classified Computer Security Program requirements. The ADP security plan is used throughout the certification and accreditation process and serves for the lifetime of the ADP system as the formal record of the system and its environment as approved for operation. The ADP security plan also serves as the basis for inspections of the classified ADP system. Each CSSO shall maintain a current copy of the ADP security plan and associated documents for each classified ADP system. Each CSSM shall maintain a current copy of all approved ADP security plans for the site along with the appropriate responses. The accrediting official shall maintain a current copy of all accredited ADP security plans and associated documentation.

Note: An ADP security plan may contain classified information and shall be marked and protected accordingly.

1. ATTACHED DOCUMENTS. Where sections of the following information are common to several classified ADP systems at a site, the information may be contained in a separate document and that document attached to or referenced in each ADP security plan.

2. ADP SECURITY PLAN CONTENTS. The ADP security plan formally documents the operation of a classified ADP system and the mechanisms that are used to control access and protect the ADP system and its information. To make appropriate accreditation decisions, the accrediting official needs to understand the complete ADP system environment. Therefore, as a minimum, each ADP security plan shall contain the following information

   a. The identification and location of the ADP system.

   b. The name, location, and phone number of the responsible CSSO and CSSM.

   c. A narrative description of the classified ADP system and the rules for permitting and denying access to the information that is processed, stored, transferred, or accessed by the ADP system. These rules must describe how access will be controlled based on the classification of information processed, and the clearance level and need-to-know of users.

   d. A Statement of Threat to the Classified ADP System. This statement shall be based on the site Statement of Threat for Classified Computers and shall address the threats to the classified ADP system unique to this system that are not addressed in the site Statement of Threat for Classified Computers.

e. A description of the ADP Computer Security environment that includes at least:

(1) Determination of the protection requirements for the ADP system based on the Protection Index described on page III-14, paragraph 5.

(2) Description of the methods used to meet the above protection requirements including a description of security related software.

(3) The level and amount of classified information to be processed, stored, transferred, or accessed in the ADP system.

(4) The architecture of the ADP system, including all hardware components, showing the organization, interconnections, and interfaces of these components. (A schematic drawing may be used to satisfy this requirement.)

(5) A detailed inventory of the classified ADP system components including software and hardware.

(6) Description of the control mechanisms to be used for review and approval of modifications to the classified ADP system.

f. The evidence, or basis for certification, that each of the requirements of this Order have been met. This description shall specifically address the requirements of at least the following areas: (1) Personnel Security; (2) Physical Security; (3) Telecommunications Security; (4) Hardware and Software Security; and (5) Administrative Security.

g. A description of the management controls established to prevent waste, fraud, and abuse.

h. A risk assessment which provides a measure of the relative vulnerabilities and threats. A qualitative risk assessment technique may be used.

i. A description of the ADP security training required for the personnel associated with the classified ADP system.

j. The procedures to be used by the personnel associated with the classified ADP system for reporting any computer security incidents to appropriate management and DOE. These procedures shall include the actions to be taken to secure the classified ADP system during a security-related incident.

k. The contingency plan and recovery procedures for the classified ADP system, including the designation of persons responsible for carrying out particular procedures, and the plan for testing the operations of the contingency plan.

l. A description of the process used to protect the current backup copies of critical software, data, and documentation.

m. Escort procedures, including procedures unique to this classified ADP system.

n. A description of the controls for access to the classified ADP system. If passwords are used for access control, describe how they are selected, their length, the size of the password space, and so forth.

o. The procedures for operating the ADP system in an interim period during updates or changes to the system.

p. If remote diagnostic services are to be used, specify the methods of connection, disconnection, and security measures.

PASSWORD MANAGEMENT

Authentication mechanisms that use passwords shall be developed in accordance with this Attachment. It is recommended that, whenever possible, the mechanisms discussed in this guide be automated. Additional information and recommendations on password management may be found in CSC-STD-002-85, "Department of Defense Password Management Guideline."

1. CSSO RESPONSIBILITIES.

a. Initial System Passwords. Many ADP systems come from the vendor with a few standard user IDs (e.g., SYSTEM, TEST, MASTER, etc.) already enrolled in the system. The CSSO shall ensure that the passwords for all standard user IDs are changed before allowing the general user population to access the ADP system. The CSSO must also ensure that these passwords are changed after a new system release is installed or other action is taken that might result in the restoration of these standard passwords.

b. Initial Password Assignment.

(1) The CSSO is responsible for generating and assigning the initial password for each user ID. The user must then be informed of this password. It is desirable to prevent exposure of the password to the CSSO. Whatever method is used to distribute passwords, the CSSO must verify the identity of the recipient of the password.

(2) When a user's initial password must be exposed to the CSSO, it is desirable that this exposure be nullified by having the user immediately cause a change of the password. (Presumably, this change procedure does not expose the new password to the CSSO.)

(3) Passwords shall be controlled at the highest level and most restrictive category of classified information processed or stored in the ADP system or, if all users do not have access to the highest level and most restrictive category of information processed, the password shall be stored at the highest level of access for the user.

c. Password Change Authorization. Occasionally, a user will forget a password or it may be determined that a user's password has, or may have been compromised. To correct these problems, it is recommended that the CSSO be permitted to generate a new password for any user. The CSSO should not have to know the user's password in order to do this, but should follow the same rules for distributing the new password that apply to initial password assignment. Positive identification of the user by the CSSO is required when a password must be replaced.

2. USER RESPONSIBILITIES.

a. Security Awareness. Users shall be advised of the responsibility to keep passwords private and to report suspected security incidents or changes in the user status. The CSSM shall establish a formal mechanism (such as requiring each user to sign a statement) to ensure that each user acknowledges responsibility to keep passwords private and to report changes in user status. These records shall be kept at least for the duration of the user authorization to use the ADP system.

b. Password Protection. Passwords shall be physically protected at a level [commensurate with the classification level and category of the information to which they allow access. The password shall not be shared with anyone.

c. Changing Passwords.

(1) The maximum lifetime of a password shall be no greater than one year, with a recommended lifetime of 6 months. The presence of known threats may indicate a need for a shorter maximum lifetime. Depending on the size of the password space and on how fast a penetrator can execute an attempt, it may be necessary to change passwords even more frequently.

(2) To avoid needless exposure of user passwords to the CSSO, it is recommended that users be able to change their own passwords without intervention by the CSSO. If there is the capability for the users to change their own password, users (other than the CSSO) shall be permitted to change only their own passwords.

3. PASSWORD FUNCTIONALITY.

a. Password Generation. All passwords shall be machine-generated. In no case shall a user “supply” his own password. Password acceptability shall be based on the method of selection, the length of password, and the size of the password space. The password selection method, the length of the password, and the size of the password space shall be described or referenced in the ADP security plan.

b. Interal Storage of Passwords. Stored passwords shall be protected by access controls provided by the ADP system, by password encryption, or both.

(1) Use of Access Control Mechanisms. If available, access control mechanisms shall be used to protect the password database from unauthorized modification and disclosure.

(2) Use of Encryption. Encryption of stored passwords shall be used whenever the access control mechanisms provided by the ADP system are not adequate to prevent exposure of the stored passwords,

c. Entry. When an ADP system cannot prevent a password from being echoed (e.g., in a half-duplex connection), a random overprint mask shall be printed before or after the password is entered to conceal the typed password.