MANUAL OF SECURITY REQUIREMENTS

FOR THE

CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM

U.S. Department of Energy

Office of Security Affairs

Office of Safeguards and Security

MANUAL OF SECURITY REQUIREMENTS
FOR THE
CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM

1. PURPOSE. This Manual provides specific instructions and delineates the requirements to ensure the graded security of classified information entrusted to the Department of Energy (DOE) that is processed, stored, transferred, or accessed on Automated Information Systems (AISs) and AIS networks. The requirements contained in this Manual are specified by the provisions of DOE 5639.6A, CLASSIFIED AUTOMATED INFORMATION SYSTEMS (AISs) SECURITY PROGRAM, of 7-15-94. Where it is impossible or impractical to implement these requirements in the hardware or software of the classified AIS, alternative protection methods, such as increased or expanded physical, technical, or administrative security measures, may be approved following the procedures described in DOE 5630.11B, SAFEGUARDS AND SECURITY PROGRAM, of 12-7-92.

2. SUMMARY. This Manual is composed of 14 chapters that provide management and technical information to managers and classified AIS security technical personnel.

3. REFERENCES. See Attachment 1.

4. DEFINITIONS. See Attachment 2, DOE 5639.6A.

5. ASSISTANCE. Questions concerning this Manual should be referred through the cognizant Classified AIS Security Operations Manager (CSOM) to, the Classified AIS Security Program Manager (CSPM), Information Security Policy Branch, Office of Safeguards and Security, telephone number:

(301) 903-3019.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for
Human Resources and Administration

REFERENCES

1. DOE 5639.6A, CLASSIFIED AUTOMATED INFORMATION SYSTEM (AIS) SECURITY PROGRAM, of 7-15-94, which establishes uniform policy, responsibilities, and authorities for implementation of the DOE Classified AIS Security Program.

2. 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 measures.

3. 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 AISs.

4. NCSC-TG-005, Trusted Network Interpretation, of 7-31-87, which provides interpretations of DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," for trusted computer/ communications network systems published by the National Center for Computer Security.

5. FIPS PUB 146 (Federal Information Processing Standard Publication 146), "Government Open Systems Interconnection Profile," of 7-89, which establishes open systems interconnection requirements for computer network products or services and communications systems or services acquired for use in the Federal Government.

6. Information Systems Security Products and Services Catalogue, of 1-92, published by the National Security Agency, contains the Evaluated Products List for Trusted Computer Systems.

TABLE OF CONTENTS

CHAPTER III - MODES OF OPERATION

CHAPTER IV - PROTECTION INDICES

CHAPTER I

CLASSIFIED AUTOMATED INFORMATION SYSTEMS SECURITY PROGRAM MANAGEMENT

1. OVERVIEW. Managers and users are responsible for ensuring the implementation of the Classified Automated Information Systems (AIS) Security Program. This responsibility also applies to all personnel who interact with a Classified AIS.

2. PROTECTION REQUIREMENTS AND COUNTERMEASURES. Protection requirements and countermeasures for DOE classified AISs are designed to provide for the protection of the resources and the information therein from compromise or loss. The protection is to be commensurate with the classification level and classification category of the information, the threats, and the operational requirements associated with the environment of the classified AIS.

3. PROTECTION METHODOLOGY. The Classified AIS Security Program promotes the use of a combination of management, personnel security, physical security, telecommunications security, administrative security, and technical security requirements to provide protection for classified information processed, stored, transferred, or accessed by the classified AIS and protection of the classified AIS itself. When used appropriately, these protection requirements and countermeasures provide protection for hardware, software, firmware, and classified information against destruction, disclosure, or modification. The following provisions are intended to satisfy the basic requirements for the protection of information stored or processed in classified AISs. The requirements include assurance that access to the classified information is granted only to properly cleared and authorized individuals. The classified AIS shall be accredited before processing classified information.

4. RISK MANAGEMENT CONCEPT OF OPERATION.

   a. Risk Management. Is the integrated process of assessing the threat, the vulnerabilities, and the value of the asset, and applying cost effective countermeasures. The purpose of risk management is to balance the risk of loss, damage, or disclosure of an asset against the costs of countermeasures and to select a mix that provides adequate protection without excessive cost in dollars

or in the efficient flow of information to those who require ready access to it. The use of the risk management process provides a rational, cost-effective framework as the underlying basis for security decision making. Risk management consists of the following five-step process:

(1) Asset valuation and judgement about consequence of loss. The determination of what is to be protected and its value. Note: Assets may have a value to an adversary that differs from the owner.

(2) Identification and characterization of the threats to specific assets. Intelligence assessments must address threats to the asset in as much detail as possible based on the needs of the customer.

(3) Identification and characterization of the vulnerability of specific assets. Vulnerability assessments help identify weaknesses in the asset that could be exploited.

(4) Identification of countermeasures, costs, and tradeoffs. There may be a number of different countermeasures available, each with varying costs and effectiveness.

(5) Risk Assessment. The consideration of asset valuation, threat analysis, and vulnerability assessments, along with the acceptable level of risk and any uncertainties to make a judgment of what countermeasures to apply.

b. Residual Risk. The most successful design and implementation of the requirements and countermeasures detailed in DOE 5639.6A and this Manual cannot eliminate all risks associated with the use of a classified AIS. Therefore, the goal of these requirements and countermeasures is to reduce the risk remaining (residual risk), after implementation of the protections and countermeasures, to a range that is acceptable to DOE management. Independent Validation and Verification teams will be used to identify risks and vulnerabilities in high risk classified AISs and networks. In accrediting the classified AIS, the Designated Accrediting Authority (DAA) accepts the residual risk of operating the classified AIS.

c. Site and Facility Risk Assessments. The security requirements established by DOE 5639.6A and this Manual provide countermeasures to the Revised DOE Design Basis Threat, as well as threats and risks defined in the Annual DOE Classified AIS Security Program Risk Assessment (Annual Risk Assessment). Sites and facilities do not need to conduct additional documented risk assessments unless a unique local threat has been identified and the provisions of the 5639.6A and this Manual do not provide mitigation of that threat; or unless directed by the DAA.

d. Annual DOE Classified AIS Security Program Risk Assessment. The Classified AIS Security Program Manager (CSPM) shall perform and document the Annual Risk Assessment. This assessment shall determine if the countermeasures identified in DOE 5639.6A and this Manual are adequate to minimize the risk accepted against the

nationally recognized threat.

e. Threat Identification. The Annual Risk Assessment shall be considered in assessing the threat to DOE classified AISs.

(1) The Classified AIS System Security Officer (CSSO), in coordination with the managers of the Classified AIS and the data owners, shall identify and document any threats unique to the classified AIS or the information contained therein.

(2) The Classified AIS Security Site Manager (CSSM) shall identify and document any threats unique to the site; for instance: natural phenomena such as earthquakes, tornados, etc; unique emissions repression (TEMPEST) requirements; proximity to potential adversaries (e.g., foreign nationals with access to resources). These threats shall be documented in the Site Safeguards and Security Plan or the Site Security Plan and referenced in the Classified AIS Security Plan.

(3) If there are threats to the information, classified AIS, or site, the DAA shall determine if the implementation of this Manual's requirements mitigates those threats or that an additional documented risk assessment is necessary.

(4) The Classified AIS Security Plan shall either state that there are no unique or different threats; or identify by reference those threats to the information, Classified AIS, or site that are unique or different and describe how they are to be mitigated.

f. Vulnerability Identification. The CSSO shall identify any known hardware/software vulnerabilities and determine if the countermeasures required by DOE 5639.6A and this Manual are satisfactory to mitigate the vulnerabilities and meet the security requirements. The results of this vulnerability identification shall be documented in the Classified AIS Security Plan and shall include any unique countermeasures that shall be implemented as a result.

g. Risk Acceptance. A DAA accredits the classified AIS to operate within certain parameters: within a particular security Mode of Operation; with a prescribed set of technical and nontechnical security countermeasures; against a defined threat; in a given operating environment; under a stated operational concept; with stated interconnections to other classified AISs; under a stated configuration; and at a level of risk for which the DAA has been formally authorized to assume responsibility.

5. CONFIGURATION MANAGEMENT PROGRAM.

a. Baseline Requirements. The AIS security baseline for AIS configuration management shall encompass the Hardware/Software Descriptions outlined below, the test plans, the Classified AIS Security Plans, and the procedures for making changes to these descriptions and plans.

Note: This Configuration Management Program does not include the

life cycle assurance requirements for vendor supplied security products supporting classified AISs operating with a Protection Index of three or greater.

b. Hardware/Software Description. The description requirements are defined as follows:

(1) Hardware Type Description. A Hardware Type Description is defined as containing the major components of the classified AIS. It shall identify the type of AIS component (workstations/Personal Computers (but does not include connected support equipment (printers, hard drives, etc.), hosts, servers, multiplexers, routers, gateways, etc.), its connectivity (to what the component is connected), physical location, and the communication media that support the AIS (ethernet, broadband, modems, etc.).

(2) Detailed Hardware/Software Description. A Detailed Hardware/ Software Description shall include the hardware model numbers and the software product names and release numbers.

(3) Hardware/Software Description Implementation.

(a) For Single-user, Standalone Classified AISs. A Hardware Type Description is required.

(b) For Classified AISs Operating With a Protection Index of Zero, One, or Two. A Hardware Type Description is required plus the Detailed Hardware/Software Description for the Security Support Structure.

(c) For Classified AISs Operating With a Protection Index of Three or Greater. The description shall include the same requirements as detailed in paragraph b above, plus the identification of the sensitivity level (Secret-Restricted Data, Confidential-Restricted Data, Secret-National Security Information, Confidential-National Security Information) and, where applicable, the unclassified sensitivity level (Proprietary, Privacy Act, Unclassified Controlled Nuclear Information, Unclassified Sensitive) of each connection (Port) to the Security Support Structure.

(d) Controlled Interfaces. For AISs functioning as Controlled Interfaces supporting Interconnected Networks, the Hardware/Software Descriptions will include the requirements described in paragraph (b) above, plus the identification of the sensitivity level of each connection (Port) to the Controlled Interface.

c. Ongoing Security Performance Test Plans. The Configuration Management Program shall include procedures for ensuring that the ongoing security performance test plan for the classified AIS is updated and maintained.

d. Classified AIS Security Plans. The Configuration Management Program shall include procedures for ensuring that the classified

AIS Security Plan is updated and maintained.

e. Media Resources. Media containing classified information shall be controlled in accordance with approved site accountability requirements, DOE 5635.1A, and Information Resources Management practices.

6. SOFTWARE PROTECTION. Software resident on any classified AIS shall be limited to only the software authorized for that classified AIS. Authorized software shall be determined by the responsible manager or supervisor.

a. Malicious Activities. Policies and procedures shall be established and documented by the CSSM to detect and deter incidents caused by malicious logic or unauthorized modification to software.

b. Public Domain Software. The use of public domain software on a classified AIS is strongly discouraged. Policies regarding the installation of public domain software shall be established, documented, and implemented by the CSSM. If such software is required or is desired to enhance the operation of the classified AIS, each use of such software shall be approved by the CSSM. This software shall be examined carefully and determined to contain no subversive or malicious code before it is introduced into the operating environment of the classified AIS.

c. Personally Owned Software. The use of personally owned software on a Classified AIS is prohibited.

d. Proprietary Software. Any software that is owned and licensed by a commercial vendor is considered proprietary and shall only be introduced into the operating environment of the classified AIS after the proper license to use the software has been acquired.

e. Custom Software Developed by DOE or Covered Contractors. DOE or covered contractor organizations developing security-relevant, custom software specifically for use in classified AIS facilities shall use software engineering techniques as described in DOE 1330.1D, COMPUTER SOFTWARE MANAGEMENT, of 5-18-92, and the SOFTWARE MANAGEMENT GUIDE, DOE/AD-0028, of June 1992. Such software shall be tested for correct operation and for the presence of any malicious or subversive code before being used on a Classified AIS. Problems that are identified in custom software that has been developed by other DOE sites or organizations shall be reported to the developing organization.

7. SECURITY-RELEVANT SOFTWARE MODIFICATIONS. All modifications to security-relevant resources (software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved by the responsible manager (or designee) and the CSSO for the classified AIS prior to implementation. All security-relevant modifications shall be subject to the provisions of the Configuration Management Program.

a. Those modifications which could have an effect upon the security of the Classified AIS shall be reviewed by the CSSM.

b. All security-relevant software that is resident in a Classified AIS

is included in these requirements, including operating systems, utilities, and security-relevant application programs.

(1) The responsible manager (or designee) and the CSSO may review and approve nonsecurity-related changes or additions (e.g., adding or deleting applications software) to existing classified AISs that do not deviate from the requirements of the approved Classified AIS Security Plan.

(2) Requests for changes to resources for accredited classified AISs that deviate from the requirements of the approved Classified AIS Security Plan shall be forwarded in writing to the CSSM for approval. Examples include: adding, deleting, or changing security-relevant software or hardware; or modifications to software (including the operating system) that represent a security impact.

(3) The CSSM shall notify the CSOM and the DAA of requests for changes to the resources for the classified AIS that deviate from the requirements of the approved Classified AIS Security Plan. The DAA shall consider the classified AIS for reaccreditation.

8. CLASSIFIED AIS ACQUISITION SPECIFICATIONS. DOE and covered contractor organizations shall ensure that appropriate technical, administrative, physical, and personnel security requirements are considered in specifications for the acquisition of classified AIS equipment, software, or related services to be utilized in the classified AIS environment. These security requirements shall reflect the requirements of the Protection Index for the classified AIS. The acquisition specifications shall be reviewed and approved by the CSSM. This approval shall be documented prior to issuance of the procurement and included in the classified AIS procurement documents.

9. CONTINUITY OF OPERATIONS PLANNING. A decision concerning the need for a continuity of operations plan (including contingency planning and disaster recovery planning) for each classified AIS shall be made by the manager or supervisor directly responsible for the classified AIS. This decision shall be documented and signed by the manager or supervisor. A statement of the decision and the basis for that decision shall be documented in the Classified AIS Security Plan. If a continuity of operations plan is not needed, a statement to that effect shall be included in the Classified AIS Security Plan. If a continuity of operations plan is needed, it shall be developed by site management and designed to ensure that users can continue to perform essential functions in the event the classified AIS cannot continue to perform its functions. The plan will be signed by the manager or supervisor and, at a minimum, the following topics shall be addressed:

a. Mission Essential Applications. Mission essential applications shall be identified.

b. Mission Essential Resources. Mission essential hardware and software resources related to a Classified AIS, key response and recovery personnel, and alternate site processing requirements shall be identified.

c. Response. The type of response (i.e., hot site, cold site, exchange agreements, etc.) necessary to continue the mission shall be determined based on the projected recovery time and response requirements.

d. Responsible Personnel. Site management is responsible for ensuring that the continuity of operations plan is properly implemented.

e. Backup Frequency and Location. Frequency of performing backups shall be established to ensure, at a minimum, that current backup copies of mission essential software and data exist (i.e., software or data essential to the operation of the classified AIS, and software or data necessary to support any mission essential application). The location of the backups shall be identified.

f. Documentation. Procedures shall be established to assure that all necessary documentation is maintained and available for continuity of operations and for disaster recovery. The location of documentation for continuity of operations or disaster recovery operations shall be identified.

g. Exercise of Continuity of Operations Plans. Continuity of operations plans shall be exercised (tested) and the results documented. The frequency of the testing shall be commensurate with the magnitude of loss or harm that could result from disruption of service and as approved by the DAA in the classified AIS Security Plan.

h. Cost to Exercise Plan. The documentation for the procedures shall include an estimate of the cost of exercising the plan.

10. DATA AND OPERATING SYSTEM BACKUP PROCEDURES. The CSSO is responsible for ensuring that procedures are established, documented, and implemented to back up all essential data, utility, and operating system files (including network interface software) on a regular basis. Media containing such backups shall be stored at a remote location.

11. CLASSIFIED AIS SECURITY PROGRAM EVALUATIONS. Program evaluations ensure that the Classified AIS Security Program management process continues to meet the requirements of the policies and procedures of the Department.

a. CSOM Review. Each CSOM shall ensure the review of the Classified AIS security program implemented by each CSSM. These reviews shall be conducted in compliance with DOE 5634.1B, FACILITY APPROVALS, SECURITY SURVEYS AND NUCLEAR MATERIALS SURVEYS, and they shall be documented.

b. CSSM Review. Each CSSM shall perform a self assessment of the site Classified AIS Security Program as defined in DOE 5639.1, INFORMATION SECURITY PROGRAM, including compliance by each CSSO with the site Classified AIS Security Program midway between the surveys conducted as defined in DOE 5634.1B, FACILITY APPROVALS, SECURITY SURVEYS, AND NUCLEAR MATERIALS SURVEYS. The CSSM shall prepare a summary of this review, including actions taken to correct identified findings or vulnerabilities, and transmit it to the site senior management official and notify the CSOM of this action. For sites that have many small Classified AISs (e.g.,

personal workstations, process control AISs) or have many similar systems such as distributed processors, this review may be performed on a selected basis so that each such classified AIS is reviewed by the CSSM at least once every 3 years.

12. ALTERNATIVE PROTECTION MEANS AND DEVIATIONS. Where it is impossible or impracticable to implement the protection requirements and countermeasures described in DOE 5639.6A and this Manual in the classified AIS, alternative protection means and deviations (variances, waivers, or exceptions) shall be approved under the procedures described in DOE 5630.11A.

13. USER AWARENESS AND RESPONSIBILITIES.

    a. User Guidelines. Each site shall have a site-specific Classified AIS Security Guideline available to all users. The purpose of this guideline is to provide all users with a basic understanding of their responsibilities for protecting classified information contained in classified AIS and of the local security procedures for the use of classified AISs. The information in this guideline shall be included in user training. Additionally, the guideline shall include at least the following site:

        (1) Physical security procedures;

        (2) Systems and data backup policy and procedures;

        (3) Locked door policies; and

        (4) Protection procedures for special purpose computers and equipment (i.e., facsimile machines) processing classified information.

    b. Code of Conduct. Each user of a Classified AIS shall be required to read and sign a Code of Conduct statement before initially accessing a Classified AIS. These statements shall be maintained for the period that the user requires access. Included in this statement shall be acknowledgement of the responsibility for at least the following:

        (1) For protecting his/her unique authenticator (password);

        (2) For protecting information accessed or controlled by the user;

        (3) Not to use the classified AIS resources to defraud, cause waste, or abuse resources;

        (4) Not to introduce unauthorized software into the processing environment;

        (5) To use his/her access authorization appropriately; and

        (6) To respect the operating rules of the classified AIS Security Program.

    c. Nondisclosure Agreements. Specific requirements may also exist for users to sign a nondisclosure agreement before initial access to

information with special access or disclosure requirements, such as Special Access Programs. Where these requirements exist, no user shall access such data before signing the required agreement. Such agreements shall be maintained.

14. AIS SECURITY TRAINING AND AWARENESS PROGRAM. A training program shall be established, documented, and periodically reviewed for updating. The program shall ensure that all personnel who have access to the Classified AIS are aware of and familiar with the Classified AIS Security Program, the security aspects of the classified AIS, and the contents of associated DOE directives.

    a. Training Responsibilities. Each DOE or covered contractor manager or supervisor shall ensure that all personnel under his/her direction or supervision who are authorized to use or have access to a Classified AIS have received the required training in the use of the classified AIS, and that users are familiar with their responsibilities for the protection of classified information.

    b. Qualification Training. The CSPM shall ensure that qualification training programs for CSOMs and CSSMs are developed, periodically presented, and documented. This training program shall be a preparation for the role of managing the Classified AIS Security Program. Personnel occupying either position shall complete the prescribed training programs within 1 year of appointment.

    c. Participation. DOE Site Directors, Contractor and Management and Operating Facility Managers, Director, Office of Information Technology Services and Operations, Assistant Secretary for Human Resources and Administration, and the Director of Headquarters Operations Division, Office of Security Affairs, shall ensure that CSSMs under their cognizance participate in the qualification training specified in paragraph 14b.

    d. Classified AIS Security Awareness Training. Each CSSM shall ensure that classified AIS security awareness training programs for CSSOs, data owners, and users under his/her cognizance are developed, presented, and documented. Each CSSO, data owner, and user shall participate in this training annually. This participation shall be documented.

    e. Classified AIS Escort Training. Each CSSM shall ensure the development, documentation, and presentation of a site training program to train classified AIS escorts in their responsibilities and in the proper techniques for monitoring the actions of visitors, the work of maintenance personnel, and the transport of classified AIS equipment. Completion of this training shall be documented. Each classified AIS escort shall participate in the training at least annually.

15. WASTE, FRAUD, AND ABUSE PROTECTION. The Classified AIS Security Plan shall address the frequency of the review and document the management controls established to detect and deter waste, fraud, and abuse of Government property and resources.

16. CLASSIFIED AIS SECURITY INCIDENT HANDLING. Procedures for the recording, reporting, investigating, documenting, and responding to AIS

security incidents shall be established by the CSSM and approved by the cognizant CSOM for all classified AISs that process, store, transfer, or provide access to classified information. These procedures shall 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 as described in DOE 5000.3B, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, of 1-19-93.

a. System-Specific Vulnerabilities. The CSSM shall ensure that any discovery of a hardware or software system-specific security vulnerability is also reported to the Department Computer Incident Advisory Capability. This will facilitate communication to the community of a newly discovered vulnerability. The Computer Incident Advisory Capability shall provide assistance in resolving software vulnerabilities.

b. Special Attention for Malicious Logic, Viruses, and Intruders.

(1) All incidents involving malicious logic, active viruses or intruders, proven or suspected, shall be reported to the CSSM immediately and measures shall be taken to prevent the spread of the virus or the continuing activity of the intruder.

(2) Any discovery of malicious logic, an active virus or an intruder shall be reported as an incident in accordance with DOE 5000.3B.

(3) The DOE Computer Incident Advisory Capability shall provide assistance in categorizing, preventing infection by, and handling of malicious logic, viruses and intruders.

CHAPTER II

CERTIFICATION AND ACCREDITATION

1. OVERVIEW. In making the decision to accredit, the Designated Accrediting Authority (DAA) shall consider the security protections of the classified AIS as documented in the Classified AIS Security Plan, the results of the certification tests, the certification by the Classified AIS Security Site Manager (CSSM), and any risk of operating the classified AIS.

a. Certification. Certification provides documentation stating that the classified AIS and its environment comply with requirements of the DOE Classified AIS Security Program (DOE 5639.6A and this Manual), as specified in the approved Classified AIS Security Plan. The CSSM certifies the classified AIS and provides a report of the results of the certification tests to the DAA to aid in the accreditation decision.

b. Accreditation. Accreditation is the written formal management decision to approve and authorize an organization to operate a classified AIS to process, store, transfer, or provide access to classified information. Accreditation remains in effect for 3 years, unless there are modifications to the classified AIS that

impact its security, that impact the security aspects of its environment, or that change the security requirements.

2. CLASSIFIED AIS APPROVAL AND ACCREDITATION PROCESS. All requests for approval and recommendations related to the accreditation of a Classified AIS shall proceed through the accreditation channels (see Figure II-1).

   a. Preparation of the Classified AIS Security Plan. To begin the accreditation process, the responsible Classified AIS Security Officer (CSSO) shall develop the Classified AIS Security Plan (see Chapter V) to define the manner in which the classified AIS and its information shall be protected.

   b. CSSM Review of the Classified AIS Security Plan. The completed Classified AIS Security Plan shall be reviewed by the CSSM and, if it is acceptable, forwarded to the Classified AIS Security Operations Manager (CSOM) for approval by the DAA.

   c. Approval of the Classified AIS Security Plan. The CSOM shall review the Classified AIS Security Plan within 30 days of receipt and, if acceptable, approve the plan. If the CSOM is not the DAA, the CSOM shall forward the plan, if acceptable, to the DAA. When the plan is approved, the written approval shall be forwarded through the accreditation chain for retention by the CSSM and the CSSO. Review of Classified AIS Security Plans by the DAA shall be completed or refused within 30 days of receipt. For a Classified AIS located within a Sensitive Compartmented Information Facility, see page II-6, paragraph 6f.

   d. Security Performance Test Plan Approval. Following approval of the Classified AIS Security Plan, the CSSO with the assistance of the CSSM shall develop a plan for testing the security features of the Classified AIS. The test plan is forwarded through the accreditation chain to the DAA for approval or returned for recommended revision. The test plan may be submitted for concurrent approval with the approval request for the Classified AIS Security Plan.

   e. Certification Security Performance Testing. After the Classified AIS Security Plan and the security performance test plan are approved and the classified AIS implementation is complete, certification testing shall be performed under the direction of the CSSM. The CSSM shall evaluate and certify the implementation of the security features for the classified AIS and verify that the classified AIS operates in accordance with the approved Classified AIS Security Plan. A summary of the certification test results and the certification shall be forwarded through accreditation channels to the DAA. Classified information shall not be introduced into the AIS until the accreditation has been accomplished and documented by the DAA.

   f. Independent Validation and Verification Support. For classified AISs with a Protection Index of two or greater, the cognizant CSSM shall forward a request for Independent Validation and Verification of the classified AIS design and support for the certification testing. The request shall be forwarded through the accreditation

chain to the CSPM and shall provide for funding.

g. Accreditation. The DAA shall review the certification and test result summary and formally issue a written accreditation accepting the risk of operating the classified AIS and authorizing its use to process classified information as documented in the Classified AIS Security Plan. The written accreditation shall be returned through the accreditation chain for retention by the CSSM and the CSSO. Accreditation shall be completed or refused within 30 days of receipt of the certification by the DAA.

h. Accreditation of Similar Classified AISs. Where two or more similar classified AISs are to be operated in the same operational environment (i.e., the Security Requirements Specifications are the same and the physical security requirements are similar), a Classified AIS Security Plan may be written and approved by the DAA, to cover all such Classified AISs (generally Personal Computers and standalone workstations). Each such Classified AIS Security Plan shall contain the information described in Chapter V. The Classified AIS Security Plan for these classified AISs shall specify the information required for each certification for a Classified AIS to be accredited under this procedure. The DAA shall accredit the first Classified AIS under the plan. All the other individual classified AISs to be operated under such a Classified AIS Security Plan shall be tested by the CSSO and certified by the CSSM as meeting the conditions of the accredited Classified AIS Security Plan. This certification, in effect, accredits the individual classified AISs to operate under the Classified AIS Security Plan. A copy of each certification report shall be retained with the approved copy of the Classified AIS Security Plan.

3. CLASSIFIED AIS SECURITY PLANS. A Classified AIS Security Plan shall be developed by the CSSO following the subject headings shown in Chapter V. The Classified AIS Security Plan shall provide a basis for determining that the classified AIS correctly implements the Classified AIS Security Program.

a. Security Plan Contents. The Classified AIS Security Plan shall describe the classified AIS, its interconnections, and the security protections and countermeasures. It shall document the manner in which the requirements of this Manual are to be met for the classified AIS. The requirements to be met for the protection of the classified AIS shall be based on the Protection Index and the classification levels and categories of the information to be processed.

b. Security Plan Approval. Prior to certification of the classified AIS by the CSSM, each Classified AIS Security Plan shall be reviewed and approved by the cognizant DAA.

4. SECURITY PERFORMANCE TESTING. Certification security performance testing and ongoing security performance testing provide assurance that the classified AIS is operating in accordance with the approved Classified AIS Security Plan. The certification test results, when satisfactory, provide the DAA with supporting documentation for the accreditation of the classified AIS.

a. Certification Security Performance Test Plans. The CSSO, with the assistance and approval of the CSSM, shall develop the certification security performance test plan to assure that the classified AIS has been implemented and is operating in accordance with the Classified AIS Security Plan. The certification security performance test plan shall be approved by the DAA. If the security features of the classified AIS, as specified in the Classified AIS Security Plan, are expected to restrict user access, for example, these features shall be tested to ensure that they are implementing the specified security requirements.

b. Certification Security Performance Test Performance.

(1) CSSO Specified Testing. For classified AIS with a Protection Index of zero or one, the CSSO shall assure that the specified tests are performed.

(2) Independent Validation and Verification Team Testing. For classified AISs with a Protection Index of two or greater, an Independent Validation and Verification team, in coordination with the CSSM and CSSO, shall assist in the design phase for the AIS, assist in determining and developing the certification test requirements, assist in the testing, and evaluate the security of the classified AIS.

(a) The CSPM shall appoint and be responsible for the direction of the Independent Validation and Verification team.

(b) The Independent Validation and Verification team shall be funded by the site.

(c) The CSSO shall assure that the specified tests are performed.

(3) Independent Validation and Verification Team Planning. The CSSM shall plan for three to six-person weeks of effort by the Independent Validation and Verification Team during the preliminary design phase for the AIS. From this effort the Team will develop a management plan and cost requirement estimate to prescope the Team efforts during the design phase and the test plan review and the performance of the tests. The management plan and cost requirement estimate shall be approved by the CSSM, CSOM, DAA, and the CSPM prior to proceeding with the AIS implementation.

c. Ongoing Security Performance Testing. Ongoing security performance testing of the classified AIS shall be conducted on a regular basis to ensure that the security features continue to function as stated in the Classified AIS Security Plan. The plan for ongoing security performance testing shall be described in the Certification Security Performance Test Plan. The ongoing security performance tests may include all or parts of the certification security performance test plan depending on the level of risk associated with the classified AIS and the decision of the DAA.

d. Vulnerabilities. Should any vulnerabilities or failures be revealed during the certification security performance tests or the ongoing security performance tests, the CSSM shall ensure that necessary actions are taken to eliminate or minimize their impact. Any modifications, changes, or additions to the security measures of the classified AIS shall be included in a revised Classified AIS Security Plan (or a list of changes, if the DAA concurs), and the plan shall be submitted for approval as revised. The classified AIS shall be retested as modified before the certification process is completed.

e. Documentation. The results of certification tests and an analysis of the results shall be documented.

f. Additional Tests. Following receipt of the certification documentation from the CSSM, the DAA may designate additional tests that shall be performed prior to meeting accreditation requirements.

5. CERTIFICATION. The CSSM shall evaluate the implementation of the classified AIS and the results of the certification tests to verify that the classified AIS has been implemented as described in the Classified AIS Security Plan and that the specified security controls are in place and operating properly.

a. Certification Statement. After successful completion of certification testing, the CSSM shall issue a written certification statement that assures the DAA that all requirements have been met and that the classified AIS is ready for accreditation.

b. Certification Report. The CSSM shall compile a certification report as supporting evidence for the certification statement. This report shall be forwarded through the accreditation chain. The report shall, at a minimum, be composed of the test plan, an analysis of the certification test results, the certification statement, and, at the discretion of the DAA, the approved Classified AIS Security Plan.

6. DETERMINATION OF DESIGNATED ACCREDITING AUTHORITY. The determination of the DAA shall be based on the factors described below. The DAA and the certifying official (the CSSM) shall not be the same person. For all classified AISs, the DAA shall be a DOE employee. The DAA shall review the certification report of the classified AIS (including the results of the certification testing) and, if acceptable, shall formally accredit, in writing, the classified AIS to process classified information.

a. Classified AISs Operated Under the Jurisdiction of More Than One Operations Office. For classified AISs to be operated under the jurisdiction of more than one Operations Office (including the Rocky Flats Office), the CSPM shall designate the DAA. The selected DAA shall ensure the identification of security officials to be responsible for the implementation of the Classified AIS Security Plan at each DOE site.

b. Classified AISs for Which the DAA Cannot be Determined. For classified AISs for which the DAA cannot be determined, the CSPM shall designate the DAA.

c. Classified AISs Operated With a Protection Index of Zero, One, Two, Three, or Four. For classified AISs (including non-Sensitive Compartmented Information collateral intelligence AISs operated under the cognizance of a single Operations Office, or the Rocky Flats Office, that are not located within a Sensitive Compartmented Information Facility) that are to be operated with a Protection Index of zero, one, or two, the Operations Office Classified AIS Security Operations Manager (CSOM) shall be the DAA. Classified AISs that are to be operated with a Protection Index of three or four are to be accredited by a senior management official, designated by the Operations Office Manager (or the Manager, Rocky Flats Office) as the DAA, in coordination with the CSPM.

d. Classified AIS Operated With a Protection Index of Five. For classified AISs (including non-Sensitive Compartmented Information collateral intelligence AISs that are not located within a Sensitive Compartmented Information Facility) that are to be operated with a Protection Index of five, the Operations Office Manager, or the Manager, Rocky Flats Office, in coordination with the Classified AIS Security Program Manager (CSPM), shall be the DAA.

e. Classified AISs Operated by the Headquarters. For Classified AISs (including non-Sensitive Compartmented Information collateral intelligence AISs that are not located within a Sensitive Compartmented Information Facility) operated by:

(1) Heads of Headquarters Elements,

(2) Headquarters contractor organizations, and

(3) Organizations reporting to the Headquarters.

(a) With a Protection Index of zero, one, or two, the Headquarters Operations Division, Office of Safeguards and Security, CSOM shall be the DAA.

(b) With a Protection Index of three or four, the Director of Headquarters Operations Division, Office of Safeguards and Security, shall designate a senior management official, of the Headquarters Operations Division, to be the DAA, in coordination with the CSPM.

(c) With a Protection Index of five, the Director, Headquarters Operations Division, Office of Safeguards and Security, shall be the DAA, in coordination with the CSPM.

f. Intelligence Information. For classified AISs that process intelligence information and are located in a Sensitive Compartmented Information Facility, the cognizant CSOM and CSPM shall review the Classified AIS Security Plan and the certification of the classified AIS and, if acceptable, direct it to the Office of Intelligence, Office of Nonproliferation and National Security, CSSO, with a recommendation that the Classified AIS Security Plan and the certification be forwarded for approval or accreditation to

the Director, Office of Intelligence, Office of Nonproliferation and National Security, DAA.

g. Director of Naval Reactors Program. For classified AIS networks that are solely under the jurisdiction of the Director of Naval Reactors Program and whose external components extend into the jurisdiction of different Naval Reactor Offices, the Director of Naval Reactors Program shall designate one of the Naval Reactor Office senior managers to be the DAA. Notification of the accreditation of a classified AIS with a Protection Index of two or greater shall be furnished to the CSPM.

7. PROVISIONAL ACCREDITATION. A DAA may grant provisional accreditation (temporary authority to operate) of a Classified AIS to meet documented programmatic requirements or to permit a major conversion of the classified AIS. This provisional accreditation may be granted for up to 180 days. DAA-approved protection measures shall be in place and functioning during the period of provisional accreditation. A copy of the provisional accreditation documents shall be forwarded to the CSPM.

8. REACCREDITATION. Following the intent of OMB Circular A-130, "Management of Federal Information Resources," each classified AIS shall be reaccredited by the DAA every 3 years at a minimum. Reaccreditation shall also occur if there are to be modifications to a Classified AIS that impact its security, if the security aspects of its environment change, or if the applicable security requirements change.

a. Updated Classified AIS Security Plan. The CSSO shall prepare an update to the Classified AIS Security Plan and forward it to the CSSM.

b. Review of the Classified AIS Security Plan. The updated Classified AIS Security Plan shall be reviewed by the CSSM and, if it is acceptable, approved and forwarded to the CSOM.

c. Continuation of Reaccreditation Process. From this point, the reaccreditation process should follow the certification and accreditation procedures as specified above. In those cases where there have been no security related changes to the accredited classified AIS, the DAA may elect to accept a report of ongoing security performance testing in lieu of the certification security performance testing as sufficient for reaccreditation.

**** DATABASE NOTE:
ATTACHMENT OF FIGURE II-1 - CLASSIFIED AIS SECURITY ACCREDITATION FLOWCHART (PAGE II-9 AND II-10) IS NOT INCLUDED IN DATABASE, DUE TO ITS FORMAT.

CHAPTER III

MODES OF OPERATION

1. OVERVIEW. Four Modes of Operation (dedicated, system high, compartmented, and multilevel) are authorized for classified AISs processing, storing, transmitting, or accessing classified information.

a. Boundary and Perimeter of the Classified AISs. In order to determine the Mode of Operation, it is necessary to identify both the boundary and perimeter of the classified AIS.

(1) Boundary. The conceptual limit of a Classified AIS that extends to all intended users of an AIS, both directly and indirectly connected, who receive output from the classified AIS without a reliable human review by an appropriately cleared authority.

(2) Perimeter. The conceptual limit that encompasses all components of a Classified AIS to be accredited by the DAA.

b. Determination of Mode of Operation. To determine the Mode of Operation of a Classified AIS, only two sets of facts are considered. The relationship of these two sets of facts determines the Mode of Operation of the classified AIS:

(1) The classification levels, classification categories, and handling caveats of the information processed, stored, transferred, or accessed in the classified AIS; and

(2) The security clearance types, formal access approvals, and need-to-know of all users.

Note: The available or proposed security features of the classified AIS are not relevant in determining the classified AISs actual or proposed Mode of Operation nor is the method of implementation.

2. PERIODS PROCESSING. When processing sensitive unclassified information during periods processing on a Classified AIS, the need-to-know of the users is the most important factor in determining how the information is to be protected.

3. DEFINITIONS OF MODES OF OPERATION.

a. Dedicated Mode. A Classified AIS is operating in the dedicated mode when each user with direct or indirect access to the classified AIS, its peripherals, remote terminals, or remote hosts has all of the following:

(1) A valid security clearance for all information on the classified AIS.

(2) Formal access approval for all the information processed, stored, transferred, or accessed.

(3) A valid need-to-know for all information contained within the classified AIS.

b. System High Mode. A Classified AIS is operating in the system high mode when each user with direct or indirect access to the classified AIS, its peripherals, remote terminals, or remote hosts has all of the following:

(1) A valid security clearance for all information on the classified AIS or network.

(2) Formal access approval for all the information processed, stored, transferred, or accessed.

(3) A valid need-to-know for some of the information contained within the classified AIS.

NOTE: Based on the need-to-know approvals given to them by an appropriate authority (e.g., the owners of the information or the data base administrator, different users may have access to some or all of the information processed or stored in an AIS, provided they have been cleared for such information.

c. Compartmented Mode. A Classified AIS is operating in the compartmented mode when each user with direct or indirect access to the classified AIS, its peripherals, remote terminals, or remote hosts has all of the following:

(1) A valid security clearance for all information on the classified AIS.

(2) Formal access approval for that information to which the user is to have access (i.e., some users do not have formal access approval for all Special Access Programs or intelligence compartments or subcompartments processed by the classified AIS).

(3) A valid need-to-know for that information to which the user is to have access.

d. Multilevel Mode. A Classified AIS is operating in the multilevel mode when all the following statements are satisfied concerning the users with direct or indirect access to the classified AIS, its peripherals, remote terminals, or remote hosts:

(1) Some users do not have a valid security clearance for all the information processed, stored, transferred, or accessed in the classified AIS.

(2) All users have the proper security clearance and appropriate formal access approval (i.e., signed nondisclosure agreements) for that information to which they are to have access.

(3) All users have a valid need-to-know for the information to which they are to have access.

CHAPTER IV

PROTECTION INDICES

1. PROTECTION INDICES. To provide a graded method for categorizing the risk level involved in the different Modes of Operation, the following Protection Indices have been developed. The particular protection

measures (security features and assurances) to be used are a function of the operating environment and Mode of Operation for the classified AIS. The description of the implementation of security features and security assurances assumes that physical, personnel, telecommunication, and administrative controls appropriate to the classification level of the data are in place. A general description of each requirement is contained in this Chapter. A detailed description of each requirement is contained in Chapter X.

a. Protection Index 0. This applies to classified AIS operating in the Dedicated Mode of Operation. Protection measures include:

   (1) Security Features. For multiuser classified AIS, the security features shall provide for identification, authentication, and audit capability.

   (2) Security Assurances. The security measures shall provide for configuration management, examination of hardware and software, and security performance testing.

b. Protection Index 1. This applies to classified AIS operating in the System High Mode of Operation. Protection measures include:

   (1) Security Features. The security program shall provide for resource reallocation, file access controls, file access authorizations, time lockout, and the security features of subparagraph a(1) above.

   (2) Security Assurances. The security program shall provide the assurances of subparagraph a(2) above.

c. Protection Index 2. This applies to classified AIS operating in the Compartmented Mode of Operation.

   (1) Security Features. The security program shall provide resource access controls, non-discretionary access controls, continuous on-line monitoring, and the security features of subparagraphs a(1) and b(1) above.

   (2) Security Assurances. The security program shall provide for confidence in source, flaw discovery, security penetration testing, description of Security Support Structure protections, independent validation, independent verification, security label integrity, detail design of Security Support Structure, and the security assurances of subparagraphs a(2) and b(2) above. (The Security Support Structure is described in Chapter X).

d. Protection Index 3. This applies to classified AISs operating in the Multilevel Mode of Operation where personnel with two adjacent clearance levels are allowed access to the classified AIS (i.e., the information on the AIS is a maximum of Secret-Restricted Data and personnel with "L" and "Q" clearance levels are allowed access), and is located in a secure facility.

   (1) Security Features. The security program shall provide for continuous online, automated monitoring, security level

changes, and the security features of subparagraphs a(1), b(1), and c(1) above.

(2) Security Assurances. The security program shall provide for flaw tracking and remediation, life-cycle assurance, separation of function, device labels, and the security assurances of subparagraphs a(2), b(2), and c(2) above.

e. Protection Index 4. Reserved.

f. Protection Index 5. Multilevel Mode of Operation (if at least one terminal is located in a Property Protection Area and no terminal is located outside a Property Protection Area, and is processing unclassified information). The "user security clearance" meets or exceeds the classification level for all of the data for which the user has access.

(1) Security Features. The security program shall provide for trusted path, security isolation, and all the security features of subparagraphs a(1), b(1), c(1), and d(1) above.

(2) Security Assurances. The security program shall provide for detailed design of the Security Support Structure and the security assurances of subparagraphs a(2), b(2), c(2), and d(2) above.

g. Protection Index 6. Reserved.

h. Protection Index 7. Reserved.

i. Protection Index 8. Reserved.

2. DETERMINATION OF THE PROTECTION INDEX. Tabular forms of the specification of these requirements are in Figures X-2 and X-3. (See Chapter X for detailed descriptions of Security Features and Security Assurances). The applicability of the specific security features and assurances is specified in these tables; e.g., the appropriate row of Figure X-2 is chosen based on the Protection Index and the required security features for that Protection Index are marked.

a. Example 1.

(1) A Classified AIS processing Confidential and Secret Restricted Data, but which has at least one user with an L access authorization (i.e., Protection Index 3), would require identification; authentication; audit capability; resource reallocation; file access controls; file access authorizations; time lockout; resource access controls; non-discretionary access controls; continuous on-line automated monitoring; security level changes; and physical, personnel, telecommunication, and administrative controls appropriate to the sensitivity of the data.

(2) The security assurances necessary for this Protection Index include: examination of hardware and software; security performance testing; configuration management; confidence in the software source; flaw discovery; security penetration

testing; description and detailed design of the Security Support Structure; independent validation; independent verification; security label integrity; flaw tracking and remediation; life-cycle assurance; separation of function; and device labels.

b. Example 2.

(1) If all users of the Classified AIS had, at a minimum, a Q access authorization and the need-to-know all data on the classified AIS (i.e., Protection Index 0), the classified AIS would require identification; authentication; audit capability, and the physical, personnel, telecommunications, and administrative security controls appropriate for the sensitivity of the data.

(2) The security assurances necessary for this Protection Index include: examination of hardware and software; security performance testing; and configuration management.

3. INDETERMINATE PROTECTION INDEX. When it is not clear what the Protection Index should be for a Classified AIS, the CSPM shall make the determination of the required Protection Index.

CHAPTER V

CLASSIFIED AIS SECURITY PLAN

1. OVERVIEW.

a. The Classified AIS Security Plans are prepared by the CSSO as the basic classified AIS security document and as evidence that the proposed classified AIS, or update to an existing classified AIS, meets the appropriate Classified AIS Security Program requirements. The Classified AIS Security Plan is used throughout the certification and accreditation process and serves for the lifetime of the classified AIS as the formal record of the AIS and its environment as approved for operation. The Classified AIS Security Plan also serves as the basis for inspections of the Classified AIS. Each CSSO shall maintain the copy of record of the Classified AIS Security Plan and associated documents for each classified AIS. Each CSSM shall (at a minimum) maintain a current list of the classified AIS on his/her site or facility. The designated DAA shall maintain accreditation documentation for each of the classified AIS he/she has accredited.

b. Each AIS, such as a standalone mainframe, minicomputer, personal work station, Unified Network, or Interconnected Network that processes classified information shall be covered by a Classified AIS Security Plan. Two or more similar Classified AISs may be combined under a Classified AIS Security Plan (see page II-2, paragraph 2h).

Note: If a Classified AIS Security Plan is determined to contain classified information, the plan shall be appropriately marked and

protected.

2. COMMON DOCUMENTS. Information common to several classified AISs at a site or information contained in other documents may be attached to or referenced in the Classified AIS Security Plan.

3. CLASSIFIED AIS SECURITY PLAN. The Classified AIS Security Plan formally documents the operation of a Classified AIS and the measures that are used to control access and protect the classified AIS and its information. To make appropriate accreditation decisions, the DAA needs to understand the complete classified AIS environment. Therefore, at a minimum, each Classified AIS Security Plan (including Classified AIS Security Plans covering two or more similar classified AISs) shall contain the following information:

   a. Introduction.

      (1) The identification and location of the classified AIS.

      (2) A brief narrative description of the classified AIS including its mission or purpose.

   b. Security Requirements Specification. The Security Requirements Specification is a unique sub-set of the Classified AIS Security Plan that defines the secure operating environment of the classified AIS (see Figure V-1). The Security Requirements Specification shall be developed as an attachment to the Classified AIS Security Plan for use if the classified AIS is to become part of an interconnected network. If at any time it is necessary or desirable to link a classified AIS into a network, the information in the Security Requirements Specification will be used to determine any necessary changes in or additions to protections or countermeasures.

      (1) Security Personnel. The name, location, and phone number of the responsible System Owner, DAA, CSSO, CSSM, and Data/ Application Owner (if appropriate).

      (2) Secure Operating Environment. Brief description of the secure operating environment of the classified AIS.

      (3) Data Sensitivity. The determination of the data sensitivity by analysis and documentation of the following:

         (a) The classification levels (i.e., Top Secret, Secret, Confidential) and categories (i.e., Restricted Data, Formerly Restricted Data, National Security Information) of the data, and the percentages of each, to be processed, stored, transferred, or accessed;

         (b) Any compartments (as defined in Director Central Intelligence Directive, 1/16) or special access programs for the data;

         (c) Any special formal access approvals necessary for access to the data (e.g., Access to Special Access Programs);

(d) Any special handling instructions or caveats (e.g., NO CONTRACT, WNINTEL);

(e) The need-to-know restrictions on all users, directly connected to the classified AIS; and

(f) The presence of any sensitive unclassified data (e.g., Privacy, Proprietary, Unclassified Controlled Nuclear Information).

(4) Personnel Security. State the range of security clearance levels, the set of formal access approvals, and the need-to-know of users of the classified AIS.

(5) Protection Index. Identify the mode of operation and the protection index (as described in Chapters III and IV).

(6) Physical Protection. The documentation of any special physical protection requirements that are unique to the classified AIS.

(7) Security Contracts. A copy of any security contracts (memoranda of understanding) with other Federal agencies or entities and a list of all security contracts associated with the classified AIS.

(8) Approved Waivers, Variances, or Exceptions. A descriptive list and a copy of the approval documentation of any approved waivers, variances, or exceptions.

(9) Special Security Countermeasures. The details of any special security countermeasures in use in the classified AIS.

c. System Description. A brief description of the classified AIS, including all hardware components, showing the organization, interconnections, and interfaces of these components (block diagrams may be used to satisfy this requirement).

d. Configuration Management Program. A brief description of, or reference to, the Configuration Management Program associated with the classified AIS.

e. Risks and Vulnerabilities.

(1) A statement about the risk assessment of any unique vulnerabilities or threats to the classified AIS shall document or reference threats unique to the site, the information, or threats unique to the classified AIS itself. If there are no unique threats or vulnerabilities, a statement to that effect will be entered (see page I-2, paragraph 4d).

(2) Another statement shall document vulnerability identification by the CSSO and the implemented countermeasures to mitigate these vulnerabilities (see page I-2, paragraph 4e).

f. Security Measures. Using the topics in Chapters VI - XIII as a reference, a description of how these requirements have been met

shall be provided. This description shall specifically address:

(1) Personnel Security. Describe, attach, or reference the classified AIS escort procedures (see page I-10, paragraph 14e).

(2) Physical Security. Provide a brief description of the physical security environment, e.g., type of Security Area, minimum security clearance level allowed without escort (reference Site Safeguards and Security Plan or Safeguards and Security Plan, DOE 5630.13A, MASTER SAFEGUARDS AND SECURITY AGREEMENTS, or DOE 5630.14A, SAFEGUARDS AND SECURITY PROGRAM PLANNING).

(3) Telecommunications Security. Include or reference the Protected Distribution System documentation and the provisions for TEMPEST security.

(4) Administrative Security.

(a) If passwords are used for authentication of system access control, describe or reference procedures for administration of passwords (see page IX-2, paragraph 3c and Attachment IX-2).

(b) Describe the protection requirements and procedures for all authenticators including passwords.

(c) Describe or reference procedures to protect against scavenging.

(d) Describe the methods and procedures used to sanitize the classified AIS between users and/or classification levels when periods processing is used.

(e) Describe or reference the site marking procedures if different from the requirements described on page IX-3, paragraphs 5 and 6.

(5) Technical Security.

(a) Describe or reference the auditing procedures to be followed in the event of the failure of the auditing capability. Classified AIS shutdown criteria shall be included (see page X-2, paragraph 2c(1)).

(b) For AISs operating with a Protection Index of one or greater, define the time lockout interval of inactivity in interactive sessions and describe the restart requirements.

(c) Describe the use of Evaluated Products List products or justification for alternative methods, hardware, or software.

(d) Describe the application software certification process.

(6) Waste, Fraud, and Abuse. Describe the management controls established to deter and detect waste, fraud, and abuse.

g. Network Requirements. If the classified AIS is implemented as a network, the Classified AIS Security Plan shall also address the following items:

(1) Overview of the Network. Include descriptions of the sub-networks, servers, hosts.

(2) Communications Protocols. Briefly describe all protocols used in the network.

(3) Security Support Structure. Briefly describe the Security Support Structure including all controlled interfaces and guards, their interconnection criteria, and their security requirements. Also, describe any encryption methods used to provide discretionary/nondiscretionary controls and the communications security devices that protect intranetwork communications.

(4) Security Policies. Describe or reference the network security policies and procedures. If referenced, include a brief synopsis of the referenced policies and procedures, including:

(a) Access control policies.

(b) Authorization and authentication policies.

(c) Audit policies.

h. Remote Maintenance/Diagnostics. If approved remote diagnostic or maintenance services are to be used, specify the methods of connection, disconnection, and security measures.

i. Ongoing Security Performance Test Plan. Describe the plan for ongoing security performance testing and the frequency of such testing.

j. Security Incidents. Attach or reference the procedures to be used by the personnel associated with the classified AIS for reporting any classified AIS security incidents to appropriate management and DOE. These procedures shall include the actions to be taken to secure the classified AIS during a security-related incident.

k. Continuity of Operations.

(1) State the continuity of operations decision. If the decision was made to have a continuity of operations plan, reference the plan, and include a short abstract of the plan. Include the documentation of the frequency and cost to exercise the plan, the DAA approval documentation, and provide or reference a list of the applications on the classified AIS that require a continuity of operations plan.

(2) If the decision was made not to require a Continuity of Operations Plan, describe the process used to protect the

current backup copies of software, data, applications, and the documentation judged to be essential to the continued operation of the classified AIS.

4. INTERCONNECTED CLASSIFIED AIS SECURITY PLAN. A network operating as an Interconnected Network shall have an Interconnected Classified AIS Security Plan that:

   a. Designates the individuals responsible for the secure operation (e.g., CSOM, CSSM) of the Interconnected Network;

   b. Describes the secure operating environment and protections of the Network Security Support Structure including a description of the operation of any Controlled Interfaces;

   c. Identifies any special security responsibilities of the users of the Interconnected Network;

   d. Lists the networks (Interconnected or Unified) and AISs that comprise the Interconnected Network.

   e. Includes a copy of the Security Contract for each separately accredited network or AIS with a copy of the Security Requirements Specification. Also includes copies of the Security Requirements Specifications for each network as attachments; and provides a Security Requirements Specification for the Interconnected Network (see Page XI-4. paragraph c.).

**** DATABASE NOTE:
ATTACHMENT OF FIGURE V-1 - DEVELOPMENT OF SECURITY REQUIREMENTS SPECIFICATIONS (PAGE V-7 AND V-8) IS NOT INCLUDED IN DATABASE, DUE TO ITS FORMAT.

CHAPTER VI

PERSONNEL SECURITY REQUIREMENTS

1. BASELINE REQUIREMENTS. The requirements of DOE 5631.2C, PERSONNEL SECURITY PROGRAM, shall be met. All classified AISs shall have adequate controls to ensure that personnel having access to the hardware, software, or data have the proper security clearance, formal access approvals, and need-to-know.

2. PERSONNEL ACCESS. Personnel who (a) operate the classified AIS, (b) control access, or (c) design, develop, install, modify, service, or maintain the security features that control user access or program access to the classified AIS or to the operating system shall have been cleared for access to the highest classification level and most restrictive classification category of information for which the classified AIS or any connected classified AIS is accredited. If it is necessary for maintenance or other personnel who are not so cleared to have temporary access to the classified AIS, they shall be escorted by a trained classified AIS escort authorized by the CSSO.

3. USERS OF THE CLASSIFIED AIS.

a. Protection Index Zero, One, or Two. Personnel (including application programmers) who are authorized access to the classified AIS shall have been cleared for access to the highest classification level and most restrictive classification category of information processed, stored, transferred, or accessed in the classified AIS.

b. Protection Index Three or Greater. Personnel (including application programmers) who are authorized access to the classified AIS shall have been cleared for access to the highest classification level and most restrictive classification category of information for which they are authorized and to which they have access.

CHAPTER VII

PHYSICAL SECURITY REQUIREMENTS

1. BASELINE REQUIREMENTS. Each classified AIS, including remote terminals, printers, or other output devices, communication links, memory, and other interconnected devices, shall be afforded physical security commensurate with the highest classification level and most restrictive classification category of information to which it provides access. Components of the classified AIS shall be contained in security areas authorized by an approved Site Safeguards and Security Plan or a Site Security Plan. Security controls to protect the equipment apply not only to the classified AIS and its components but also to all removable media such as magnetic tapes, magnetic disk packs, and spare or replacement parts once they are identifiable with a specific Classified AIS or Network.

2. PROTECTION REQUIREMENTS FOR PROTECTION INDEX ZERO, ONE, TWO, OR THREE. Any accredited classified AISs with a Protection Index of zero, one, two, or three shall be located in at least a DOE Limited Area. The following protection requirements also apply:

   a. The classified AIS or components can only be left unattended, without additional action as described in subparagraph (b) below, under the following conditions:

      (1) The area is authorized by an approved Site Safeguards and Security Plan or Site Security Plan for the open storage of classified information; and,

      (2) All personnel authorized unescorted access have a need-to-know for all the information processed, stored, transferred, or accessed by the classified AIS.

   b. If the classified AIS or any of its components is to be left unattended and the area is not authorized by an approved Site Safeguards and Security Plan or Site Security Plan for the open storage of classified information, then:

      (1) All classified information shall be removed from the

classified AIS and its components and shall be stored in DOE-approved security containers as defined by DOE 5632.5, PHYSICAL PROTECTION OF CLASSIFIED MATTER;

(2) The classified AIS and/or component shall be sanitized as described in Chapter IX; and

(3) All interfaces to Protected Distribution Systems shall be disconnected and shall be secured (both the disconnection and securing of the interface shall be accomplished with a DAA-approved mechanism).

3. PROTECTION REQUIREMENTS FOR PROTECTION INDEX OF FOUR OR FIVE. Any accredited classified AIS with a Protection Index of four or five (see Chapter IV) shall be located in at least a DOE Limited Area and the following restrictions shall also apply:

a. Components that are exclusively in the unclassified portion of a multilevel AIS shall be located within at least a DOE Property Protection Area as described by DOE 5632.1B, PROTECTION PROGRAM OPERATIONS.

b. The physical security controls over the components and their associated communications channels shall be commensurate with the highest classification level and most restrictive classification category of information released to or processed by that component.

c. The classified AIS or components can only be left unattended, without additional action as described in subparagraph (d) below, under the following conditions:

(1) The area is authorized by an approved Site Safeguards and Security Plan or Site Security Plan for the open storage of classified information; and,

(2) All personnel authorized unescorted access have a common need-to-know for all the information processed, stored, transferred, or accessed by the classified AIS.

d. If the classified AIS or any of its components is to be left unattended and the area is not authorized by an approved Site Safeguards and Security Plan or Site Security Plan for the open storage of classified information, then:

(1) All classified information shall be removed from the classified AIS or its components and shall be stored in DOE-approved security containers as defined by DOE 5632.5;

(2) The classified AIS or component shall be sanitized as described in guidance published periodically by the CSPM; and

(3) All interfaces to a Protected Distribution System shall be disconnected and shall be secured (both the disconnection and securing of the interface shall be accomplished with a DAA-approved mechanism).

4. UNESCORTED PHYSICAL ACCESS TO THE CLASSIFIED AIS.

a. Protection Index of Zero, One, or Two. Unescorted physical access to a Classified AIS shall be controlled and limited to personnel whose "need-to-know" has been verified by the CSSO and cleared for access to the highest classification level and most restrictive classification category of information processed, stored, transferred, or accessible by the classified AIS.

b. Protection Index of Three or Greater. Unescorted physical access to components of a classified AIS shall be controlled and limited to personnel whose "need-to-know" has been verified by the CSSO, and cleared for access to the highest classification level and most restrictive classification category of information processed, stored, transferred, or accessible by that component.

c. Temporary Access. If it is necessary for personnel who are not cleared to the highest classification level and most restrictive classification category to have temporary access to the Classified AIS security area, they shall be escorted by a trained classified AIS escort authorized by the CSSO.

5. VISUAL ACCESS REQUIREMENTS. Each classified AIS shall be protected in a manner which prevents unauthorized personnel from having visual access to the information being displayed.

CHAPTER VIII

TELECOMMUNICATIONS SECURITY REQUIREMENTS

1. BASELINE REQUIREMENTS. Each communication link which supports a Classified AIS with a Protection Index of zero, one, or two shall be protected commensurate with the classification level and classification category for which the classified AIS is accredited. Communication links supporting classified AISs with a Protection Index of three or greater shall be protected according to the highest classification level and most restrictive classification category of information carried by that link. Unless a Classified AIS is approved for multilevel processing, all physical and logical connections will be protected at the highest classification level and most restrictive classification category of the information that the AIS is accredited to process. Protection must be provided by National Security Agency-approved encryption devices, Protected Distribution Systems, products from the Evaluated Products List, or other accepted physical protections, in accordance with DOE Orders.

2. TRANSMISSIONS SECURITY. Protected Distribution Systems or National Security Agency approved cryptographic devices shall be used to protect classified information on communication lines that pass outside the Security Area of a classified AIS or classified AIS Facility. The specific security area of a classified AIS Facility and the security-related devices to be used shall be described in the Classified AIS Security Plan.

a. Communications Security. When National Security Agency approved cryptographic devices are used in connection with a Classified AIS, the classified AIS security certification documentation shall

contain assurance that the installation of the encryption devices and facility are in accordance with DOE 5300.3D, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY.

b. Protected Distribution Systems. When a Protected Distribution System is used in connection with a classified AIS, the classified AIS security certification documentation shall contain assurance that the Protected Distribution System meets the requirements of DOE 5300.4D, TELECOMMUNICATIONS: PROTECTED DISTRIBUTION SYSTEMS.

c. Use of STU-III as an Encryption Device. The use of a STU-III instrument to transmit and receive classified information as a designed-in, integrated part of a classified AIS application constitutes the establishment of a network. In this case, all requirements for the accreditation of a network are applicable.

3. EMISSION SECURITY. Measures shall be implemented to control compromising emanations from telecommunications equipment and classified AISs in accordance with DOE 5300.2D, TELECOMMUNICATIONS: EMISSION SECURITY (TEMPEST). These measures shall comply with Site TEMPEST Plan requirements. The accreditation process shall confirm that TEMPEST requirements are being met.

CHAPTER IX

ADMINISTRATIVE SECURITY REQUIREMENTS

1. BASELINE REQUIREMENTS. Procedures shall be established to ensure that all classified AIS and classified AIS Facilities have adequate administrative controls for access to the facility and appropriate handling of classified information. These procedures shall be documented in each classified AIS Security Plan. The CSSO is responsible for ensuring that these security procedures are enforced. DOE 5635.1A, CONTROL OF CLASSIFIED DOCUMENTS AND INFORMATION, applies to all classified matter removed from the boundary of the classified AIS.

2. USER WARNING NOTICE.

a. Notice to All Users. All users of classified AISs shall be notified prior to gaining access to a Classified AIS that system usage is monitored, recorded, and subject to audit. The user must also be advised that using the system grants the consent of the user to such monitoring and recording and that unauthorized use is prohibited and subject to criminal and civil penalties.

(1) Initial Screen Notice. Where the operating system of the classified AIS permits, each initial screen (displayed before user logon) shall contain a warning text to the user. The following is a suggested warning text to the user. The user must take positive action to remove the notice from the screen.

"WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated

Information System is prohibited and could be subject to criminal and civil penalties."

(2) Other Methods of Notification. Where it is not possible to provide an "initial screen" Warning Notice, other methods of notification shall be developed by the CSSM for approval of the DAA.

b. Monitoring and Recording. Monitoring and recording is a requirement of this Manual.

3. USER ACCESS CONTROLS. Each person having access to a multiuser classified AIS shall have the proper security clearances and authorizations and be uniquely identified and authenticated before access to the classified AIS is permitted. The identification and authentication methods used shall be specified and approved in the Classified AIS Security Plan. User access controls in multiuser classified AISs shall be assigned by the CSSO and shall include authorization, user identification, and authentication.

a. User Authorizations. The manager or supervisor of each user of a Classified AIS shall determine the required authorizations, such as need-to-know, for that user.

b. User Identification (User IDs). Each user ID shall be assigned to only one person at any one time. No person shall share the same user ID with another person. A record of the user ID assignment shall be kept available for a minimum of 12 months after the user access has been terminated.

Note: Alternate forms for identifying users (e.g., group IDs, functional titles) may be used for nonidentification purposes (e.g., data base access control, mail).

(1) User ID Reuse. Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) shall be removed from the classified AIS.

(2) User ID Removal. The CSSM shall ensure the development and implementation of a procedure whereby prompt notification is given to the CSSO when a user ID and its authentication shall be removed from the classified AIS (e.g., when an employee leaves the sponsoring organization, when notified of the need to remove access for cause).

(3) User ID Revalidation. 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) are updated as necessary.

c. Authentication. Each user of a multiuser Classified AIS shall be authenticated before access is permitted. This authentication can be based on any one of 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 IX-2 and shall be changed at least every 6 months (For classified AISs operated at a Protection Index of zero or one, that only process information at the Confidential level, the DAA may approve the changing of passwords every 12 months).

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

(2) Protection of Authenticator. An authenticator that is in the form of knowledge or possession (password, smart card, keys,) shall not be shared with anyone.

(a) Protection Index of Zero, One, or Two. When passwords are used as authenticators, they shall be protected at a level commensurate with the accreditation level of the classified AIS.

(b) Protection Index of Three or Greater. When passwords are used as authenticators, they shall be protected at a level commensurate with the classification level and classification category of the information to which it allows access.

4. USER ACCOUNTABILITY. The classified AIS shall ensure individual accountability. This shall be accomplished by identifying the user, authenticating the user, and maintaining audit trails.

5. MARKING OF CLASSIFIED AIS COMPONENTS. The CSSM shall develop procedures to ensure that all components of a Classified AIS, including input/output devices, terminals, standalone microprocessors, or word processors used as terminals, shall bear a conspicuous, external label which states the highest classification level and most restrictive classification category of the information accessible to the component in the classified AIS. This labeling may be accomplished using permanent markings on the component; a sign placed on the terminal (e.g., DOE Computer/Terminal Processing Warning Signs); or labels generated by the classified AIS and displayed on the screen.

6. MARKING OF CLASSIFIED AIS MEDIA. The CSSM shall ensure the development and implementation of procedures to ensure that the security classification levels and categories of information are clearly identified as outlined below.

a. Hardcopy Output. Hardcopy output includes paper, fiche, film, and other printed media. The CSSO shall ensure that personnel handling classified information or Protect as Restricted Data information (see Attachment IX-1) apply the appropriate markings to hardcopy output. Security measures appropriate to the classification level, classification category, and other controls shall be utilized to protect the information, such as the use of an approved secure storage container or vault for storage of classified information.

(1) Protection Index Zero, One, or Two. The accreditation level of the accredited classified AIS shall be marked on all hardcopy output that is retained in, or distributed from, the

Classified AIS Facility unless an appropriate classification review has been conducted or the information has been output by a tested program verified to produce consistent results and approved by the DAA. Such programs will be tested on a statistical basis to assure continuing performance.

(2) Protection Index Three or Greater. The highest classification level and classification category of the information recorded on the hardcopy shall be marked on all hardcopy output that is retained in, or distributed from, the Classified AIS Facility.

b. Removable Media. The CSSO shall ensure that personnel handling removable media apply visible, human-readable, external markings to the media.

(1) Protection Index of Zero, One, or Two. Removable media shall be marked with the accreditation level of the classified AIS unless an appropriate classification review has been conducted or the information on the media has been outputted by a tested program or methodology verified to produce consistent results and approved by the DAA.

(2) Protection Index of Three or Greater. Removable media shall be marked with the highest classification level and most restrictive classification category of the information ever recorded on the media since it was last sanitized.

(3) Classified AIS Facilities. In Classified AIS Facilities where some of the AISs are operated as classified and some are dedicated to unclassified operation, the removable unclassified media shall be uniquely marked to protect from the mixing of the media.

(4) Additional Requirements. The following additional external labeling requirements apply:

(a) Information Security Oversight Office standard labels denoting the classification level of the media shall be used where it is practical to apply the label without impeding the operation of the removable media. (Information Security Oversight Office labels denoting only "Classified" shall not be used.)

(b) If the label can impede the operation of the removable media, (e.g., not allowing the media to properly seat), then alternate marking methods are required. The classification markings shall be visible and human-readable, and shall easily communicate the classification level and category of the information. Marking procedures that differ from this shall be submitted in the Classified AIS Security Plan for approval by the DAA.

(c) If Information Security Oversight Office labels are used, then either:

1 The category shall be overprinted or written in; or

2 An additional label shall be utilized to display the classification category information.

(d) If other labels are to be used, their use shall follow CSSM established procedures to display the classification level and classification category.

(e) Classifier or classification source documentation are not required to be applied to the removable media unless the media is to be transferred beyond the boundary of the classified AIS.

(f) In accordance with Director Central Intelligence Directive 1/16 or other programmatic requirements, additional markings and accountability controls shall be applied to all removable media, as required.

(5) Security Labels. Procedures shall be implemented internal to classified AISs processing at Protection Index of two or greater to ensure that output media (magnetic tape, magnetic disks) that are to be reused by the classified AIS or transferred beyond the boundary of the classified AIS have both security labels and external markings indicating classification level, classification category, and handling instructions.

7. TRANSFER OF REMOVABLE MEDIA. Removable media being transferred beyond the boundary of the classified AIS that contain classified information shall be marked as described above and protected and controlled in accordance with DOE 5635.1A.

8. PROTECTION OF MEDIA CONTAINING SYSTEM SOFTWARE.

a. Protection Index Zero, One, or Two. All media containing program software including operating systems, security systems, utilities, and vendor-supplied diagnostics, application programs, and data that have been used on a Classified AIS shall be protected at the accreditation level for the classified AIS, unless the media has been subjected to a process, approved by the DAA, which proves that the media has not been contaminated with classified information.

b. Protection Index Three or Greater. All media containing program software including operating systems, security systems, utilities, and vendor-supplied diagnostics, application programs, and data that have been used on the Classified AIS shall be protected at the highest level of classification and most restrictive category of information authorized in the component using the media.

9. PROTECTION OF PRINTER MEDIA. Specific methods for protecting printer media shall be described in the Classified AIS Security Plan and approved by the DAA.

a. Protection and Destruction of Multistrike Printer Ribbons. Multi-strike printer ribbons used in a Classified AIS or in the classified component of a Classified AIS need not be labeled for classification or sensitivity if they remain in the printer. They

may remain in the printer if the printer is located in at least a DOE Limited Security Area. When these media are removed and replaced, they shall be destroyed in a manner approved for the disposal of classified waste. If a ribbon is removed for purposes other than destruction, it must be appropriately marked, handled, and stored at the highest level and category of the classified information that it printed.

b. Laser Toner Cartridges. Laser printer toner cartridges that have been used in a Classified AIS must be protected as classified until they have been sanitized.

(1) Sanitization of Laser Printer Toner Cartridges. Laser printer toner cartridges shall be sanitized by running five "full" pages of randomly-generated characters through the printer. The pages of text must contain no blanks or solid black areas and shall be treated as unclassified. Once the cartridge is sanitized, the cartridge may either be recycled, released for destruction as unclassified waste, or used on an unclassified AIS.

(2) Maintenance of Laser Printer Toner Cartridges. Laser toner cartridges used in a Classified AIS must be sanitized before sending them out for maintenance. If the cartridge cannot be sanitized, it must be treated as classified waste when replaced.

10. CLEARING AND SANITIZATION. When a Classified AIS resource has been used to process classified information, all residual data shall be removed before reallocation of the resource. More detailed information on the procedures required can be found in guidance issued periodically by the CSPM.

a. Clearing. Clearing permits the reuse of the resource within the same environment (i.e., the same Protection Index and operating environment). Clearing does not lower the classification level or the classification category of the resource.

(1) Clearing of Storage Media. Storage media, such as magnetic tape or disks, on which classified information has been recorded may be cleared by overwriting the media once with unclassified information. Detailed instructions on the clearing of storage media shall be issued periodically by the CSPM.

(2) Clearing of Memory. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to the higher classification level or more restrictive classification category of information. Detailed instructions on the clearing of memory shall be issued periodically by the CSPM.

b. Sanitization. Sanitization permits the reuse of the media on a classified AIS operating at another classification level and/or classification category or at an unclassified level. Sanitization of a classified AIS resource shall be accomplished before it may be released from classified information controls or released for use

at a lower classification level. To sanitize storage media, memory, and hardware, the following requirements shall be met:

(1) Sanitization of Storage Media. The media shall be degaussed with an approved degausser for that specific type of media or destroyed before it can be considered sanitized. Clearing is not an approved method for sanitization. Detailed instructions issued periodically by the CSPM detail the sanitization and destruction procedures for different storage technologies.

(2) Sanitization of Memory. Volatile semiconductor memory normally can be sanitized by the removal of main and auxiliary or backup power. Nonvolatile memory shall be sanitized using the procedures outlined in guidance periodically issued by the CSPM.

(3) Sanitization of Hardware Components. Hardware that has been used to process classified information shall be sanitized in accordance with the guidance issued periodically by the CSPM.

(4) Visual Examination of Hardware Components. To complete sanitization of a Classified AIS, any classified media such as diskettes, disk cartridges, disks, tapes, printer ribbons, and hardcopy output shall be physically removed. An examination of the display device for evidence of residual information shall be conducted.

11. DESTRUCTION PROCEDURES.

a. Destruction of Media. Procedures shall be established by the CSSM to ensure the sanitization of media such that the media can be released for destruction without classification or other sensitivity labels. The CSSO shall ensure that the established procedures are followed for the destruction of media. Destruction procedures for storage media, memory, and hardware are provided in guidance issued periodically by the CSPM.

b. Destruction of Output. Classified printed data shall be destroyed in accordance with procedures in the DOE 5635.1A.

12. MOVEMENT OF CLASSIFIED EQUIPMENT AND SOFTWARE. When the hardware or software resources of a Classified AIS are used or marked for use in a classified environment, they shall not be removed from the security area except in the custody of trained classified AIS escort (see Page I-10, paragraph 14.e) unless properly sanitized.

13. RELEASE OF CLASSIFIED AIS EQUIPMENT. The CSSM shall establish procedures to assure that classified AIS equipment contains no classified information before it is released to uncleared personnel or to personnel without the proper access authorizations. Where practical, markings and labels which indicate previous use or classification shall be removed before release. The CSSO shall ensure compliance with procedures to eliminate classified information from classified AIS equipment.

14. RELEASE OF MEDIA. If information is to be released from a classified

environment to an environment at a lower classification level, it shall be produced on new or sanitized media and subjected to a review by a properly authorized, cleared individual (e.g., the data owner) or it shall have been produced by a verified program approved by the DAA.

15. WASTE, FRAUD, AND ABUSE REVIEW. The files contained on all classified AISs shall be randomly reviewed by the CSSO to identify any cases of use of the equipment or AISs in a way that would constitute waste, fraud, or abuse. At a minimum, one-third of all classified AISs shall be reviewed annually (see Page I-10, paragraph 15). These reviews shall be nonperiodic and unannounced. The reviews shall be documented and the results reported to the CSSM. As an alternative, for facilities with a large number of similar classified AISs, a statistical sampling method of reviewing may be approved by the DAA.

16. REMOTE DIAGNOSTIC OR MAINTENANCE SERVICES FOR CLASSIFIED AISs. If remote diagnostic or maintenance services are required, the classified AIS shall be sanitized and disconnected from any communication links to a network prior to the connection of any nonsecured communication line.

    a. Site Procedures. The CSSM shall establish site procedures for the use of the remote diagnostic or maintenance service. The use of a remote diagnostic or maintenance service in a Classified AIS shall be specified in the Classified AIS Security Plan. During normal operation of the Classified AIS, this communication line shall be physically disconnected from the Classified AIS by means of some positive control measure such as a lockbox with a controlled key.

    b. Secure Remote Classified Diagnostic Facility. If a secure remote classified diagnostic facility can be established, and approved by the CSPM, the DAA may approve the connection of the communication line without previous sanitization of the classified AIS.

PROTECTION REQUIREMENTS FOR INFORMATION MARKED "PROTECT AS RESTRICTED DATA"

1. SITES AUTHORIZED TO USE PARD DESIGNATION. The following DOE or covered contractor sites have been authorized to use the PARD designation:

    a. Los Alamos National Laboratory, Los Alamos, New Mexico.

    b. Lawrence Livermore National Laboratory, Livermore, California.

    c. Sandia National Laboratories - Albuquerque, Albuquerque, New Mexico.

    d. EG&G, Energy Measurements Inc. - North Las Vegas Facility, Las Vegas, Nevada, and Nevada Test Site, Mercury, Nevada.

    e. Los Alamos National Laboratory, Lawrence Livermore National Laboratory and Sandia National Laboratory, Albuquerque - North Las Vegas Facility, Las Vegas, Nevada, and Nevada Test Site, Mercury, Nevada.

2. HANDLING AND CONTROL OF PARD INFORMATION.

a. Authorization to Use the PARD Designation. Approval by the Director of Nonproliferation and National Security is required prior to using the designation of PARD at any site. Authorizations to use the PARD designation are valid for only 1 year.

b. PARD Protection Requirements. The security measures contained herein apply only to PARD information as it appears as output. Within the classified AIS (including communication lines), PARD information shall be protected consistent with the highest level of the information in the classified AIS or, at a minimum, at the Secret-Restricted Data level. To ensure against abuse of the policy, the CSSM shall conduct periodic and selective reviews of the material marked by the users as PARD.

c. Determination of Use. The user shall determine the use of the PARD marking for his/her information. The PARD marking shall only be used if all the following criteria are met:

(1) A classified AIS output is generated that may contain limited quantities of classified information that is not readily recognized as classified or unclassified due to its being contained in large quantities of unclassified information.

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

(3) The classified AIS output contains a substantial volume with a low density of potentially classified information.

(4) Examples of classified AIS output 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 weapon code.

(5) PARD information shall be marked as follows:

(a) The classified AIS output shall be conspicuously marked on each page or sheet with the words "PROTECT AS RESTRICTED DATA." On output where space does not allow, the letters "PARD" may be used.

(b) This marking shall be applied at the time of origination of the classified AIS output (e.g., printouts, microfiche).

(c) When the "Protect as Restricted Data" marking cannot be included in a Cathode Ray Tube display, the marking shall be affixed to the Cathode Ray Tube.

(d) All PARD output shall show the date of origination.

(6) PARD information shall be generated and used only in a DOE Limited Area wherein all assigned personnel have been cleared to the accreditation level of classified information approved for the classified AIS.

(7) PARD classified AIS output 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 (DOE 5635.1A);

(b) In a secure storage 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, at a minimum, within a security area where it is administratively controlled during workhours and maintained under locked conditions during nonworkhours.

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

(9) 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 (DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION) marked accordingly and, if classified, marked, handled, protected, and transferred as other classified documents (DOE 5635.1A).

(b) PARD documents may be electronically transmitted between sites authorized to originate and use PARD without such classification review. However, the data shall be protected at the accreditation level of the classified AIS on which it was produced.

(c) The transfer of PARD documents between points within a Security Area shall be made in the personal custody of Q cleared personnel or other appropriately cleared person approved by the DAA.

(d) PARD documents transferred between Security 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 DAA. 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 classified address 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 shall bear the dispatcher's or recipient's name

and address.

(e) 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 are destroyed without delay.

PASSWORD MANAGEMENT

Authentication measures that use passwords shall be developed in accordance with this Attachment. It is recommended that, whenever possible, the measures 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 classified AIS come from the vendor with a few standard user IDs (e.g., SYSTEM, TEST, MASTER) 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 access to the classified AIS. The CSSO shall 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. Password Length. When passwords are used for the authentication of users for access control purposes, they shall contain a minimum of six nonblank characters.

c. Initial Password Assignment. The CSSO is responsible for ensuring the generation and assignment of the initial password for each user ID. It is desirable to prevent exposure of the password. Whatever method is used to distribute passwords, the CSSO shall technically or visually verify the identity of the recipient of the password.

d. Password Change Authorization. Occasionally, a user may 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 and suspend the previous password. Positive identification of the user by the CSSO is required. 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.

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 site procedure (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. The CSSO is responsible for ensuring that this procedure is followed before each user is granted access to any classified AIS. These records shall be kept at least for the duration of the user authorization to use any classified AIS under the CSSMs cognizance.

b. Password Protection. Passwords used to control access to classified AIS shall be protected at a level commensurate with the highest classification level and most restrictive classification category of the information accredited for processing on the system unless the system is accredited for multilevel processing. For multilevel classified AIS, passwords shall be protected consistent with the highest classification level and most restrictive classification category to which they grant access. When used to authenticate personal identity, the password shall not be shared with anyone.

c. Changing Passwords. 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 produced by a method approved by the DAA. In no case shall a user "supply" his/her 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 Classified AIS Security Plan.

b. Internal Storage of Passwords. Stored passwords shall be protected by access controls provided by the automated information system, by encryption, or both.

(1) Use of Access Control Measures. If available, access control measures 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 measures provided by the classified AIS are not adequate to prevent exposure of the stored passwords.

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

CHAPTER X

TECHNICAL SECURITY REQUIREMENTS

1. BASELINE REQUIREMENTS. A combination of technical 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 classified AIS. This chapter delineates those technical security features and assurances that shall be activated and certified as operational prior to accreditation. Tabular forms of the specification of these requirements are in Figures X-2 and X-3. The determination of the particular measures to be used are a function of the Protection Index of the Classified AIS.

2. SECURITY FEATURES. The following features shall be implemented as required by the Protection Index of the classified AIS.

   a. Identification Controls. Multiuser classified AISs shall control and limit user access based on identification and authentication of the user. The requirements for user authorization and use of user IDs are found on page IX-2, paragraphs 3a and b.

   b. Authentication. Multiuser classified AISs shall ensure that each user of the classified AIS is authenticated before access is permitted.

      (1) Requirements. Requirements for authentication controls and the use of authenticators are found on page IX-2, paragraph 3c.

      (2) Additional Authentication Countermeasures. Where the operating system provides the capability, the following features shall be implemented:

         (a) Logon Attempt Rate. Successive logon attempts shall be controlled by denying access after multiple (maximum of five) unsuccessful attempts on the same user ID; by limiting the number of access attempts in a specified time period; by the use of a time delay control system; or other such methods, subject to approval by the DAA.

         (b) Notification to the User. The user shall be notified upon successful logon 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 the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

   c. Audit Capability. A record of each logon and logoff to any multiuser classified AIS shall be maintained. Where there are multiple users of the classified AIS and where an automated capability does not exist, a manual log shall be maintained at the discretion of the DAA.

      (1) Audit Capability Failure. The Classified AIS Security Plan shall provide procedures to be followed in the event of a failure in the audit record capability. These procedures shall include shutdown criteria for the classified AIS.

(2) Accountability for Electronic Information. Accountability for information that is accessed electronically shall be via the classified AIS accountability records (audit trail).

(3) User Accountability. The classified AIS shall ensure individual accountability. This shall be accomplished by identifying the user, authenticating the user, and maintaining audit trails.

(4) Audit Trail Generation and Protection. Where the classified AIS provides the capability, audit records shall be generated automatically. To ensure user accountability, the accountability records shall be protected from access by unauthorized users (i.e., only the CSSO or other authorized person shall have access to these records).

(5) Audit Trail Requirements. For classified AISs that implement automated access controls, the classified AIS shall create an audit trail of user IDs, authentication records, and subsequent changes to these as an accountability record. Audit trails shall provide the capability to reconstruct a security incident.

(a) Recording Anomalies. The events causing an entry in the audit trail shall include at least the following:

1 For all classified AISs:

a Use of authentication changing procedures.

b Unsuccessful logon attempts.

c The blocking of a user ID and the reason for the blocking (e.g., due to its password reaching the end of its lifetime).

2 For classified AISs to be operated at a Protection Index of one or greater:

a Actions to open, close, create, and destroy files.

b Unauthorized system file access attempts.

3 For classified AISs to be operated at a Protection Index of two or greater, changes to security labels that lower the classification levels or reduce the restrictions of a classification category.

(b) Additional Events. Other events that may be included for the purpose of reconstructing security incidents are:

1 Start and stop of classified periods processing.

2 Initiation and termination of pertinent system security related events.

(c) The DAA may decide to supplement or reduce the recorded events, described in subparagraph (b) above, in order to meet operational requirements.

(6) Audit Trail Monitoring. All audit trails created by multiuser classified AIS shall be monitored by the CSSO for unauthorized access, attempted access, or other anomalies on a scheduled basis but at least weekly. These reviews shall be documented. Large AISs and AISs with a high level of activity shall require more frequent monitoring. The frequency of the review shall be stated in the Classified AIS Security Plan. Other audit trail monitoring capabilities shall be implemented as follows:

(a) Automated Extraction of Audit Data. For classified AIS operating with a Protection Index of two or greater, the AIS shall provide tools for the automated extraction of audit data.

(b) Automated Analysis of Audit Data. For classified AIS operating with a Protection Index of three or greater, the AIS shall provide tools for the automated analysis of audit data.

(c) Continuous, Online Automated Monitoring and Real Time Warning. For classified AISs operating with a Protection Index of three or greater, the AIS shall provide for continuous, online monitoring (audit) of use and real time warning to the CSSO of suspected misuse.

(7) Audit Records Retention. Audit records shall be retained for a minimum of 6 months.

d. Resource Reallocation and Allocation.

(1) Resource Reallocation. Classified AISs with a Protection Index of one or greater shall clear memory and storage before reallocation to a different user (see page IX-6, paragraph 10a).

(2) Resource Allocation. For classified AISs operating with a Protection Index of two or greater, the Security Support Structure shall provide the capability to control a defined set of system resources (e.g., memory, disk space) such that no one user can deny access to the resources of another user.

e. File Access Controls. For classified AISs operating with a Protection Index of one or greater, classified files shall be protected by a secondary access control measure. This may be implemented by measures such as file passwords, access control lists, or other techniques, as approved by the DAA.

f. File Access Authorization. For classified AISs operating with a Protection Index of one or greater, the operating system shall provide a file access control measure that allows the data owner to specify which other users can access each file that he or she owns

and the specific type of access granted (such as read, write, or execute).

g. Time Lockout. For classified AISs operating with a Protection Index of one or greater, the AIS shall time lockout an interactive session after an interval of user inactivity. The time interval and restart requirements shall be specified in the Classified AIS Security Plan.

h. Resource Access Controls. Classified AISs operating with a Protection Index of two or greater shall store and preserve the integrity of the classification and other sensitivity of all information internal to the classified AIS.

(1) Security Labels. The classified AIS shall place security labels on all entities.

(a) Resource security labels reflect the sensitivity (classification level, classification category, and handling caveats) of the information on the resource (e.g., files). Resource labels shall be an integral part of the electronic data or media.

(b) User security labels reflect the authorizations (security clearances, need-to-know, formal access approvals) of users.

(c) Resource and user security labels shall be compared and validated before a user is granted access to a resource.

(2) Export of Security Labels. Security labels exported from the classified AIS shall be accurate representations of the corresponding security labels on the information in the originating classified AIS.

i. Nondiscretionary Access Controls. For classified AISs operating with a Protection Index of two or greater, nondiscretionary access controls shall be provided. These controls shall provide a means of restricting access to objects based on the sensitivity (as represented by the label) of the information contained in the objects and the formal authorization (i.e. security clearance) of subjects to access information of such sensitivity.

j. Security Level Changes. For classified AISs operating with a Protection Index of three or greater, the system shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A user shall be able to query the system as desired for a display of the user's complete sensitivity label.

k. Trusted Path. For classified AISs operating with a Protection Index of five or greater, the AIS shall support a trusted path between itself and the classified AIS user for initial identification and authentication.

l. Security Isolation. For classified AISs operating with a

Protection Index of five or greater, the AIS Security Support Structure shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the Security Support Structure shall provide isolation and noncircumventability of isolation functions.

3. SECURITY ASSURANCES. Security assurances provide the confidence that the classified AIS is operating as expected and in accordance with the Classified AIS Security Plan.

   a. Examination of Hardware and Software. Classified AIS hardware and software shall be examined when received from the vendor and before being placed into use.

      (1) Classified AIS Hardware. Commercially procured hardware shall be examined to assure that the hardware contains no features which might be detrimental to the security of the classified AIS. Subsequent changes and developments which affect security may require additional examination.

      (2) Classified AIS Software. Commercially procured software shall be examined to assure that the software contains no features which might be detrimental to the security of the classified AIS. Security related software shall be examined to assure that the security features function as specified.

      (3) Custom Software or Hardware Systems. New or significantly changed software and hardware developed by or specifically for the Department shall be subject to testing and review at all stages of development. Security requirements shall be defined by the data owner. Security reviews shall occur at the Design Review, System Testing, and Operational Review stages.

   b. Security Performance Testing. Security performance testing includes both certification testing that is performed before the classified AIS is accredited and ongoing performance testing that is performed on a regular basis. Requirements for certification testing are found on page II-3, paragraph 4, and requirements for ongoing security testing are found in page I-5, paragraph 5c.

   c. Configuration Management. The requirements for configuration management are specified on page I-3, paragraph 5.

   d. Confidence in Software Source. In acquiring resources to be used as part of a classified AIS operating with a Protection Index of two or greater, consideration shall be given to the level of confidence placed in the vendor to provide a quality product, to support the security features of the product, and to assist in the correction of any flaws.

   e. Flaw Discovery. For classified AIS with a Protection Index of two or greater, the vendor shall provide a method for ensuring the discovery of flaws in the system (hardware, firmware, or software) that may have an effect on the security of the AIS.

   f. Security Penetration Testing. In addition to testing the

performance of the classified AIS with a Protection Index of two or greater for certification and for ongoing testing, there shall be testing to attempt to penetrate the security countermeasures of the system. The test procedures shall be documented in the test plan for certification and also in the test plan for ongoing testing.

g. Description of Security Support Structure Protections. The protections and provisions of the Security Support Structure shall be documented in such a manner to show the underlying planning for the security of a Classified AIS with a Protection Index of two or greater. Hardware and software features shall be provided that can be used to periodically validate the correct operation of the elements of the Security Support Structure.

h. Independent Validation. An Independent Validation and Verification team shall assist in the certification testing of a Classified AIS with a Protection Index of two or greater and shall perform validation of the system as required by the CSPM.

i. Independent Verification. An Independent Validation and Verification team shall assist in the certification testing of classified AIS with a Protection Index of two or greater and shall perform verification testing of the system as required by the CSPM.

j. Security Label Integrity. For a classified AIS accredited to operate with a Protection Index of two or greater, the methodology shall ensure the following:

(1) Integrity of the security labels;

(2) The association of a security label with the transmitted data; and

(3) Enforcement of the control features of the security labels.

k. Detailed Design of Security Support Structure.

(1) For classified AISs operating with a Protection Index of two or greater, an informal description of the security policy model enforced by the system shall be available.

(2) For classified AISs operating with a Protection Index of five or greater, a formal description of the security policy model enforced by the AIS shall be available and an explanation provided to show that it is sufficient to enforce the security policy. All interfaces to the Security Support Structure shall be included in the design documentation.

l. Flaw Tracking and Remediation. For classified AISs operating with a Protection Index of three or greater, the vendor shall provide evidence that all discovered flaws have been tracked and remedied.

m. Life-Cycle Assurance. The development of the classified AIS hardware, firmware, and software shall be under life-cycle control and management (i.e., control of the classified AIS from the earliest design stage through decommissioning) for a Classified AIS with a Protection Index of three or greater. (This assurance shall

be contractually imposed upon the vendor.)

n. Separation of Functions. For classified AISs with a Protection Index of three or greater, the functions of the CSSO and the classified AIS manager shall not be performed by the same person.

o. Device Labels. For a Classified AISs accredited to operate with a Protection Index of three or greater, the methodology shall ensure that the originating and destination device labels are a part of each message header and enforce the control features of the data flow between originator and destination.

4. USE OF EVALUATED PRODUCTS LIST. The Department endorses the use of products from the Evaluated Products List. When determined to be properly implemented, these products shall be accepted as meeting the security requirements for the portion of the classified AIS where they are used.

Note: Caution should be used in combining Evaluated Products List products either with other products from the Evaluated Products List or with products that are not on the Evaluated Products List to assure that they are being used in the same configuration that they were tested; to assure that all the protection features are properly used; and to assure that the integration of these products with other products (Evaluated Products List listed or not) provides the necessary protection for the classified AIS. (Figure X-1 is provided for comparison to Evaluated Products List values.)

Mode of Operation	Protection Index	Evaluated Products List Rating
Single-user, Standalone	0	D
Dedicated (Multiuser)	0	C1
System High	1	C2
Compartmented	2	B1
Multilevel A *	3	B1+***
Multilevel B**	5	B3

* Multilevel A is the Mode of Operation if the AIS has only one security clearance level difference (minimum Confidential), and it is located in a controlled (secure areas only) facility.

** Multilevel B is the Mode of Operation if the AIS has at least one security clearance level difference (minimum unclassified), and it is located in a controlled (secure and property protection areas) facility.

*** The B1+ level of protection can be achieved by attaining the functionality of an National Computer Security Center, Evaluated Products List rating of B1 (same as compartmented mode) plus the following B2 security criteria:

	1. Security Level Changes.
	2. Device Labels.
	3. Flaw Tracking and Remediation.
	4. Separation of Functions. System Manager/Security Officer.
	5. Life-Cycle Assurance.
	6. Informal Model. More detailed than B1 but less than the formal model required at B2.

Figure X-1
Equivalence Table

**** DATABASE NOTE:
ATTACHMENT OF FIGURE X-2 - SECURITY FEATURES (SUMMARY) (PAGE X-9 AND X-10) IS NOT INCLUDED IN DATABASE, DUE TO ITS FORMAT.

CHAPTER XI

CLASSIFIED AIS NETWORK SECURITY REQUIREMENTS

1. OVERVIEW. The characteristics and capabilities of classified AISs implemented as networks require special security considerations. This chapter imposes additional requirements on a network or expands on previously stated security requirements as they apply to a network.

   a. Scope. A Classified AIS implemented as a network may be small (two or three personal workstations) or very large (several supercomputers and supporting equipment with thousands of connected terminals). Networks may be internal to a site or location, local to a municipal area, or global in nature. Networks may be internal to a contractor (including a global network) or external with connections from various contractors or agencies.

   b. Security Protections. As with other classified AISs, the Protection Index of the network determines the security protections and countermeasures required for the network.

   c. Classified AIS Networks. For the purposes of this Manual, there are two types of networks, a Unified Network and an Interconnected Network. A Unified Network is a network operating under a single Protection Index (Security Requirements Specification). An Interconnected Network is composed of two or more networks or separately accredited AISs separated by a Security Support Structure that adjudicates the differences in security requirements between the networks or AISs. This can be as simple as the Security Support Structure only being used to adjudicate need-to-know differences between networks or AISs with the same protection indexes or as complex as using the Security Support Structure to adjudicate the security differences of networks or AISs with different protection indexes.

   d. Security Plans and Security Requirements Specification. Each Unified Network shall have a Classified AIS Security Plan (see Chapter V). The Classified AIS Security Plan for the Interconnected Network consists of the Security Requirements Specification from each connected network or AIS plus the Security

Requirements Specification for the Interconnected Network and any additional paperwork needed to describe and secure the Interconnected Security Support Structure adjudicating the security differences of the Interconnected networks or AISs (See page XI-4, paragraph 4a.)

e. Accreditation.

(1) Unified Network. Unified Networks are accredited by a single DAA to operate under a single Protection Index.

(2) Interconnected Networks. Interconnected Networks are also accredited by a single DAA to operate under a single Protection Index. This Protection Index may be different than the Protection Indices of each attached network or AIS. Interconnected Networks are composed of networks or AISs that were each separately accredited before they were interconnected. These networks or AISs do not need to be reaccredited; they are now part of an Interconnected Network and can continue to operate as separate, independently, accredited networks. The DAA for the Interconnected Network shall authorize these networks or AISs to operate together and accredits only the Interconnected Network Security Support Structure as capable of adjudicating the security differences of the networks or AISs that now make up the Interconnected Network.

2. SECURITY SUPPORT STRUCTURE. The Security Support Structure includes all the resources (hardware, software, firmware, and communications) of a Classified AIS that perform security functions directly related to the transfer of information over communications lines, such as Controlled Interfaces, Network Security Controllers, and Secure File Servers. The secure operation of the classified AIS depends on the reliable operation of the Security Support Structure. No reliance for secure operation will be placed on resources that are not part of the Security Support Structure.

a. Secure Operation. All the trust for the secure operation of the classified AIS is placed in the components of the Security Support Structure.

b. Secure Transmission. The network Security Support Structure shall ensure that the security parameters are delivered to the correct component without change or loss.

c. Certification Testing. For a Classified AIS implemented as a network with a Protection Index of two or greater, the secure operation of the Security Support Structure shall be validated and verified by an Independent Verification and Validation team appointed by the CSPM.

3. UNIFIED NETWORK. A Unified Network is composed of network components or AISs and has a well-defined network architecture and design. It is generally administered by a single organizational authority (e.g., contractor, Operations Office). A Unified Network operates under one Classified AIS Security Plan, under one DAA, and with one set of Security Requirements Specifications.

Note: A Unified Network may be as simple as two Personal Computers connected together or a single host and collection of terminals or it may be as complex as an interconnection of local area networks that provide computing services for an entire facility.

a. Forming a Unified Network. Before linking two classified AISs together to form a Unified Network, the Security Requirements Specification of each Classified AIS to be linked into the network shall be compared to determine the Protection Index of the resulting network. This comparison of the Security Requirements Specifications shall be used to determine any conflicts created by linking the Classified AISs together and what additional countermeasures shall be required to provide the necessary level of security. The Security Requirements Specifications shall be compared and any conflicts resolved whether the classified AISs consist of standalone AISs, Personal Computers, or personal workstations.

b. Adding a Classified AIS to a Unified Network. When adding a Classified AIS to a Unified Network, the CSSM responsible for the network shall compare the Security Requirements Specification for the new network classified AIS with the Security Requirements Specification for the currently accredited network.

(1) No Difference. If there is no difference between the Security Requirements Specifications, the classified AIS may be added to the network without reaccreditation of the network. The CSSO is responsible for ensuring that the Classified AIS Security Plan is current.

(2) Difference. If there is a difference between the Security Requirements Specifications, the classified AIS shall not be added until the differences have been resolved and the network CSSM has certified that there are no differences. If the differences cannot be resolved, the Security Requirements Specification for the network shall be revised and the network reaccredited.

c. Security Support Structure. The Security Support Structure of a Unified Network consists of any and all portions of the Unified Network that are relied upon to provide security for the network.

d. Classified AIS Security Plan. A Classified AIS Security Plan shall be developed showing how the network complies with requirements for secure operation as described in DOE 5639.6A and Chapter V of this Manual. An abbreviated copy of the Classified AIS Security Plan may be distributed to each CSSO.

4. INTERCONNECTED NETWORK. An Interconnected Network consists of two or more networks or AISs interconnected with a DAA approved network Security Support Structure. The networks or AISs that make up the Interconnected Network may belong to different Federal agencies, different Operations Offices, different DOE Programs, or simply different Divisions of the same organization. A Partitioned Classified Network, as described in Attachment XI-1, is a method of implementing an Interconnected Network using controlled interfaces. An Interconnected

Network operating at a Protection Index of 3 or greater must utilize a Controlled Interface as the Network Security Support Structure.

a. Interconnected Security Support Structure. The software, hardware, firmware, and equipment that mediates the differences in security and need-to-know between the attached networks or AISs that make up the Interconnected Network is called the Network Security Support Structure. This is used to limit information shared or transmitted between attached networks or AISs. The Security Support Structure of the Interconnected Network may overlap with its associated networks or AISs. Where such an overlap occurs, it shall be the responsibility of both DAAs and so documented in the Interconnected Classified AIS Security Plan.

b. Controlled Interface Implementation. Each Controlled Interface shall be implemented to monitor and enforce the security protections and requirements of the network and adjudicate the differences in security attributes between the separately accredited networks or AISs to ensure compliance and security. Controlled Interfaces are described in paragraph 8 of this Chapter.

c. Security Contract. An Interconnected Network shall have a security contract (memorandum of understanding) between the administrative entities (Agencies, contractors, etc.) involved which describes the management of the network, the sensitivity of the data to be transmitted, any special security considerations, and the requirement that all parties to the security contract shall not change the Security Requirements Specification of their network or AIS without renegotiating the security contract. Each security contract shall be reviewed annually for currency. A copy of each network or AIS Security Requirements Specification shall be attached to each security contract.

d. Certification Testing. The operation and security of the Interconnected Security Support Structure shall be tested and approved before accreditation of the Interconnected Network.

e. Interconnected Classified AIS Security Plan. A network operating as an Interconnected Network shall have an Interconnected Classified AIS Security Plan that meets the requirements of DOE 5639.6A and Chapter V of this Manual. Copies of the Interconnected Classified AIS Security Plan will be furnished to the CSOM and the CSSM for each network or AIS.

f. Interconnection. A network or AIS connected as a component of an Interconnected network shall not connect to another network or AIS. The only method of adding networks or AISs to an existing Interconnected network is through the Interconnected Security Support Structure and the revision of the Interconnected Classified AIS Security Plan.

g. Adding to an Interconnected Network. A network or AIS must be separately accredited before adding it to an Interconnected Network.

h. Perimeter of a Network. For the purpose of determining the security responsibilities of the DAA who accredits an

Interconnected Network, the perimeter of an Interconnected Network is the network Security Support Structure. This perimeter does not include the separately accredited networks or AISs, unless the network Security Support Structure has components or parts in those networks or AISs or other attached separately accredited networks or AISs. The perimeter of the network does include any interface component(s) (hardware or software) that may be installed in the separately accredited classified AIS, terminal, or workstation (i.e., any portion of the separately accredited AIS that is a component of the network Security Support Structure).

5. NETWORK MODE OF OPERATION AND PROTECTION INDICES. See Chapters III and IV.

6. CLASSIFIED AIS NETWORK MANAGEMENT. A Classified AIS Network shall comply with all the management requirements specified for a Classified AIS in Chapter I of this Manual. In addition, a Classified AIS network (Unified or Interconnected) shall comply with the following requirements:

   a. Designated Accrediting Authority. The selection of a DAA for a Classified AIS Network is based on the requirements of DOE 5639.6A and Chapter II of this Manual. The DAA shall ensure the designation of security officials (such as CSSO, CSSM) responsible for the secure operation of the network.

   b. Configuration Management Program. Since network configurations change frequently, the Classified AIS Security Plan shall specify procedures for configuration management and the methods for ensuring continuing security as changes are implemented through the Configuration Management Program. The CSSO who is responsible for the network shall advise the cognizant CSSM of any proposed or planned alterations to the network design or operation which impact upon network security. The CSSM shall, in turn, advise the DAA for the network of these proposed changes.

   c. Software Implementation. If any component of the interconnected Security Support Structure or Controlled Interface resides partly in the software or firmware of a connecting Classified AIS, its installation in the classified AIS shall be subjected to review in the certification process conducted in support of that network's accreditation.

   d. Certification Testing.

      (1) Network certification testing shall be conducted to demonstrate that the implementation of the network meets the requirements specified in the classified AIS Security Plan. The tests to be performed shall be specified in writing. Each feature shall be tested to ensure that it does not adversely impact any of the other network security features.

      (2) For classified AIS networks with a Protection Index of two or greater, an Independent Verification and Validation team shall assist in the certification testing.

   e. Certification. The CSSM responsible for the network shall perform

the certification. The CSSM is responsible for ensuring compatibility between the overall Classified AIS Security Plan and the individual Classified AIS Security Plan of each network component. The CSSM shall evaluate the implementation of the classified AIS and the results of the certification tests to verify that the network has been implemented as described in the Classified AIS Security Plan and that the specified security controls are in place and operating properly.

(1) Certification Statement. The CSSM shall issue a written certification statement that assures the DAA that all requirements have been met and that the classified AIS network is ready for accreditation.

(2) Certification Report. The CSSM shall compile a certification report as supporting evidence for the certification statement. This report shall be forwarded through the accreditation chain. The report shall, at a minimum, be composed of the test plan, an analysis of the certification test results, and the certification statement.

f. Accreditation. A network shall be accredited prior to its operational use. Accreditation shall be accomplished or refused within 30 days of receipt of certification documentation by the office of the DAA.

g. Reaccreditation. Each classified AIS implemented as a network shall be reaccredited by the DAA, at a minimum, every 3 years. Reaccreditation shall also occur if there are modifications to a classified AIS that impact its security; if the security aspects of its environment change; or if the applicable security requirements change.

7. CLASSIFIED NETWORK SECURITY REQUIREMENTS. The security requirements for a Classified AIS network (Unified or Interconnected) follow the same topical areas as those for a Classified AIS. In a network, the failure of a security function may impact the security of not only a single Classified AIS but also of the entire network and its individual components. The following requirements are in addition to those specified in Chapter X and shall be addressed and documented when applied to a Classified AIS implemented as a network.

a. Access Control.

(1) Identification and Authentication Forwarding. Reliable forwarding of the identification shall be used between classified AIS when users are connecting through a network. When identification forwarding cannot be verified, a request for access from a remote classified AIS shall require authentication before permitting access to the system.

(2) Protection of Authenticator Data. In forwarding the authenticator information and any tables (e.g., password tables) associated with it, the data shall be protected from access by unauthorized users (e.g., by encryption), and its integrity shall be ensured.

b. Audit Trails and Monitoring.

(1) The classified AIS implemented as a network shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of successful and unsuccessful accesses to the classified AIS network components within the perimeter of the accredited network. The audit data shall be protected so that access is limited to the CSSO or his/her designee.

(2) As Protection Index levels increase, monitoring of network activity becomes more crucial to the security posture of the network. Methods of continuous, online monitoring of network activities shall be included in each network with a Protection Index three or greater. This monitoring shall also include real time notification to the CSSO of any system anomalies.

(3) The network audit trail shall contain the following types of information.

(a) Identification of the user accessing any component of the network.

(b) Starting and ending times of each access to any component (including file access) of the network.

(c) For networks operating with a Protection Index of two or greater, the changing of the configuration of the network (e.g., a component leaving the network or rejoining).

(4) For each recorded event, the audit record shall contain, at a minimum: date and time of the event; the user ID; type of event; and success or failure of the event.

(5) Identification shall be included in the audit trail records to allow association of all related (e.g., involving the same network event) audit trail records (e.g., at different hosts) with each other.

(6) Provisions shall be made and the procedures documented to control the loss of audit data due to unavailability of resources.

(7) The CSSO responsible for the Classified network shall be able to selectively audit the actions of any one or more users based on individual identity.

(8) Audit trail information sufficient to allow reconstruction of possible information leakages or misrouted information in the event of a malfunction.

(9) Alarm features that automatically terminate the data flow in case of a malfunction and then promptly notify the CSSO of the anomalous condition.

c. Secure Message Traffic. The communications methodology for the network shall ensure the detection of errors in traffic across the

network links and the retransmission of erroneous traffic.

d. Communications Security For Classified AIS Networks. See Chapter VIII.

8. CONTROLLED INTERFACES. Controlled Interfaces are a special class of Security Support Structure components. They are unique in that no user code runs on these components. This means that more trust can be placed in Controlled Interfaces and fewer resources may be needed for certification. In many cases, products that can be utilized as Controlled Interfaces are available from the Evaluated Products List.

a. Controlled Interface Implementation. All separately accredited networks or AISs that make up the Interconnected Network shall be attached to the Controlled Interface, and the Controlled Interface shall have the following properties:

(1) The Controlled Interface shall be implemented to monitor and enforce the security requirements of the network and adjudicate the differences in security attributes between the attached networks or AISs.

(2) The Controlled Interface shall base its routing decisions on information that is not supplied by the user.

(3) The Controlled Interface shall support the security requirements of the most restrictive attached networks or AISs.

(4) The Controlled Interface shall not run any user code.

b. Controlled Interface Functions. The Controlled Interface function of a Classified AIS is composed of a combination of gateway and guard functions. These two elements of the Controlled Interface have significantly different functions, although the functions are often interrelated and interdependent.

(1) Gateway Functions. Gateways provide a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts and provide a reliable exchange of security information to allow secure interconnections between components.

(2) Guard Functions. Automated guard processes(ors) and security filters (hereafter referred to as guards) are software or hardware/software techniques or specialized equipment that filter information in a data stream based on associated security labels and/or data content. For example, a guard might accept an input data stream of information of mixed classifications up to Secret but permit only data classified up to Confidential to pass.

CHAPTER XI

CLASSIFIED AIS NETWORK SECURITY REQUIREMENTS

1. OVERVIEW. The characteristics and capabilities of classified AISs

implemented as networks require special security considerations. This chapter imposes additional requirements on a network or expands on previously stated security requirements as they apply to a network.

a. Scope. A Classified AIS implemented as a network may be small (two or three personal workstations) or very large (several supercomputers and supporting equipment with thousands of connected terminals). Networks may be internal to a site or location, local to a municipal area, or global in nature. Networks may be internal to a contractor (including a global network) or external with connections from various contractors or agencies.

b. Security Protections. As with other classified AISs, the Protection Index of the network determines the security protections and countermeasures required for the network.

c. Classified AIS Networks. For the purposes of this Manual, there are two types of networks, a Unified Network and an Interconnected Network. A Unified Network is a network operating under a single Protection Index (Security Requirements Specification). An Interconnected Network is composed of two or more networks or separately accredited AISs separated by a Security Support Structure that adjudicates the differences in security requirements between the networks or AISs. This can be as simple as the Security Support Structure only being used to adjudicate need-to-know differences between networks or AISs with the same protection indexes or as complex as using the Security Support Structure to adjudicate the security differences of networks or AISs with different protection indexes.

d. Security Plans and Security Requirements Specification. Each Unified Network shall have a Classified AIS Security Plan (see Chapter V). The Classified AIS Security Plan for the Interconnected Network consists of the Security Requirements Specification from each connected network or AIS plus the Security Requirements Specification for the Interconnected Network and any additional paperwork needed to describe and secure the Interconnected Security Support Structure adjudicating the security differences of the Interconnected networks or AISs (See page XI-4, paragraph 4a.)

e. Accreditation.

(1) Unified Network. Unified Networks are accredited by a single DAA to operate under a single Protection Index.

(2) Interconnected Networks. Interconnected Networks are also accredited by a single DAA to operate under a single Protection Index. This Protection Index may be different than the Protection Indices of each attached network or AIS. Interconnected Networks are composed of networks or AISs that were each separately accredited before they were interconnected. These networks or AISs do not need to be reaccredited; they are now part of an Interconnected Network and can continue to operate as separate, independently, accredited networks. The DAA for the Interconnected Network shall authorize these networks or AISs to operate together and

accredits only the Interconnected Network Security Support Structure as capable of adjudicating the security differences of the networks or AISs that now make up the Interconnected Network.

2. SECURITY SUPPORT STRUCTURE. The Security Support Structure includes all the resources (hardware, software, firmware, and communications) of a Classified AIS that perform security functions directly related to the transfer of information over communications lines, such as Controlled Interfaces, Network Security Controllers, and Secure File Servers. The secure operation of the classified AIS depends on the reliable operation of the Security Support Structure. No reliance for secure operation will be placed on resources that are not part of the Security Support Structure.

   a. Secure Operation. All the trust for the secure operation of the classified AIS is placed in the components of the Security Support Structure.

   b. Secure Transmission. The network Security Support Structure shall ensure that the security parameters are delivered to the correct component without change or loss.

   c. Certification Testing. For a Classified AIS implemented as a network with a Protection Index of two or greater, the secure operation of the Security Support Structure shall be validated and verified by an Independent Verification and Validation team appointed by the CSPM.

3. UNIFIED NETWORK. A Unified Network is composed of network components or AISs and has a well-defined network architecture and design. It is generally administered by a single organizational authority (e.g., contractor, Operations Office). A Unified Network operates under one Classified AIS Security Plan, under one DAA, and with one set of Security Requirements Specifications.

   Note: A Unified Network may be as simple as two Personal Computers connected together or a single host and collection of terminals or it may be as complex as an interconnection of local area networks that provide computing services for an entire facility.

   a. Forming a Unified Network. Before linking two classified AISs together to form a Unified Network, the Security Requirements Specification of each Classified AIS to be linked into the network shall be compared to determine the Protection Index of the resulting network. This comparison of the Security Requirements Specifications shall be used to determine any conflicts created by linking the Classified AISs together and what additional countermeasures shall be required to provide the necessary level of security. The Security Requirements Specifications shall be compared and any conflicts resolved whether the classified AISs consist of standalone AISs, Personal Computers, or personal workstations.

   b. Adding a Classified AIS to a Unified Network. When adding a Classified AIS to a Unified Network, the CSSM responsible for the network shall compare the Security Requirements Specification for

the new network classified AIS with the Security Requirements Specification for the currently accredited network.

(1) No Difference. If there is no difference between the Security Requirements Specifications, the classified AIS may be added to the network without reaccreditation of the network. The CSSO is responsible for ensuring that the Classified AIS Security Plan is current.

(2) Difference. If there is a difference between the Security Requirements Specifications, the classified AIS shall not be added until the differences have been resolved and the network CSSM has certified that there are no differences. If the differences cannot be resolved, the Security Requirements Specification for the network shall be revised and the network reaccredited.

c. Security Support Structure. The Security Support Structure of a Unified Network consists of any and all portions of the Unified Network that are relied upon to provide security for the network.

d. Classified AIS Security Plan. A Classified AIS Security Plan shall be developed showing how the network complies with requirements for secure operation as described in DOE 5639.6A and Chapter V of this Manual. An abbreviated copy of the Classified AIS Security Plan may be distributed to each CSSO.

4. INTERCONNECTED NETWORK. An Interconnected Network consists of two or more networks or AISs interconnected with a DAA approved network Security Support Structure. The networks or AISs that make up the Interconnected Network may belong to different Federal agencies, different Operations Offices, different DOE Programs, or simply different Divisions of the same organization. A Partitioned Classified Network, as described in Attachment XI-1, is a method of implementing an Interconnected Network using controlled interfaces. An Interconnected Network operating at a Protection Index of 3 or greater must utilize a Controlled Interface as the Network Security Support Structure.

a. Interconnected Security Support Structure. The software, hardware, firmware, and equipment that mediates the differences in security and need-to-know between the attached networks or AISs that make up the Interconnected Network is called the Network Security Support Structure. This is used to limit information shared or transmitted between attached networks or AISs. The Security Support Structure of the Interconnected Network may overlap with its associated networks or AISs. Where such an overlap occurs, it shall be the responsibility of both DAAs and so documented in the Interconnected Classified AIS Security Plan.

b. Controlled Interface Implementation. Each Controlled Interface shall be implemented to monitor and enforce the security protections and requirements of the network and adjudicate the differences in security attributes between the separately accredited networks or AISs to ensure compliance and security. Controlled Interfaces are described in paragraph 8 of this Chapter.

c. Security Contract. An Interconnected Network shall have a security

contract (memorandum of understanding) between the administrative entities (Agencies, contractors, etc.) involved which describes the management of the network, the sensitivity of the data to be transmitted, any special security considerations, and the requirement that all parties to the security contract shall not change the Security Requirements Specification of their network or AIS without renegotiating the security contract. Each security contract shall be reviewed annually for currency. A copy of each network or AIS Security Requirements Specification shall be attached to each security contract.

d. Certification Testing. The operation and security of the Interconnected Security Support Structure shall be tested and approved before accreditation of the Interconnected Network.

e. Interconnected Classified AIS Security Plan. A network operating as an Interconnected Network shall have an Interconnected Classified AIS Security Plan that meets the requirements of DOE 5639.6A and Chapter V of this Manual. Copies of the Interconnected Classified AIS Security Plan will be furnished to the CSOM and the CSSM for each network or AIS.

f. Interconnection. A network or AIS connected as a component of an Interconnected network shall not connect to another network or AIS. The only method of adding networks or AISs to an existing Interconnected network is through the Interconnected Security Support Structure and the revision of the Interconnected Classified AIS Security Plan.

g. Adding to an Interconnected Network. A network or AIS must be separately accredited before adding it to an Interconnected Network.

h. Perimeter of a Network. For the purpose of determining the security responsibilities of the DAA who accredits an Interconnected Network, the perimeter of an Interconnected Network is the network Security Support Structure. This perimeter does not include the separately accredited networks or AISs, unless the network Security Support Structure has components or parts in those networks or AISs or other attached separately accredited networks or AISs. The perimeter of the network does include any interface component(s) (hardware or software) that may be installed in the separately accredited classified AIS, terminal, or workstation (i.e., any portion of the separately accredited AIS that is a component of the network Security Support Structure).

5. NETWORK MODE OF OPERATION AND PROTECTION INDICES. See Chapters III and IV.

6. CLASSIFIED AIS NETWORK MANAGEMENT. A Classified AIS Network shall comply with all the management requirements specified for a Classified AIS in Chapter I of this Manual. In addition, a Classified AIS network (Unified or Interconnected) shall comply with the following requirements:

a. Designated Accrediting Authority. The selection of a DAA for a Classified AIS Network is based on the requirements of DOE 5639.6A

and Chapter II of this Manual. The DAA shall ensure the designation of security officials (such as CSSO, CSSM) responsible for the secure operation of the network.

b. Configuration Management Program. Since network configurations change frequently, the Classified AIS Security Plan shall specify procedures for configuration management and the methods for ensuring continuing security as changes are implemented through the Configuration Management Program. The CSSO who is responsible for the network shall advise the cognizant CSSM of any proposed or planned alterations to the network design or operation which impact upon network security. The CSSM shall, in turn, advise the DAA for the network of these proposed changes.

c. Software Implementation. If any component of the interconnected Security Support Structure or Controlled Interface resides partly in the software or firmware of a connecting Classified AIS, its installation in the classified AIS shall be subjected to review in the certification process conducted in support of that network's accreditation.

d. Certification Testing.

(1) Network certification testing shall be conducted to demonstrate that the implementation of the network meets the requirements specified in the classified AIS Security Plan. The tests to be performed shall be specified in writing. Each feature shall be tested to ensure that it does not adversely impact any of the other network security features.

(2) For classified AIS networks with a Protection Index of two or greater, an Independent Verification and Validation team shall assist in the certification testing.

e. Certification. The CSSM responsible for the network shall perform the certification. The CSSM is responsible for ensuring compatibility between the overall Classified AIS Security Plan and the individual Classified AIS Security Plan of each network component. The CSSM shall evaluate the implementation of the classified AIS and the results of the certification tests to verify that the network has been implemented as described in the Classified AIS Security Plan and that the specified security controls are in place and operating properly.

(1) Certification Statement. The CSSM shall issue a written certification statement that assures the DAA that all requirements have been met and that the classified AIS network is ready for accreditation.

(2) Certification Report. The CSSM shall compile a certification report as supporting evidence for the certification statement. This report shall be forwarded through the accreditation chain. The report shall, at a minimum, be composed of the test plan, an analysis of the certification test results, and the certification statement.

f. Accreditation. A network shall be accredited prior to its

operational use. Accreditation shall be accomplished or refused within 30 days of receipt of certification documentation by the office of the DAA.

g. Reaccreditation. Each classified AIS implemented as a network shall be reaccredited by the DAA, at a minimum, every 3 years. Reaccreditation shall also occur if there are modifications to a classified AIS that impact its security; if the security aspects of its environment change; or if the applicable security requirements change.

7. CLASSIFIED NETWORK SECURITY REQUIREMENTS. The security requirements for a Classified AIS network (Unified or Interconnected) follow the same topical areas as those for a Classified AIS. In a network, the failure of a security function may impact the security of not only a single Classified AIS but also of the entire network and its individual components. The following requirements are in addition to those specified in Chapter X and shall be addressed and documented when applied to a Classified AIS implemented as a network.

a. Access Control.

(1) Identification and Authentication Forwarding. Reliable forwarding of the identification shall be used between classified AIS when users are connecting through a network. When identification forwarding cannot be verified, a request for access from a remote classified AIS shall require authentication before permitting access to the system.

(2) Protection of Authenticator Data. In forwarding the authenticator information and any tables (e.g., password tables) associated with it, the data shall be protected from access by unauthorized users (e.g., by encryption), and its integrity shall be ensured.

b. Audit Trails and Monitoring.

(1) The classified AIS implemented as a network shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of successful and unsuccessful accesses to the classified AIS network components within the perimeter of the accredited network. The audit data shall be protected so that access is limited to the CSSO or his/her designee.

(2) As Protection Index levels increase, monitoring of network activity becomes more crucial to the security posture of the network. Methods of continuous, online monitoring of network activities shall be included in each network with a Protection Index three or greater. This monitoring shall also include real time notification to the CSSO of any system anomalies.

(3) The network audit trail shall contain the following types of information.

(a) Identification of the user accessing any component of the network.

(b) Starting and ending times of each access to any component (including file access) of the network.

(c) For networks operating with a Protection Index of two or greater, the changing of the configuration of the network (e.g., a component leaving the network or rejoining).

(4) For each recorded event, the audit record shall contain, at a minimum: date and time of the event; the user ID; type of event; and success or failure of the event.

(5) Identification shall be included in the audit trail records to allow association of all related (e.g., involving the same network event) audit trail records (e.g., at different hosts) with each other.

(6) Provisions shall be made and the procedures documented to control the loss of audit data due to unavailability of resources.

(7) The CSSO responsible for the Classified network shall be able to selectively audit the actions of any one or more users based on individual identity.

(8) Audit trail information sufficient to allow reconstruction of possible information leakages or misrouted information in the event of a malfunction.

(9) Alarm features that automatically terminate the data flow in case of a malfunction and then promptly notify the CSSO of the anomalous condition.

c. Secure Message Traffic. The communications methodology for the network shall ensure the detection of errors in traffic across the network links and the retransmission of erroneous traffic.

d. Communications Security For Classified AIS Networks. See Chapter VIII.

8. CONTROLLED INTERFACES. Controlled Interfaces are a special class of Security Support Structure components. They are unique in that no user code runs on these components. This means that more trust can be placed in Controlled Interfaces and fewer resources may be needed for certification. In many cases, products that can be utilized as Controlled Interfaces are available from the Evaluated Products List.

a. Controlled Interface Implementation. All separately accredited networks or AISs that make up the Interconnected Network shall be attached to the Controlled Interface, and the Controlled Interface shall have the following properties:

(1) The Controlled Interface shall be implemented to monitor and enforce the security requirements of the network and adjudicate the differences in security attributes between the attached networks or AISs.

(2) The Controlled Interface shall base its routing decisions on information that is not supplied by the user.

(3) The Controlled Interface shall support the security requirements of the most restrictive attached networks or AISs.

(4) The Controlled Interface shall not run any user code.

b. Controlled Interface Functions. The Controlled Interface function of a Classified AIS is composed of a combination of gateway and guard functions. These two elements of the Controlled Interface have significantly different functions, although the functions are often interrelated and interdependent.

(1) Gateway Functions. Gateways provide a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts and provide a reliable exchange of security information to allow secure interconnections between components.

(2) Guard Functions. Automated guard processes(ors) and security filters (hereafter referred to as guards) are software or hardware/software techniques or specialized equipment that filter information in a data stream based on associated security labels and/or data content. For example, a guard might accept an input data stream of information of mixed classifications up to Secret but permit only data classified up to Confidential to pass.

PARTITIONED NETWORKS

1. PARTITIONING IN A NETWORK. Partitioning is a method of implementing an Interconnected Network (see Page XI-3, paragraph 4) using Controlled Interfaces such as guards and gateways to separate portions of the network into different segments, each of which has different maximum classification levels, categories, and/or compartments of information. This is done by securely preventing data from one specific segment of the network (e.g., one operating at the Secret Restricted Data level) crossing the boundary (gateway) to another segment of the network (e.g., one operating at the unclassified level).

2. PARTITIONING WITHIN A SINGLE AIS. Partitioning is sometimes implemented within a single AIS by treating the AIS as though it were two or more different virtual machines. This implementation is not a partitioned network. This method of partitioning shall not be permitted for use in DOE classified AISs with a Protection Index of three or greater.

3. PARTITIONED NETWORKS.

a. Discussion. In a Partitioned Classified Network, the network control nodes segregate the users and host AISs into logically-separate, single-level AIS networks. In practice, the nodes that implement this separation are the Controlled Interfaces (Controlled Interfaces). For a secure Partitioned Classified Network, the control nodes shall base their routing decisions on information not supplied by the user. For example, the routing decisions can be

based on the physical line onto which the user is logged. This last characteristic allows the Controlled Interfaces, for example, to refuse to link between an illegal (e.g., open) terminal and a secure host AIS under all conditions. The Controlled Interfaces shall prevent the access violation that would occur if a user with the proper user ID and password attempted to sign onto a secure host AIS from a host or terminal of lesser security level.

b. Security Support Structure. Implicit in this description of a Partitioned Classified Network is the fact that the Controlled Interfaces, along with other components of the Security Support Structure, are "trusted" to make multilevel access decisions. This further requires that the classified AISs's CSSO understand what the Security Support Structure is doing.

(1) Software Security. The security of the software can be established by formal software validation and verification techniques or by having all the software in the Controlled Interface either written by, or meticulously examined by, several cleared personnel.

(2) Hardware Security. The security of the hardware can be established by using formally verified hardware or by using multiple Controlled Interfaces in series. A security failure involving Controlled Interfaces in series requires multiple, concurrent and synergistic hardware failures; such failures are unlikely.

(3) Certification Testing. For Partitioned Classified Network with a Protection Index of two or greater, the secure operation of the Security Support Structure shall be validated and verified by an Independent Verification and Validation team appointed by the CSPM.

c. Host. In the context of a Partitioned Classified Network, a host is a network component that runs user code.

NOTE: No matter what a network component is called by its developer, if that component runs any user code, that component is a host.

d. Server. In the context of a Partitioned Classified Network, a server is a network component that (1) is not a host AIS, (2) is not a Controlled Interface, and (3) provides some needed functionality to the network's hosts and/or Controlled Interfaces. Examples of servers include file systems, network printing systems, and network graphic recording systems. If a network component executes any user code, it is a HOST AIS, not a SERVER.

e. Multilevel Security. A Partitioned Classified Network can run at multiple security levels securely and can use relatively untrustworthy host hardware. All the separation trust is placed in the Controlled Interfaces and other components of the Security Support Structure. Because these Controlled Interfaces can be, and usually are, smaller classified AISs that are running a dedicated program (as opposed to a typical operating system), the Controlled Interfaces are well-understood and reliable.

f. Host AIS. In contrast to a Classified AIS operating with a Protection Index of zero, one, or two, the security of a Partitioned Classified Network depends least on the security capabilities of the host AISs. These machines are the only components of the network that are directly accessible by the users. As a rule, the other network components are, if not transparent, at least "translucent" to the users. A Partitioned Classified Network is designed assuming that, because the host AISs run user programs, the actions of the host AISs cannot be given any security credence. This does not mean that security features in the host AISs are unnecessary or undesirable; it does mean that the network itself can have no confidence in the actions of a host AIS.

4. REQUIREMENTS. A secure Partitioned Classified Network shall be in compliance with the following design requirements because, without such compliance, the Partitioned Classified Network degenerates into a simple network running at multiple security levels. Thus, violation of any of these assumptions results in what is, in effect, a complicated AIS system running at multiple security levels. At the overview level, the requirements for implementing a secure Partitioned Classified Network are:

a. Location of Components. The network routing entities (e.g., Controlled Interfaces) know the partition that a host or terminal is in based on information not supplied by the host or terminal. For example, in most Partitioned Classified Networks, the partition that a terminal is in is determined by the physical line a terminal uses to communicate to the Partitioned Classified Network. In one extant Partitioned Classified Network, approximately 32 dial-up lines lead into the open partition. In the same Partitioned Classified Network, lines from terminals in the secure partition come into the network through a Protected Distribution System from secure areas.

b. Location of User Code. The only machines in the Partitioned Classified Network that can execute a user's programs are the host AISs. No user code can be executed in the Controlled Interfaces or servers. This assumption is the basis for the trust placed in the network routing nodes and in the servers.

c. Servers. Servers that allow read/write access by hosts will separate data by partition. Because servers do not execute user programs, this assumption is usually validated by having the server's software written and checked by cleared people. Techniques for assuring this separation are straight forward.

d. Perimeter of the Classified AIS. The security perimeter of a secure Partitioned Classified Network includes all Controlled Interfaces, all lines from Controlled Interfaces, all secure terminals, all secure hosts, and all lines to secure terminals.

e. Security Controls. Some trusted node in the Partitioned Classified Network has a list of user IDs, passwords, and privileges. Many Partitioned Classified Networks refer to this node as a Network Security Controller. This is the node from which first-level Controlled Interfaces request permission to make a terminal-to-host

connection.

f. Star (*) Property. Servers that allow read/write access, such as common file systems, enforce the "star (*) property." Star (*) property is a process in a partition which can, with proper authorization, read a file from a less sensitive partition, but not vice versa. In other words, a secure host can read a "lower level" file but cannot write to a file accessible from the lower level partition.

g. Untrustworthy. The terminals (that is, the users at terminals) and host AISs are assumed to be untrustworthy. For example, the Partitioned Classified Network, itself, shall prevent a terminal from accessing a secure host, even if both the terminal and the secure host want to make the connection. The Partitioned Classified Network, itself, shall prevent a secure terminal or host from placing data in an unapproved partition.

5. INDEPENDENT VALIDATION AND VERIFICATION REQUIREMENT. Partitioned Classified Networks have demonstrated their usefulness in effective implementation of security policies involving secure, multilevel processing. However, this utility is obviated if any of the above assumptions are violated. CSSOs should be aware that unintentional violations of these requirements can be subtle and difficult to detect. An outside examination of a Partitioned Classified Network by an Independent Validation and Verification team shall be required before accreditation of the classified AIS.

CHAPTER XII

SECURITY REQUIREMENTS FOR STANDALONE SINGLE-USER AIS

1. SINGLE-USER CLASSIFIED AIS. A single-user Classified AIS is a Classified AIS in which only one user controls all system resources at any specific time. For a single-user Classified AIS that is not connected to another classified AIS, administrative controls such as accountability, personnel controls, and physical controls appropriate to the classification level of the data being processed are sufficient protection.

   NOTE: "Personal workstation" is defined as a general purpose classified AIS used by a single user. This includes personal computers, microcomputers, and minicomputers. It does not include special purpose computers such as numerical control or process control machines.

2. SECURITY REQUIREMENTS. Personal workstations shall comply with the requirements for the Protection Index zero. These requirements include: a Classified AIS Security Plan; testing, certification and accreditation of the security procedures; physical security protections appropriate to the classification level of the data processed, stored, transferred, or accessed on the classified AIS; personnel security protections; and administrative protections.

3. ADMINISTRATIVE PROCEDURES. The administrative procedures required for personal workstations are addressed below:

   a. Waste, Fraud, and Abuse Review. Each personal workstation and the

information therein shall be reviewed annually to determine that the workstation and the data are not being used to defraud the Government or that the workstation and data are not being used in an inappropriate manner that could constitute waste or abuse of the equipment or data (see page I-10, paragraph 15, and page IX-8, paragraph 15). Where large numbers of AIS are involved, at least one-third of the classified AISs shall be reviewed annually. As an alternative, a statistical sampling method of reviewing may be approved by the DAA.

b. Marking.

(1) All personal workstations shall be clearly marked to indicate the classification level and most restrictive classification category of information that can be processed, stored, transferred, or accessed on the classified AIS.

(2) Media containing classified information shall be visibly marked with the accreditation level authorized for processing on the AIS unless an appropriate review has been conducted or it is output by a tested program or methodology verified to produce consistent results and approved by the DAA.

(3) All printed matter from the personal workstation shall be marked at the accreditation level of the classified AIS unless an appropriate review has been conducted or it is output from a tested program verified to produce consistent results and approved by the DAA.

c. Protection of Media Containing Software. All media containing software including operating systems, security systems, utilities, vendor supplied diagnostics, and applications program which have been used on the classified AIS shall be protected at the accreditation level of the classified AIS.

d. Protection of Media Containing Data. All media containing data used on a single-user Classified AIS shall be protected at the accreditation level of the AIS.

e. Media Clearing, Sanitization, and Destruction. Clearing, sanitization, and destruction procedures are detailed in Chapter IX. Users of personal workstations shall follow these procedures.

f. Removal of Classified AIS Equipment. No user of a personal workstation shall move any of the components of the classified AIS from the location specified in the Classified AIS Security Plan without approval of the CSSO.

4. SPECIAL EMPHASIS. Requirements needing special emphasis for personal workstations are as follows:

a. User Responsibility. Each user of a personal workstation is responsible for assuring that it is used in accordance with the procedures specified in the Classified AIS Security Plan.

b. Removable Media Handling. Removable media shall be properly labeled and stored.

c. Release of Removable Media. Before removable media is released, it shall be properly sanitized.

d. Viruses and Intruders. All users of personal workstations shall be advised by the CSSO of procedures for preventing viruses and reporting suspected viruses or intruders (e.g., hackers).

e. Physical Access. The CSSO is responsible for informing users of personal workstations about their responsibilities concerning access to the workstation by unauthorized users (including visual access).

f. Backup Procedures. Each user is responsible for assuring that the information on his/her personal workstation is backed up in accordance with procedures in the Classified AIS Security Plan.

CHAPTER XIII

REQUIREMENTS FOR PERIODS PROCESSING

1. OVERVIEW. Periods processing is a method of sequential operation of a classified AIS that provides the capability to process various levels of sensitivity of information at distinctly different times. Periods processing provides the capability to either: (a) have more than one user (sequentially) on a single-user Classified AIS with different levels of information or need-to-know; (b) use a Classified AIS at more than one classification level (sequentially); or (c) use a Classified AIS in more than one Protection Index. The requirements of DOE 5639.6A and this Manual do not apply when processing in the unclassified mode.

2. SANITIZATION AFTER USE. If a Classified AIS is used for periods processing either by more than one user or for segregating information by classification level onto separate media, the Classified AIS Security Plan shall specify the sanitization procedures to be employed by each user before and after each session of use of the classified AIS.

3. SANITIZATION BETWEEN PERIODS. The classified AIS shall be sanitized of all information before transitioning from one period to the next (e.g., whenever there will be a new user(s) who does not have security clearance or the need-to-know for data processed during the previous period, changing from one Protection Index to another). These procedures shall be documented in the Classified AIS Security Plan and approved by the DAA. Such procedures could include, among others, sanitizing nonvolatile storage, exchanging disks, and powering down the classified AIS and its peripherals.

4. MEDIA FOR EACH PERIOD. Classified AISs employed in periods processing shall have separate media for each period of processing, including copies of operating systems, utilities, and applications software. For classified AIS operating at a Protection Index of zero, one, or two, the same media may be used for both periods if the media has been subjected to a process approved by the DAA, which proves that the media has not been contaminated by the addition of classified information.

5. AUDIT. Where there are multiple users of the classified AIS and where the classified AIS is not capable of automated logging, manual logging

shall be done at the discretion of the DAA. Audit trails are not required for single-user standalone classified AIS processing classified information.

CHAPTER XIV

SECURITY REQUIREMENTS FOR AISs USED AS ALARM SYSTEMS

1. OVERVIEW. Alarm systems that process classified information shall be protected and accredited to process classified information under the requirements of DOE 5639.6A and this Manual. The differences from the requirements for classified AISs are detailed below.

2. COMMUNICATIONS SECURITY. The communication lines that connect the AIS to its sensors and leave the Limited Area shall be protected at a level commensurate with the sensitivity of the information being transmitted.

   a. Transmitting Classified Information. If the alarm information being transmitted is classified, the information shall either be encrypted using an National Security Agency approved encryption device or the transmission lines shall be protected using a Protected Distribution System as described in DOE 5300.4D.

   b. Transmitting Unclassified Information. If the alarm information being transmitted is unclassified, the transmission lines do not need protection beyond that which is required by DOE 5632.2A, PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL AND VITAL EQUIPMENT.

   c. Other Communication Lines. The communication lines that provide remote terminal or operator access or that interconnect with other alarm systems shall be protected at the accreditation level of the alarm system as described by DOE 5639.6A and this Manual.

3. CERTIFICATION TESTING. Certification testing of the alarm system shall include the determination that the alarm system cannot be captured or brought under remote control through its sensor ports. If it is determined that the alarm AIS can be captured or controlled by attacking the alarm AIS through its sensor ports, then the sensor wirelines shall be protected by one of the following methods.

   a. Encryption. The sensor wirelines shall be encrypted with an NSA-approved encryption device.

   b. Protected Distribution System. The sensor wirelines shall be protected using a Protected Distribution System as described in DOE 5300.4D.

   c. Change of Functionality. The functionality of the sensor port shall be changed so the classified AIS cannot be captured or brought under control through the sensor port.

<<EOD>>