Print

DOE M 471.2-2

8-3-99

CLASSIFIED INFORMATION SYSTEMS SECURITY MANUAL

CANCELED

U.S. DEPARTMENT OF ENERGY

Office of Security Affairs

Distribution:	Initiated By:
All Departmental Elements	Office of Safeguards and Security

CLASSIFIED INFORMATION SYSTEMS SECURITY MANUAL

1. PURPOSE. This Manual provides requirements and implementation instructions for the graded protection of the confidentiality, integrity, and availability of information processed on all automated information systems used to collect, create, process, transmit, store, and disseminate classified information by, or on behalf of, the Department of Energy (DOE). The requirements are based upon applicable Federal statutes, regulations, National Security Directives, Executive Orders, procedures in Office of Management and Budget (OMB) Circulars and Bulletins, and Federal standards.

2. SUMMARY. All information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, DOE on automated information systems requires some level of protection. The loss or compromise of information entrusted to DOE or its contractors may affect the nation's economic competitive position, the environment, the national security, DOE missions, or the citizens of the United States. The risk management approach defined in this Manual for DOE and its contractors provides for the graded, cost-effective protection of automated information systems containing classified information. Protection of unclassified automated information systems is provided for in DOE N 205.1, UNCLASSIFIED CYBER SECURITY PROGRAM.

3. CANCELLATION. DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM, dated 7-15-94, is canceled. Cancellation of a Manual does not, by itself, modify or otherwise affect any contractual obligation to comply with such a Manual. Canceled Manuals incorporated by reference in a contract must remain in effect until the contract is modified to delete the reference to the requirements in the canceled Manuals.

4. APPLICABILITY.

   a. General. This Manual applies to Departmental elements responsible for protection of automated information that is classified.

   b. Application to Contracts. This Manual applies to covered contractors (a DOE contractor or subcontractor subject to DOE Acquisition Regulation, Part 952.204-2, or other clause requiring protection of classified information, nuclear material, or other sensitive information or activities). For contractor requirements, see the contractor requirements document in Attachment 1.

5. IMPLEMENTATION. Security requirements for classified information systems contained in this Manual and in DOE O 471.2A, INFORMATION SECURITY PROGRAM, must be implemented as follows.

   a. This Manual must be implemented no later than 6 months from the date of issuance.

CANCELED

b. Existing accredited classified information systems shall remain accredited until reaccreditation is required, either because the systems have passed the 3-year accreditation expiration date or because of significant changes in the security requirements of the classified information system. After implementation of this Manual, reaccreditation must be in accordance with this Manual and DOE O 471.2A.

c. Classified information systems that have begun the certification and accreditation process before implementation of this Manual may be accredited under DOE M 5639.6A-1. These systems will remain accredited until reaccreditation is required, either because the systems have passed the 3-year accreditation expiration date or because of significant changes in the security requirements of the information system. Reaccreditation must be in accordance with this Manual and DOE O 471.2A.

d. New classified information systems that are under development and that have not begun the certification and accreditation process before implementation of this Manual must meet the requirements of this Manual and DOE O 471.2A.

5. DEFINITIONS. See Attachment 2.

6. CONTACT. Questions concerning this Manual should be directed to the Classified Information Systems Security Program Manager at 301-903-2122.

BY ORDER OF THE SECRETARY OF ENERGY:

David M. Klaus
Director of Management
and Administration

CANCELED

CONTENTS

CHAPTER I - CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM OVERVIEW

CHAPTER II - MANAGEMENT STRUCTURE AND RESPONSIBILITIES

CHAPTER III - RISK AND PROGRAM MANAGEMENT

CHAPTER IV - PROTECTION PROFILES

CANCELED

CONTENTS (continued)

CANCELED

CONTENTS (continued)

CANCELED

CANCELED

CHAPTER I

CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM OVERVIEW

1. INTRODUCTION. The Classified Information Systems Security Program provides for the protection of classified information on DOE and contractor information systems. This Manual consists of three main elements: Management Structure, Risk Management, and Requirements. In this document, the term(s) "classified information system," "information system," or "system" are used to mean systems that process classified information.

2. MANAGEMENT STRUCTURE. Management of the Classified Information Systems Security Program is performed through a multi-tiered structure. DOE positions include the Classified Information Systems Security Program Manager (ISPM), Designated Approving Authority(s) (DAA), and Classified Information Systems Security Operations Manager(s) (ISOM). Site positions, which may be held by DOE or contractor employees, include Classified Information Systems Security Site Manager(s) (ISSMs) and Classified Information Systems Security Officer(s) (ISSO). Site positions also include application owners/data custodians and users. Details of the management structure and responsibilities are in Chapter II.

3. RISK MANAGEMENT. Risk management is a process that considers the prevailing DOE threat analysis, the effect of countermeasures applied to the processing environment, the remaining vulnerability of the processing environment (residual risk), and the protection requirements and value of the information being processed. Countermeasures are increased until the risk is reduced to an acceptable level or until the cost of reducing the risk becomes prohibitive. If the DAA determines that the remaining risk is not acceptable, management must then determine if the automation requirements are sufficient to justify additional costs. Details of the risk management process and other program management requirements are in Chapter III. The certification and accreditation process is described in Chapter V.

4. REQUIREMENTS. The Department's classified information systems security process for achieving adequate protection based on levels of concern for the confidentiality, integrity, and availability of information is detailed in Chapter V. Requirements common to all systems are detailed in Chapter VI. These include sanitization, maintenance, personnel, and physical requirements. Protection requirements graded by levels of concern and confidentiality protection level are detailed in Chapter VII. These include audit, documentation, and testing requirements. Additional requirements for interconnected systems (networks) are detailed in Chapter VIII.

5. OTHER RELATED POLICIES. This Manual provides protection requirements for classified information systems. Other DOE Orders and Manuals provide the specific requirements for classified communications, protected transmission systems, classified matter protection, and personnel and physical requirements. Determination of classification must be accomplished in accordance with DOE classification policy.

CANCELED

CHAPTER II

MANAGEMENT STRUCTURE AND RESPONSIBILITIES

The Classified Information Systems Security Program is managed through a multi-tiered structure. The structure includes an ISPM at DOE Headquarters, DAA(s), ISOM(s) at each DOE Operations Office, and ISSMs and ISSOs at the sites. The structure also includes application owners/data custodians and users of the systems. This chapter describes the roles and responsibilities of the individuals involved in the decision-making activities in the Program.

1. CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISPM). The ISPM is a DOE employee knowledgeable in information systems security and is appointed by the Director of the Office of Safeguards and Security (NN-51). The ISPM is responsible for the following.

   a. Serves as the program manager for Classified Information Systems Security and ensures implementation of the Classified Information Systems Security Program within DOE.

   b. Develops and recommends DOE policies, standards, procedures, and guidelines for protecting information systems that collect, create, process, transfer, store, or provide access to classified information.

   c. Maintains a continuing review of this Manual to ensure that current technology is being applied to the protection of information systems that create, process, store, transfer, or provide access to classified information and to eliminate those practices that are no longer needed or effective.

   d. Approves secure remote diagnostic and maintenance facilities proposed for use with information systems that process classified information.

   e. Annually reviews and updates, as needed, the Periodic Risk Assessment for the DOE Classified Information Systems Security Program and the DOE Statement of Generic Threat to Automated Information Systems.

   f. In coordination with the field, designates the DAA for information systems that operate under the jurisdiction of more than one Headquarters and field element.

   g. Reviews and concurs on accreditation for systems operating at Protection Level 5 or 6 that operate under the jurisdiction of one Headquarters or field element.

   h. Represents the DOE before Federal, private, and public organizations concerned with protecting classified information systems.

i. Reports changes in ISOM and DAA appointments to all DAAs.

j. Coordinates–

(1) with the Unclassified Computer Security Program Manager;

(2) with the Office of Energy Intelligence on the protection of Sensitive Compartmented Information (SCI);

(3) implementation of the Classified Information Systems Security Program with Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, Materials Control and Accountability, and other programs, as appropriate; and

(4) the development, publication, and distribution of guidelines for the protection of classified information systems.

k. Provides education, awareness, and training activities that–

(1) ensure that education in DOE's Classified Information Systems Security Program policies and practices is available to the ISOMs and ISSMs (scheduling of these educational activities must allow all ISOMs and ISSMs to participate within 1 year of their appointment);

(2) maintain a capability to facilitate the electronic exchange of information systems security information, such as awareness alerts on sniffer attacks, viruses, etc.;

(3) periodically present information systems security workshops; and

(4) periodically sponsor an Information Systems Security Program training conference.

l. Supports, maintains, and coordinates an advice and assistance capability for use by any ISOM or ISSM within DOE. The services provided by this capability must include the following.

(1) Advice and Assistance Reviews. Reviews of information systems protection as requested by the site, such as reviews of network designs or protection profiles of networks or systems.

(2) Independent Validation and Verification (IV&V). Design, certification, and performance test reviews of networks or systems that process classified information.

CANCELED

m. Maintains and coordinates an incident response capability to provide timely assistance and system vulnerability information to DOE sites.

n. Provides guidance for a technology development program to support the Classified Information Systems Security Program and periodically briefs DAAs, ISOMs, and ISSMs on activities and results of the program.

o. Collects and disseminates information relevant to the Classified Information Systems Security Program.

p. Monitors the Classified Information Systems Security Program findings and deficiencies resulting from surveys, inspections, and reviews.

q. Conducts timely reviews of the system protection documentation and the certification for information systems located in Sensitive Compartmented Information Facilities (SCIFs) received from cognizant ISOMs and provides comments to the Office of Energy Intelligence.

2. DESIGNATED APPROVING AUTHORITY (DAA). The DAA is a DOE employee appointed by the Operations Office Manager. He/she is responsible for evaluating the protection measures in an information system as described in the Classified Information Systems Security Plan (ISSP), the results of any certification tests, the certification of the system, and any residual risks of operating the system. The DAA may designate additional tests that must be performed prior to meeting accreditation requirements.

With this appointment, the Operations Manager provides the DAA with written authorization to accept the residual risks and responsibility for the loss of confidentiality, availability, and/or integrity of all classified information systems under DAA jurisdiction. The authorization must include accreditation, provisional accreditation, withdrawal of accreditation, and suspension of operations for all classified information systems with operational boundaries fully contained under his/her jurisdiction. The ISOM may also be appointed as the DAA. The DAA is responsible for the following.

a. Serves as accrediting authority for each DOE and covered contractor classified information system with operational boundaries fully contained under his/her jurisdiction.

b. Ensures that this Manual is implemented for each classified information system under his/her jurisdiction, that each system is accredited or reaccredited every 3 years (except for information systems that process SCI), and that the accreditation or reaccreditation is documented.

c. Ensures that the accreditation of each system under his/her jurisdiction is withdrawn, and that the system is properly sanitized when the system no longer processes classified information or when changes occur that might affect accreditation.

CANCELED

d. Ensures that DAA authorities are delegated only to DOE employees who are knowledgeable in information systems security.

e. Reports any changes in ISOM or ISSM appointments to the ISPM.

3. CLASSIFIED INFORMATION SYSTEMS SECURITY OPERATIONS MANAGER(s) (ISOM). The ISOM is a DOE employee, knowledgeable in information systems security and appointed by the Operations Office Manager. The ISOM must participate in ISPM-sponsored training in the Classified Information Systems Security Program within 1 year of his/her appointment. The ISOM is responsible for the following.

a. Communicates appropriate incident reports received from sites to the ISPM.

b. Ensures periodic review of the Classified Information Systems Security Program consistent with the Operations Office Survey Program at each site under the jurisdiction of the DOE operations office.

c. Evaluates information systems for accreditation and provides results to the DAA.

d. Monitors responses to findings and other deficiencies identified in surveys, inspections, and reviews of each site’s Classified Information Systems Security Program to ensure that any necessary corrective or compensatory actions have been completed.

e. Coordinates the following:

(1) the Classified Information Systems Security Program with the Unclassified Information Systems Security Program;

(2) implementation of the Classified Information Systems Security Program with requirements of other DOE programs, as appropriate, such as Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, and Materials Control and Accountability Programs.

4. CLASSIFIED INFORMATION SYSTEMS SECURITY Site Manager(s) (ISSM). The ISSM is appointed by the Site Manager to be responsible for implementation of the site Classified Information Systems Security Program. A separate ISSM may be appointed for information systems in an SCIF if the site determines that another ISSM is needed. In this capacity, the ISSM also functions as the site point of contact (POC) for all classified information systems security issues. The ISSM is responsible for the following.

a. Ensures the development, documentation, and presentation of information systems security education, awareness, and training activities for site management, information security personnel, data custodians, and users. This training and awareness program must include,

CANCELED

but is not limited to, various combinations of classes (both self-paced and formal), security education bulletins, training films, computer-aided instruction, security briefings, and related educational aids.

b. Ensures the development, documentation, and presentation of Information systems security training for escorts in information systems operational areas.

c. Establishes, documents, implements, and monitors the Classified Information Systems Security Program for the site and ensures site compliance with DOE requirements for information systems.

d. Ensures the development of procedures for use in the site Classified Information Systems Security Program.

e. Identifies and documents unique threats to information systems at the site.

f. Ensures that the site's Classified Information Systems Security Program is coordinated with the Site Safeguards and Security Plan (SSSP) or the Site Security Plan (SSP) (see DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM, Chapter I).

g. Coordinates the following:

(1) implementation of the site Classified Information Systems Security Program with the other site programs, as appropriate, such as Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, and Materials Control and Accountability;

(2) development of a site self-assessment program for the Classified Information Systems Security Program; and

(3) self-assessment of the site's Classified Information Systems Security Program, which is to be performed between operations office surveys.

h. Ensures the development of site procedures to–

(1) govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information;

(2) ensure that vendor-supplied authentication features (e.g., passwords, account names) or security-relevant features are properly implemented;

(3) report classified information systems security incidents;

CANCELED

(4) require that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for the security of classified information systems and classified information;

(5) detect malicious code, viruses, and intruders (hackers); and

(6) review and approve ISSPs, certification test plans, and certification test results.

i. Determines, using guidance from the data custodian(s), the appropriate levels of concern for confidentiality, integrity, and availability for each information system that processes classified information.

j. Certifies to the DAA, in writing, that each ISSP has been implemented, that the specified protection measures are in place and properly tested, and that the classified information system is functioning as described in the ISSP.

k. Recommends to the DAA, in writing, approval or disapproval of the ISSP test results and the certification statement.

l. Ensures that the DAA is notified when a system no longer processes classified information or when changes occur that might affect accreditation.

m. Participates in ISPM-sponsored information systems security training within 1 year of his/her appointment.

n. Ensures that personnel are trained on the information system's prescribed security restrictions and safeguards before they are initially allowed to access a system.

5. <u>CLASSIFIED INFORMATION SYSTEMS SECURITY OFFICER(s) (ISSO)</u>. The ISSO is responsible for the following.

a. Ensures implementation of security measures for each classified information system for which he/she is responsible.

b. Identifies and documents any unique threats to classified information systems for which he/she is the ISSO and forwards them to the ISSM.

c. If so directed by the DAA and/or if an identified unique local threat exists, performs a risk assessment to determine if additional countermeasures beyond those identified in this Manual are required.

d. Develops and implements a certification test plan for each classified information system for which he/she is the ISSO, as required by this Manual and the DAA.

CANCELED

e. Prepares, maintains, and implements an ISSP that accurately reflects the installation of protection measures for each classified information system for which he/she is responsible.

f. Maintains the record copy of the ISSP and related documentation for each classified information system for which he/she is the ISSO.

g. Notifies the DAA (through the ISSM) when a system no longer processes classified information, or when changes occur that might affect accreditation.

h. Ensures the following:

(1) that the sensitivity level of the information is determined prior to use on the classified information system and that the proper security measures are implemented to protect this information;

(2) that unauthorized personnel are not granted use of, or access to, a classified information system; and

(3) that formal access controls are implemented for each classified information system, except stand-alone personal computers and stand-alone workstations.

i. Documents any special protection requirements identified by the data custodians and the protection measures implemented to fulfill these requirements for the information contained in the classified information system.

j. Ensures that confidentiality, integrity, and availability levels of concern are determined for each classified information system for which he/she is responsible.

k. Implements site procedures to–

(1) govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information;

(2) ensure that vendor-supplied authentication features (e.g., passwords, account names) or security-relevant features are properly implemented;

(3) report classified information systems security incidents;

(4) require that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for protecting classified information systems and classified information;

(5) detect malicious code, viruses, and intruders (hackers); and

CANCELED

(6) review and approve ISSPs, certification test plans, and certification test results.

l. Ensures that users are properly trained in system security by identifying classified information systems security training needs (including system-specific training) and personnel who need to attend system security training programs.

m. Conducts ongoing security reviews and tests of classified information systems to periodically verify that security features and operating controls are functional and effective.

n. Evaluates proposed changes or additions to the classified information systems and advises the ISSM of their security relevance.

6. CLASSIFIED INFORMATION SYSTEMS APPLICATION OWNER/DATA CUSTODIAN.

a. Determines and declares the sensitivity level of information prior to the information being processed, stored, transferred, or accessed on the classified information system.

b. Advises the ISSO of any special protection requirements for information to be processed on the classified information system.

c. Determines and documents the data and application(s) that are essential to the fulfill the site mission and ensures that requirements for contingencies are determined, implemented, and tested.

d. Ensures that information is processed on a classified information system that is accredited at a level sufficient to protect the information.

7. USERS OF CLASSIFIED INFORMATION SYSTEMS.

a. Comply with the Classified Information Systems Security Program requirements.

b. Be aware of and knowledgeable about their responsibilities in regard to classified information systems security.

c. Be accountable for their actions on a classified information system.

d. Ensure that any authentication mechanisms (including passwords) issued for the control of their access to classified information systems are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.

CANCELED

e. Acknowledge, in writing, their responsibilities (Code of Conduct) for protecting classified information systems and classified information.

f. Participate in training on the information system's prescribed security restrictions and safeguards before initial access to a system. As a follow-up to this initial training, participate in an ongoing security education, training, and awareness program.

CANCELED

CANCELED

CHAPTER III

RISK AND PROGRAM MANAGEMENT

1. INTRODUCTION. The cornerstone of the Classified Information Systems Security Program is the risk management process, which determines the protection requirements for DOE information. Risk management balances the data custodian's perceived value of the information and his/her assessment of the consequences of loss of confidentiality, integrity, and availability against the costs of protective countermeasures and day-to-day operations. DOE's risk management process includes the following interrelated phases:

   a. threat analysis;

   b. risk analysis that evaluates generic threats, technologies, and architectures and integrates associated findings into DOE directives governing information systems;

   c. data custodians' declarations of the consequences of loss of confidentiality, integrity, and availability;

   d. site program implementation that evaluates the unique concerns of the site (i.e., threats, protective technologies, procedures, etc.) and integrates those concerns with site operations;

   e. system implementation that identifies, evaluates, and integrates the impact of information loss, system vulnerabilities, data custodian protection requirements, cost of protective measures, and mission requirements; and

   f. system operation where the remaining risk (residual risk) is accepted and oversight is initiated to ensure that the level of residual risk is managed throughout the information system's life cycle.

2. THREAT ANALYSIS. The analysis of information threats identified by national and DOE organizations provides the basis for protecting DOE's classified information. The ISPM must annually review the national information threat posture. The results of this review must be used to develop or update the DOE Statement of Generic Threat to Automated Information Systems.

3. DEPARTMENTAL RISK ANALYSIS. This process begins with an analysis of information architectures and technologies to determine how information with different sensitivities can be protected on a system. A risk assessment is then performed using this analysis and the DOE Statement of Generic Threat to Automated Information Systems. The results of this risk assessment are used as the basis to develop the protection countermeasures for DOE's information.

a. Periodic Risk Assessment. For DOE Classified Information Systems Security Program, the ISPM must maintain a constant awareness of how technology, technology trends, information architectures and information standards relate to protecting information. The ISPM must use this information and the DOE Statement of Generic Threat to Automated Information Systems to perform and update the Periodic Risk Assessment for the Classified Information Systems Security Program.

b. Changes to Directives. If either the DOE Statement of Generic Threat to Automated Information Systems or the Periodic Risk Assessment for the Classified Information Systems Security Program is changed, the ISPM must identify and recommend changes to requirements in DOE O 471.2A and this Manual.

4. DATA CUSTODIAN RESPONSIBILITIES. The custodian of each piece of information collected, created, processed, transmitted, or stored on an automated system must ensure the determination of the level of sensitivity and classification of information on the automated system.

5. SITE PROGRAM IMPLEMENTATION. The site risk assessment, performed as a function of the Site Security Plan (SSP) or the Site Safeguards and Security Plan (SSSP), must include the Departmentwide Classified Information Systems Security Risk Assessment as a baseline and must identify any site-specific threats. The site risk assessment must consider any protection technologies unique to the site. The results of the site risk assessment must be documented and used to augment, as needed, the Classified Information Systems protection profiles to be applied to information systems at the site.

6. NEW OR MODIFIED SYSTEM IMPLEMENTATION. The system implementation process begins when the levels of concern and protection level of the information to be processed are identified, as described in Chapter IV. This information forms the basis for the protection profile. The protection profile requirements are then integrated into the information system's design, implementation, and operation.

7. SYSTEM OPERATION. The final phase of the risk management process is acceptance of risk through certification and accreditation (see Chapter V) and the protection of information during day-to-day operations.

8. INCIDENT REPORTING. In addition to the reporting requirements of DOE O 232.1A, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, dated 7-21-97, the ISOM must ensure that incidents affecting DOE or national interests are reported (via telephone or other electronic means) to the ISPM. The report must include at least the location of the incident, possible effect on DOE or national interests, a description of the incident, and a description of the actions that were taken to protect information after the incident was discovered. All individual(s) collecting information about or reporting an incident must ensure that any sensitive or classified information involved in the incident or report is properly protected.

CANCELED

a. The following incident reporting requirements apply.

(1) Affects Site Interests. If the incident affects only site interests, the site must collect and maintain information about the incident, such as location, description, resources needed to respond to the incident, and actions that were taken to protect information after the incident was discovered. The DAA must provide this information on request from the ISPM. A quarterly summary report must be submitted to the ISPM through the ISOM.

(2) Affects DOE or National Interests. Any incident that affects DOE or national interests must be reported to the ISOM immediately after detection. The ISOM must report the incident to the ISPM within 1 hour of receiving the site report.

b. The ISPM will periodically issue instructions regarding what constitutes an incident and specifying information to be reported.

9. OVERSIGHT.

a. ISOM Program Reviews. The ISOM must ensure that periodic reviews of the site's Classified Information Systems Security Program are performed.

b. ISSM Self-Assessments. The ISSM must ensure that periodic self-assessments of the site's program are performed. Upon completion of each review, the ISSM must ensure that a corrective action plan is prepared and implemented for all findings or vulnerabilities as directed by DOE O 470.1, Chapter IX, Paragraph 10a. A record of each review and the subsequent corrective action plan must be retained and made available during future surveys and inspections.

10. SITE SAFEGUARDS AND SECURITY PLAN. The SSSP must contain information regarding the Classified Information Systems Security Program as detailed in DOE O 470.1.

CANCELED

CANCELED

CHAPTER IV

PROTECTION PROFILES

1. INTRODUCTION. A protection profile is a description of the protection measures required for a particular information system. A protection profile reflects the prescribed protection measures, which are determined by–

   a. the protection level for confidentiality,

   b. the level of concern for integrity and availability, and

   c. the operating environment of the system as reflected by the level(s) of trust embodied in the user environment.

2. LEVEL OF CONCERN. The level of concern reflects the perceived sensitivity of the information and the consequences of the loss of confidentiality, integrity, or availability.

   a. Information Sensitivity Matrices. The information sensitivity matrices presented here are designed to assist in determining the appropriate protection level and the levels of concern for confidentiality, integrity, and availability for a given classified information system processing a given set of information. The matrices (Tables 1, 2, and 3) should be used as follows.

      (1) A determination of high, medium, or low must be made for each of the three attributes: confidentiality, integrity, and availability. It is not necessary for the level of concern to be the same for all attributes of the system.

      (2) The DAA or the data custodian may determine that additional protection measures (beyond those required by the specified levels of concern) are necessary to achieve an acceptable level of risk.

   b. Confidentiality Level of Concern. In considering confidentiality, the principal question is the necessity for supporting the classification levels and the types of information (e.g., Secret Restricted Data [SRD] Sigma 15) on the system in question. The Protection Level Table for Confidentiality (Table 4) combines the processing environment with the level of concern for confidentiality to provide a protection level. The protection level is then applied to Table 5 to provide a set of graded requirements to protect the confidentiality of the information on the system. This graded approach to requirements provides sufficient and necessary protection for the information on the system without requiring unnecessary protections for systems where the level of concern for confidentiality is low or medium.

CANCELED

Table 1. Information Sensitivity Matrix for Confidentiality.

Level of Concern	Qualifiers
High	All SCI All Special Access Programs (SAPs)/Special Access Required (SAR) All information protecting intelligence sources, methods, and analytical procedures All Single Integrated Operational Plan (SIOP) All Crypto SECRET RD (SIGMAs 1,2,14,15) and TOP SECRET
Medium	SECRET SECRET RD (All other SIGMAs)
Low	CONFIDENTIAL

NOTE: The DAA or the data custodian may determine that additional protection measures (beyond those required by the specified level of concern) are necessary to achieve an acceptable level of risk.

Table 2. Information Sensitivity Matrix for Integrity.

Level of Concern	Qualifiers
High	Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.
Medium	High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.
Low	Reasonable degree of accuracy required for mission accomplishment.

NOTE: The DAA or the data custodian may determine that additional protection measures (beyond those required by the specified level of concern) are necessary to achieve an acceptable level of risk.

c. Integrity Level of Concern. In considering integrity, the principal consideration is the need for accuracy of the information on the system in question.

d. Availability Level of Concern. In considering availability, the principal consideration is the need for the information on the system in question to be available in a fixed time frame to accomplish a mission.

Table 3. Information Sensitivity Matrix for Availability.

Level of Concern	Qualifiers
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.
Medium	Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Low	Information must be available with flexible tolerance for delay.

NOTE: In this context, "High - no tolerance for delay" means no delay; "Medium - minimum tolerance for delay" means a delay of seconds to hours; and "Low - flexible tolerance for delay" means a delay of days to weeks.

NOTE: The DAA or the data custodian may determine that additional protection measures (beyond those required by the specified level of concern) are necessary to achieve an acceptable level of risk.

CANCELED

3. PROTECTION LEVEL. The protection level of a classified information system is determined by the relationship between two sets of facts: (1) the clearance levels, formal access approvals, and users' need-to-know; and (2) the level of concern for classification. The protection level translates into a set of requirements that must be implemented in the resulting system. Table 4 presents the criteria for determining the following six protection levels for confidentiality:

a. Systems are operating at Protection Level 1 when all users have all required clearances, formal access approvals, and the need-to-know for all information on the system.

b. Systems are operating at Protection Level 2 when all users have all required formal approvals for access to all information on the system, but at least one user lacks administrative approvals for some of the information on the system. This means that all users have all required clearances and all required formal access approvals, but at least one user lacks the need-to-know for some of the information on the system.

c. Systems are operating at Protection Level 3 when at least one user lacks at least one required formal approval for access to some information on the system. This means that all users have all required clearances, but at least one user lacks formal access approval for some of the information on the system.

d. Systems are operating at Protection Level 4 when at least one user has only a DOD Secret or DOE L clearance, and the level of concern for confidentiality is high.

e. Systems are operating at Protection Level 5 when at least one user has no clearance, and the information on the system is classified no higher than Secret and contains no Sigma 1, 2, 14, or 15 (i.e., the level of concern for confidentiality is low or medium).

f. Systems are operating at Protection Level 6 when at least one user has no clearance, and the level of concern for confidentiality is high.

4. PROTECTION PROFILES.

a. Common Requirements. Requirements common to all systems are detailed in Chapter VI.

b. Graded Requirements. Protection requirements graded by levels of concern and confidentiality protection level are detailed in Chapter VII. The tables included here present the requirements detailed in Chapter VII. To use these tables, find the column representing the protection level for confidentiality, or find the column representing the level of concern for integrity or availability.

(1) Confidentiality Components. Confidentiality components describe the confidentiality protection requirements that must be implemented in an information system using the profile. Confidentiality protection requirements are graded according to the confidentiality protection levels that incorporate levels of concern.

Table 4. Protection Level Table for Confidentiality.

Level of Concern	**Lowest Clearance**	**Formal Access Approval**	**Need-To-Know**	**Protection Level**
High	Uncleared	NOT ALL Users Have ALL	NOT ALL Users Have ALL	6
Medium or Low	Uncleared	NOT ALL Users Have ALL	NOT ALL Users Have ALL	5
High or Medium	DOD Secret or DOE L	NOT ALL Users Have ALL	NOT ALL Users Have ALL	4
High, Medium, or Low	At Least Equal to Highest Data	NOT ALL Users Have ALL	NOT ALL Users Have ALL	3
High, Medium, or Low	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	2
High, Medium, or Low	At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	1

CANCELED

Table 5. Protection Profile Table for Confidentiality.

	Confidentiality Protection Level					
Requirements (Paragraph)	**1**	**2**	**3**	**4**	**5**	**6**
Audit Capability (VII.3)	AUD-1	AUD-2	AUD-3	AUD-4	AUD-4	AUD-5
Communications (VII.6)	COM-1	COM-1	COM-1	COM-2	COM-1	COM-1
Configuration Management (VII.7)	CM-1	CM-1	CM-2	CM-3	CM-3	CM-3
Independent Validation and Verification (VII.9)				IVV-1	IVV-1	IVV-2
Resource Access Controls (VII.10)		RAC-1	RAC-2	RAC-3	RAC-3	RAC-3
Resource Utilization (VII.11)		RU-1	RU-2	RU-2	RU-2	RU-2
Session Controls (VII.12)	SC-1	SC-2	SC-2	SC-3	SC-3	SC-3
Security Documentation (VII.13)	SD-1	SD-1	SD-1	SD-2	SD-2	SD-2
Separation of Functions (VII.14)			SF-1	SF-1	SF-1	SF-1
System Recovery (VII.15)	SR-1	SR-1	SR-1	SR-2	SR-2	SR-2
Security Support Structure (VII.16)	SSS-1	SSS-1	SSS-2	SSS-3	SSS-3	SSS-3
Security Testing (VII.17)	ST-1	ST-2	ST-2	ST-3	ST-3	ST-3
Trusted Path (VII.18)					TP-1	TP-1

CANCELED

(2) Integrity Components. Integrity components describe the integrity protection requirements that must be implemented in an information system using the profile. The integrity protection requirements are graded according to the integrity level of concern.

(3) Availability Components. Availability components describe the availability protection requirements that must be implemented in an information system using the profile. The availability protection requirements are graded according to the availability level of concern.

5. SIGNIFICANT RISK SYSTEMS. Systems operating at Protection Level 5 or 6 present a *significant* risk of the loss of classified information. Systems operating at these levels may operate in within a protected environment or have connections that provide encrypted data to pass over public switched networks. Direct connections to public switched networks, without absolute assurance that all communications are encrypted, are not permitted.

Table 6. Protection Profile Table for Integrity.

	Integrity Level of Concern		
Requirements (Paragraph)	**Low**	**Medium**	**High**
Audit Capability (VII.3)	AUD-1	AUD-2	AUD-4
Backup and Restoration of Data (VII.4)	BRD-1	BRD-2	BRD-3
Changes to Data (VII.5)	CD-1	CD-1	CD-2
Communications (VII.6)	COM-1	COM-1	COM-2
Configuration Management (VII.7)	CM-1	CM-2	CM-3
Security Support Structure (VII.16)	SSS-1	SSS-2	SSS-3
Security Testing (VII.17)	ST-1	ST-2	ST-3

Table 7. Protection Profile Table for Availability.

	Availability Level of Concern		
Requirements (Paragraph)	**Low**	**Medium**	**High**
Alternate Power Source (VII.2)	APS-1	APS-2	APS-3
Backup and Restoration of Data (VII.4)	BRD-1	BRD-2	BRD-3
Disaster Recovery Planning (VII.8)	DRP-1	DRP-2	DRP-3
Security Support Structure (VII.16)	SSS-1	SSS-2	SSS-3

Any connection of these systems to other agencies will require a memorandum of understanding stating that the system/network being connected either–

a. is not connected to the public switched network,

b. is not connected to another system/network that does not use encrypted connections to the public switched network, or

CANCELED

c. is connected to the public switched network and uses approved encryption methods for that connection..

6. SUBSTANTIAL RISK SYSTEMS. Systems operating at Protection Level 4 present a *substantial* risk of the loss of the separation and need-to-know protection provided by compartmentation. DAAs must recognize the technical risk of operating such systems.

7. SPECIAL CATEGORIES. Several categories of systems can be adequately secured without implementing the protection measures specified in Chapter VII. These systems are *not* "exceptions" or "special cases" of the protection levels specified in this chapter; however, applying the protection requirements specified in Chapter VII to these systems by rote results in unnecessary costs and operational impacts. In general, the technical questions are where, when, and how to apply a given set of protection measures, rather than whether to apply the measures. For many of these "special" systems (such as guards or pure servers and tactical, embedded, data-acquisition, and special-purpose systems), the physical security protections for the system provide the required access control while the application running on the platform provides the required user separation.

a. Pure Servers.

(1) Certain specialized systems, when acting as pure servers in a network, do not fit the protection level criteria and may need fewer protection measures. These systems have the following characteristics:

(a) no user code is present on the system,

(b) only system administrators and maintainers can access the system,

(c) the system provides non-interactive services to clients (e.g., packet routing or messaging services),

(d) the hardware and/or application providing network services otherwise meets the protection requirements of the network,

(e) the risk of attack against the Security Support Structure (SSS) using network communication paths is sufficiently low, and

(f) the risk of attack against the SSS using physical access to the system itself is sufficiently low.

(2) The *platform (i.e., hardware and operating system)* on which the guard or pure server runs usually needs to meet no more than Protection Level 3 security requirements. The guard or pure server may have a large number of clients (i.e.,

CANCELED

individuals who use the guard's or server's functional capabilities in a severely constrained way). The guard *application* or server *application* itself will have to provide the more stringent protection requirements appropriate for the system's protection level and operational environment. Assurances appropriate to the levels of concern for the system must be implemented.

(3) Systems that *do have general users or do execute general user code* are not "pure servers" within the meaning of this section and so must meet all protection requirements specified for their protection level and operational environment.

(4) The term "pure server" is not intended to limit the applicability of this section to systems that have traditionally been referred to as servers. For example, a messaging system that happened to be implemented on a general-purpose computer platform could be accredited under this Manual, and if such a system meets the specifications in (1), above, the system's protection requirements could be categorized by this section of the Manual.

(5) The above easing of protection requirements does not imply any relaxation in other security requirements (e.g., physical and communications security requirements), which are determined by the information handled or protected by the system. As stated above, this easing of protection requirements is predicated upon adequate application of physical security and other appropriate security disciplines.

b. Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems. Some systems cannot be altered by users and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called "embedded" systems fall into this category, as do some data-acquisition systems and some other special-purpose systems. These systems also have the characteristics that first, and most importantly, there are *no general users* on the system and, second, there is *no user code* running on the system. If the DAA determines that such a system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security, then the system does not have to meet additional protection requirements specified for more-general-purpose systems in this Manual. DAAs and implementors are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system's protection level.

c. Systems with Group Authenticators. Many protection measures specified in this Manual implicitly assume that the system includes an acceptable level of individual accountability. This is normally ensured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/authenticator combination. Such situations often require the use of group authenticators.

CANCELED

In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators must be used only for broader access *after* the use of a unique authenticator for initial identification and authentication. The use of group authenticators must be approved by the DAA.

d. Single-User, Stand-Alone Systems. Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. DAAs can approve administrative and environmental protection measures for such systems, in lieu of technical ones. Systems that have one user at a time, but have a total of more than one user with no sanitization between users, are multi-user systems, and the DAA must consider the systems as such in determining the protection level and the resulting protection requirements. Systems that have one user at a time, and are sanitized between users, are periods processing systems as described below.

e. Periods Processing. Periods processing is a method of operating an information system sequentially that provides the capability to process information at various levels of sensitivity at distinctly different times. Periods processing provides the capability to either have more than one user or group of users (sequentially) on a single-user information system who do not have the same need-to-know or who are authorized to access different levels of information *or* use an information system at more than one protection level (sequentially).

(1) Sanitization After Use. If an information system is used for periods processing either by more than one user or for segregating information by classification level onto separate media, the ISSP must specify the sanitization procedures to be employed by each user before and after each use of the system.

(2) Sanitization Between Periods. The information system must be sanitized of all information before transitioning from one period to the next [e.g., whenever a new user does not have access authorization or the need-to-know for data processed during the previous period, which is changing from one protection level to another]. The DAA must document and approve such procedures, which could include, among others, sanitizing nonvolatile storage, exchanging disks, and powering down the information system and its peripherals.

(3) Media for Each Period. Information systems employed in periods processing must have separate media for each period of processing, including copies of operating systems, utilities, and applications software.

(4) Audit. If several people are using the system, and the system is not capable of automated logging, the DAA must consider requiring manual logging. Audit trails are not required for single-user, stand-alone systems.

CANCELED

8. PROTECT AS RESTRICTED DATA (PARD).

a. Site Authorization to Use PARD Designation. Any site wishing to use the PARD designation must receive prior approval from the Director, Office of Nonproliferation and National Security. The ISOM may limit use of the PARD designation to specific organizations at a site. Use of the PARD designator will be discontinued permanently on June 30, 2002.

b. Handling and Control of PARD Information. The security measures contained herein apply only to PARD information as it appears as output, hereafter referred to as "PARD output."

(1) Only printed computer output may be marked PARD. Electronic media (disks, tapes, etc.) and computer systems may not be marked PARD. Within the classified information system (including communication lines), information that will be labeled PARD when it is in printed form is designated as Secret Restricted Data.

(2) PARD output may be generated only on classified information systems that have been accredited to process information at the high level of concern for confidentiality.

(3) PARD output may be used only in a DOE limited or protected area.

(4) PARD output may be accessed only by personnel who have a Q access authorization and a need-to-know.

(5) Appropriately trained users (see Paragraph 8c, below) may determine the use of the PARD marking for their information. The PARD marking must be used only–

- if the output may contain limited quantities of classified information that is not readily recognized as classified because it is contained in large quantities of unclassified information and

- if the PARD output contains a substantial volume of data with a low density of potentially classified information.

(6) PARD output must be conspicuously marked on each page or sheet with the words "PROTECT AS RESTRICTED DATA." Where space does not allow, the letters "PARD" may be used. This marking must be applied when the PARD output is originated. All PARD output must show the date of origination.

(7) When not in use, PARD output must be stored as follows:

- within a limited or protected area in a manner authorized for Secret Restricted Data documents (see DOE M 471.2-1B, CLASSIFIED MATTER PROTECTION AND CONTROL MANUAL);

CANCELED

- in a secure storage container or filing cabinet equipped with a locking device; or
- in an area that is administratively controlled during work hours and maintained under locked conditions during nonwork hours.

The keys/combinations for any locks used to protect PARD must be administratively controlled and available only to persons with at least a Q access authorization and a need-to-know.

(8) PARD output must be destroyed in the same manner as Secret Restricted Data documents (see DOE M 471.2-1B).

(9) PARD output to be transferred from the site on which it was originated to another site must be reviewed for classification (DOE M 475.1-1, IDENTIFYING CLASSIFIED INFORMATION) and, if classified, must be marked, handled, protected, and transferred as any other classified document (DOE M 471.2-1B). PARD output transferred between points within a limited or protected area or between limited or protected areas located at the same site must be in the personal custody of a person who has a Q access authorization. Between limited or protected areas, PARD output must be protected as a Secret Restricted Data document (DOE M 471.2-1B).

c. <u>Training of PARD Users</u>. The Classified Matter Protection and Control (CMPC) Manager at a site approved for the use of PARD output must ensure proper control and use of PARD output by ensuring that each user is aware of the special security measures necessary for handling PARD output. A user must not be allowed to use the PARD designation until he/she has received appropriate training as specified by the CMPC Manager. The CMPC Manager must ensure that periodic reviews are conducted to ensure that accumulation of PARD output is kept to a minimum and that the PARD marking is being used in compliance with this Manual.

CANCELED

CHAPTER V

CERTIFICATION AND ACCREDITATION

1. OVERVIEW. The certification and accreditation process begins after protection measures have been implemented and any required classified information system protection documentation has been approved. The certification process confirms that the protection profile described in the ISSP has been implemented and that the protection measures are functioning properly. This process culminates in an accreditation for the system to operate.

2. CERTIFICATION PROCESS. The certification process confirms that the system's protection measures have been correctly implemented in accordance with the selected protection profile.

   a. Independent Validation and Verification. For information systems intended to operate in Protection Level 5 or 6, an Independent Validation and Verification (IV&V) review must be conducted and funded by the cognizant site.

   b. Sensitive Compartmented Information. For information systems located in an SCIF that processes SCI, the cognizant ISSM, ISOM, and ISPM must review the information system protection documentation and the certification of the information system. Once they have completed their review, they send it, with their comments, to the Office of Energy Intelligence and the Office of Nonproliferation and National Security.

3. ACCREDITATION. The DAA must review and accredit all systems before they become operational to ensure they maintain the confidentiality, availability, and integrity of all classified information.

   a. Provisional Accreditation. The DAA may grant provisional accreditation (temporary authority) to operate an information system because of incomplete documentation or to permit a major conversion of the information system. Provisional accreditation may be granted for up to 180 days. DAA-approved protection measures must be in place and functioning during the period of provisional accreditation.

   b. Reaccreditation. As outlined in National Policy contained in OMB Circular A-130, "Management of Federal Information Resources," and National Security Telecommunications and Information Systems Security Directives (NSTISSDs), each information system must be reaccredited every 3 years or whenever security-significant changes are made to the accredited information system. The ISSO/ISSM/ISOM must review proposed modifications to information systems to determine if the proposed modifications will impact the protections on the system. If the protection aspects of the systems environment change, if the applicable protection requirements change, or if the protection mechanisms implemented for the system change, the system must be reaccredited.

CANCELED

During the reaccreditation cycle, the DAA may choose to grant an interim accreditation for the system.

c. Withdrawal of Accreditation. The DAA must evaluate the risks and consider withdrawal of accreditation if the protection measures approved for the system do not remain effective or whenever any of the following items change: levels of concern, protection level, technical or nontechnical protection measures, vulnerabilities, operational environment, operational concept, or interconnections. The DAA must withdraw accreditation and ensure proper sanitization when the system is no longer required to process classified information, or if the operational need for the system no longer outweighs the risk of operating the system.

d. Invalidation of an Accreditation. An accreditation becomes invalid immediately whenever detrimental, security-significant changes occur to any of the following: the required protection level, the operational environment, the operational concept/mission, or the interconnections.

e. Certification and Accreditation of Multiple Systems. If two or more similar information systems are to be operated in equivalent operational environments (e.g., the levels of concern and protection level are the same and the physical security requirements are similar), the ISSO may write and the DAA may approve a Master ISSP to cover all such information systems. The information systems covered by a Master ISSP may range from personal computers up to and including multi-user information systems and local area networks that meet the criteria for a Master ISSP approach.

(1) Master Systems Security Plan. The Master ISSP must conform to the ISSP requirements in this Manual and specify the information required for each certification for an information system to be accredited under the plan.

(2) Information Systems Certification Report (ISCR). The ISCR must contain–

(a) the information system’s identification,

(b) the information system’s location, and

(c) a statement signed by the ISSM certifying that the information system implements the requirements in the Master ISSP.

(3) The DAA must accredit the first information system under the Master ISSP. The ISSM must certify that all other individual information systems to be operated under the Master ISSP meet the conditions of the approved Master ISSP. This certification, in effect, accredits the individual information systems to operate under the Master ISSP. A copy of each certification report must be retained with the approved copy of the Master ISSP.

CANCELED

(4) Recertification of Information Systems. All information systems certified under a Master ISSP remain certified until the Master ISSP is changed or 3 years have elapsed since the information system was certified. If either the levels of concern or the protection level described in the Master ISSP changes, all information systems certified under the Master ISSP must be recertified.

4. DESIGNATED APPROVING AUTHORITY.

a. Systems at Protection Level 5 or 6. Accreditation for systems at Protection Level 5 or 6 will require the concurrence of the ISPM.

b. Delegation of Approval Authority. The DAA may delegate approval authority provided that–

(1) all delegations are in writing and for a specified time period not to exceed 3 years,

(2) the DAA (or his/her delegate) and the person certifying the system are not the same person,

(3) the delegate cannot redelegate the approval authority, and

(4) the delegate is a DOE employee.

c. Systems under Multiple Designated Approving Authorities. For a system that involves multiple DAAs, the ISPM, in coordination with the field, must designate the DAA. Each site involved in the system must identify, in writing, the security officials to be responsible for implementing information system protection on the system components at the site.

d. Director of Naval Reactors Program. For classified information systems 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 must designate one of the Naval Reactor Office senior managers to be the DAA. Notification of the accreditation of any information system with a protection level of 4, 5, or 6 must be furnished to the ISPM.

5. DEVIATIONS. If it is impossible or impracticable to implement the protection requirements and countermeasures described in this Manual, deviations (variances, waivers, or exceptions), including alternative protection measures, must be requested under the procedures described in DOE O 470.1.

CANCELED

CHAPTER VI

BASELINE REQUIREMENTS

1. INTRODUCTION. This chapter describes protection requirements common to all systems.

2. CLEARING AND SANITIZATION.

   a. Clearing. All internal memory, buffer, or other reusable memory must be cleared to effectively deny access to previously stored information. Detailed instructions on clearing must be issued periodically by the ISPM.

   b. Sanitization. Classified information systems resources must be sanitized before they are released from classified information controls or released for use at a lower classification level. Detailed instructions on sanitization must be issued periodically by the ISPM.

3. EXAMINATION OF HARDWARE AND SOFTWARE. Information systems hardware and software must be examined when received from the vendor and before being used.

   a. Information Systems Software. Commercially procured software must be tested to ensure that it contains no obvious features that might be detrimental to the security of the information system. Security-related software must be tested to ensure that the security features function as specified.

   b. Information Systems Hardware. The equipment must be examined to determine that it appears to be in good working order and has no "parts" that might be detrimental to the secure operation of the information system when placed under site control and cognizance. Subsequent changes and developments that affect security may require additional examination.

4. IDENTIFICATION AND AUTHENTICATION MANAGEMENT. Identification and authentication are required to ensure that users are associated with the proper security attributes, such as identity, protection level, or location. Controls, such as biometrics or smart cards, may be used at the discretion of the ISSO with approval of the ISSM and DAA.

   a. Identifier Management. User identifiers must be managed in accordance with documented procedures.

   b. Authenticator Management. User authenticators must be managed in accordance with documented procedures.

CANCELED

c. Unique Identification. Each user must be uniquely identified and that identity must be associated with all auditable actions taken by that individual.

d. Authentication at Logon. Users must be required to authenticate their identities at “logon” time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior to the execution of any application or utility on the system.

e. Access to Authentication Data. Access to authentication data must be restricted to authorized personnel through the use of encryption, file access controls, or both.

f. User ID Reuse. Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) must be removed from the system.

g. User ID Removal. When an employee leaves the sponsoring organization or loses access to the system for cause, that individual’s user ID and authentication must be removed or disabled from the system.

h. User ID Revalidation. All active user IDs must be revalidated at least annually, and information such as sponsor and means of off-line contact (e.g., phone number, mailing address) must be updated as necessary.

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

j. Protection of Passwords. When passwords are used as authenticators, the following must apply.

(1) Passwords must be protected at a level commensurate with the classification level and most restrictive classification category of the information to which they allow access.

(2) Passwords must contain a minimum of six nonblank characters.

(3) Passwords must be generated by a method approved by the DAA. Password acceptability must be based on the method of generation, the length of the password, and the size of the password space. The password generation method, the length of the password, and the size of the password space must be documented. In no case must a user develop his/her own password.

(4) When an information system cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask must be printed before the password is entered to conceal the typed password.

CANCELED

(5) User software, including operating system and other security-relevant software, comes with a few standard authenticators (e.g., System, Test, Master) and passwords already enrolled in the system. Passwords for all standard authenticators must be changed before allowing the general user population access to the information system. These passwords must be changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.

(6) If the level of concern for confidentiality is low, the lifetime of a password must not exceed 12 months. If the level of concern is medium or high, the lifetime of a password must not exceed 6 months.

5. MAINTENANCE. Information systems are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.

a. Cleared Maintenance Personnel. Personnel who perform maintenance on systems must be cleared to the highest classification level of information on the system and indoctrinated for all information processed on that system. Cleared personnel who perform maintenance or diagnostics on information systems do not require an escort. When possible, however, an appropriately cleared and technically knowledgeable, facility employee must be present within the area where the maintenance is performed to ensure that proper security and safety procedures are followed.

b. Uncleared (or Lower-Cleared) Maintenance Personnel.

(1) If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided a fully cleared and technically qualified escort monitors and records his/her activities in a maintenance log.

(2) If maintenance personnel are uncleared, system initiation and termination must be performed by the fully cleared and technically qualified escort. In addition, their keystrokes must be monitored during their access to the system.

(3) Prior to maintenance by uncleared personnel, the information system must be completely cleared and all nonvolatile data storage media must be removed or physically disconnected and secured. When a system cannot be cleared, ISSM-approved procedures must be enforced to deny the uncleared individual visual and electronic access to any classified or sensitive data contained on the system.

(4) A separate, unclassified copy of the operating system, including any micro-coded floppy disks or cassettes integral to the operating system, must be used for all maintenance operations performed by uncleared personnel. The copy must be labeled

CANCELED

"UNCLASSIFIED — FOR MAINTENANCE ONLY" and protected in accordance with documented procedures. Maintenance procedures for an information system using a nonremovable storage device on which the operating system is resident must be considered by the ISSM on a case-by-case basis.

c. General Maintenance Requirements.

(1) The ISOM must identify the need for, and format of, a maintenance log.

(2) Systems maintenance must be performed on site whenever possible. Equipment repaired off site and intended for reintroduction into a facility may require protection from association with that particular facility or program.

(3) If systems or system components are removed from the facility for repair, they must first be purged and downgraded to an appropriate level or sanitized of all classified and sensitive data and declassified in accordance with ISSM-approved procedures. The ISSO must approve the release of all systems and all parts removed from the system.

(4) Introduction of network analyzers (e.g., sniffers) that would allow maintenance personnel to monitor keystrokes must be approved by the DAA prior to being introduced into an information system. The DAA must approve use of these devices by uncleared maintenance personnel when a system cannot be cleared or sanitized of all classified and sensitive data. The ISSM must approve use of these devices by maintenance personnel who are cleared to the highest classification level processed by the system.

(5) If maintenance personnel bring into a facility diagnostic test programs (e.g., software/firmware used for maintenance or diagnostics), the following procedures must be implemented.

(a) The media containing the programs must be checked for malicious codes before the media are connected to the system.

(b) The media must remain within the facility and must be stored and controlled at the level of the information system.

(c) Prior to entering the facility, maintenance personnel must be advised that they will not be allowed to remove media from the facility.

(d) If this procedure cannot be followed because of special circumstances, the following must occur each time the diagnostic test media are introduced into a facility.

CANCELED

1 The media must undergo stringent integrity checks (e.g., virus scanning, checksum, etc.) prior to being used on the information system.

2 Before leaving the facility, the media must be checked to ensure that no classified information has been written on the media.

3 The DAA must approve the revised procedure.

(6) All diagnostic equipment and other devices carried into a facility by maintenance personnel must be handled as follows.

(a) Systems and system components being brought into the facility must be inspected for improper modification.

(b) Before being released, maintenance equipment capable of retaining information must be appropriately sanitized by procedures issued by the ISPM. If the equipment cannot be sanitized, the equipment must remain within the facility, be destroyed, or be released under procedures approved by the DAA.

(c) Replacement components may be brought into the facility to swap with facility components; however, any component placed into an information system must remain in the facility until proper release procedures are completed. Any component not placed in an information system may be released from the facility provided the component was under control of a trained escort or reviewed under approved procedures.

(d) Communication devices with transmit capability (e.g., pagers, RF LAN connections, etc.) belonging to the maintenance personnel or any data storage media not required for the maintenance visit must remain outside the system facility and be returned to the maintenance personnel when they leave the facility.

(7) Maintenance changes that affect the security of the system must receive a configuration management review.

(8) After maintenance has been performed, the security features on the information systems must be checked and documented to ensure they are still functioning properly.

d. Remote Maintenance.

(1) Remote diagnostic maintenance service may be provided by a service or organization that **does** provide the same level and category(ies) of security. The communications links connecting the components of the systems, associated data communications, and

CANCELED

networks must be protected in accordance with national policies and procedures applicable to the sensitivity level of the data being transmitted.

(2) If remote diagnostic or maintenance services are required from an organization that *does not* provide the same level of security required for the system being maintained, the following procedures must be implemented.

(a) The information system must be sanitized and in a stand-alone mode prior to connection of the remote-access line.

(b) If the system cannot be sanitized (e.g., due to a system crash), remote diagnostic and maintenance services must not be allowed.

(c) The ISSO must initiate and terminate the remote access.

(d) Keystrokes must be monitored on all remote diagnostic or maintenance services. Before beginning remote diagnostics/maintenance activities, maintenance technicians performing these activities must be advised (contractually, verbally, by banner, etc.) that keystroke monitoring must be performed.

(e) A technically qualified person must review the maintenance log to ensure the detection of unauthorized changes.

(f) Maintenance personnel accessing the information systems at the remote site must be cleared to the highest level of information processed on that system prior to sanitization.

(g) Procedures for installing and using remote diagnostic links must be approved by the DAA.

(h) An audit log of all remote maintenance, diagnostic, and service transactions must be maintained and periodically reviewed. This review must be documented.

(i) Other techniques to consider include encryption and decryption of diagnostic communications, strong identification and authentication techniques (e.g., tokens), and remote disconnect verification.

(3) System maintenance requirements and vulnerabilities must be addressed during all phases of the system life cycle. Specifically, contract negotiations must consider the security implications of system maintenance.

6. <u>MALICIOUS CODE</u>.

CANCELED

CANCELED

a. Site Policies. Policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, must be implemented.

b. Personal Software. The use of software purchased or developed by an individual for personal use is discouraged. If such software is required or desired to enhance the information system operation, each installation of the software must be approved in accordance with site policies.

c. Public Domain Software. The use of public domain software is strongly discouraged. If such software is required or needed to enhance system operation, procedures must be implemented to carefully examine this software for malicious code before it is introduced into the information system environment.

7. MARKING HARDWARE, OUTPUT, AND MEDIA. Markings on hardware, output, and media must conform to instructions issued by the ISPM. If the required marking is impractical or interferes with operation of the media, the DAA may approve alternate marking procedures. The alternate marking procedures must be documented.

a. Hardware Components. Procedures must be implemented to ensure that all components of an information system, including input/output devices, terminals, stand-alone microprocessors, or word processors used as terminals, bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the information system. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the information system and displayed on the screen.

b. Hard-Copy Output. Hard-copy output includes paper, fiche, film, and other printed media. The accreditation level of the accredited information system must be marked on all hard-copy output that is retained in, or distributed from, the facility unless an appropriate classification review has been conducted or the information has been generated by a tested program verified to produce consistent results and approved by the DAA. Such programs will be tested on a statistical basis to ensure continuing performance. Once hard copy has been reviewed by an authorized classifier, it must be marked in accordance with DOE M 471.2-1B, CLASSIFIED MATTER PROTECTION AND CONTROL MANUAL.

c. Removable Media. Procedures must be implemented to ensure that personnel handling removable media apply visible, human-readable, external markings to the media. Removable media must be marked with the accreditation level of the information system unless an appropriate classification review has been conducted, or the information on the media has been generated by a tested program or methodology verified to produce consistent results and approved by the DAA.

d. Unclassified Media. In facilities where some of the information systems are operated as classified and some are dedicated to unclassified operation, removable unclassified media must be uniquely marked to prevent them from being mixed with classified media.

8. PERSONNEL SECURITY. Personnel with system access play an integral role in protecting information, defining their system security policies, and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their information systems. Personnel directly involved with a system may be users, operators, administrators, Communications Security (COMSEC) custodians, and installers/maintainers. Duties, responsibilities, privileges, and specific limitations of information systems users, both general and privileged, must be specified in writing. So far as feasible, security duties must be distributed to preclude any one individual from adversely affecting operations or the integrity of the system.

a. Access Approvals. Individuals requiring access to classified information must be processed for access authorization in accordance with DOE O 472.1B, PERSONNEL SECURITY ACTIVITIES.

(1) For systems that process classified information at Protection Level 1, 2, or 3, individuals must be *cleared* to the highest level of classification processed on that system. For Protection Level 4, 5, or 6 systems, individuals need only be *cleared* for the information to which they are allowed access.

(2) For Protection Level 1 or 2 systems, the individuals must have all required formal access approval(s) for all information on the systems. For Protection Level 3, 4, 5, or 6 systems, individuals need formal access approval for only that information to which they are allowed access.

b. General Users.

(1) General users must–

(a) access only the data, control information, and software for which they are authorized access and have a need-to-know;

(b) immediately report all security incidents and potential threats and vulnerabilities involving the information system to the appropriate ISSO;

(c) protect their authenticators and report any compromise or suspected compromise of an authenticator to the appropriate ISSO;

(d) ensure that system media and system output are properly classified, marked, controlled, and stored;

CANCELED

(e) protect terminals from unauthorized access;

(f) inform the ISSO when access to a particular information system is no longer required (e.g., completion of a project, transfer, retirement, resignation);

(g) observe rules and regulations governing the secure operation and authorized use of information systems; and

(h) use the information system only for official Government business.

(2) General users must not attempt to–

(a) introduce malicious code into any information system or physically damage the system;

(b) bypass, strain, or test security mechanisms (if security mechanisms must be bypassed for any reason, users must coordinate the procedure with the ISSO and receive written permission from the ISSM for the procedure); any ongoing or regular bypass of security mechanisms must be approved by the DAA;

(c) introduce or use unauthorized software, firmware, or hardware on an information system;

(d) assume the roles and privileges of others and attempt to gain access to information for which they have no authorization; and

(e) relocate information system equipment without proper authorization.

c. <u>Privileged Users</u>.

(1) The number of privileged users must be limited to the absolute minimum number needed to manage the system.

(2) Examples of privileged users (for multi-user systems) include–

(a) users with “super-user,” “root,” or equivalent access to a system (i.e., system administrators, computer operators, perhaps system security officers, etc.);

(b) those individuals with near or complete control of the operating system of the machine or information system or who set up and administer user accounts, authenticators, and the like;

CANCELED

(c) users with access to change control parameters (e.g., routing tables, path priorities, addresses) on routers, multiplexors, and other key information system equipment;

(d) users given the capability to control and change other users' access to data or program files (i.e., applications software administrators, administrators of specialty file systems, database managers, etc.); and

(e) users given special access for troubleshooting information systems/security monitoring functions (i.e., those using information system analyzers, management tools, etc.).

(3) All privileged users must be responsible for all the requirements as stated for general users.

(4) Privileged users must–

(a) be U.S. citizens unless otherwise approved in writing by the DAA,

(b) possess access approvals to all information on the system,

(c) possess a clearance equal to the highest classification of data processed on or maintained by the information system,

(d) protect the root or super-user authenticator at the highest level of data it secures and not share the authenticator and/or account,

(e) be responsible for all super-user or root actions under his/her account,

(f) report any and all information system problems to the ISSO, and

(g) use the special access or privileges granted only to perform authorized tasks and functions.

(5) Privileged users must not–

(a) enroll any unauthorized user on an information system or

(b) use special access or privileges to perform unauthorized tasks or functions.

9. PHYSICAL SECURITY.

a. Protection. The information and system must be located in a security area appropriate to the classification and sensitivity of the data.

CANCELED

b. Visual Access. Devices that display or output information in human-readable form must be positioned to deter unauthorized individuals from reading the information without the knowledge of the user.

c. Information Protection. Information must be protected in accordance with DOE 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, Chapter III, Paragraph 3.

d. Unescorted Access. All personnel granted unescorted physical access to the system must have an appropriate security clearance and a need-to-know or a presumptive need-to-know for all information on the information system.

10. PROTECTION OF MEDIA.

a. Media Protection. Media must be protected by at least one (or a combination) of the following until the media have been reviewed following a DAA-approved procedure:

(1) storage in an area approved for open storage of information at the accreditation level of the information system;

(2) storage in an area not approved for open storage of information at the accreditation level of the information system while continuously attended, if the area is continuously attended by appropriate personnel;

(3) Type 1 encryption of stored data; or

(4) GSA-Approved Security Container.

b. Removable Media. Removable media must be controlled and protected in a manner consistent with that used for classified matter.

CANCELED

11. REVIEW OF OUTPUT.

a. Human-Readable Output Review. An appropriate sensitivity and classification review must be performed on human-readable output before the output is released outside the system boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

b. Media Review. Electronic output, such as files, to be released outside the security boundary must be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footers) before being released. Information on media that are not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application.

Random or representative sampling techniques may be used to verify the proper marking of large volumes of output. The media sampling procedures must be defined and documented. DAA-approved automated techniques may be used to verify the proper marking of output.

12. WASTE, FRAUD, AND ABUSE PROTECTION. Management controls established to address waste, fraud, and abuse of Government property and resources must be documented. Waste, fraud, and abuse must be reported in accordance with DOE 2030.4B, REPORTING FRAUD, WASTE, AND ABUSE TO THE OFFICE OF INSPECTOR GENERAL.

CANCELED

CHAPTER VII

GRADED REQUIREMENTS

1. INTRODUCTION. Each section of this chapter describes implementation requirements for a different protection measure.

2. ALTERNATE POWER SOURCE (APS). An alternate power source ensures that the system availability is maintained if primary power is lost. An APS can also provide time for orderly system shutdown or the transfer of system operations to another system or power source.

   a. APS-1 Requirement. The decision not to use an alternate source of power, such as an uninterruptible power supply for the system, must be documented.

   b. APS-2 Requirements. Instead of APS-1, procedures for the graceful shutdown of the system must ensure no loss of data.

   c. APS-3 Requirements. Instead of APS-2, procedures for transfer of the system to another power source must ensure that the transfer is completed within the time requirements of the application(s) on the system.

   d. Profile Requirements.

Requirements	**Availability Level of Concern**		
	Low	**Medium**	**High**
Alternate Power Source	APS-1	APS-2	APS-3

3. AUDIT CAPABILITY (AUD). Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user was responsible for them.

   a. AUD-1 Requirements.

      (1) Automated Audit Trail Creation. The system must automatically create and maintain an audit trail or log. If the operating system cannot provide an automated audit capability, an alternative method of accountability for user activities on the system must be developed and documented. Audit records must be created to record the following:

         (a) successful and unsuccessful logons and logoffs;

CANCELED

(b) successful and unsuccessful accesses to security-relevant files, including creating, opening, closing, modifying, and deleting the files;

(c) changes in user authenticators;

(d) blocking or blacklisting a user ID, terminal, or access port and the reason for the action; and

(e) denial of access resulting from an excessive number of unsuccessful logon attempts.

(2) Audit Trail Protection. The contents of audit trails must be protected against unauthorized access, modification, or deletion.

(3) Audit Trail Analysis. Audit analysis and reporting must be scheduled and performed. (On Protection Level 1, 2, and 3 systems only, the frequency of the review must be documented. Results of the review must be documented.)

(4) Audit Record Retention. Audit records must be retained for at least 6 months.

b. AUD-2 Requirements. In addition to those requirements stated in AUD-1, AUD-2 includes the following requirements.

(1) Audit Trail Contents. The audit trail must include records of–

(a) privileged activities at the system console (either physical or logical consoles) and other system-level accesses by privileged users and

(b) starting and ending times for each access to the system.

(2) Audit Failure. Procedures must be implemented to ensure alternate audit capability or system shutdown in the event of audit failure.

c. AUD-3 Requirements. In addition to those requirements stated in AUD-2, AUD-3 includes the following requirements.

(1) Automated Audit Analysis. Audit analysis and reporting using automated tools must be scheduled and performed.

(2) Security Label Changes. The system must automatically record the creation, deletion, or changes in security labels.

CANCELED

d. AUD-4 Requirements. In addition to those requirements stated in AUD-3, AUD-4 includes the following requirement.

Continuous Monitoring. Auditing must include the continuous, online monitoring of auditable events. The system must notify an authorized person when imminent violations of security policies are detected.

e. AUD-5 Requirements. In addition to those requirements stated in AUD-4, AUD-5 includes the following requirement.

Intrusion Detection and Monitoring. The security posture of the system must be tested at least monthly by employing various intrusion/attack detection and monitoring tools.

f. Profile Requirements.

	Confidentiality Protection Level					
Requirements	**1**	**2**	**3**	**4**	**5**	**6**
Audit Capability	AUD-1	AUD-2	AUD-3	AUD-4	AUD-4	AUD-5

	Integrity Level of Concern		
Requirements	**Low**	**Medium**	**High**
Audit Capability	AUD-1	AUD-2	AUD-4

4. BACKUP AND RESTORATION OF DATA (BRD). The regular backup of information is necessary to ensure that users have continuing access to the information. Periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

a. BRD-1 Requirements.

(1) Backup Procedures. Procedures for the regular backup of all essential and security-relevant information, including software tables and settings (e.g., router tables, software, and documentation), must be documented.

(2) Backup Frequency. The frequency of backups must be defined, with the assistance of the data custodian(s), and documented in the backup procedures.

b. BRD-2 Requirements. In addition to those requirements stated in BRD-1, BRD-2 includes the following requirements.

CANCELED

(1) Backup Media Storage. Media containing backup files and backup documentation must be stored at another location, such as another part of the same building, a nearby building, or off site, to reduce the possibility that a common occurrence could eliminate the on-site backup data and the off-site backup data.

(2) Verification of Backup Procedures. Backup procedures must be verified periodically by confirming that the date of last backup is consistent with the backup procedures.

c. BRD-3 Requirements. In addition to those requirements stated in BRD-2, BRD-3 includes the following requirement.

Information Restoration Testing. Complete restoration of information from backup media must be tested periodically. The frequency of restoration testing must be defined and documented in the backup procedures.

d. Profile Requirements.

	Availability Level of Concern		
Requirements	**Low**	**Medium**	**High**
Backup and Restoration of Data	BRD-1	BRD-2	BRD-3

	Integrity Level of Concern		
Requirements	**Low**	**Medium**	**High**
Backup and Restoration of Data	BRD-1	BRD-2	BRD-3

5. CHANGES TO DATA (CD). The control of changes to data includes deterring, detecting, and reporting successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized changes are allowed.

a. CD-1 Requirement.

Change Procedures. Procedures and technical system features to ensure that changes to the data are executed only by authorized personnel or processes must be documented.

b. CD-2 Requirements. In addition to those requirements stated in CD-1, CD-2 includes the following requirement.

CANCELED

CANCELED

Transaction Log. A transaction log, protected from unauthorized changes, must be available to allow immediate correction of unauthorized data changes and off-line verification of all changes at all times.

c. Profile Requirements.

	Integrity Level of Concern		
Requirements	Low	Medium	High
Changes to Data	CD-1	CD-1	CD-2

6. COMMUNICATIONS (COM). Information protection is required whenever classified information is to be transmitted, carried to, or carried through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).

a. COM-1 Requirements.

Protections. One or more of the following protections must be used:

(a) information distributed only within an area approved for open storage of the information,

(b) National Security Agency (NSA)-approved encryption mechanisms appropriate for the encryption of classified information,

(c) Protected Transmission System, and

(d) trusted courier.

b. COM-2 Requirements. In addition to those requirements stated in COM-1, COM-2 includes the following requirements.

(1) Public Switched Networks. Any classified system connected to a public switched network (e.g., Internet) or an internal network that is not accredited at the same level must use a controlled interface that meets the requirements in Chapter VIII and performs the following.

(a) Review Before Release. Unclassified communication from the inside must be reviewed for classification before being released.

(b) Encryption of Message Body. The body of classified communications from the inside must be encrypted with NSA-approved encryption mechanisms appropriate for the classification of the information for encryption of stored data.

(c) Notification of Recipient. Communication from the outside must have an inside sponsor (i.e., the controlled interface will notify the sponsor of the communication and release the communication on notification from the sponsor).

(d) Review of Outside Communications. Communication from the outside must be reviewed for viruses and other malicious code.

(e) End-to-End Integrity. Integrity attributes adequate to ensure the end-to-end integrity of transmitted information (including labels and security parameters) must be included with all information transmitted externally to a system or network.

c. Profile Requirements.

	Confidentiality Protection Level					
Requirements	**1**	**2**	**3**	**4**	**5**	**6**
Communications	COM-1	COM-1	COM-1	COM-2	COM-1	COM-1

NOTE: DOE will not approve the connection of Protection Level 5 or Protection Level 6 systems to Public Switched Networks.

Requirements	**Integrity Level of Concern**		
	Low	**Medium**	**High**
Communications	COM-1	COM-1	COM-2

7. CONFIGURATION MANAGEMENT. Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

a. CM-1 Requirements.

(1) Configuration Documentation. Procedures must be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security-relevant software product names and version or release numbers, and physical location.

CANCELED

(2) System Connectivity. Procedures must be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.

(3) Review of Security-Relevant Changes. All modifications to security-relevant resources (including software, firmware, hardware, or interfaces and inter-connections to networks) must be reviewed and approved in accordance with procedures prior to implementation. All security-relevant modifications must be subject to the provisions of the system configuration management program. The ISSM must notify the DAA of requests for changes to the resources that deviate from the requirements of the approved ISSP. The DAA must consider the system for reaccreditation.

b. CM-2 Requirements. In addition to those requirements stated in CM-1, CM-2 includes the following requirements.

(1) Connection Sensitivity. The sensitivity level of each connection or port controlled by the SSS must be documented.

(2) CM Plan. The CM plan must be documented and must include–

(a) formal change control procedures for security-relevant hardware and software;

(b) procedures for management of all documentation, such as the ISSP and security test plans, used to ensure system security; and

(c) workable processes to implement, periodically test, and verify the CM plan.

c. CM-3 Requirements. In addition to those requirements stated in CM-2, CM-3 includes the following requirements.

(1) CM Plan. In addition to the requirements of the CM plan in CM-2, the CM plan must include–

(a) a CM control board that implements procedures to ensure the security review and approval of changes that affect the SSS and

(b) a verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

d. Profile Requirements.

CANCELED

	Confidentiality Protection Level					
Requirements	**1**	**2**	**3**	**4**	**5**	**6**
Configuration Management	CM-1	CM-1	CM-2	CM-3	CM-3	CM-3

	Integrity Level of Concern		
Requirements	**Low**	**Medium**	**High**
Configuration Management	CM-1	CM-2	CM-3

8. DISASTER RECOVERY PLANNING (DRP).

a. DRP-1 Requirements.

(1) Mission Essential. The system's mission-essential applications must be identified.

(2) Plan Decision. The manager or supervisor directly responsible for the system must determine the need for continuity of operations or develop a contingency plan for each information system. This decision must be documented and signed by the manager or supervisor. A statement of the decision and the basis for that decision must be documented in the ISSP. If a continuity of operations plan or contingency plan is not needed, the ISSP must so state.

(3) Procedures. Documented procedures for the backup of all essential information, software, and documentation must be implemented on a regular basis. The backup procedures must be attached to or referenced in an attachment to the ISSP. The frequency of backups must be defined by the ISSO, with the assistance of the data custodian(s), and documented in the backup procedures.

(4) Plan Elements. The elements of a disaster recovery plan defined in MA-365, "Disaster Recovery Program Guideline," dated July 1991, must be addressed in the plan(s).

b. DRP-2 Requirements. In addition to those requirements stated in DRP-1, DRP-2 includes the following requirement.

Verification of Procedures. Backup procedures must be verified periodically by confirming that the date of last backup is consistent with the backup procedures. The frequency of verification must be defined by the ISSO, with the assistance of the data custodian(s), and documented in the backup procedures.

CANCELED

c. DRP-3 Requirements. In addition to those requirements stated in DRP-2, DRP-3 includes the following requirement.

Testing of the Disaster Recovery Program. A testing plan must be developed that addresses the criteria for evaluating the test results and the schedule for performing the tests.

d. Profile Requirements.

	Availability Level of Concern		
Requirements	**Low**	**Medium**	**High**
Disaster Recovery Planning	DRP-1	DRP-2	DRP-3

9. INDEPENDENT VALIDATION AND VERIFICATION (IVV).

a. IVV-1 Requirements.

(1) IV&V Team. An IV&V team, in coordination with the ISSM, must–

(a) assist in the design phase of the system,

(b) assist in determining and developing the certification test requirements,

(c) assist in the certification testing, and

(d) evaluate the security of the implemented system.

(2) IV&V Request. The ISSM must forward the request for an IV&V team through the DAA to the ISPM. The request must identify funding sources for the IV&V team.

b. IVV-2 Requirements. In addition to those requirements stated in IVV-1, IVV-2 includes the following requirement.

Annual Evaluation. On an annual basis, the IV&V team must evaluate the security of the implemented system.

c. Profile Requirements.

	Confidentiality Protection Level					
Requirements	**1**	**2**	**3**	**4**	**5**	**6**
Independent Validation and Verification				IVV-1	IVV-1	IVV-2

CANCELED

10. RESOURCE ACCESS CONTROLS (RAC). Information systems must store and preserve the integrity of the sensitivity of all information internal to the information system.

a. RAC-1 Requirements. Discretionary access controls must be provided.

b. RAC-2 Requirements. In addition to those requirements stated in RAC-1, RAC-2 includes the following requirements.

(1) Security Labels. The information system must place electronic security labels on all entities (e.g., files) reflecting the sensitivity (classification level, classification category, and handling caveats) of the information for resources and the authorizations (access authorizations, need-to-know, formal access approvals) for users. These labels must be an integral part of the electronic data or media and must be compared to the user or resource profile and validated before a user or resource is granted access to the entity.

(2) Export of Security Labels. Security labels exported from the information system must accurately represent the corresponding security labels on the information in the originating information system.

(3) Security Label Integrity. The information system must ensure the following:

(a) integrity of the security labels,

(b) association of a security label with the transmitted data, and

(c) enforcement of the control features of the security labels.

c. RAC-3 Requirements. In addition to those requirements stated in RAC-2, RAC-3 includes the following requirements.

(1) Device Labels. The information system must ensure that the originating and destination device labels are a part of each message header and that they enforce the control features of the data flow between originator and destination.

(2) Mandatory Access Controls. Mandatory access controls must be provided.

d. Profile Requirements.

	Confidentiality Protection Level					
Requirements	**1**	**2**	**3**	**4**	**5**	**6**
Resource Access Controls		RAC-1	RAC-2	RAC-3	RAC-3	RAC-3

CANCELED

11. RESOURCE UTILIZATION (RU).

a. RU-1 Requirement.

Resource Reallocation. The system must ensure that resources contain no residual data before being assigned, allocated, or reallocated.

b. RU-2 Requirement. In addition to those requirements stated in RU-1, RU-2 includes the following requirement.

Resource Allocation. The SSS must provide the capability to control a defined set of system resources (e.g., memory, disk space) such that no one user can deny another user access to the resources.

c. Profile Requirements.

	Confidentiality Protection Level					
Requirements	**1**	**2**	**3**	**4**	**5**	**6**
Resource Utilization		RU-1	RU-2	RU-2	RU-2	RU-2

12. SESSION CONTROLS (SC). Session controls are requirements, over and above identification and authentication, for controlling the establishment of a user's session.

a. SC-1 Requirements.

(1) User Notification. All authorized information system users must be notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit. The user must also be advised that, by using the system, he/she has granted consent to such monitoring and recording. The user must also be advised that unauthorized use is prohibited and subject to criminal and civil penalties. If the operating system permits, each initial screen (displayed before user logon) must contain a warning text to the user, who must be required to take positive action to remove the notice from the screen (monitoring and recording, such as collection *and* analysis of audit trail information, must be performed).

The following is a suggested warning text to the user.

> 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 system is prohibited and could subject the user to criminal and civil penalties.

CANCELED

If an “initial screen” warning notice cannot be provided, other methods of notification must be developed and submitted for DAA approval.

(2) Successive Logon Attempts. If the operating system provides the capability, successive logon attempts must be controlled as follows:

(a) by denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same user ID;

(b) by limiting the number of access attempts in a specified time period,

(c) by use of a time-delay control system, and

(d) by other such methods, subject to approval by the DAA.

(3) System Entry. The system must grant entry only in accordance with the conditions associated with the authenticated user’s profile. If no explicit entry conditions are defined, the default must prohibit all remote activities, such as remote logons and anonymous file access.

b. SC-2 Requirements. In addition to those requirements stated in SC-1, SC-2 includes the following requirements.

(1) Multiple Logon Control. If the information system supports multiple logon sessions for each user ID or account, the information system must provide a protected capability to control the number of logon sessions for each user ID, account, or specific port of entry. The information system default must be a single logon session.

(2) User Inactivity. The information system must detect an interval of user inactivity, such as no keyboard entries, and must disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements must be documented.

(3) Logon Notification. If the operating system provides the capability, the user must 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.

CANCELED

This notice must require positive action by the user to remove the notice from the screen.

c. SC-3 Requirement. In addition to those requirements stated in SC-2, SC-3 includes the following requirement, which must include security level changes.

Security Level Changes. The information system must immediately notify the user of each change in the security level or compartment associated with that user during an interactive session. A user must be able to query the information system as desired for a display of the user's complete sensitivity label.

d. Profile Requirements.

Requirements	Confidentiality Protection Level					
	1	**2**	**3**	**4**	**5**	**6**
Session Controls	SC-1	SC-2	SC-2	SC-3	SC-3	SC-3

13. SECURITY DOCUMENTATION (SD). Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The Classified Information Systems Security Plan (ISSP) is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The ISSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The ISSP also serves as the basis for inspections of the system. Information common to several systems at a site or information contained in other documents may be attached to or referenced in the ISSP.

a. SD-1 Requirements.

(1) ISSP. The ISSP must contain the following.

(a) System Identification.

1 Security Personnel. The name, location, and phone number of the system owner, DAA, ISSM, and ISSO.

2 Description. A brief narrative description of the system or network mission or purpose and architecture, including subnetworks, communications devices, and protocols.

(b) System Requirements Specification.

CANCELED

1 Sensitivity or Classification Levels of Information. The sensitivity or classification levels and categories of all information on the system.

2 Levels of Concern for Confidentiality, Integrity, and Availability. The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern.

3 Variances from the Protection Profile Requirements. A description of any approved variances from the protection profile. A copy of the approval documentation must be attached to the ISSP.

(c) System-Specific Risks and Vulnerabilities. A description of the risk assessment of any threats or vulnerabilities unique to the system. If no threats or vulnerabilities unique to the site or system exist, the description must so state. If any vulnerabilities are identified by the assessment of unique threats, the countermeasures implemented to mitigate the vulnerabilities must be described.

(d) System Configuration. A brief description of the system architecture, including a block diagram of the components that show the interconnections between the components and any connections to other systems.

(e) Connections to Separately Accredited Networks and Systems. If connections to other systems exist, a memorandum of understanding is necessary if the systems are approved by a person other than the DAA responsible for this system. A copy of any memoranda of understanding with other agencies must be attached to the ISSP.

(f) Security Support Structure. An overview of the SSS including all controlled interfaces, their interconnection criteria, and security requirements.

(g) System Implementation of Requirements. A brief description of how the system implements each of the baseline and protection requirements.

(h) Compliance Statements. Statements of compliance that TEMPEST, Protected Transmission System (PTS), Technical Surveillance Countermeasures (TSCM), and other security requirements have been met.

b. SD-2 Requirement. In addition to those requirements stated in SD-1, SD-2 includes the following requirement.

IV&V Report. A report from the IV&V team.

CANCELED

c. Profile Requirements.

Requirements	Confidentiality Protection Level					
	1	2	3	4	5	6
Security Documentation	SD-1	SD-1	SD-1	SD-2	SD-2	SD-2

14. SEPARATION OF FUNCTIONS (SF).

a. SF-1 Requirement.

Separation of Functions. The functions of the ISSO and the system manager must not be performed by the same person.

b. Profile Requirements.

Requirements	Confidentiality Protection Level					
	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Separation of Functions			SF-1	SF-1	SF-1	SF-1

15. SYSTEM RECOVERY (SR). System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition in which all security-relevant functions are operational or system operation is suspended.

a. SR-1 Requirement.

Controlled Recovery. Procedures and information system features must be implemented to ensure that information system recovery is controlled. If any off-normal conditions arise during recovery, the information system must be accessible only via terminals monitored by the ISSO or his/her designee, or via the information system console.

b. SR-2 Requirement.

Trusted Recovery. Procedures and technical system features must be implemented to ensure that system recovery occurs in a trusted and secure manner. Procedures to mitigate all information system recovery circumstances where the restoration of protection features cannot be ensured must be implemented and documented.

CANCELED

c. Profile Requirements.

Requirements	Confidentiality Protection Level					
	1	2	3	4	5	6
System Recovery	SR-1	SR-1	SR-1	SR-2	SR-2	SR-2

16. SECURITY SUPPORT STRUCTURE (SSS). The SSS consists of those components of a system (hardware, software, firmware, and communications) essential to maintaining the security policy(ies) of the system.

a. SSS-1 Requirement.

Access to Protection Functions. Access to hardware, software, and firmware that perform systems or security functions must be limited to authorized personnel.

b. SSS-2 Requirements. In addition to those requirements stated in SSS-1, SSS-2 includes the following requirements.

(1) SSS Protection Documentation. The protections and provisions, including identification of all controlled interfaces, their interconnection criteria, and security requirements, of the SSS must be documented.

(2) Informal Description of Policy Model. An informal description of the security policy model enforced by the SSS must be documented.

(3) Periodic Validation of SSS. Procedures must exist to periodically validate correct operation of the hardware, firmware, and software elements of the SSS.

c. SSS-3 Requirements. In addition to those requirements stated in SSS-2, SSS-3 includes the following requirements.

(1) SSS Isolation. The SSS must maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modifying its code and data structures).

(2) Policy Description. A description of the security policy model enforced by the SSS must be documented with an explanation that shows it is sufficient to enforce the security policy. All interfaces to the SSS must be included in the explanation.

d. Profile Requirements.

CANCELED

	Confidentiality Protection Level					
Requirements	**1**	**2**	**3**	**4**	**5**	**6**
Security Support Structure	SSS-1	SSS-1	SSS-2	SSS-2	SSS-3	SSS-3

	Integrity Level of Concern		
Requirements	**Low**	**Medium**	**High**
Security Support Structure	SSS-1	SSS-2	SSS-3

	Availability Level of Concern		
Requirements	**Low**	**Medium**	**High**
Security Support Structure	SSS-1	SSS-2	SSS-3

CANCELED

17. SECURITY TESTING (ST). Certification and ongoing security testing are used to verify correct operation of a system's protection measures.

a. ST-1 Requirements.

(1) Certification Testing. Certification testing must include security function verification tests, tests to verify that the security functions do not have any undesired effect(s) on the information system, tests to verify that the security functions perform correctly when activated with abnormal input values, and documentation of the test results.

(2) Ongoing Testing. Ongoing security performance testing must be conducted regularly to ensure that the system's security features continue to function correctly. The ongoing security performance tests may include all or parts of the security function verification and certification tests. The methods for determining that these features continue to be implemented during the life cycle of the information system (e.g., after system updates) must be documented.

c. ST-2 Requirements. In addition to those requirements stated in ST-1, ST-2 includes the following requirements.

Certification Test Reporting. Certification testing provides assurance that the information system is operating in accordance with the approved ISSP. The certification test results, when satisfactory, provide the DAA with supporting documentation for the accreditation of the information system.

(a) Certification Test Plans. The certification test plan must confirm that the information system has been implemented and is operating in accordance with the ISSP. If the security features of the information system, as specified in the ISSP, are expected to restrict user access, for example, these features must be tested to ensure that they are implementing the specified security requirements.

(b) Documentation. The results of certification tests and an analysis of the results must be documented.

d. ST-3 Requirements. In addition to those requirements stated in ST-2, ST-3 includes the following requirements.

(1) Penetration Testing. Ongoing periodic penetration testing must be performed to identify major or obvious vulnerabilities in the system. The test methodology and procedures must be described in a security test plan. The ongoing penetration tests may include all or parts of the security function verification tests.

(2) Independent Validation and Verification. An IV&V team must assist in the certification testing of an information system and must perform validation testing of the system as required by the DAA.

e. Profile Requirements.

	Confidentiality Protection Level					
Requirements	**1**	**2**	**3**	**4**	**5**	**6**
Security Testing	ST-1	ST-2	ST-2	ST-3	ST-3	ST-3

	Integrity Level of Concern		
Requirements	**Low**	**Medium**	**High**
Security Testing	ST-1	ST-2	ST-3

18. TRUSTED PATH (TP). Users often need to perform functions, such as authentication, through direct interaction with the SSS. A trusted path ensures that the user is communicating directly with the SSS. Trusted path exchanges may be initiated by a user or the SSS. A user response via the trusted path guarantees that untrusted processes cannot intercept or modify the user’s response.

CANCELED

a. TP-1 Requirements.

Authentication Path. The information system must support a trusted path between itself and the user for initial identification and authentication.

b. Profile Requirements.

Requirements	**Confidentiality Protection Level**					
	1	**2**	**3**	**4**	**5**	**6**
Trusted Path					TP-1	TP-1

CANCELED

CHAPTER VIII

REQUIREMENTS FOR INTERCONNECTED SYSTEMS

CANCELED

1. INTERCONNECTED SYSTEMS MANAGEMENT. The characteristics and capabilities of classified information systems implemented as networks require special protection considerations. This chapter *imposes additional requirements* on a network or expands on the protection requirements stated in Chapters VI and VII as they apply to a network.

   a. When connecting two or more networks, the DAA(s) must review the security attributes of each network (even if the networks are accredited at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.

   b. A *unified* network is a connected collection of systems or networks that are accredited *(1) under a single ISSP, (2) as a single entity, and (3) by a single DAA.* Such a network can be as simple as a small stand-alone LAN operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single ISSO. Conversely, it can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy, accredited as a single entity by a single DAA. The perimeter of each network encompasses all its hardware, software, and attached devices. Its boundary extends to all of its users.

   c. An *interconnected* network is comprised of *two or more separately accredited systems and/or networks.* Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating system or network has its own ISSO. The interconnected network must have an SSS capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires accreditation as a unit.

   d. Systems that process information at differing classification levels or with differing compartmentation (i.e., at least two kinds of information that require different formal access approvals) can be interconnected if–

      (1) they are interconnected through a controlled interface (as defined below) that provides the separation appropriate to the combination of the level(s) and compartment(s) being processed on both systems;

      (2) both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or

(3) both systems are accredited to process the level(s) and compartment(s) of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.

e. Any classified information system connected to another system that does not meet either Paragraph 1d(2) or 1d(3) above must use a controlled interface(s) that performs the following.

(1) A communication of lower classification level from within the system perimeter must be reviewed for classification before being released.

(2) A classified communication from within the system perimeter must have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

(3) Communications from outside the system perimeter must have an authorized user as the addressee (i.e., the controlled interface must notify the user of the communication and release the communication only on request from the user). If classified information exists in the communication, it must be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

2. CONTROLLED INTERFACE FUNCTIONS.

a. The functions of the controlled interface include–

(1) providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts;

(2) providing a reliable exchange of security-related information; and

(3) filtering information in a data stream based on associated security labels for data content.

b. Controlled interfaces have several characteristics including the following.

(1) There are *no general users* on the controlled interface

(2) There is *no user code* running on the controlled interface.

(3) The controlled interface provides a protected conduit for the transfer of user data.

(4) Communications from outside the perimeter of the system must be reviewed for viruses and other malicious code.

3. CONTROLLED INTERFACE REQUIREMENTS. The controlled interface must have the following properties.

CANCELED

a. Adjudicated Differences. The controlled interface must be implemented to monitor and enforce the network protection requirements and to adjudicate the differences in security policies.

b. Routing Decisions. The controlled interface must base its routing decisions on information that is supplied or alterable only by the SSS.

c. Restrictive Protection Requirements. The controlled interface must support the protection requirements of the most restrictive of the attached networks or information systems.

d. User Code. The controlled interface must not run any user code.

e. Fail-secure. The controlled interface must be implemented so that all possible failures must result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.

f. Communication Limits. The controlled interface must ensure that communication policies and connections that are not explicitly permitted are prohibited.

g. Technical Protection Requirements. The technical protection requirements for Protection Level 3 are usually adequate for the platform on which the controlled interface is operating. In general, such systems have only privileged users; that is, system administrators and maintainers. The controlled interface may have a large number of clients; that is, individuals who use the controlled interface's functional capabilities in a severely constrained way. The controlled interface application itself must provide the more stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the controlled interface if each application (and the resources associated with it) is protected from unauthorized access or circumvention from other applications or users.

4. ASSURANCES FOR CONTROLLED INTERFACES. Each controlled interface must be tested and evaluated to ensure that the controlled interface, as implemented, can provide the separation required for the system's protection level. Specifically, the platform on which the controlled interface runs does not necessarily have to provide the needed separation alone.

CANCELED

CONTRACTOR REQUIREMENTS DOCUMENT

CANCELED

1. Purpose. This Contractor Requirements Document (CRD) is issued to aid procurement request initiators in identifying Classified Information Systems Security Program requirements that must be incorporated into contracts by contracting officers. All contractor responsibilities must be accomplished in compliance with DOE M 471.2-2, CLASSIFIED INFORMATION SYSTEMS SECURITY MANUAL.

2. Management Structure. The contractor must assign individuals to serve as Classified Information Systems Security Site Managers (ISSMs) and Classified Information Systems Security Officer(s) (ISSOs).

3. Classified Information Systems Security Site Manager (ISSM). The ISSM is responsible for implementing the Classified Information Systems Security Program at the site. A separate ISSM may be appointed for information systems in a Sensitive Compartmented Information Facility (SCIF) if the site determines that another ISSM is needed. In this capacity, the ISSM also functions as the site point of contact for all classified information systems security issues. The ISSM carries out the following responsibilities.

   a. Ensures the development, documentation, and presentation of information systems security education, awareness, and training activities for site management, information security personnel, data custodians, and users. This training and awareness program must include, but is not limited to, various combinations of classes (both self-paced and formal), security education bulletins, training films, computer-aided instruction, security briefings, and related educational aids.

   b. Ensures the development, documentation, and presentation of information systems security training for escorts in information systems operational areas.

   c. Establishes, documents, implements, and monitors the Classified Information Systems Security Program for the site and ensures site compliance with DOE requirements for information systems. These include the baseline protection requirements common to all systems, which are detailed in DOE M 471.2-2, Chapter VI.

   d. Ensures the development of procedures for use in the site Classified Information Systems Security Program.

   e. Identifies and documents unique threats to information systems at the site.

   f. Ensures that the site's Classified Information Systems Security Program is coordinated with the Site Safeguards and Security Plan or the Site Security Plan (see DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM, Chapter I).

   g. Coordinates the following:

(1) implementation of the site Classified Information Systems Security Program with the other site programs, as appropriate, such as Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, and Materials Control and Accountability;

(2) development of a site self-assessment program for the Classified Information Systems Security Program; and

(3) self-assessment of the site's Classified Information Systems Security Program, which is to be performed between operations office surveys.

h. Ensures the development of site procedures to–

(1) govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information;

(2) ensure that vendor-supplied authentication features (e.g., passwords, account names) or security-relevant features are properly implemented;

(3) report classified information systems security incidents;

(4) require that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for the security of classified information systems and classified information;

(5) detect malicious code, viruses, and intruders (hackers); and

(6) review and approve Classified Information Systems Security Plans (ISSPs), certification test plans, and certification test results.

i. Determines, using guidance from the data custodian(s), the appropriate levels of concern for confidentiality, integrity, and availability for each information system that processes classified information.

j. Certifies to the Designated Approving Authority (DAA), in writing, that each ISSP has been implemented, that the specified protection measures are in place and properly tested, and that the classified information system is functioning as described in the ISSP.

k. Recommends to the DAA, in writing, approval or disapproval of the ISSP test results and the certification statement.

l. Ensures that the DAA is notified when a system no longer processes classified information, or when changes occur that might affect accreditation.

m. Participates in information systems security training sponsored by the Classified Information Systems Security Program Manager (ISPM) within 1 year of his/her appointment.

n. Ensures that personnel are trained on the information system's prescribed security restrictions and safeguards before they are initially allowed to access a system.

4. <u>Classified Information Systems Security Officer (ISSO)</u>.

CANCELED

a. Ensures implementation of security measures for each classified information system for which he/she is responsible.

b. Identifies and documents any unique threats to classified information systems for which he/she is the ISSO and forwards them to the ISSM.

c. If so directed by the DAA and/or if an identified unique local threat exists, performs a risk assessment to determine if additional countermeasures beyond those identified in DOE M 471.2-2 are required.

d. Develops and implements a certification test plan for each classified information system for which he/she is the ISSO, as required by DOE M 471.2-2 and the DAA.

e. Prepares, maintains, and implements an ISSP that accurately reflects the installation of protection measures for each classified information system for which he/she is responsible.

f. Maintains the record copy of the ISSP and related documentation for each classified information system for which he/she is the ISSO.

g. Notifies the DAA (through the ISSM) when a system no longer processes classified information or when changes occur that might affect accreditation.

h. Ensures the following:

(1) that the sensitivity level of the information is determined prior to use on the classified information system and that the proper security measures are implemented to protect this information;

(2) that unauthorized personnel are not granted use of, or access to, a classified information system; and

(3) that formal access controls are implemented for each classified information system, except stand-alone personal computers and stand-alone workstations.

i. Documents any special protection requirements identified by the data custodians and the protection measures implemented to fulfill these requirements for the information contained in the classified information system.

j. Ensures that confidentiality, integrity, and availability levels of concern are determined for each classified information system for which he/she is responsible.

k. Implements site procedures to–

(1) govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information;

(2) ensure that vendor-supplied authentication features (e.g., passwords, account names) or security-relevant features are properly implemented;

(3) report classified information systems security incidents;

(4) require that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for protecting classified information systems and classified information;

CANCELED

(5) detect malicious code, viruses, and intruders (hackers); and

(6) review and approve ISSPs, certification test plans, and certification test results.

l. Ensures that users are properly trained in system security by identifying classified information systems security training needs (including system-specific training) and personnel who need to attend system security training programs.

m. Conducts ongoing security reviews and tests of classified information systems periodically to verify that security features and operating controls are functional and effective.

n. Evaluates proposed changes or additions to the classified information systems and advises the ISSM of their security relevance.

5. Classified Information Systems Application Owner/Data Custodian. Contractor personnel responsible for information systems applications and/or custody of data must accomplish the following responsibilities.

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

b. Advise the ISSO of any special protection requirements for information to be processed on the classified information system.

c. Determine and document the data and application(s) that are essential to fulfill the site mission and ensure that requirements for contingencies are determined, implemented, and tested.

d. Ensure that information is processed on a classified information system that is accredited at a level sufficient to protect the information.

e. Declare the consequences of losing information confidentiality, integrity, and availability.

6. Users of Classified Information Systems. Contractor personnel who use classified information systems must accomplish the following.

a. Comply with the Classified Information Systems Security Program requirements.

b. Be aware of and knowledgeable about their responsibilities in regard to classified information systems security.

c. Be accountable for their actions on a classified information system.

d. Ensure that any authentication mechanisms (including passwords) issued for the control of their access to classified information systems are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.

CANCELED

e. Acknowledge, in writing, their responsibilities (Code of Conduct) for protecting classified information systems and classified information.

f. Participate in training on the information system's prescribed security restrictions and safeguards before initial access to a system. As a follow-up to this initial training, participate in an ongoing security education, training, and awareness program.

7. Site Security Plan and Site Safeguards and Security Plan. The contractor must prepare a Site Security Plan or (SSP) or Site Safeguards and Security Plan (SSSP), which must include a site risk assessment and the information detailed in DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM.

8. Site Risk Assessment.

a. Site risk assessments must include the Departmentwide Classified Information Systems Security Risk Assessment developed by DOE as a baseline.

b. Site risk assessments must identify any site-specific threats and any protection technologies unique to the site.

c. Site risk assessment results must be documented and used to augment, as needed, the Classified Information Systems protection profiles to be applied to information systems at the site.

9. Protection Profiles. The contractor must develop a protection profile for the site as the first step in implementing a Classified Information Systems Security Program. The protection profile must comply with the requirements in Chapter IV of DOE M 471.2-2.

10. Certification and Accreditation. The contractor must comply with the certification and accreditation requirements of Chapter V of DOE M 471.2-2. Certification confirms that the Classified Information Systems Security Program protection measures have been implemented correctly in accordance with the protection profile. Accreditation, which is performed by the DOE DAA, grants authority to operate the Classified Information Systems Security Program.

11. Independent Validation and Verification. For information systems intended to operate in Protection Level 5 or 6, the contractor must conduct and fund an Independent Validation and Verification review.

12. Reaccreditation. The ISSO and ISSM must work with the Classified Information Systems Security Operations Manager (ISOM) to review proposed modifications to information systems to determine their effect on the system protections.

13. Incident Reporting. Contractor personnel must report to the ISOM any incidents that may affect DOE or national interests. (Incidents may be reported via telephone or other electronic means.)

CANCELED

The report must include at least the location of the incident, possible effect on DOE or national interests, a description of the incident, and a description of the actions that were taken to protect information after the incident was discovered. All individual(s) collecting information about or reporting an incident must ensure that any sensitive or classified information involved in the incident or report is properly protected. All information reported must comply with DOE M 471.2-2.

14. Self-Assessments. The ISSM must ensure that periodic self-assessments of the site's program are performed. Upon completion of each review, the ISSM must ensure that a corrective action plan is prepared and implemented for all findings or vulnerabilities as directed by DOE O 470.1, Chapter IX, Paragraph 10a. A record of each review and the subsequent corrective action plan must be retained and made available during future surveys and inspections.

15. Graded Requirements. The ISSM must ensure that the Classified Information Systems Security Program is implemented according to the graded requirements direction in Chapter VII of DOE M 471.2-2.

16. Interconnected Systems. The ISSM must implement the additional requirements in Chapter VIII of DOE M 471.2-2 for classified information systems implemented as networks.

CANCELED

CANCELED

ATTACHMENT 2

DEFINITIONS

ACCREDITATION. The formal acknowledgment (written or electronic) of the designated approval authority's decision to authorize an information system to process, store, transfer, or provide access to classified information in a specific information system's security environment established by a specific Classified Information Systems Security Plan (ISSP).

AVAILABILITY. The attribute of information being in the place, at the time, and in the form needed by the user. Denotes the goal of ensuring that information and information processing resources both remain readily accessible to their authorized users.

BOUNDARY. The conceptual limit of an information system that extends to all directly and indirectly connected users who receive output from the system without a reliable human review by an appropriately authorized or cleared authority.

CLASSIFIED INFORMATION SYSTEMS SECURITY OFFICER (ISSO). The person responsible for ensuring that protection measures are installed and operational security is maintained for one or more specific classified information system(s).

CLASSIFIED INFORMATION SYSTEMS SECURITY OPERATIONS MANAGER (ISOM). A DOE employee who is the technical expert responsible to the Designated Approval Authority (DAA) for ensuring that security is provided for and implemented throughout the life cycle of a classified information system.

CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISPM). The DOE employee appointed by the Director of the Office of Safeguards and Security to be responsible for the development of DOE policies, standards, guidelines, and procedures for the protection of classified information in information systems.

CLASSIFIED INFORMATION SYSTEMS SECURITY SITE MANGER (ISSM). The manager responsible for a site Classified Information Systems Security Program.

CLEARING. Removal of data from an information system or media, performed so that the data may not be reconstructed using normal system capabilities (i.e., through the keyboard). NOTE: Clearing of classified information from media does not permit the reuse of the media at a lower classification level or in an unclassified mode.

CONFIDENTIALITY. The critical information attribute of being inaccessible except to persons or processes that have an authorization and a legitimate need to know that information.

DATA CUSTODIAN. The person responsible for having information reviewed for sensitivity and classification. This person is responsible for its generation, management, and destruction.

DESIGNATED APPROVING AUTHORITY (DAA). The official with the authority to formally grant approval for operating a classified information system; the person who determines the acceptability of the residual risk in a system that is prepared to process classified information and either accredits or denies operation of the system.

INFORMATION SYSTEM. As defined in *National Security Telecommunications and Information Systems Security (NSTISSC) 4009, National Information Systems Security (INFOSEC) Glossary*, dated 5 June 1992, "any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware." NOTE: Communications Security (COMSEC) and Technical Surveillance Countermeasures (TSCM) requirements are contained in other directives.

INTEGRITY. The information attribute of being a true, complete representation of its original content, even when undergoing changes in form or storage medium.

LEVELS OF CONCERN. An expression of the consequences of loss of the information's integrity, availability, or confidentiality.

PERIMETER. All those components of the information system that are to be accredited. NOTE: As a rule, separately accredited components are not included within the perimeter, but those components are within the boundary.

PRESUMPTIVE NEED TO KNOW. A "need to know" by reason of association or assignment to the area in which the data is exposed (e.g., for a janitor, guard, etc).

PROTECTION LEVEL. The protection level for confidentiality as determined by the relationship between two sets of facts: first, the access authorizations, formal access approval(s), and need-to-know of users; and second, the level of concern for confidentiality for the system. Protection level indicates an implicit level of trust placed in the system's technical capabilities.

RESIDUAL RISK. The remaining risk of operating a classified information system after application of mitigating factors. NOTE: Such mitigating factors often include, but are not limited to–

- minimizing initial risk by selecting a system known to have fewer vulnerabilities,

- reducing vulnerabilities by implementing countermeasures,

- reducing consequence by limiting the amounts and kinds of information on the system, and

- using classification and compartmentation to lessen the threat by limiting the adversaries' knowledge of the system.

CANCELED

SANITIZATION. The removal of information from media or equipment such that data recovery using any known technique or analysis is prevented. NOTE: Sanitization must include the removal of data from the media or equipment, as well as the removal of all sensitivity or classified labels, markings, and activity logs.

SITE MANAGER. The person responsible for management of all activities at a site.

USER. An individual who can receive information from, input information to, or modify information on an information system without an independent human review. In a processing context, this also includes a process acting on behalf of a user.

Direct User. A user with physical or electronic access to any component of the information system.

Indirect User. A user with access to information from the information system without an independent human review, but who does not have physical or electronic access to the system itself.

Privileged User. A user with access to control, monitoring, or administration functions of the information system (e.g., system administrator, system security officer, maintainers, system programmers, etc.). NOTE: It is often convenient to refer to a user who is **NOT** a privileged user as a general user.

CANCELED