JOINT
AIR FORCE - ARMY – NAVY

JAFAN 6/3

Manual

Protecting Special Access Program Information Within Information Systems

15 October 2004

FOREWORD

This Manual is promulgated pursuant to authorities and responsibilities assigned to the Deputy Secretary of Defense (DEPSECDEF) for the protection of Department of Defense (DoD) Special Access Programs (SAPs). These DEPSECDEF authorities and responsibilities may be found in the National Security Act of 1947, as amended; in Executive Order 12958, as amended; in the Code of Federal Regulations, 32CFR2103 (per Information Security Oversight Office Directive No. 1); and in other applicable laws and orders.

The Director of Central Intelligence Directive (DCID) 6/3 was used as the model publication from which this Manual was crafted. The subject matter and order of presentation closely resemble DCID 6/3. No specific security measure contained in this Manual exceeds the requirements for standards supporting Sensitive Compartmented Information (SCI). This Manual provides enhanced security measures exceeding those normally required by DoD 5200.1-R, "Information Security Program", for information at the same classification level in accordance with the delegated DoD military department authorities granted to protect authorized SAP activities.

The provisions of this Manual are applicable to all government and contractor personnel participating in the administration of DoD SAPs. In cases of doubt over the requirements of this Manual, users should consult the Program Security Officer prior to taking any action. In cases of extreme emergency requiring immediate attention, the action taken should protect the Government's interest and the security of the program from compromise.

This Manual is effective upon publication and will be implemented as outlined in the next paragraph. Appropriate implementation instructions will be specified in contractual documents. Documentation requirements to complete the certification and accreditation (C&A) process are addressed in this manual and may also be specified in contractual documents.

New systems will be accredited in accordance with this Manual. Legacy systems operating with a final Approval to Operate (ATO) issued in accordance with requirements listed in the DoD Overprint to the National Industrial Security Program Operating Manual Supplement need not be re-accredited in accordance with this Manual until expiration of the existing ATO. If an expiration date was not specified, these systems must comply with requirements outlined in this manual three years from the date of the approval memorandum or letter. Changes to legacy systems affecting the security posture, mode of operation or Protection Level will require accreditation in accordance with this manual.

This Manual is intended to be a living document. Users are encouraged to submit change recommendations to service component SAPCOs via their Program Security Officers. In addition, the implementation of requirements having documented major cost impact to programs or those identified as "A/R" in Table D.1 of this Manual will be coordinated with the appropriate PAA.

JOHN B. HENNESSEY
Director, Security and Special Program Oversight

USAF

MICHAEL KOBBE 14 Oct 04
Director, Technology Management Office (TMO)

USA

10/12/04
JOHN E. PIC
Director, Special Programs Office (CNO(N7SP))

USN

TABLE OF CONTENTS

PREFACE

1. This Manual establishes the security policy and procedures for storing, processing, and communicating classified DoD SAP information in information systems (ISs). An information system is 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 (digital or analog); it includes software, firmware, and hardware.
2. DoD SAP information constitutes an asset vital to the effective performance of our national security roles. It is essential that this information be properly managed, and that its confidentiality, integrity, and availability be ensured. Therefore, this policy and its implementation manual:
    a. Provide policy and procedures for the security and protection of systems that create, process, store, and transmit SAP information.
    b. Provide administrative and system security requirements, including those for interconnected systems.
    c. Define and mandate the use of a risk management process.
    d. Define and mandate the use of a certification and accreditation process.
    e. Promote the use of efficient procedures and cost-effective, computer-based security features and assurances.
    f. Describe the roles and responsibilities of the individuals who constitute the decision-making segment of the IS security community and its system users.
    g. Require a life-cycle management approach to implementing system security requirements. Introduce the concepts Levels-of-Concern and Protection Level of information.
3. SAP information shall be appropriately safeguarded at all times, including when used in information systems. The information systems shall be protected. Safeguards shall be applied such that (1) individuals are held accountable for their actions; (2) information is accessed only by authorized individuals* and processes; (3) information is used only for its authorized purpose(s); (4) information retains its content integrity; (5) information is available to satisfy mission requirements; and (6) information is appropriately marked and labeled.

[*Authorized individuals are those with the appropriate clearance, formal access approvals, and need-to-know.]

4. Appropriate security measures shall be implemented to ensure the confidentiality, integrity, and availability of that information. The mix of security safeguards selected for systems that process SAP information shall ensure that the system meets the policy requirements set forth in this Manual.
    a. Information systems security shall be an integral part of all system life-cycle phases for all systems.

b. The security of systems shall be reviewed whenever changes occur to missions, information systems, security requirements, or threat, and whenever there are significant adverse changes to system vulnerabilities.

c. Appropriate authorities, as defined in the Manual, shall be immediately notified of any threats or vulnerabilities impacting systems that process their data.

d. All ISs are subject to monitoring consistent with applicable laws and regulations, and as provided for by agency policies, procedures, and practices. As a minimum, monitoring will assess the adequacy of the confidentiality, integrity, and availability controls.

5. All systems shall be certified and accredited in compliance with the requirements stated in this Manual and following the direction and guidance provided in the Designated Accrediting Authority (DAA) approved certification and accreditation (C&A) process. C&A is a comprehensive process to ensure implementation of security measures that effectively counter relevant threats and vulnerabilities. C&A consists of several iterative, interdependent phases and steps whose scope and specific activities vary with the IS being certified and accredited.

   a. A risk assessment shall be performed for each IS to identify specific areas that require safeguards against deliberate or inadvertent unauthorized disclosure, modification, or destruction of information; denial of service; and unauthorized use of the IS. Countermeasures shall be applied in those areas to eliminate or adequately reduce the identified risk. The risk assessment shall be based on this Manual, input from the organization's counterintelligence (CI) component, the organization's mission requirements, the classification and sensitivity of the information, and a balanced, cost-effective application of security disciplines and technologies. These security disciplines include, but are not limited to, information systems security, operations and administrative security, personnel security, physical security, and communications security.

   b. Systems shall be reviewed for compliance with this Manual and the security documents derived therefrom.

6. Principal Accrediting Authorities (PAAs) for SAPs of the Military Departments.

   a. The PAA with responsibility for all Department of the Air Force Special Access Programs is the Director, Security and Special Programs Oversight, Administrative Assistant to the Secretary of the Air Force. The PAA shall accredit all Air Force SAP ISs that operate at Protection Levels 4 and 5, and all components of such systems. The PAA may delegate, in writing, to the extent the PAA considers appropriate, the authority to accredit systems operating at Protection Levels 1, 2, or 3; but the PAA retains the ultimate responsibility for the security of the information processed in those systems.

   b. The PAA with responsibility for all Department of the Navy Special Access Programs is the Director of Special Programs Office (OPNAV(N7SP)), Department of Navy. The PAA shall accredit all Navy SAP ISs that operate at Protection Levels 4 and 5, and all components of such systems. The PAA may delegate, in writing, to the extent the PAA considers appropriate, the authority to accredit systems operating at

Protection Levels 1, 2, or 3; but the PAA retains the ultimate responsibility for the security of the information processed in those systems.

c. The PAA with responsibility for all Department of the Army Special Access Programs is the US Army Technology Management Office, DACS DMP. The PAA shall accredit all Army SAP ISs that operate at Protection Levels 4 and 5, and all components of such systems. The PAA may delegate, in writing, to the extent the PAA considers appropriate, the authority to accredit systems operating at Protection Levels 1, 2, or 3; but the PAA retains the ultimate responsibility for the security of the information processed in those systems.

7. The PAA shall ensure the establishment of an information systems security incident response and reporting capability that detects incidents, establishes a trained response element, maintains statistics, initiates an investigation, and recovers operational capability for the information.

8. This Manual applies to all United States government organizations', their commercial contractors', and Allied governments' ISs that process, store, or communicate SAP information.

9. Nothing in this Manual supersedes the requirements of the Atomic Energy Act of 1954, as amended (Chapter II, Public Law 585), for the control, use, and dissemination of Restricted Data or Formerly Restricted Data.

10. Nothing in this Manual supersedes any statutory or Presidential requirement for the handling of cryptologic data or Communications Security (COMSEC) related material.

11. This Manual is effective for five years. At that time, it shall be reviewed for continued applicability.

1 INTRODUCTION

1.A Purpose and Content

This manual provides uniform policy guidance and requirements for ensuring adequate protection of all Department of Defense (DoD) Special Access Program (SAP) information that is stored or processed on an information system (IS). An information system is defined as 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 (digital or analog); it includes software, firmware, and hardware. The Secretary of Defense requires all United States Government departments and agencies, their contractors, and Allied governments processing SAP information to establish, implement, maintain, and abide by the protection measures identified in this manual.

1.A.1 This manual includes:

1.A.1.a Requirements for an Information System Security Program;

1.A.1.b Guidance on an approach to risk management for systems;

1.A.1.c Technical and administrative security requirements for a system in a given environment; and

1.A.1.d Examples of appropriate documentation.

1.A.2 This manual provides guidance to assist a Designated Accrediting Authority (DAA) or DAA Representative (described in Chapter 2) in determining the appropriate set of technical and non-technical safeguards for protecting the information in a given system.

1.A.3 This manual provides guidance to assist an Information System Security Manager (ISSM) or Information System Security Officer/Network Security Officer (ISSO/NSO) in structuring and implementing the security protections for a system.

1.B Applicability

1.B.1 This manual applies to all entities that process, store, or communicate DoD SAP information, including United States government organizations, their commercial contractors, and Allied governments.

1.B.2 The term “information system,” as defined in this manual, makes the distinction between traditional systems (e.g., computers, hosts) and networks irrelevant to the selection of protection requirements. Unless noted otherwise, the terms “system” and “information system” and “IS” are used interchangeably throughout this manual.

1.B.3 Traditionally, providing security for a system has meant protecting the confidentiality of the information on it, although for some systems protecting data integrity and system and data availability has always been a concern. While the traditional operational concern over confidentiality of classified information has not diminished, integrity and availability have become critical parts of security for all systems. The requirements in this manual reflect that understanding.

1.B.4 The operational elements of a government organization have, in the past, been concerned with and fiscally responsible for ensuring the integrity and availability of the information on the system. While this manual describes requirements for ensuring the integrity and availability of the system and of the information on it, nothing in this manual shall be construed to state or imply that there has been a transfer of fiscal responsibility to the security element(s) from the operational element(s).

1.B.5 This manual establishes the security requirements for all applicable systems. Accrediting authorities may establish additional security measures, if deemed appropriate. Any such measures shall comply with the relevant references listed in this manual.

1.C Administration

1.C.1 The DDCI/CM has designated the Community Management Staff (CMS) to act in matters pertaining to the administration of this manual for intelligence related issues.

1.C.2 The PAA shall be responsible for addressing any unresolved conflicts to this manual and the associated policy as it pertains to the individual service.

1.C.3 This manual supersedes Chapter 8 of the Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement (NISPOMSUP).

1.D Background

1.D.1 US SAP information has three attributes that require protection: confidentiality, integrity, and availability. The degree of emphasis on each varies with the type of information processed and the mission of the organization responsible for the data.

1.D.2 This manual recognizes the contributions to security made by operating environments, and allows the technical safeguards of systems to be modified accordingly. For example, while encryption can be an effective way to protect the confidentiality of information during transmission, if the information passes only through areas that are approved for open storage of the information or across a protected distribution system within an inspectable space, then encryption of the information for that purpose may be unnecessary.

1.D.3 The requirements specified in this manual are based on the assumption that the system is otherwise protected at an appropriate level for the information processed on it. These other protections include appropriate levels of physical, personnel, communications, emanations, and technical surveillance countermeasures (TSCM) security, as required in other directives.

1.E System Information Collection

The following information must be collected to determine the requirements for operating a system:

1.E.1 The category, classification, and all applicable security markings for all of the information on, or to be put on, the system;

1.E.2 The need-to-know status of the users on the system, including their formal access approval(s), clearance(s), and nationality(ies);

1.E.3 The perimeter and boundary of the system;

1.E.4 The operating environment of the system and connecting systems, including the service provided (e.g., electronic mail, Internet access), and foreign access to the system, connecting systems, and the facilities housing these systems; and

1.E.5 The technical and administrative security requirements of the system.

1.F How to Use This Manual

Eleven steps are required to accredit an IS. The following summarizes those steps and in each case refers to the relevant chapter or chapters of this manual:

1.F.1 Determine Levels-of-Concern (Chapter 3). The DAA, using formal specifications from the Data Owner, examines the information* characteristics in light of the material in Table 3.1 and determines the appropriate Level-of-Concern ratings, one each for confidentiality, integrity, and availability. The Level-of-Concern ratings for integrity and availability are each Basic, Medium, or High. Because all of the ISs covered by this manual process classified DoD SAP information, the Level-of-Concern rating for confidentiality is always High.

[*In this context, information is expressed as human-recognizable data and machine-recognizable data, in hardware, software, firmware, and, especially, data that is used to control security functions, such as router table entries.]

1.F.2 Determine Protection Level (Chapter 3). Based on the guidance provided in Chapter 3, the DAA determines a Protection Level for confidentiality for the system and also determines any threats unique to the system or the information.

1.F.3 Determine Interconnected System Requirements (Chapter 7) and Administrative Requirements (Chapter 7). The DAA determines the appropriate security requirements for interconnected systems and for the use of advanced technology specified in Chapter 7 and the administrative requirements specified in Chapter 8.

1.F.4 Identify Technical Security and Assurance Requirements (Chapters 4, 5, and 6). The applicable technical security requirements and assurances are identified. Chapter 4 presents the technical security requirements and assurances for confidentiality organized by Protection Levels. Chapters 5 and 6 present the technical security requirements and assurances for integrity and availability, respectively, organized by Levels-of-Concern.

1.F.5 Determine Required Documentation and Testing Activities (Chapters 4, 5, and 6). The assurance requirements in Chapters 4, 5, and 6 are examined to determine the appropriate documentation and testing activities required for the system.

1.F.6 Write the System Security Plan (Chapter 9 and Appendix C). The System Security Plan (SSP), described in Appendix C, is written to describe the planned operating conditions of the system and the expected residual risk of operating the system (Chapter 9). The DAA and/or ISSM approves the SSP, and the system is then implemented with the security requirements that have been determined for it (paragraphs 1.F.1 through 1.F.5). In the case of operational systems (with their security requirements already implemented), the SSP is written to describe the operating conditions of the system and the residual risk of operating the system.

1.F.7 Validate Security in Place. The ISSO ensures that the security requirements and procedures are in place for the system.

1.F.8 Testing against Security Requirements (Chapters 4, 5, and 6). The system is tested based on the security testing requirements in Chapters 4, 5, and 6.

1.F.9 Prepare Certification Package (Chapters 4, 5, 6, and 9). The ISSO and ISSM prepare the certification package, based on the documentation requirements in Chapters 4, 5, and 6, and the certification package requirements specified in Chapter 9.

1.F.10 Forward Certification Package. The certification package is presented to the DAA for accreditation.

1.F.11 Accreditation Decision by the DAA. The DAA* determines whether the level of residual risk is acceptable and consistent with that indicated in the SSP, and if it is, accredits the system. Testing shall be performed to validate the extent of residual risk.

[*When this manual refers to the DAA, the DAA Representative is assumed to be included, at the discretion of the DAA.]

1.F.11.a If the DAA accredits the system, the system goes into operation (or continues to operate) according to the accreditation.

1.F.11.b If the DAA grants an interim approval to operate, the system may be operated for up to 180 days, and the interim approval to operate can be renewed once for an additional 180 days. The DAA must indicate, in the agreement granting interim approval to operate, the actions necessary to meet accreditation. By the end of the second 180-day period, the system shall either be accredited or cease operation.

1.F.11.c If the DAA neither accredits the system, nor grants an interim approval to operate, then the requester must modify the system or its safeguards, and the process repeats from paragraph 1.F.6, above, until the DAA accredits the system, grants an interim approval to operate, or decides to disallow system operation.

1.G Use of Cryptography

1.G.1 Cryptography is a critical tool used to protect confidentiality of data, to assure the authenticity of information, and to detect the alteration of information. National policy requires the National Security Agency (NSA) to review and approve all cryptography used to protect classified information from access by unauthorized persons (i.e., not cleared for the information).

1.G.2 Cryptography may also be used to separate compartments or protect “need-to-know” among cleared users on classified systems. For such uses the DAA may select the cryptographic mechanisms (including commercially available products) to be used after consulting with the Data Owner on requirements. DAAs should also consult with NSA for assistance and advice regarding the security of the proposed implementation. They should pay particular attention to key management, since appropriate secure key management is an important factor in overall system security.

1.H General Notes

1.H.1 In the following pages, the term "good engineering practice" refers to the state of the engineering art for commercial systems that have equivalent problems and solutions; a good engineering practice by definition meets commercial requirements. These practices are usually part of the normal installation and operating procedures for systems. When placing security reliance on items that implement good engineering practice (such as commercial off-the shelf [COTS] software), the DAAs or their designees shall verify that the item(s) are set up properly and are operating as expected.

1.H.2 In this manual, the word "or" is used in its common English meaning that includes all three cases of a single element in a list, any combination of elements in a list, and all elements in the list.

1.H.3 Conventionally, information protection has been expressed as a combination of the following characteristics: confidentiality, integrity, and availability. Other expressions include other characteristics (such as utility, user accountability, authenticity, possession, currency, and non-repudiation), but most of these other characteristics are not independent of confidentiality, integrity, and availability. In other words, these additional characteristics can be expressed as some function of confidentiality, integrity, and availability. Thus, this manual will use the conventional characteristics (confidentiality, integrity, and availability) as the appropriate descriptive elements, while recognizing that some systems have additional operational requirements for services.

1.H.4 The Security Support Structure consists of those components (hardware, firmware, and software) that are essential to maintaining the security policies of the system. To prevent access by general users, the Security Support Structure is normally protected at a greater level than the rest of the system.

1.H.5 While this manual primarily discusses protection mechanisms for the information on systems, it explicitly assumes that the hardware, software, and firmware related to the system are given appropriate levels of protection.

1.H.6 The terms "department" and "agency" refer to the organization that is responsible for information systems security in a given situation. When stating requirements, the terms "department" or "agency" are not limiting, but rather are intended to include all subordinate organizations involved in a given information systems security situation. For example, the Secretary of Defense may delegate many of the operational aspects of compliance with this policy to a tactical military field command responsible for systems that contain classified information.

2 ROLES AND RESPONSIBILITIES

2.A Overview

This chapter describes eight roles pertaining to IS security and assigns responsibilities to each.

2.A.1 Separation of Roles

2.A.1.a Some systems are extensive enough to require a different individual to fill each of the eight roles.

2.A.1.b More typically, however, the eight roles can be collapsed into four or five, depending on whether the Principal Accrediting Authority (PAA) is also the Data Owner. There is only one restriction on collapsing roles: at the operational level, implementers and examiners shall not be the same person. For example, this structure prohibits the Designated Accrediting Authority from also being the Information System Security Officer. In some agencies, the same individual (e.g., a PAA) may fill management roles at a high level, as both chief examiner and chief implementer, but no single individual can fill both operational roles.

2.A.1.c The SSP shall specify which roles may be collapsed and which must remain separate.

2.A.2 Applicability. In the following subsections, the "system" referred to is the system or systems under the purview of the individual whose roles are being defined.

2.B Roles and Responsibilities

2.B.1 Special Provision for Waivers of Citizenship Requirements. All concerned PAAs and Data Owners shall approve, per paragraph 8.E.1, any exception to the citizenship requirements set forth below, including for systems jointly operated by the US and a foreign allied government.

2.B.2 Principal Accrediting Authority

2.B.2.a Definition: The Director, Special Programs Office (N7SP), Department of the Navy, is the PAA with responsibility for all Department of Navy SAPs. The Director, Security and Special Programs Oversight, Administrative Assistant to the Secretary of the Air Force is the PAA with responsibility for Department of the Air Force SAPs. (However, for some programs, this responsibility belongs to the cognizant security authority.) The US Army Technology Management Office, DACS-DMP, is the PAA for all Department of the Army SAPs.

2.B.2.b Responsibilities of the PAA include:

2.B.2.b(1) Establishing and maintaining the PAA's department or agency's SAP Information System Security Program, including the certification and accreditation programs.

2.B.2.b(2) Requiring the establishment and operation of similar certification and accreditation programs in those components to which the PAAs have delegated accreditation authority.

2.B.2.b(3) Ensuring the formal written appointment of DAAs and approval or disapproval of the further delegation of the DAA's authority.

2.B.2.b(4) Exercising top-level management oversight of the development, implementation, and evaluation of the information system security program in the PAA's organization. In general, much of the PAA's operational authority is delegated to DAAs.

2.B.2.b(5) Implementing the security policy requirements set forth in this manual.

2.B.2.b(6) Ensuring the establishment of an information security incident response and reporting capability.

2.B.2.b(7) Ensuring accountability for the protection of the information under the PAA's purview, including maintenance of required documents concerning the accreditation status of systems.

2.B.2.b(8) Establishing IS security education, training, and awareness programs to ensure consistency and reciprocity.

2.B.2.b(9) Establishing a compliance validation and oversight mechanism to ensure consistent implementation of the security policy requirements set forth in this manual.

2.B.2.b(10) When justified, approving the operation of a system that does not meet the requirements specified in this manual. However, such approval shall be in writing, and the PAA granting such approval shall also accept, in writing, the responsibility for the resulting residual risks and shall inform the other PAAs responsible for systems interconnected to this system. The PAA may choose to delegate this authority to the DAA.

2.B.2.b(11) Ensuring that security is incorporated as an element of the life-cycle process.

2.B.3 Data Owner

2.B.3.a Definition: The head of the organization that has final statutory and operational authority for specified information.

2.B.3.b Responsibilities of the Data Owner include:

2.B.3.b(1) Providing instruction to the PAA/DAA concerning the sensitivity of information under the Data Owner's purview to assist in the PAA/DAA's decision regarding the Levels-of-Concern for confidentiality, integrity, and availability.

2.B.3.b(2) Determining whether foreign nationals may access information systems accredited under this manual. Access must be consistent with the NDP-1, DoD Directive 5230.11, DoD Directive 5530.3, enclosure 7, the International Program Security Handbook, DoD 5220.22-M-Sup 1, et al.

2.B.3.b(3) The Data Owner may revoke permission to process the information on any system if unsatisfied with the protections it provides, and will notify the PAA/DAA of any decision to revoke.

2.B.4 Designated Accrediting Authority

2.B.4.a Definition: The official with the authority to assume formal responsibility for operating a system at an acceptable level of risk based on the implementation of an approved set of technical, managerial, and procedural safeguards.

2.B.4.b The DAA shall:

2.B.4.b(1) Be a United States citizen;

2.B.4.b(2) Be an employee of United States government;

2.B.4.b(3) Have a level of authority commensurate with accepting, in writing, the risk of operating all ISs under the DAA's jurisdiction. Though the DAA need not be technically trained to evaluate an IS, the appointing authority shall ensure that the DAA is supported by individuals knowledgeable in all areas of security such that a technically correct assessment of the security characteristics of the IS can be made.

2.B.4.b(4) Understand the operational need for the system(s) in question and the operational consequences of not operating the system(s).

2.B.4.c The DAA grants formal accreditation to operate a system processing SAP information. The DAA has the authority to withdraw accreditation, suspend operations, grant interim approval to operate, or grant variances when circumstances warrant. The approval shall be a written, dated statement of accreditation that clearly sets forth any conditions or restrictions to system operation. DAAs are responsible and accountable for the security of the information and systems that they accredit.

2.B.4.d The DAA has the authority to specify, notwithstanding the requirements of this manual, a greater Level-of-Concern or amount of protection for any given system in any given environment.

2.B.4.e Responsibilities of the DAA include:

2.B.4.e(1) Ensuring that each system is properly accredited based on (a) its environment and sensitivity levels, and (b) the review and approval of security safeguards and the issuing of written accreditation statements.

2.B.4.e(2) Providing written notification to the cognizant PAA and Data Owner prior to granting any foreign national access to the system.

2.B.4.e(3) Ensuring documentation is maintained for all IS accreditations under the DAA's purview.

2.B.4.e(4) Ensuring all of the appropriate roles and responsibilities outlined in this directive are accomplished for each IS.

2.B.4.e(5) Ensuring that operational IS security policies are promulgated for each system, project, program, and site for which the DAA has approval authority.

2.B.4.e(6) Ensuring an IS's security education, training, and awareness program is developed and implemented.

2.B.4.e(7) Overseeing and periodically reviewing system security to accommodate possible changes that may have taken place.

2.B.4.e(8) Ensuring that organizations plan, budget, allocate, and spend adequate resources in support of IS security.

2.B.4.e(9) Determining the Levels-of-Concern for confidentiality, integrity, and availability for the data on a system, and informing the ISSM/ISSO of the determination.

2.B.4.e(10) Ensuring that security is incorporated as an element of the life-cycle process.

2.B.4.e(11) Ensuring that the responsibilities of the DAA Representative (see paragraph 2.B.5, below) are performed.

2.B.4.e(12) Approving incident reporting procedures developed by the ISSM.

2.B.4.e(13) Reporting security-related events to affected parties (i.e., interconnected systems), Data Owners, and all involved PAAs.

2.B.4.e(14) Ensuring consideration and acknowledgment of Counter Intelligence activities during the C&A process.

2.B.4.f Should the DAA choose to accredit a system even though the system implementers are unable (within fiscal and operational constraints) to implement all the requirements as specified in this manual, the DAA shall, prior to accreditation:

2.B.4.f(1) Identify in writing to the Data Owner(s) of all data on the system any requirements that are not being implemented and which mitigating safeguards are being applied to the system.

2.B.4.f(2) Identify in writing to the DAAs of directly connected systems any requirements that are not being implemented and which mitigating safeguards are being employed on the system.

2.B.4.f(3) State in writing that the DAA accepts responsibility for the risk of operating the system with lessened protection.

2.B.5 Designated Accrediting Authority Representative (DAA Rep)

2.B.5.a Definition: The technical expert responsible to the DAA for ensuring that security is integrated into and implemented throughout the life cycle of a system. The DAA assigns responsibilities to the DAA Rep. The responsibilities listed below are those normally performed by a DAA Rep. In any given organization, there need not be a DAA Rep (i.e., the DAA or ISSM could perform these functions).

2.B.5.b The DAA Rep shall:

2.B.5.b(1) Be a United States citizen.

2.B.5.b(2) Have a working knowledge of system function, security policies, technical security safeguards, and operational security measures.

2.B.5.c Responsibilities of the DAA Rep (under the direction of the DAA) include:

2.B.5.c(1) Developing and overseeing the implementation of the security policy and providing guidance for securing ISs.

2.B.5.c(2) Ensuring that security testing and evaluation are completed and documented.

2.B.5.c(3) Advising the DAA on the selection and effective use of specific security mechanisms.

2.B.5.c(4) Maintaining appropriate system accreditation documentation.

2.B.5.c(5) Evaluating threats and vulnerabilities to ascertain whether additional safeguards are needed.

2.B.5.c(6) Ensuring that a record of all security-related vulnerabilities and incidents is maintained, and reporting serious or unresolved violations to the DAA.

2.B.5.c(7) Ensuring that certification is accomplished for each IS.

2.B.5.c(8) Evaluating certification documentation and providing written recommendations for accreditation to the DAA.

2.B.5.c(9) Ensuring that all ISSMs and ISSOs receive technical and security education and training to carry out their duties.

2.B.5.c(10) Assessing changes in the system, its environment, and operational needs that could affect the accreditation.

2.B.6 Information System Security Manager (ISSM)

2.B.6.a Definition: The manager responsible for an organization's IS security program.

2.B.6.b The ISSM shall:

2.B.6.b(1) Be a United States citizen.

2.B.6.b(2) Have a working knowledge of system functions, security policies, technical security safeguards, and operational security measures.

2.B.6.b(3) Hold US Government security clearances/access approvals commensurate with the level of information processed by the system.

2.B.6.b(4) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

2.B.6.c Responsibilities of the ISSM include:

2.B.6.c(1) Developing and maintaining a formal Information Systems Security Program.

2.B.6.c(2) Implementing and enforcing IS security policies.

2.B.6.c(3) Reviewing all SSPs (described in Appendix C) and endorsing those found to be acceptable.

2.B.6.c(4) Overseeing all ISSOs to ensure that they are following established information security policies and procedures.

2.B.6.c(5) Ensuring that all ISSOs receive the necessary technical and security training to carry out their duties.

2.B.6.c(6) Ensuring the development of system certification documentation by reviewing and endorsing such documentation and recommending action by the DAA.

2.B.6.c(7) Ensuring approved procedures are in place for clearing, purging, declassifying, and releasing system memory, media, and output.

2.B.6.c(8) Maintaining, as required by the DAA, a repository for all system certification documentation and modifications.

2.B.6.c(9) Coordinating IS security inspections, tests, and reviews.

2.B.6.c(10) Developing procedures for responding to security incidents, and for investigating and reporting (to the DAA Representative and to local management) security violations and incidents, as appropriate.

2.B.6.c(11) Ensuring proper protection or corrective measures have been taken when an incident or vulnerability has been discovered within a system.

2.B.6.c(12) Ensuring that data ownership and responsibilities are established for each IS, to include accountability, access rights, and special handling requirements.

2.B.6.c(13) Ensuring development and implementation of an information security education, training, and awareness program.

2.B.6.c(14) Ensuring development and implementation of procedures for authorizing the use of software, hardware, and firmware on the system.

2.B.6.c(15) If a configuration management board exists, serving as a member of the board. (However, the ISSM may elect to delegate this responsibility to the ISSO).

2.B.7 Information System Security Officer (ISSO)

2.B.7.a Definition: The person responsible to the ISSM for ensuring that operational security is maintained for a specific IS; sometimes referred to as a Network Security Officer.

2.B.7.b The ISSO shall:

2.B.7.b(1) Be a United States citizen.

2.B.7.b(2) Have a working knowledge of system functions, security policies, technical security safeguards, and operational security measures.

2.B.7.b(3) Hold US Government security clearances/access approvals commensurate with the level of information processed by the system.

2.B.7.b(4) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

2.B.7.c Responsibilities of the ISSO include:

2.B.7.c(1) Ensuring systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the security plan.

2.B.7.c(2) Ensuring that all users have the requisite security clearances, authorization, and need-to-know, and are aware of their security responsibilities before granting access to the IS.

2.B.7.c(3) Reporting all security-related incidents to the ISSM.

2.B.7.c(4) Initiating, with the approval of the ISSM, protective or corrective measures when a security incident or vulnerability is discovered.

2.B.7.c(5) Developing and maintaining an SSP as described in Appendix C.

2.B.7.c(6) Conducting periodic reviews to ensure compliance with the SSP.

2.B.7.c(7) Ensuring configuration management (CM) for security-relevant IS software, hardware, and firmware is maintained and documented. If a CM board exists, the ISSO may be a member of the CM board if so designated by the ISSM.

2.B.7.c(8) Ensuring that system recovery processes are monitored to ensure that security features and procedures are properly restored.

2.B.7.c(9) Ensuring all IS security-related documentation is current and accessible to properly authorized individuals.

2.B.7.c(10) Formally notifying the ISSM and the DAA when a system no longer processes intelligence or SAP information.

2.B.7.c(11) Formally notifying the ISSM and the DAA when changes occur that might affect accreditation.

2.B.7.c(12) Ensuring that system security requirements are addressed during all phases of the system life cycle.

2.B.7.c(13) Following procedures developed by the ISSM, authorizing software, hardware, and firmware use before implementation on the system.

2.B.8 Privileged Users

2.B.8.a Definition: A user who has access to system control, monitoring, or administration functions. Example of privileged users include:

2.B.8.a(1) Users having “superuser,” “root,” or equivalent access to a system (e.g., system administrators, computer operators, perhaps ISSOs); users with near or complete control of an IS or who set up and administer user accounts, authenticators, and the like.

2.B.8.a(2) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexers, and other key IS equipment.

2.B.8.a(3) Users who have been given the authority to control and change other users’ access to data or program files (e.g., applications software administrators, administrators of specialty file systems, database managers).

2.B.8.a(4) Users who have been given special access for troubleshooting or monitoring an IS’s security functions (e.g., those using IS analyzers, management tools).

2.B.8.b Privileged users shall:

2.B.8.b(1) Be United States citizens.

2.B.8.b(2) Have a working knowledge of system functions, security policies, technical security safeguards, and operational security measures.

2.B.8.b(3) Be limited to the absolute minimum number of privileged users needed to manage the system.

2.B.8.b(4) Where technically feasible, be limited to the minimum number of privileges needed to perform their assigned duties.

2.B.8.b(5) Possess a clearance equal to or higher than the highest classification of data processed on or maintained by the IS.

2.B.8.b(6) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

2.B.8.c Responsibilities of privileged users include:

2.B.8.c(1) Protecting the root or superuser authenticator at the highest level of data it secures and not sharing the authenticator and/or account.

2.B.8.c(2) Reporting all suspected security-related IS problems to the ISSO or ISSM.

2.B.8.c(3) Using special access or privileges granted only to perform authorized tasks and functions.

2.B.8.c(4) Enrolling authorized users in an IS.

2.B.8.c(5) Notifying the ISSO of any system configuration changes that might adversely impact system security.

2.B.9 General Users

2.B.9.a Definition: An individual who can receive information from, input information to, or modify information on, a system without a reliable human review.

2.B.9.b General users shall:

2.B.9.b(1) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

2.B.9.b(2) Immediately report all security incidents and potential threats and vulnerabilities involving an IS to the appropriate ISSO.

2.B.9.b(3) Protect their authenticators and report any compromise or suspected compromise of an authenticator to the appropriate ISSO.

2.B.9.b(4) Ensure that system media and system output are properly classified, marked, controlled, stored, transported, and destroyed.

2.B.9.b(5) Protect terminals/workstations from unauthorized access.

2.B.9.b(6) Inform the ISSO when access to a particular IS is no longer required (e.g., completion of project, transfer, retirement, resignation).

2.B.9.b(7) Observe rules and regulations governing the secure operation and authorized use of an IS.

2.B.9.b(8) Use the IS only for authorized purposes.

2.B.9.b(9) Not introduce malicious code into any IS or physically damage the system.

2.B.9.b(10) Not bypass, strain, or test security mechanisms. If security mechanisms must be bypassed for any reason, users shall coordinate the procedure with the ISSO and receive written permission from the ISSM for the procedure.

2.B.9.b(11) Not introduce or use unauthorized software, firmware, or hardware on an IS.

2.B.9.b(12) Not relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization.

3 LEVELS-OF-CONCERN AND PROTECTION LEVELS

3.A Overview

This chapter introduces and defines the concepts of Levels-of-Concern and Protection Levels, and explains how to use them to ascertain the appropriate technical security requirements for confidentiality, integrity, and availability that each IS must meet.

3.A.1 Conformance with Technical Security Requirements. In order to be certified and accredited, each IS must conform to a set of technical security requirements for confidentiality, integrity, and availability. The specific technical security requirements and associated assurances with which an IS must comply are provided in Chapters 4 (confidentiality), 5 (integrity), and 6 (availability) of this manual. To determine which of these requirements are appropriate for a given IS, the DAA must first ascertain the appropriate Levels-of-Concern and Protection Level for the IS.

3.A.2 Non-Multi-User Systems. The technical requirements provided in Chapters 4, 5, and 6 are intended for multi-user systems. Applying them by rote to non-multi-user systems is likely to result in unnecessary costs and detrimental operational impact. Paragraph 9.G provides supplemental guidance for dealing with "special" systems that may be secured without applying all of the technical requirements of Chapters 4, 5, and 6.

3.B Description of Levels-of-Concern

3.B.1 Overview

3.B.1.a The DAA, using guidance from the Data Owner, and after examining the information characteristics of the IS in question, must determine the appropriate Levels-of-Concern ratings for confidentiality, integrity, and availability. The Level-of-Concern rating for each of these areas can be Basic, Medium, or High. *The Level-of-Concern rating is independent for each of these three areas*. Thus, for example, a system's Level-of-Concern for confidentiality could be High, for integrity could be Basic, and for availability could be Medium. When a system has more than one kind of information on it, the Level-of-Concern assigned is the *highest* Level-of-Concern for *any information* on the system.

3.B.1.b The DAA shall determine and assign a Level-of-Concern rating for confidentiality, integrity, and availability for each IS that is to be accredited.

3.B.1.c The decision regarding the Levels-of-Concern shall be explicit for all (including interconnected) systems. The record of this decision shall be written, and the DAA shall ensure that these records are retained for the operational life of the system(s) involved. At the DAA's discretion, the decision can be made for groups of systems, but it shall be explicit.

3.B.2 Determining the Level-of-Concern

3.B.2.a Confidentiality. Here the Level-of-Concern rating is based on the sensitivity of the information that the IS maintains, processes, and transmits. The more sensitive the information, the higher the IS's Level-of-Concern. Systems that process DoD SAP information require a High Level-of-Concern. *Since all systems accredited under the*

authority of this manual by definition process SAP information, all systems accredited under this manual must be assigned a High Confidentiality Level-of-Concern.

3.B.2.b Integrity. Here the Level-of-Concern rating is based on the degree of resistance to unauthorized modification of the information maintained, processed, and transmitted by the IS that is necessary for accomplishing the mission of its users. The greater the needed degree of resistance to unauthorized modification, the higher is the Level-of-Concern.

3.B.2.c Availability. Here the Level-of-Concern rating is based on the degree of ready availability required for the information maintained, processed, and transmitted by the IS in order to accomplish the mission of its users. The greater the need for rapid information availability the higher the Level-of-Concern.

3.B.2.d Table 3.1 is designed to assist those involved in system development, implementation, certification, and accreditation in determining the appropriate Levels-of-Concern for confidentiality, integrity and availability for a given system processing a given set of information.

3.C Protection Levels

3.C.1 Protection Level Overview

3.C.1.a *The concept of Protection Levels applies only to confidentiality*. Having verified that an IS will maintain, process, or transmit SAP information and therefore that its Level of Concern for confidentiality must be High, the DAA must next ascertain the appropriate Protection Level for the IS based on the required clearance(s), formal access approval(s), and need-to-know of all direct and indirect users who receive information from the IS *without* manual intervention and reliable human review. It indicates an implicit level of trust that is placed in the system's technical capabilities.

3.C.1.b The DAA must assign a Protection Level to each IS that is to be accredited. The decision regarding the Protection Levels shall be explicit for all (including interconnected) systems. The record of this decision shall be in writing, and the DAA shall ensure that these records are retained for the operational life of the system(s) involved. At the DAA's discretion, the decision can be made for groups of systems, but it shall be explicit.

3.C.2 Determining Protection Levels

3.C.2.a Table 4.1 presents the criteria for determining which of the five Protection Levels is appropriate for the IS being accredited.

3.C.2.a(1) An IS operates at Protection Level 1 when *all* users have all required approvals for access to all information on the IS. This means that all users have all required clearances, formal access approvals, and the need to know for all information on the IS.

3.C.2.a(2) An IS operates at Protection Level 2 when all users have all required *formal* approvals for access to all information on the IS, but at least one user lacks administrative approval for some of the information on the IS. 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 IS.

3.C.2.a(3) An IS operates at Protection Level 3 when at least *one user* lacks at least one required *formal* approval for access to all information on the IS. 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 IS.

3.C.2.a(4) An IS operates at Protection Level 4 when at least *one user* lacks *sufficient* clearance for access to some of the information on the IS, but all users have at least a Secret clearance.

3.C.2.a(5) An IS operates at Protection Level 5 when at least *one user* lacks *any* clearance for access to some of the information on the IS.

3.C.2.b An IS operating at Protection Level 3 presents a potential risk of loss of compartmented information to users lacking the necessary formal access approvals. An IS operating at Protection Levels 4 or 5 presents a potential risk of the loss of classified information to users lacking the necessary clearance. DAAs must recognize the technical risk of operating such ISs, and shall require all reasonably available assurances of the effectiveness of the protection mechanisms for such ISs.

3.D Determining Security Features and Assurances

3.D.1 Having determined the appropriate Levels-of-Concern and Protection Level for an IS, the DAA next needs to ascertain the specific technical security requirements and assurances for confidentiality, integrity, and availability provided in Chapters 4, 5, and 6, respectively. For example, assume that a system has a Protection Level of 2, a Medium Integrity Level-of-Concern, and a High Availability Level-of-Concern. That system would have to conform to the security features and assurance requirements of Protection Level 2 in Chapter 4, the security features and assurance requirements for a Medium Integrity Level-of-Concern provided in Chapter 5, and the security features and assurance requirements for a High Availability Level-of-Concern provided in Chapter 6.

3.D.2 The security features and assurances for confidentiality, integrity, and availability are independent of each other. The DAA is responsible for ascertaining the appropriate security features and assurances for confidentiality, integrity, and availability.

Table 3.1 - Consolidated Levels-of-Concern

Level of Concern	Confidentiality Indicators (Chapter 4)	Integrity Indicators (Chapter 5)	Availability Indicators (Chapter 6)
Basic	Not applicable to this manual	Reasonable degree of resistance required against unauthorized modification, or loss of integrity will have an adverse effect.	Information must be available with flexible tolerance for delay[1], or loss of availability will have an adverse effect.
Medium	Not applicable to this manual	High degree of resistance required against unauthorized modification, or bodily injury might result from loss of integrity, or loss of integrity will have an adverse effect on organizational-level interests.	Information must be readily available with minimum tolerance for delay[2], or bodily injury might result from loss of availability, or loss of availability will have an adverse effect on organizational-level interests.
High[3]	All Information Protecting Intelligence Sources, Methods, and Analytical Procedures. All Sensitive Compartmented Information.	Very high degree of resistance required against unauthorized modification, 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.	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.

Notes

1. In this context, "flexible tolerance for delay" means that routine system outages do not endanger mission accomplishment; however, extended system outages (days to weeks) may endanger the mission.
2. In this context, "minimum tolerance for delay" means that routine system outages do not endanger mission accomplishment; however, extended system outages (seconds to hours) may endanger the mission.
3. See (Table 4.1 Protection Levels) for more information regarding requirements for High Level-of-Concern.

4 CONFIDENTIALITY SYSTEM SECURITY FEATURES AND ASSURANCES

4.A Overview

4.A.1 This chapter provides the detailed confidentiality* technical security features and assurances. As noted in Chapter 3, the DAA must select the appropriate technical security features and assurances for an IS based on the Protection Level of the IS.

[*Integrity and availability security features and assurances are provided in Chapters 5 and 6, respectively. As noted in Chapter 3, the DAA must ascertain the technical security requirements and assurances for confidentiality, integrity, and availability prior to accrediting an IS.]

4.A.2 This chapter separately sets forth the confidentiality requirements for systems operating at each of the five Protection Levels.

4.A.3 The underscored terms in brackets preceding the sets of requirements (e.g., [Access1]) indicate how those requirements are identified in the tabular presentation in Appendix D.

4.A.4 The notations PL1, PL2, PL3, PL4, and PL5 refer to Protection Levels 1, 2, 3, 4 and 5, respectively.

4.A.5 Requirements listed in **boldface** type are in addition to (or different from) the requirements for the previous Protection Level. Entries for Protection Level 1 are in **boldface** type because the lowest level is the first entry for a given requirement.

4.B Confidentiality Requirements

Each IS shall incorporate security features that will control the release of information commensurate with the sensitivity of the information being processed, as well as with the clearance, formal access approval, and need-to-know of the users* of the IS, as determined by the Protection Level assigned. For each IS, assurance commensurate with the Protection Level shall be provided.

Table 4.1 identifies the factors used to select the appropriate Protection Level, and cites the paragraphs of this chapter where the relevant requirements can be located.

[*As noted in the previous chapter, the Protection Level for confidentiality is based on clearance(s), formal access approval(s), and need-to-know of all users, where users refers to direct and indirect users who receive information from the IS without manual intervention and reliable human review. But, when applying the confidentiality requirements of this chapter the term user refers only to the direct users of the system.]

Table 4.1 - Protection Levels

Lowest Clearance	Formal Access Approval	Need To Know	Protection Level
At Least Equal to Highest Data	All Users Have ALL	All Users Have ALL	1 (paragraph 4.B.1)
At Least Equal to Highest Data	All Users Have ALL	NOT ALL Users Have ALL	2 (paragraph 4.B.2)
At Least Equal to Highest Data	NOT ALL users have ALL	Not Contributing to Decision	3 (paragraph 4.B.3)
Secret	Not Contributing to Decision	Not Contributing to Decision	4 (paragraph 4.B.4)
Uncleared	Not Contributing to Decision	Not Contributing to Decision	5 (paragraph 4.B.5)

4.B.1 **Protection Level 1**

4.B.1.a A system operating at Protection Level 1 shall employ the following features:

4.B.1.a(1) **[Access1] Access control, including:**

4.B.1.a(1)(a) **Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.**

4.B.1.a(1)(b) **Procedures for controlling access by users and maintainers to IS resources, including those that are at remote locations.**

4.B.1.a(2) **[I&A1] Identification and Authentication (I&A) procedures that include provisions for uniquely identifying and authenticating the users. Procedures can be external to the system (e.g., procedural or physical controls) or internal to the system (i.e., technical). Electronic means shall be employed where technically feasible.**

4.B.1.a(3) **[ParamTrans] Parameter Transmission. Security parameters (e.g., labels, markings) shall be reliably associated (either explicitly or implicitly) with information exchanged between systems.**

4.B.1.a(4) **[Recovery] Recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.**

4.B.1.a(5) **[ScrnLck] Screen Lock. Unless there is an overriding technical or operational problem, a terminal/desktop/laptop screen-lock functionality shall be associated with each terminal/desktop/laptop computer. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal/desktop/laptop, totally hiding what was previously visible on the screen. Such a capability shall:**

4.B.1.a(5)(a) **Be enabled either by explicit user action or if the terminal/desktop/laptop is left idle for a specified period of time (e.g., 15 minutes or more).**

4.B.1.a(5)(b) **Ensure that once the terminal/desktop/laptop security/screen-lock software is activated, access to the terminal/desktop/laptop requires knowledge of a unique authenticator.**

4.B.1.a(5)(c) **Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).**

4.B.1.a(6) **[SessCtrl1] Session Controls, including:**

4.B.1.a(6)(a) **Notification to all users prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible.**

4.B.1.a(6)(b) **Notification to all users that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is prohibited and subject to criminal and civil penalties. Electronic means shall be employed where technically feasible.**

4.B.1.a(7) **[Storage] Data Storage, implementing at least one of the following:**

4.B.1.a(7)(a) **Information stored in an area approved for open storage* of the information.**

[*In the context of storage confidentiality, "approved for open storage" must include consideration of the possibility of access by all users who have direct access to the system or network, wherever physically located.]

4.B.1.a(7)(b) **Information stored in an area approved for continuous personnel access control (when continuous personnel access control is in effect), i.e., a 24-hour, 7-day-per-week operational area.**

4.B.1.a(7)(c) **Information secured as appropriate for closed storage.**

4.B.1.a(7)(d) **Information encrypted using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of stored data.**

4.B.1.a(8) **[Trans1] Data Transmission.**

4.B.1.a(8)(a) **Data transmission that implements at least one of the following:**

4.B.1.a(8)(a)(1) **Information distributed only within an area approved for open storage of the information.**

4.B.1.a(8)(a)(2) **Information distributed via a Protected Distribution System* (PDS).**

[*A PDS provides physical protection or intrusion detection for communications lines. A PDS can also provide need-to-know isolation for communications lines.]

4.B.1.a(8)(a)(3) **Information distributed using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of the information.**

4.B.1.a(8)(a)(4) **Information distributed using a trusted courier.**

4.B.1.a(8)(b) **Dial-up lines, other than those that are protected with nationally certified cryptographic devices or PDSs, shall not be used for gaining access to system resources that process SAP information unless the DAA provides specific written authorization for a system to operate in this manner.**

4.B.1.b **If the DAA requires technical controls, a system operating at Protection Level 1 shall employ all of the following features in addition to those mandated in paragraph 4.B.1.a:**

4.B.1.b(1) **[AcctMan] Account Management procedures that include:**

4.B.1.b(1)(a) **Identifying types of accounts (individual and group, conditions for group membership, associated privileges).**

4.B.1.b(1)(b) **Establishing an account (i.e., required paperwork and processes).**

4.B.1.b(1)(c) **Activating an account.**

4.B.1.b(1)(d) **Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators).**

4.B.1.b(1)(e) **Terminating an account (i.e., processes and assurances).**

4.B.1.b(2) **[Audit1] Auditing procedures, including:**

4.B.1.b(2)(a) **Providing the capability to ensure that all audit records include enough information to allow the ISSO to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.**

4.B.1.b(2)(b) **Protecting the contents of audit trails against unauthorized access, modification, or deletion.**

4.B.1.b(2)(c) **Maintaining collected audit data at least 12 months or one security review cycle, whichever is longer, and reviewing at least weekly.**

4.B.1.b(2)(d) **The system's creating and maintaining an audit trail that includes selected records of:**

4.B.1.b(2)(d)(1) **Successful and unsuccessful logons and logoffs.**

4.B.1.b(2)(d)(2) **Accesses to *security-relevant* objects and directories, including opens, closes, modifications, and deletions.**

4.B.1.b(2)(d)(3) **Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.**

4.B.1.b(3) **[I&A2] An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified:***

[*Alternative controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternative methods may have similar requirements. For example, the electronically stored version of biometric authentication patterns needs to be protected, as do password authenticators.]

4.B.1.b(3)(a) **Initial authenticator content and administrative procedures for initial authenticator distribution.**

4.B.1.b(3)(b) **Individual and Group authenticators. (Group authenticators may only be used in conjunction with an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator).**

4.B.1.b(3)(c) **Length, composition, and generation of authenticators.**

4.B.1.b(3)(d) **Change Processes (periodic and in case of compromise).**

4.B.1.b(3)(e) **Aging of static authenticators (i.e., not one-time passwords or biometric patterns)**

4.B.1.b(3)(f) **History of static authenticator changes, with assurance of nonreplication of individual authenticators, per direction in approved SSP.**

4.B.1.b(3)(g) **Protection of authenticators to preserve confidentiality and integrity.**

4.B.1.b(4) **[I&A3] Identification and Authentication (I&A). Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links (extranets, Internet, phone lines) that are outside of the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks).**

4.B.1.c **Requirements for system assurance at Protection Level 1.**

4.B.1.c(1) **[Doc1] Documentation shall include:**

4.B.1.c(1)(a) **A System Security Plan (see Appendix CAppendix A).**

4.B.1.c(1)(b) **A Security Concept of Operations (CONOPS). (The Security CONOPS may be included in the System Security Plan). The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture, the system's accreditation schedule, the system's Protection Level, integrity Level-of-Concern, availability Level-of-Concern, and a description of the factors that determine the system's Protection Level, integrity Level-of-Concern, and availability Level-of-Concern.**

4.B.1.c(2) **[SysAssur1] System Assurance shall include:**

4.B.1.c(2)(a) **Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware.**

4.B.1.c(2)(b) **Features or procedures for protection of the operating system from improper changes.**

4.B.1.c(3) **[Test1] Assurance shall be provided by the ISSM to the DAA that the system operates in accordance with the approved SSP, and that the security features, including access controls and configuration management, are implemented and operational.**

4.B.2 **Protection Level 2**

4.B.2.a **A system operating at Protection Level 2 shall employ the following features:**

4.B.2.a(1) [Access1] Access control, including:

4.B.2.a(1)(a) Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

4.B.2.a(1)(b) Procedures for controlling access by users and maintainers to IS resources, including those that are at remote locations.

4.B.2.a(2) **[Access2] Access Control, including a Discretionary Access Control (DAC) Policy. A system has implemented DAC when the Security Support Structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The DAC policy includes administrative procedures to support the policy and its mechanisms. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest [COIs], encryption) shall allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The DAC mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.**

4.B.2.a(3) [AcctMan] Account Management procedures that include:

4.B.2.a(3)(a) Identifying types of accounts (individual and group, conditions for group membership, associated privileges).

4.B.2.a(3)(b) Establishing an account (i.e., required paperwork and processes).

4.B.2.a(3)(c) Activating an account.

4.B.2.a(3)(d) Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators).

4.B.2.a(3)(e) Terminating an account (i.e., processes and assurances).

4.B.2.a(4) [Audit1] Auditing procedures, including:

4.B.2.a(4)(a) Providing the capability to ensure that all audit records include enough information to allow the ISSO to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

4.B.2.a(4)(b) Protecting the contents of audit trails against unauthorized access, modification, or deletion.

4.B.2.a(4)(c) Maintaining collected audit data at least 12 months or one security review cycle, whichever is longer, and reviewing at least weekly.

4.B.2.a(4)(d) The system's creating and maintaining an audit trail that includes selected records of:

4.B.2.a(4)(d)(1) Successful and unsuccessful logons and logoffs.

4.B.2.a(4)(d)(2) Accesses to security-relevant objects and directories, including opens, closes, modifications, and deletions.

4.B.2.a(4)(d)(3) Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.

4.B.2.a(5) **[Audit2] Auditing procedures, including:**

4.B.2.a(5)(a) **Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual).**

4.B.2.a(5)(b) **Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion.**

4.B.2.a(6) **[Audit3] At the discretion of the DAA, audit procedures that include the existence and use of audit reduction and analysis tools.**

4.B.2.a(7) [I&A2] An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified:*

[*Alternative controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternative methods may have similar requirements. For example, the electronically stored version of biometric authentication patterns needs to be protected, as do password authenticators.]

4.B.2.a(7)(a) Initial authenticator content and administrative procedures for initial authenticator distribution.

4.B.2.a(7)(b) Individual and Group Authenticators. (Group authenticators may only be used in conjunction with the use of an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator).

4.B.2.a(7)(c) Length, composition, and generation of authenticators.

4.B.2.a(7)(d) Change Processes (periodic and in case of compromise).

4.B.2.a(7)(e) Aging of static authenticators (i.e., not one-time passwords or biometric patterns)

4.B.2.a(7)(f) History of static authenticator changes, with assurance of non-replication of individual authenticators, per direction in approved SSP.

4.B.2.a(7)(g) Protection of authenticators to preserve confidentiality and integrity.

4.B.2.a(8) [I&A3] Identification and Authentication (I&A). Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links (extranets, Internet, phone lines) that are outside of the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks).

4.B.2.a(9) **[I&A4] Identification and Authentication. In those instances where the means of authentication is user-specified passwords, the ISSO or ISSM may employ (under the auspices of the DAA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password.**

4.B.2.a(10) **[LeastPrv] Least Privilege procedures, including the assurance that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks shall be employed.**

4.B.2.a(11) **[Marking] Marking procedures and mechanisms to ensure that either the user or the system itself marks all data transmitted or stored by the system to reflect the sensitivity of the data (i.e., classification level, classification category, and handling caveats). Markings shall be retained with the data.**

4.B.2.a(12) [ParamTrans] Parameter Transmission. Security parameters (e.g., labels, markings) shall be reliably associated (either explicitly or implicitly) with information exchanged between systems.

4.B.2.a(13) [Recovery] Recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.

4.B.2.a(14) **[ResrcCtrl] Resource Control. All authorizations to the information contained within an object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the Security Support Structure's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. There must be no residual data from the former object.**

4.B.2.a(15) [ScrnLck] Screen Lock. Unless there is an overriding technical or operational problem, a terminal/desktop/laptop screen-lock functionality shall be associated with each terminal/desktop/laptop computer. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal/desktop/laptop, totally hiding what was previously visible on the screen. Such a capability shall:

4.B.2.a(15)(a) Be enabled either by explicit user action or if the terminal/desktop/laptop is left idle for a specified period of time (e.g., 15 minutes or more).

4.B.2.a(15)(b) Ensure that once the terminal/desktop/laptop security/screen-lock software is activated, access to the terminal/desktop/laptop requires knowledge of a unique authenticator.

4.B.2.a(15)(c) Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

4.B.2.a(16) [SessCtrl1] Session Controls, including:

4.B.2.a(16)(a) Notification to all users prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible.

4.B.2.a(16)(b) Notification to all users that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is prohibited and subject to criminal and civil penalties. Electronic means shall be employed where technically feasible.

4.B.2.a(17) **[SessCtrl2] Enforcement of Session Controls, including:**

4.B.2.a(17)(a) **Procedures for controlling and auditing concurrent logons from different workstations.**

4.B.2.a(17)(b) **Station or session time-outs, as applicable.**

4.B.2.a(17)(c) **Limited retry on logon as technically feasible.**

4.B.2.a(17)(d) **System actions on unsuccessful logons (e.g., blacklisting of the terminal or user identifier).**

4.B.2.a(18) [Storage] Data Storage, implementing at least one of the following:

4.B.2.a(18)(a) Information stored in an area approved for open storage* of the information.

[*In the context of storage confidentiality, "approved for open storage" must include consideration of the possibility of access by all users who have direct access to the system or network, wherever physically located.]

4.B.2.a(18)(b) Information stored in an area approved for continuous personnel access control (when continuous personnel access control is in effect), i.e., a 24-hour, 7-day-per week operational area.

4.B.2.a(18)(c) Information secured as appropriate for closed storage.

4.B.2.a(18)(d) Information encrypted using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of stored data.

4.B.2.a(19) [Trans1] Data Transmission.

4.B.2.a(19)(a) Data transmission that implements at least one of the following:

4.B.2.a(19)(a)(1) Information distributed only within an area approved for open storage of the information.

4.B.2.a(19)(a)(2) Information distributed via a Protected Distribution System* (PDS).

[*A PDS provides physical protection or intrusion detection for communications lines. A PDS can also provide need-to-know isolation for communications lines.]

4.B.2.a(19)(a)(3) Information distributed using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of the information.

4.B.2.a(19)(a)(4) Information distributed using a trusted courier.

4.B.2.a(19)(b) Dial-up lines, other than those that are protected with nationally certified cryptographic devices or PDSs, shall not be used for gaining access to system resources that process SAP information unless the DAA provides specific written authorization for a system to operate in this manner.

4.B.2.b **Requirements for system assurance at Protection Level 2.**

4.B.2.b(1) [Doc1] Documentation shall include:

4.B.2.b(1)(a) A System Security Plan (see Appendix C).

4.B.2.b(1)(b) A Security Concept of Operations (CONOPS) (the Security CONOPS may be included in the System Security Plan). The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture, the system's accreditation schedule, the system's Protection Level, integrity Level-of-Concern, availability Level-of-Concern, and a description of the factors that determine the system's Protection Level, integrity Level-of-Concern, and availability Level-of-Concern.

4.B.2.b(2) **[Doc2] Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.**

4.B.2.b(3) **[Doc3] The DAA may direct that documentation also shall include:**

4.B.2.b(3)(a) **Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level.**

4.B.2.b(3)(b) **Reports of test results.**

4.B.2.b(3)(c) **A general user's guide that describes the protection mechanisms provided and that supplies guidelines on how the mechanisms are to be used and how they interact.**

4.B.2.b(4) [SysAssur1] System Assurance shall include:

4.B.2.b(4)(a) Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware.

4.B.2.b(4)(b) Features or procedures for protection of the operating system from improper changes.

4.B.2.b(5) **[SysAssur2] System Assurance shall include:**

4.B.2.b(5)(a) **Control of access to the Security Support Structure (i.e., the hardware, software, and firmware that perform operating system or security functions).**

4.B.2.b(5)(b) **Assurance of the integrity of the Security Support Structure.**

4.B.2.b(6) **[Test2] The ISSM shall provide written verification to the DAA that the system operates in accordance with the approved SSP, and that the security features, including access controls, configuration management, and discretionary access controls, are implemented and operational.**

4.B.2.b(7) **[Test3] Additional testing, at the discretion of the DAA.**

4.B.2.b(7)(a) **Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.**

4.B.2.b(7)(b) **A test plan and procedures shall be developed and include:**

4.B.2.b(7)(b)(1) **A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability.**

4.B.2.b(7)(b)(2) **A detailed description of the assurances that have been implemented, and how this implementation will be verified.**

4.B.2.b(7)(b)(3) **An outline of the inspection and test procedures used to verify this compliance.**

4.B.3 **Protection Level 3**

4.B.3.a A system operating at Protection Level 3 shall employ the following features:

4.B.3.a(1) [Access1] Access control, including:

4.B.3.a(1)(a) Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

4.B.3.a(1)(b) Procedures for controlling access by users and maintainers to IS resources, including those that are at remote locations.

4.B.3.a(2) [Access2] Access Control, including a Discretionary Access Control (DAC) Policy. A system has implemented DAC when the Security Support Structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The DAC policy includes administrative procedures to support the policy and its mechanisms. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest [COIs], encryption) shall allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The DAC mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

4.B.3.a(3) **[Access3] Access Control, including:**

4.B.3.a(3)(a) **Some process or mechanism(s) that allows users (or processes acting on their behalf) to determine the formal access approvals (e.g., compartments into which users are briefed) granted to another user. This process or mechanism is intended to aid the user in determining the appropriateness of information exchange.**

4.B.3.a(3)(b) **Some process or mechanism(s) that allow users (or processes acting on their behalf) to determine the sensitivity level (i.e., classification level, classification category, and handling caveats) of data. This process or mechanism is intended to aid the user in determining the appropriateness of information exchange.**

4.B.3.a(4) [AcctMan] Account Management procedures that include:

4.B.3.a(4)(a) Identifying types of accounts (individual and group, conditions for group membership, associated privileges).

4.B.3.a(4)(b) Establishing an account (i.e., required paperwork and processes).

4.B.3.a(4)(c) Activating an account.

4.B.3.a(4)(d) Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators).

4.B.3.a(4)(e) Terminating an account (i.e., processes and assurances).

4.B.3.a(5) [Audit1] Auditing procedures, including:

4.B.3.a(5)(a) Providing the capability to ensure that all audit records include enough information to allow the ISSO to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

4.B.3.a(5)(b) Protecting the contents of audit trails against unauthorized access, modification, or deletion.

4.B.3.a(5)(c) Maintaining collected audit data at least 12 months or one security review cycle, whichever is longer, and reviewing at least weekly.

4.B.3.a(5)(d) The system's creating and maintaining an audit trail that includes selected records of:

4.B.3.a(5)(d)(1) Successful and unsuccessful logons and logoffs.

4.B.3.a(5)(d)(2) Accesses to security-relevant objects and directories, including opens, closes, modifications, and deletions.

4.B.3.a(5)(d)(3) Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.

4.B.3.a(6) [Audit3] Audit procedures that include the existence and use of audit reduction and analysis tools.

4.B.3.a(7) **[Audit4] An audit trail, created and maintained by the IS, that is capable of recording changes to the mechanism's list of user formal access permissions. (NOTE: Applicable only if the [Access3] access control mechanism is automated.)**

4.B.3.a(8) **[Audit5] Auditing procedures, including:**

4.B.3.a(8)(a) **Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual).**

4.B.3.a(8)(b) **Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion. These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.**

4.B.3.a(9) [I&A2] An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified:*

[*Alternative controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternative methods may have similar requirements. For example, the electronically stored version of biometric authentication patterns needs to be protected, as do password authenticators.]

4.B.3.a(9)(a) Initial authenticator content and administrative procedures for initial authenticator distribution.

4.B.3.a(9)(b) Individual and Group authenticators. (Group authenticators may only be used in conjunction with the use of an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator).

4.B.3.a(9)(c) Length, composition, and generation of authenticators.

4.B.3.a(9)(d) Change Processes (periodic and in case of compromise).

4.B.3.a(9)(e) Aging of static authenticators (i.e., not one-time passwords or biometric patterns)

4.B.3.a(9)(f) History of static authenticator changes, with assurance of non-replication of individual authenticators, per direction in approved SSP.

4.B.3.a(9)(g) Protection of authenticators to preserve confidentiality and integrity.

4.B.3.a(10) [I&A4] Identification and Authentication. In those instances where the means of authentication is user-specified passwords, the ISSO or ISSM may employ (under the auspices of the DAA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password.

4.B.3.a(11) **[I&A5] Identification and Authentication. In those instances where the users are remotely accessing the system, the users shall employ a strong authentication mechanism (i.e., an I&A technique that is resistant to replay attacks).**

4.B.3.a(12) [LeastPrv] Least Privilege procedures, including the assurance that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks shall be employed.

4.B.3.a(13) [Marking] Marking procedures and mechanisms to ensure that either the user or the system itself marks all data transmitted or stored by the system to reflect the sensitivity of the data (i.e., classification level, classification category, and handling caveats). Markings shall be retained with the data.

4.B.3.a(14) [ParamTrans] Parameter Transmission. Security parameters (e.g., labels, markings) shall be reliably associated (either explicitly or implicitly) with information exchanged between systems.

4.B.3.a(15) [Recovery] Recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.

4.B.3.a(16) [ResrcCtrl] Resource Control. All authorizations to the information contained within an object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the Security Support Structure's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. There must be no residual data from the former object.

4.B.3.a(17) [ScrnLck] Screen Lock. Unless there is an overriding technical or operational problem, a terminal/desktop/laptop screen-lock functionality shall be associated with each terminal/desktop/laptop computer. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal/desktop/laptop, totally hiding what was previously visible on the screen. Such a capability shall:

4.B.3.a(17)(a) Be enabled either by explicit user action or if the terminal/desktop/laptop is left idle for a specified period of time (e.g., 15 minutes or more).

4.B.3.a(17)(b) Ensure that once the terminal/desktop/laptop security/screen-lock software is activated, access to the terminal/desktop/laptop requires knowledge of a unique authenticator.

4.B.3.a(17)(c) Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

4.B.3.a(18) **[Separation] Separation of Roles. The functions of the ISSO and the system manager/system administrator shall not be performed by the same person.**

4.B.3.a(19) [SessCtrl1] Session Controls, including:

4.B.3.a(19)(a) User notification such that all IS users shall be notified prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible.

4.B.3.a(19)(b) The user shall also be advised that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is prohibited and subject to criminal and civil penalties. Electronic means shall be employed where technically feasible.

4.B.3.a(20) [SessCtrl2] Enforcement of Session Controls, including:

4.B.3.a(20)(a) Procedures for controlling and auditing concurrent logons from different workstations.

4.B.3.a(20)(b) Station or session time-outs, as applicable.

4.B.3.a(20)(c) Limited retry on logon as technically feasible.

4.B.3.a(20)(d) System actions on unsuccessful logons (e.g., blacklisting of the terminal or user identifier).

4.B.3.a(21) [Storage] Data Storage, implementing at least one of the following:

4.B.3.a(21)(a) Information stored in an area approved for open storage* of the information.

[*In the context of storage confidentiality, "approved for open storage" must include consideration of the possibility of access by all users who have direct access to the system or network, wherever physically located.]

4.B.3.a(21)(b) Information stored in an area approved for continuous personnel access control (when continuous personnel access control is in effect), i.e., a 24-hour, 7-day-per week operational area.

4.B.3.a(21)(c) Information secured as appropriate for closed storage.

4.B.3.a(21)(d) Information encrypted using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of stored data.

4.B.3.a(22) [Trans1] Data Transmission.

4.B.3.a(22)(a) Data transmission that implements at least one of the following:

4.B.3.a(22)(a)(1) Information distributed only within an area approved for open storage of the information.

4.B.3.a(22)(a)(2) Information distributed via a Protected Distribution System* (PDS).

[*A PDS provides physical protection or intrusion detection for communications lines. A PDS can also provide need-to-know isolation for communications lines.]

4.B.3.a(22)(a)(3) Information distributed using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of the information.

4.B.3.a(22)(a)(4) Information distributed using a trusted courier.

4.B.3.a(22)(b) Dial-up lines, other than those that are protected with nationally certified cryptographic devices or PDSs, shall not be used for gaining access to system resources that process SAP information unless the DAA provides specific written authorization for a system to operate in this manner.

4.B.3.b **Requirements for system assurance at Protection Level 3.**

4.B.3.b(1) [Doc1] Documentation shall include:

4.B.3.b(1)(a) A System Security Plan (see Appendix C).

4.B.3.b(1)(b) A Security Concept of Operations (CONOPS) (the Security CONOPS may be included in the System Security Plan). The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture, the system's accreditation schedule, the system's Protection Level, integrity Level-of-Concern, availability Level-of-Concern, and a description of the factors that determine the system's Protection Level, integrity Level-of-Concern, and availability Level-of-Concern.

4.B.3.b(2) [Doc2] Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.

4.B.3.b(3) [Doc3] Documentation **shall include:**

4.B.3.b(3)(a) Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level.

4.B.3.b(3)(b) Reports of test results.

4.B.3.b(3)(c) A general user's guide that describes the protection mechanisms provided, and that supplies guidelines on how the mechanisms are to be used, and how they interact.

4.B.3.b(4) [SysAssur1] System Assurance shall include:

4.B.3.b(4)(a) Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware.

4.B.3.b(4)(b) Features or procedures for protection of the operating system from improper changes.

4.B.3.b(5) [SysAssur2] System Assurance shall include:

4.B.3.b(5)(a) Control of access to the Security Support Structure (i.e., the hardware, software, and firmware that perform operating system or security functions).

4.B.3.b(5)(b) Assurance of the integrity of the Security Support Structure.

4.B.3.b(6) **[SysAssur3] System Assurance shall include:**

4.B.3.b(6)(a) **Isolating the Security Support Structure, by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions.**

4.B.3.b(6)(b) **Using up-to-date vulnerability assessment tools to validate the continued integrity of the Security Support Structure by ensuring that the system configuration does not contain any well-known security vulnerabilities.**

4.B.3.b(7) [Test2] The ISSM shall provide written verification to the DAA that the system operates in accordance with the approved SSP, and that the security features, including access controls, configuration management, and discretionary access controls, are implemented and operational.

4.B.3.b(8) **[Test3]** Additional testing.

4.B.3.b(8)(a) Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.

4.B.3.b(8)(b) A test plan and procedures shall be developed and include:

4.B.3.b(8)(b)(1) A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability.

4.B.3.b(8)(b)(2) A detailed description of the assurances that have been implemented, and how this implementation will be verified.

4.B.3.b(8)(b)(3) An outline of the inspection and test procedures used to verify this compliance.

4.B.3.b(9) **[Test4] Testing, as required by the DAA:**

4.B.3.b(9)(a) **Security Penetration Testing shall be conducted to determine the level of difficulty in penetrating the security countermeasures of the system.**

4.B.3.b(9)(b) **An Independent Validation and Verification team shall be formed to assist in the security testing and to perform validation and verification testing of the system.**

4.B.4 **Protection Level 4**

4.B.4.a **A system operating at Protection Level 4 shall employ the following features:**

4.B.4.a(1) [Access1] Access control, including:

4.B.4.a(1)(a) Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

4.B.4.a(1)(b) Procedures for controlling access by users and maintainers to IS resources, including those that are at remote locations.

4.B.4.a(2) [Access2] Access Control, including a Discretionary Access Control (DAC) Policy. A system has implemented DAC when the Security Support Structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The DAC policy includes administrative procedures to support the policy and its mechanisms. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest [COIs], encryption) shall allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The DAC mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

4.B.4.a(3) **[Access4] Access Control, including assurance that each user shall receive from the system only that information to which the user is authorized access.**

4.B.4.a(4) **[Access5] Access Control, including a Mandatory Access Control (MAC) Policy that shall require:**

4.B.4.a(4)(a) **The Security Support Structure to enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices).**

4.B.4.a(4)(b) **These subjects and objects to be assigned sensitivity labels that combine hierarchical classification levels and non-hierarchical categories; the labels shall be used as the basis for mandatory access control decisions.**

4.B.4.a(4)(c) **The Security Support Structure to be able to support two or more such security levels.**

4.B.4.a(4)(d) **Identification and authentication data to be used by the Security Support Structure to authenticate the user's identity and to assure that the security level and authorization of subjects external to the Security Support Structure that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user.**

4.B.4.a(4)(e) **Application of the following restrictions to all accesses between subjects and objects controlled by the Security Support Structure:**

4.B.4.a(4)(e)(1) **A subject can read an object only if the security level of the subject dominates* the security level of the object (i.e., a subject can "read down").**

[*Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the non-hierarchical categories of S1 include all those of S2]

4.B.4.a(4)(e)(2) **A subject can write to an object only if two conditions are met: the security level of the object must dominate the security level of the subject, and the security level of the user's clearance* must dominate the security level of the object (i.e., a subject can "write up," but no higher than the user's clearance).**

[*In those instances where a subject is an electronic entity (e.g., a process), then the subject is generally acting on the behalf of a user]

4.B.4.a(5) [AcctMan] Account Management procedures that include:

4.B.4.a(5)(a) Identifying types of accounts (individual and group, conditions for group membership, associated privileges).

4.B.4.a(5)(b) Establishing an account (i.e., required paperwork and processes).

4.B.4.a(5)(c) Activating an account.

4.B.4.a(5)(d) Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators).

4.B.4.a(5)(e) Terminating an account (i.e., processes and assurances).

4.B.4.a(6) [Audit1] Auditing procedures, including:

4.B.4.a(6)(a) Providing the capability to ensure that all audit records include enough information to allow the ISSO to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

4.B.4.a(6)(b) Protecting the contents of audit trails against unauthorized access, modification, or deletion.

4.B.4.a(6)(c) Maintaining collected audit data at least 12 months or one security review cycle, whichever is longer, and reviewing at least weekly.

4.B.4.a(6)(d) The system's creating and maintaining an audit trail that includes selected records of:

4.B.4.a(6)(d)(1) Successful and unsuccessful logons and logoffs.

4.B.4.a(6)(d)(2) Accesses to security-relevant objects and directories, including opens, closes, modifications, and deletions.

4.B.4.a(6)(d)(3) Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.

4.B.4.a(7) [Audit3] Audit procedures that include the existence and use of audit reduction and analysis tools.

4.B.4.a(8) [Audit5] Auditing procedures, including:

4.B.4.a(8)(a) Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual).

4.B.4.a(8)(b) Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion. **These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.**

4.B.4.a(9) **[Audit6] Auditing procedures, including :**

4.B.4.a(9)(a) **Enforcement of the capability to audit changes in security labels.**

4.B.4.a(9)(b) **Enforcement of the capability to audit accesses or attempted accesses to objects or data whose labels are inconsistent with user privileges.**

4.B.4.a(9)(c) **Enforcement of the capability to audit all program initiations, information downgrades and overrides, and all other security-relevant events (specifically including identified events that may be used in the exploitation of covert channels).**

4.B.4.a(9)(d) **In the event of an audit failure, system shutdown unless an alternative audit capability exists.**

4.B.4.a(10) **[Audit7] Auditing procedures, including:**

4.B.4.a(10)(a) **The capability of the system to monitor occurrences of, or accumulation of, auditable events that may indicate an imminent violation of security policies.**

4.B.4.a(10)(b) **The capability of the system to notify the ISSO of suspicious events and taking the least-disruptive action to terminate the suspicious events.**

4.B.4.a(11) [I&A2] An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified:*

[*Alternative controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternative methods may have similar requirements. For example, the electronically stored version of biometric authentication patterns needs to be protected, as do password authenticators.]

4.B.4.a(11)(a) Initial authenticator content and administrative procedures for initial authenticator distribution.

4.B.4.a(11)(b) Individual and Group authenticators. (Group authenticators may only be used in conjunction with the use of an individual/unique authenticator, that is,

individuals must be authenticated with an individual authenticator prior to use of a group authenticator).

4.B.4.a(11)(c) Length, composition, and generation of authenticators.

4.B.4.a(11)(d) Change Processes (periodic and in case of compromise).

4.B.4.a(11)(e) Aging of static authenticators (i.e., not one-time passwords or biometric patterns)

4.B.4.a(11)(f) History of static authenticator changes, with assurance of non-replication of individual authenticators, per direction in approved SSP.

4.B.4.a(11)(g) Protection of authenticators to preserve confidentiality and integrity.

4.B.4.a(12) [I&A4] Identification and Authentication. In those instances where the means of authentication is user-specified passwords, the ISSO or ISSM may employ (under the auspices of the DAA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password.

4.B.4.a(13) [I&A5] Identification and Authentication. In those instances where the users are remotely accessing the system, the users shall employ a strong authentication mechanism (i.e., an I&A technique that is resistant to replay attacks).

4.B.4.a(14) **[I&A6] Identification and Authentication (I&A) management mechanisms that include:**

4.B.4.a(14)(a) **Implementation and support of a trusted communications path between the user and the Security Support Structure of the desktop for login and authentication. Communication via this path shall be initiated exclusively by the user and shall be unmistakably distinguishable from other paths.**

4.B.4.a(14)(b) **In the case of communication between two or more systems (e.g. client server architecture), bi-directional authentication between the two systems.**

4.B.4.a(15) **[Label1] Labeling procedures, including:**

4.B.4.a(15)(a) **Internal security labels that are an integral part of the electronic data or media.**

4.B.4.a(15)(b) **Procedures for managing content, generation, attachment, and persistence of internal labels that are documented in the SSP.**

4.B.4.a(15)(c) **Security labels that reflect the sensitivity (i.e., classification level, classification category, and handling caveats) of the information.**

4.B.4.a(15)(d) **Maintenance by the Security Support Structure of a record of the kind(s) of data allowed on each communications channel.**

4.B.4.a(15)(e) **A means for the system to ensure that labels a user associates with information provided to the system are consistent with the sensitivity levels that the user is allowed to access.**

4.B.4.a(16) **[Label2] Labeling procedures, including internal and external labeling such as label integrity, exportation, subject-sensitivity labels, and device labels, as applicable.**

4.B.4.a(17) [LeastPrv] Least Privilege procedures, including the assurance that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

4.B.4.a(18) [ParamTrans] Parameter Transmission. Security parameters (e.g., labels, markings) that are reliably associated (either explicitly or implicitly) with information exchanged between systems.

4.B.4.a(19) [Recovery] Recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.

4.B.4.a(20) [ResrcCtrl] Resource Control. All authorizations to the information contained within an object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the Security Support Structure's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. There must be no residual data from the former object.

4.B.4.a(21) [ScrnLck] Screen Lock. Unless there is an overriding technical or operational problem, a terminal/desktop/laptop screen-lock functionality shall be associated with each terminal/desktop/laptop computer. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal/desktop/laptop, totally hiding what was previously visible on the screen. Such a capability shall:

4.B.4.a(21)(a) Be enabled either by explicit user action or if the terminal/desktop/laptop is left idle for a specified period of time (e.g., 15 minutes or more).

4.B.4.a(21)(b) Ensure that once the terminal/desktop/laptop security/screen-lock software is activated, access to the terminal/desktop/laptop requires knowledge of a unique authenticator.

4.B.4.a(21)(c) Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

4.B.4.a(22) [Separation] Separation of Roles. The functions of the ISSO and the system manager/system administrator shall not be performed by the same person.

4.B.4.a(23) [SessCtrl1] Session Controls, including:

4.B.4.a(23)(a) User notification such that all IS users shall be notified prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible.

4.B.4.a(23)(b) The user shall also be advised that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is

prohibited and subject to criminal and civil penalties. Electronic means shall be employed where technically feasible.

4.B.4.a(24) [SessCtrl2] Enforcement of Session Controls, including:

4.B.4.a(24)(a) Procedures for controlling and auditing concurrent logons from different workstations.

4.B.4.a(24)(b) Station or session time-outs, as applicable.

4.B.4.a(24)(c) Limited retry on logon as technically feasible.

4.B.4.a(24)(d) System actions on unsuccessful logons (e.g., blacklisting of the terminal or user identifier).

4.B.4.a(25) [Storage] Data Storage, implementing at least one of the following:

4.B.4.a(25)(a) Information stored in an area approved for open storage* of the information.

[*In the context of storage confidentiality, "approved for open storage" must include consideration of the possibility of access by all users who have direct access to the system or network, wherever physically located.]

4.B.4.a(25)(b) Information stored in an area approved for continuous personnel access control (when continuous personnel access control is in effect), i.e., a 24-hour 7-day-per-week operational area.

4.B.4.a(25)(c) Information secured as appropriate for closed storage.

4.B.4.a(25)(d) Information encrypted using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of stored data.

4.B.4.a(26) [Trans1] Data Transmission.

4.B.4.a(26)(a) Data transmission that implements at least one of the following:

4.B.4.a(26)(a)(1) Information distributed only within an area approved for open storage of the information.

4.B.4.a(26)(a)(2) Information distributed via a Protected Distribution System* (PDS).

[*A PDS provides physical protection or intrusion detection for communications lines. A PDS can also provide need-to-know isolation for communications lines.]

4.B.4.a(26)(a)(3) Information distributed using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of the information.

4.B.4.a(26)(a)(4) Information distributed using a trusted courier.

4.B.4.a(26)(b) Dial-up lines, other than those that are protected with nationally certified cryptographic devices or PDSs, shall not be used for gaining access to system resources that process SAP information unless the DAA provides specific written authorization for a system to operate in this manner.

4.B.4.a(27) **[TranSep] Separation of Data. Information transmissions of different security levels shall be segregated from each other (e.g., encryption, physical separation).**

4.B.4.b **Requirements for system assurance at Protection Level 4.**

4.B.4.b(1) **[CCA] At the discretion of the DAA, a thorough search for covert channels shall be conducted, and a determination shall be made of the maximum bandwidth of each identified channel.**

4.B.4.b(2) [Doc1] Documentation shall include:

4.B.4.b(2)(a) A System Security Plan (see Appendix C).

4.B.4.b(2)(b) A Security Concept of Operations (CONOPS) (the Security CONOPS may be included in the System Security Plan). The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture, the system's accreditation schedule, the system's Protection Level, integrity Level-of-Concern, availability Level of-Concern, and a description of the factors that determine the system's Protection Level, integrity Level-of-Concern, and availability Level-of-Concern.

4.B.4.b(3) [Doc2] Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.

4.B.4.b(4) **[Doc4] Documentation shall include:**

4.B.4.b(4)(a) **Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level.**

4.B.4.b(4)(b) **Reports of test results.**

4.B.4.b(4)(c) **A general user's guide that describes the protection mechanisms provided, and that supplies guidelines on how the mechanisms are to be used, and how they interact.**

4.B.4.b(4)(d) **Documentation, including System Design Documentation, if applicable.**

4.B.4.b(5) [SysAssur1] System Assurance shall include:

4.B.4.b(5)(a) Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware.

4.B.4.b(5)(b) Features or procedures for protection of the operating system from improper changes.

4.B.4.b(6) [SysAssur2] System Assurance shall include:

4.B.4.b(6)(a) Control of access to the Security Support Structure (i.e., the hardware, software, and firmware that perform operating system or security functions).

4.B.4.b(6)(b) Assurance of the integrity of the Security Support Structure.

4.B.4.b(7) [SysAssur3] System Assurance shall include:

4.B.4.b(7)(a) Isolating the Security Support Structure, by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions.

4.B.4.b(7)(b) Using up-to-date vulnerability assessment tools to validate the continued integrity of the Security Support Structure by ensuring that the system configuration does not contain any well-known security vulnerabilities.

4.B.4.b(8) **[SysAssur4] System Assurance. The Security Support Structure shall maintain separate execution domains (e.g., address spaces) for each executing process.**

4.B.4.b(9) [Test2] The ISSM shall provide written verification to the DAA that the system operates in accordance with the approved SSP, and that the security features, including access controls, configuration management, and discretionary access controls, are implemented and operational.

4.B.4.b(10) [Test3] Additional testing.

4.B.4.b(10)(a) Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.

4.B.4.b(10)(b) A test plan and procedures shall be developed and include:

4.B.4.b(10)(b)(1) A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability.

4.B.4.b(10)(b)(2) A detailed description of the assurances that have been implemented, and how this implementation will be verified.

4.B.4.b(10)(b)(3) An outline of the inspection and test procedures used to verify this compliance.

4.B.4.b(11) [Test4] Testing **shall include:**

4.B.4.b(11)(a) Security Penetration Testing to determine the level of difficulty in penetrating the security countermeasures of the system.

4.B.4.b(11)(b) Formation of an Independent Verification and Validation team to assist in the security testing and to perform validation and verification testing of the system.

4.B.5 **Protection Level 5**

4.B.5.a **A system operating at Protection Level 5 shall employ the following features:**

4.B.5.a(1) [Access1] Access control, including:

4.B.5.a(1)(a) Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

4.B.5.a(1)(b) Procedures for controlling access by users and maintainers to IS resources, including those that are at remote locations.

4.B.5.a(2) [Access2] Access Control, including a Discretionary Access Control (DAC) Policy. A system has implemented DAC when the Security Support Structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The DAC policy includes administrative procedures to support the policy and its mechanisms. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest [COIs], encryption) shall allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The DAC mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

4.B.5.a(3) [Access4] Access Control, including assurance that each user shall receive from the system only that information to which the user is authorized access.

4.B.5.a(4) [Access5] Access Control, including a Mandatory Access Control (MAC) Policy that shall require:

4.B.5.a(4)(a) The Security Support Structure to enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices).

4.B.5.a(4)(b) These subjects and objects to be assigned sensitivity labels that combine hierarchical classification levels and non-hierarchical categories; the labels shall be used as the basis for mandatory access control decisions.

4.B.5.a(4)(c) The Security Support Structure to be able to support two or more such security levels.

4.B.5.a(4)(d) Identification and authentication data to be used by the Security Support Structure to authenticate the user's identity and to assure that the security level and authorization of subjects external to the Security Support Structure that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user.

4.B.5.a(4)(e) Application of the following restrictions to all accesses between subjects and objects controlled by the Security Support Structure:

4.B.5.a(4)(e)(1) A subject can read an object only if the security level of the subject dominates* the security level of the object (i.e., a subject can "read down").

[*Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the non-hierarchical categories of S1 include all those of S2.]

4.B.5.a(4)(e)(2) A subject can write to an object only if two conditions are met: the security level of the object must dominate the security level of the subject, and the security level of the user's clearance* must dominate the security level of the object (i.e., a subject can "write up," but no higher than the user's clearance).

[*In those instances where a subject is an electronic entity (e.g., a process), then the subject is generally acting on the behalf of a user.]

4.B.5.a(5) [AcctMan] Account Management procedures that include:

4.B.5.a(5)(a) Identifying types of accounts (individual and group, conditions for group membership, associated privileges).

4.B.5.a(5)(b) Establishing an account (i.e., required paperwork and processes).

4.B.5.a(5)(c) Activating an account.

4.B.5.a(5)(d) Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators).

4.B.5.a(5)(e) Terminating an account (i.e., processes and assurances).

4.B.5.a(6) [Audit1] Auditing procedures, including:

4.B.5.a(6)(a) Providing the capability to ensure that all audit records include enough information to allow the ISSO to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

4.B.5.a(6)(b) Protecting the contents of audit trails against unauthorized access, modification, or deletion.

4.B.5.a(6)(c) Maintaining collected audit data at least 12 months or one security review cycle, whichever is longer, and reviewing at least weekly.

4.B.5.a(6)(d) The system's creating and maintaining an audit trail that includes selected records of:

4.B.5.a(6)(d)(1) Successful and unsuccessful logons and logoffs.

4.B.5.a(6)(d)(2) Accesses to security-relevant objects and directories, including opens, closes, modifications, and deletions.

4.B.5.a(6)(d)(3) Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.

4.B.5.a(7) [Audit3] Audit procedures that include the existence and use of audit reduction and analysis tools.

4.B.5.a(8) [Audit6] Auditing procedures, including:

4.B.5.a(8)(a) Enforcement of the capability to audit changes in security labels.

4.B.5.a(8)(b) Enforcement of the capability to audit accesses or attempted accesses to objects or data whose labels are inconsistent with user privileges.

4.B.5.a(8)(c) Enforcement of the capability to audit all program initiations, information downgrades and overrides, and all other security-relevant events (specifically including identified events that may be used in the exploitation of covert channels).

4.B.5.a(8)(d) In the event of an audit failure, system shutdown unless an alternate audit capability exists.

4.B.5.a(9) **[Audit8] Auditing procedures, including:**

4.B.5.a(9)(a) **Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual).**

4.B.5.a(9)(b) **At least monthly testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion. These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.**

4.B.5.a(10) **[Audit9] Auditing procedures, including:**

4.B.5.a(10)(a) **The capability of the system to monitor, in real-time, occurrences of, or accumulation of, auditable events that may indicate an imminent violation of security policies.**

4.B.5.a(10)(b) **The capability of the system to notify the ISSO of suspicious events and taking the least-disruptive action to terminate the suspicious event.**

4.B.5.a(11) [I&A2] An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified:*

[*Alternative controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternative methods may have similar requirements. For example, the electronically stored version of biometric authentication patterns needs to be protected, as do password authenticators.]

4.B.5.a(11)(a) Initial authenticator content and administrative procedures for initial authenticator distribution.

4.B.5.a(11)(b) Individual and Group authenticators. (Group authenticators may only be used in conjunction with the use of an individual/unique authenticator, that is,

individuals must be authenticated with an individual authenticator prior to use of a group authenticator).

4.B.5.a(11)(c) Length, composition, and generation of authenticators.

4.B.5.a(11)(d) Change Processes (periodic and in case of compromise).

4.B.5.a(11)(e) Aging of static authenticators (i.e., not one-time passwords or biometric patterns)

4.B.5.a(11)(f) History of static authenticator changes, with assurance of non-replication of individual authenticators, per direction in approved SSP.

4.B.5.a(11)(g) Protection of authenticators to preserve confidentiality and integrity.

4.B.5.a(12) [I&A4] Identification and Authentication. In those instances where the means of authentication is user-specified passwords, the ISSO or ISSM may employ (under the auspices of the DAA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password.

4.B.5.a(13) [I&A5] Identification and Authentication. In those instances where the users are remotely accessing the system, the users shall employ a strong authentication mechanism (i.e., an I&A technique that is resistant to replay attacks).

4.B.5.a(14) [I&A6] Identification and Authentication (I&A) management mechanisms that include:

4.B.5.a(14)(a) Implementation and support of a trusted communications path between the user and the Security Support Structure of the desktop for login and authentication. Communication via this path shall be initiated exclusively by the user and shall be unmistakably distinguishable from other paths.

4.B.5.a(14)(b) In the case of communication between two or more systems (e.g. client server architecture), bi-directional authentication between the two systems.

4.B.5.a(15) [Label1] Labeling procedures, including:

4.B.5.a(15)(a) Internal security labels that are an integral part of the electronic data or media.

4.B.5.a(15)(b) Procedures for managing content, generation, attachment, and persistence of internal labels that are documented in the SSP.

4.B.5.a(15)(c) Security labels that reflect the sensitivity (i.e., classification level, classification category, and handling caveats) of the information .

4.B.5.a(15)(d) Maintenance by the Security Support Structure of a record of the kind(s) of data allowed on each communications channel.

4.B.5.a(15)(e) A means for the system to ensure that labels a user associates with information provided to the system are consistent with the sensitivity levels that the user is allowed to access.

4.B.5.a(16) [Label2] Labeling procedures, including internal and external labeling such as label integrity, exportation, subject-sensitivity labels, and device labels, as applicable.

4.B.5.a(17) [LeastPrv] Least Privilege procedures, including the assurance that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

4.B.5.a(18) [ParamTrans] Parameter Transmission. Security parameters (e.g., labels, markings) that are reliably associated (either explicitly or implicitly) with information exchanged between systems.

4.B.5.a(19) [Recovery] Recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.

4.B.5.a(20) [ResrcCtrl] Resource Control. All authorizations to the information contained within an object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the Security Support Structure's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. There must be no residual data from the former object.

4.B.5.a(21) [ScrnLck] Screen Lock. Unless there is an overriding technical or operational problem, a terminal/desktop/laptop screen-lock functionality shall be associated with each terminal/desktop/laptop computer. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal/desktop/laptop, totally hiding what was previously visible on the screen. Such a capability shall:

4.B.5.a(21)(a) Be enabled either by explicit user action or if the terminal/desktop/laptop is left idle for a specified period of time (e.g., 15 minutes or more).

4.B.5.a(21)(b) Ensure that once the terminal/desktop/laptop security/screen-lock software is activated, access to the terminal/desktop/laptop requires knowledge of a unique authenticator.

4.B.5.a(21)(c) Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

4.B.5.a(22) [Separation] Separation of Roles. The functions of the ISSO and the system manager/system administrator shall not be performed by the same person.

4.B.5.a(23) [SessCtrl1] Session Controls, including:

4.B.5.a(23)(a) User notification such that all IS users shall be notified prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible.

4.B.5.a(23)(b) The user shall also be advised that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is prohibited and subject to criminal and civil penalties. Electronic means shall be employed where technically feasible.

4.B.5.a(24) [SessCtrl2] Enforcement of Session Controls, including:

4.B.5.a(24)(a) Procedures for controlling and auditing concurrent logons from different workstations.

4.B.5.a(24)(b) Station or session time-outs, as applicable.

4.B.5.a(24)(c) Limited retry on logon as technically feasible.

4.B.5.a(24)(d) System actions on unsuccessful logons (e.g., blacklisting of the terminal or user identifier).

4.B.5.a(25) [Storage] Data Storage, implementing at least one of the following:

4.B.5.a(25)(a) Information stored in an area approved for open storage* of the information.

[*In the context of storage confidentiality, "approved for open storage" must include consideration of the possibility of access by all users who have direct access to the system or network, wherever physically located.]

4.B.5.a(25)(b) Information stored in an area approved for continuous personnel access control (when continuous personnel access control is in effect), i.e., a 24-hour, 7-day-per week operational area.

4.B.5.a(25)(c) Information secured as appropriate for closed storage.

4.B.5.a(25)(d) Information encrypted using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of stored data.

4.B.5.a(26) [Trans1] Data Transmission.

4.B.5.a(26)(a) Data transmission that implements at least one of the following:

4.B.5.a(26)(a)(1) Information distributed only within an area approved for open storage of the information.

4.B.5.a(26)(a)(2) Information distributed via a Protected Distribution System* (PDS).

[*A PDS provides physical protection or intrusion detection for communications lines. A PDS can also provide need-to-know isolation for communications lines.]

4.B.5.a(26)(a)(3) Information distributed using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of the information.

4.B.5.a(26)(a)(4) Information distributed using a trusted courier.

4.B.5.a(26)(b) Dial-up lines, other than those that are protected with nationally certified cryptographic devices or PDSs, shall not be used for gaining access to system resources that process SAP information unless the DAA provides specific written authorization for a system to operate in this manner.

4.B.5.a(27) [TranSep] Separation of Data. Information transmissions of different security levels shall be segregated from each other (e.g., encryption, physical separation).

4.B.5.b **Requirements for system assurance at Protection Level 5.**

4.B.5.b(1) [CCA] **A thorough search** for covert channels shall be conducted, and a determination shall be made of the maximum bandwidth of each identified channel.

4.B.5.b(2) [Doc1] Documentation shall include:

4.B.5.b(2)(a) A System Security Plan (see Appendix C).

4.B.5.b(2)(b) A Security Concept of Operations (CONOPS) (the Security CONOPS may be included in the System Security Plan). The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture, the system's accreditation schedule, the system's Protection Level, integrity Level-of-Concern, availability Level-of-Concern, and a description of the factors that determine the system's Protection Level, integrity Level-of-Concern, and availability Level-of-Concern.

4.B.5.b(3) [Doc2] Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.

4.B.5.b(4) [Doc4] Documentation shall include:

4.B.5.b(4)(a) Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level.

4.B.5.b(4)(b) Reports of test results.

4.B.5.b(4)(c) A general user's guide that describes the protection mechanisms provided, and that supplies guidelines on how the mechanisms are to be used, and how they interact.

4.B.5.b(4)(d) Documentation, including System Design Documentation, if applicable.

4.B.5.b(5) [SysAssur1] System Assurance shall include:

4.B.5.b(5)(a) Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware.

4.B.5.b(5)(b) Features or procedures for protection of the operating system from improper changes.

4.B.5.b(6) [SysAssur2] System Assurance shall include:

4.B.5.b(6)(a) Control of access to the Security Support Structure (i.e., the hardware, software, and firmware that perform operating system or security functions).

4.B.5.b(6)(b) Assurance of the integrity of the Security Support Structure.

4.B.5.b(7) [SysAssur3] System Assurance shall include:

4.B.5.b(7)(a) Isolating the Security Support Structure, by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions.

4.B.5.b(7)(b) Using up-to-date vulnerability assessment tools to validate the continued integrity of the Security Support Structure by ensuring that the system configuration does not contain any well-known security vulnerabilities.

4.B.5.b(8) [SysAssur4] System Assurance. The Security Support Structure shall maintain separate execution domains (e.g., address spaces) for each executing process.

4.B.5.b(9) [Test2] The ISSM shall provide written verification to the DAA that the system operates in accordance with the approved SSP, and that the security features, including access controls, configuration management, and discretionary access controls, are implemented and operational.

4.B.5.b(10) [Test3] Additional testing.

4.B.5.b(10)(a) Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.

4.B.5.b(10)(b) A test plan and procedures shall be developed and include:

4.B.5.b(10)(b)(1) A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability.

4.B.5.b(10)(b)(2) A detailed description of the assurances that have been implemented, and how this implementation will be verified.

4.B.5.b(10)(b)(3) An outline of the inspection and test procedures used to verify this compliance.

4.B.5.b(11) **[Test5] Testing shall include:**

4.B.5.b(11)(a) **Security Penetration Testing to determine the level of difficulty in penetrating the security countermeasures of the system.**

4.B.5.b(11)(b) **Formation of an Independent Verification and Validation team that at least annually assists in security testing and performing validation and verification testing of the system.**

5 INTEGRITY SYSTEM SECURITY FEATURES AND ASSURANCES

5.A Overview

5.A.1 This chapter provides the detailed integrity* technical security features and assurances. As noted in Chapter 3, the DAA must select the appropriate integrity technical security features and assurances for an IS based on the Integrity Level-of-Concern of the IS.

[*Chapters 4 and 6 provide confidentiality and availability security features and assurances are provided in Chapters 4 and 6, respectively. As noted in Chapter 3, the DAA must ascertain the technical security requirements and assurances for confidentiality, integrity and availability prior to accrediting an IS.]

5.A.2 The chapter separately sets forth the integrity requirements for systems at each of the three Integrity Levels-of-Concern (Basic, Medium, and High).

5.A.3 The underscored terms in brackets preceding the sets of requirements (e.g., [Backup1]) indicate how they are identified in the tabular presentation in Appendix D.

5.A.4 The notations **INTEG-B**, **INTEG-M**, and **INTEG-H** indicate integrity Basic, integrity Medium, and integrity High, respectively.

5.A.5 Requirements listed in **boldface type** are in addition to (or different from) the requirements for the previous Level-of-Concern. Entries for the Basic Level-of-Concern are in **boldface** type because the lowest level is the first entry for a given requirement.

5.B Integrity Requirements

Each IS shall implement security features that will ensure the degree of resistance to unauthorized modification of the information that is commensurate with its determined Integrity Level-of-Concern (see Chapter 3 for more information on Levels-of-Concern). For each IS, assurance commensurate with the Integrity Level-of-Concern shall be provided. Table 5.1 identifies factors used to select the appropriate Integrity Level-of-Concern and cites the paragraphs of this chapter where the relevant requirements can be located.

Table 5.1 - Integrity Level-of-Concern

Level-of-Concern	Integrity Factors	Location In Manual
Basic	Reasonable degree of resistance required against unauthorized modification, or loss of integrity will have an adverse effect.	paragraph 5.B.1
Medium	High degree of resistance required against unauthorized modification, 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.	paragraph 5.B.2
High	Very high degree of resistance required against unauthorized modification, 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.	paragraph 5.B.3

5.B.1 **Integrity - Basic**

5.B.1.a **A system operating at the Basic Level-of-Concern for integrity shall implement the following features:**

5.B.1.a(1) **[Backup1] Backup procedures, including good engineering practice with regard to backup policies and procedures.**

5.B.1.a(2) **[CM1] Configuration Management (CM) that includes:**

5.B.1.a(2)(a) **Policies that assure the effectiveness of storage integrity.**

5.B.1.a(2)(b) **Procedures to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.**

5.B.1.a(3) **[Integrty1] Good engineering practice with regard to COTS integrity mechanisms, such as parity checks and Cyclical Redundancy Checks (CRCs).**

5.B.1.a(4) **[MalCode] Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).**

5.B.1.b **The following assurance shall be provided a system operating at a Basic Level-of-Concern for Integrity:**

5.B.1.b(1) **[Verif1] Verification by the ISSM that the necessary security procedures and mechanisms are in place; testing of them by the ISSM to ensure that they work appropriately.**

5.B.2 **Integrity – Medium**

5.B.2.a **A system operating at the Medium Level-of-Concern for integrity shall implement the following features:**

5.B.2.a(1) **[Backup2] Backup procedures to ensure both the existence of sufficient backup storage capability and effective restoration* of the backup data.**

[*In this context, restoration includes both incremental and complete replacement of the system's contents from the contents of the backup media.]

5.B.2.a(2) **[Backup3] Backup storage that is located to allow the prompt restoration of data. If required by the DAA, there shall additionally be off-site backup storage of data, as per approved SSP; such storage is intended to enable recovery if a single event eliminates both the original data and the on-site backup data. If regular off-site backup is not feasible, such as on a ship at sea, alternative procedures, such as secure transmission of the data to an appropriate off-site location, should be considered.**

5.B.2.a(3) **[Change1] Change Control that includes:**

5.B.2.a(3)(a) **Mechanisms that notify users of the time and date of the last change in data content.**

5.B.2.a(3)(b) **Procedures and technical system features to assure that changes to the data or to security-related items are:**

5.B.2.a(3)(b)(1) **Executed only by authorized personnel.**

5.B.2.a(3)(b)(2) **Properly implemented.**

5.B.2.a(4) [CM1] Configuration Management (CM) that includes:

5.B.2.a(4)(a) Policies that assure the effectiveness of storage integrity.

5.B.2.a(4)(b) Procedures to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.

5.B.2.a(5) **[CM2] Configuration Management that includes:**

5.B.2.a(5)(a) **A CM Plan, including:**

5.B.2.a(5)(a)(1) **Policies that assure storage integrity.**

5.B.2.a(5)(a)(2) **Procedures for identifying and documenting system connectivity, including any software, hardware, and firmware used for all communications (including, but not limited to wireless, IR, etc.).**

5.B.2.a(5)(a)(3) **Procedures for identifying and documenting the type, model, and brand of system or component, security relevant software, hardware, and firmware product names and version or release numbers, and physical locations.**

5.B.2.a(5)(b) **A CM process to implement the CM Plan.**

5.B.2.a(6) **[Integrty2] Data and software storage integrity protection, including the use of strong integrity mechanisms (e.g., integrity locks, encryption).**

5.B.2.a(7) **[Integrty3] Integrity, including the implementation of specific nonrepudiation capabilities (e.g., digital signatures), if mission accomplishment requires non-repudiation.**

5.B.2.a(8) [MalCode] Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).

5.B.2.b **The following assurances shall be provided a system operating at a Medium Level-of-Concern for Integrity:**

5.B.2.b(1) **[Validate] Security Support Structure Validation, including procedures or features to validate, periodically, the correct operation of the hardware, software, and firmware elements of the Security Support Structure.**

5.B.2.b(2) [Verif1] Verification by the ISSM that the necessary security procedures and mechanisms are in place; testing of them by the ISSM to ensure that they work appropriately.

5.B.3 **Integrity - High**

5.B.3.a **A system operating at the High Level-of-Concern for integrity shall implement the following features:**

5.B.3.a(1) **[Backup4] Backup procedures, including:**

5.B.3.a(1)(a) **A capability to conduct backup storage and restoration of data and access controls.**

5.B.3.a(1)(b) **Frequent backups of data.***

[*In this context, frequent means after any significant system hardware, software, or firmware change, and, in any case, no less often than once per year.]

5.B.3.a(1)(c) **At least annual restoration of backup data.**

5.B.3.a(1)(d) **Backup storage that is located to allow the immediate restoration of data. There shall additionally be off-site backup storage of the data, as per approved SSP; such storage is intended to enable recovery if a single event eliminates both the original data and the on-site backup data. If regular off-site backup is not feasible, such as on a ship at sea, alternative procedures, such as secure transmission of the data to an appropriate offsite location, should be considered.**

5.B.3.a(2) [Change1] Change Control that includes:

5.B.3.a(2)(a) Mechanisms that notify users of the time and date of the last change in data content.

5.B.3.a(2)(b) Procedures and technical system features to assure that changes to the data or to security-related items are:

5.B.3.a(2)(b)(1) Executed only by authorized personnel.

5.B.3.a(2)(b)(2) Properly implemented.

5.B.3.a(3) **[Change2] Change Control that includes:**

5.B.3.a(3)(a) **A secure, unchangeable audit trail that will facilitate the correction of improper data changes.**

5.B.3.a(3)(b) **Transaction-based systems (e.g., database management systems, transaction processing systems) that implement transaction roll-back and transaction journaling, or technical equivalents.**

5.B.3.a(4) [CM1] Configuration Management (CM) that includes: Policies that assure the effectiveness of storage integrity.

5.B.3.a(4)(a) Policies that assure the effectiveness of storage integrity.

5.B.3.a(4)(b) Procedures to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.

5.B.3.a(5) [CM2] Configuration Management that includes:

5.B.3.a(5)(a) A CM Plan, including:

5.B.3.a(5)(a)(1) Policies that assure storage integrity.

5.B.3.a(5)(a)(2) Procedures for identifying and documenting system connectivity, including any software, hardware, and firmware used for all communications (including, but not limited to wireless, IR, etc.).

5.B.3.a(5)(a)(3) Procedures for identifying and documenting the type, model, and brand of system or component, security relevant software, hardware, and firmware product names and version or release numbers, and physical locations.

5.B.3.a(5)(b) A CM process to implement the CM Plan.

5.B.3.a(6) **[CM3] Configuration management that includes:**

5.B.3.a(6)(a) **A CM process to test, and verify the CM Plan periodically.**

5.B.3.a(6)(b) **A CM control board, which includes the ISSM/ISSO as a member.**

5.B.3.a(6)(c) **A verification process that assures it is neither technically nor procedurally feasible to make changes to the Security Support Structure outside of the CM process.**

5.B.3.a(7) [Integrty2] Data and software storage integrity protection, including the use of strong integrity mechanisms (e.g., integrity locks, encryption).

5.B.3.a(8) [Integrty3] Integrity, including the implementation of specific nonrepudiation capabilities (e.g., digital signatures), if mission accomplishment requires non-repudiation.

5.B.3.a(9) [MalCode] Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).

5.B.3.a(10) **[Recovery] Recovery procedures and technical system features that assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.**

5.B.3.a(11) **[Trans2] Data Transmission, including:**

5.B.3.a(11)(a) **Integrity mechanisms adequate to assure the integrity of all transmitted information (including labels and security parameters).**

5.B.3.a(11)(b) **Mechanisms to detect or prevent the hijacking of a communication session (e.g., encrypted communication channels).**

5.B.3.b **The following assurances shall be provided for a system operating at a High Level-of-Concern for Integrity:**

5.B.3.b(1) **[SysIntgr1] System Integrity that includes the isolation of the Security Support Structure, by means of partitions, domains, etc., including control of**

access to, and integrity of, hardware, software, and firmware that perform security functions.

5.B.3.b(2) **[SysIntgr2] System Integrity, such that the Security Support Structure maintains separate execution domains (e.g., address spaces) for each executing process.**

5.B.3.b(3) [Validate] Security Support Structure Validation that includes procedures or features to validate, periodically, the correct operation of the hardware, software, and firmware elements of the Security Support Structure.

5.B.3.b(4) **[Verif2] Verification by the DAA Rep** that the necessary security procedures and mechanisms are in place; testing of them by **the DAA Rep** to ensure that they work appropriately.

6 AVAILABILITY SYSTEM SECURITY FEATURES AND ASSURANCES

6.A Overview

6.A.1 This chapter provides the detailed availability* technical security features and assurances. As noted in Chapter 3, the DAA must select the appropriate availability technical security features and assurances for an IS based on the Availability Level-of-Concern of the IS.

[*Chapters 4 and 5 provide confidentiality and integrity security features and assurances, respectively. As noted in Chapter 3, the DAA must ascertain the technical security requirements and assurances for confidentiality, integrity and availability prior to accrediting an IS.]

6.A.2 This chapter separately sets forth the availability requirements for systems at each of the three Availability Levels-of-Concern (Basic, Medium, and High).

6.A.3 The underscored terms in brackets preceding the sets of requirements (e.g., [Verif1]) indicate how they are identified in the tabular presentation in Appendix D.

6.A.4 The notations **AVAIL-B**, **AVAIL-M** and **AVAIL-H** indicate availability Basic, availability Medium, and availability High, respectively.

6.A.5 Requirements listed in **boldface type** are in addition to (or different from) the requirements for the previous Level-of-Concern. Entries for the Basic Level-of-Concern are all in **boldface** type because the lowest level is the first entry for a given requirement.

6.B Availability Requirements

Each IS shall implement security features that will ensure information is available for use when, where, and in the form required, commensurate with its determined Availability Level-of-Concern (see Chapter 3 for more information on Levels-of-Concern). For each IS, assurance commensurate with the Level-of-Concern for Availability shall be provided. Table 6.1 identifies factors used to select the appropriate Availability Level-of-Concern and cites the paragraphs of this chapter where the relevant requirements can be located.

Table 6.1 - Availability Level-of-Concern

Level-of-Concern	Availability Factors	Location In Manual
Basic	Information must be available with flexible tolerance for delay[1], or loss of availability will have an adverse effect.	Paragraph 6.B.1
Medium	Information must be readily available with minimum tolerance for delay[2], or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.	paragraph 6.B.2
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.	paragraph 6.B.3

Notes

1. In this context, "flexible tolerance for delay" means that routine system outages do not endanger mission accomplishment; however, extended system outages (days to weeks) may endanger the mission.
2. In this context, "minimum tolerance for delay" means that mission accomplishment requires retrieval of the information from *this* system in a short time (seconds to hours).

6.B.1 Availability - Basic

6.B.1.a A system operating at the Basic Level-of-Concern for Availability shall implement the following features:

6.B.1.a(1) [Avail] Processes and procedures to allow for the restoration* of the system.

[*Restoration of service is a necessary function to guard against both natural disasters and denial-of-service attacks.]

6.B.1.a(2) [Backup1] Backup procedures, including good engineering practice with regard to backup policies and procedures.

6.B.1.b The following assurances shall be provided for a system operating at a Basic Level-of-Concern for Availability:

6.B.1.b(1) [Verif1] Verification by the ISSM that the necessary security procedures and mechanisms are in place; testing of them by the ISSM to ensure that they work appropriately.

6.B.2 **Availability - Medium**

6.B.2.a **A system operating at the Medium Level-of-Concern for Availability shall implement the following features:**

6.B.2.a(1) [Avail] Processes and procedures to allow for the restoration* of the system.

[*Restoration of service is a necessary function to guard against both natural disasters and denial-of-service attacks.]

6.B.2.a(2) **[Backup3] Backup storage that is located to allow the prompt restoration of data. If required by the DAA, there shall additionally be off-site backup storage of the data, as per approved SSP; such storage is intended to enable recovery if a single event eliminates both the original data and the on-site backup data. If regular off-site backup is not feasible, as, for example, on a ship at sea, alternative procedures, such a secure transmission of the data to an appropriate off-site location, should be considered.**

6.B.2.a(3) **[Backup5] Backup procedures to allow the restoration of operational capabilities with minimal loss of service or data. These procedures shall require:**

6.B.2.a(3)(a) **Frequent backups of data.**

6.B.2.a(3)(b) **To the extent deemed necessary by the DAA, assurance that the system state after the restore will reflect the security-relevant changes to the system between the backup and the restore.**

6.B.2.a(3)(c) **Assurance that the availability of information in storage is adequate for all operational situations, and that catastrophic damage to any single storage entity will not result in system-wide loss of information. These policies shall include, among others, procedures for ensuring the physical protection of operational and backup media and equipment, and for ensuring the continued functionality of the operational and backup media and equipment.**

6.B.2.a(3)(d) **Restoration of any security-relevant segment of the system state (e.g., access control lists, cryptologic keys, deleted system status information) without requiring destruction of other system data.**

6.B.2.a(4) **[Commun] Communications capability that provides adequate communications to accomplish the mission when the primary operations communications capabilities are unavailable.**

6.B.2.a(5) **[Maint] Maintenance procedures that include preventive maintenance, scheduled to maximize the availability of the system, and thus to minimize interference with the operation of the system. Planning for maintenance shall include at least:**

6.B.2.a(5)(a) **On-call maintenance.**

6.B.2.a(5)(b) **On-site diagnostics.**

6.B.2.a(5)(c) **Control of Remote Diagnostics, where applicable. (See paragraph 8.B.8.d, below, for a discussion of remote diagnostics.)**

6.B.2.a(6) **[Power1] System Availability, including, by default for a multi-user system, conditioned, battery-backed power adequate to allow the system to be fail-soft. If the system is multi-user, the decision not to use an Uninterruptible Power Supply (UPS) for the system shall be explicit.**

6.B.2.a(7) **[Power2] System Availability, including, as required by the DAA, procedures for graceful transfer of the system to an alternate power source; these procedures shall ensure that the transfer is completed within the timing requirements of the application(s) on the system.**

6.B.2.a(8) **[Recovery] Recovery procedures and technical system features that assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.**

6.B.2.b **The following assurances shall be provided for a system operating at a Medium Level-of-Concern for Availability:**

6.B.2.b(1) **[Cont1] Contingency Planning that includes a Contingency/Disaster Recovery Plan.**

6.B.2.b(2) [Verif1] Verification by the ISSM that the necessary security procedures and mechanisms are in place; testing by the ISSM to ensure that they work appropriately.

6.B.3 **Availability - High**

6.B.3.a **A system operating at the High Level-of-Concern for Availability shall implement the following features:**

6.B.3.a(1) [Avail] Processes and procedures to allow for the restoration* of the system.

[*Restoration of service is a necessary function to guard against both natural disasters and denial-of-service attacks.]

6.B.3.a(2) **[Backup4] Backup procedures, including:**

6.B.3.a(2)(a) **A capability to conduct backup storage and restoration of data.**

6.B.3.a(2)(b) **Frequent backups of data.***

[*In this context, frequent means after any significant system hardware, software, or firmware change, and, in any case, no less often than once per year.]

6.B.3.a(2)(c) **At least annual restoration of backup data.**

6.B.3.a(2)(d) **Backup storage that is located to allow the immediate restoration of data. There shall additionally be off-site backup storage of the data, as per approved SSP; such storage is intended to enable recovery if a single event eliminates both the original and the on-site, backup data. If regular off-site backup is not feasible, as, for example, on a ship at sea, alternative procedures such as secure transmission of the data to an appropriate offsite location, should be considered.**

6.B.3.a(3) [Backup5] Backup procedures to allow the restoration of operational capabilities with minimal loss of service or data. These procedures shall require:

6.B.3.a(3)(a) Frequent backups of data.

6.B.3.a(3)(b) To the extent deemed necessary by the DAA, assurance that the system state after the restore will reflect security-relevant changes to the system between the backup and the restore.

6.B.3.a(3)(c) Assurance that the availability of information in storage is adequate for all operational situations, and that catastrophic damage to any single storage entity will not result in system-wide loss of information. These policies shall include, among others, procedures for ensuring the physical protection of operational and backup media and equipment, and for ensuring the continued functionality of the operational and backup media and equipment.

6.B.3.a(3)(d) Restoration of any security-relevant segment of the system state (e.g., access control lists, cryptologic keys, deleted system status information) without requiring destruction of other system data.

6.B.3.a(4) **[Backup6] Backup procedures, including:**

6.B.3.a(4)(a) **Assurance that the system state after the restore will reflect security-relevant changes to the system between the backup and the restore.**

6.B.3.a(4)(b) **Consideration to the use of technical features that enhance data integrity and availability including, among others, remote journaling, Redundant Array of Inexpensive Disks (RAID) 1 and above, and similar techniques.**

6.B.3.a(5) [Commun] Communications capability that provides adequate communications to accomplish the mission when the primary operations communications capabilities are unavailable.

6.B.3.a(6) **[DOS] Prevention of Denial of Service Attacks.* Where technically feasible, procedures and mechanisms shall be in place to curtail or prevent well-known, detectable, and preventable denial of service attacks (e.g., SYN attack).**

[*Only a limited number of denial-of-service attacks are detectable and preventable. Often, prevention of such attacks is handled by a controlled interface. (See Chapter 7 for a discussion on controlled interfaces.)]

6.B.3.a(7) [Maint] Maintenance procedures that include preventive maintenance, scheduled to maximize the availability of the system, and so minimize interference with the operation of the system. Planning for maintenance shall include at least:

6.B.3.a(7)(a) On-call maintenance.

6.B.3.a(7)(b) On-site diagnostics.

6.B.3.a(7)(c) Control of Remote Diagnostics, where applicable. (See paragraph 8.B.8.d, below, for a discussion of remote diagnostics.)

6.B.3.a(8) **[Monit] Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.**

6.B.3.a(9) [Power1] System Availability, including, by default for a multi-user system, conditioned, battery-backed power adequate to allow the system to be fail-soft. If the system is multi-user, the decision not to use an Uninterruptible Power Supply (UPS) for the system shall be explicit.

6.B.3.a(10) [Power2] System Availability, including procedures for graceful transfer of the system to an alternate power source; these procedures shall ensure that the transfer is completed within the timing requirements of the application(s) on the system.

6.B.3.a(11) **[Priority] Priority protection that includes no "Deny Up" (i.e., a lower priority process shall not be able to interfere with the system's servicing of any higher-priority process).**

6.B.3.a(12) [Recovery] Recovery procedures and technical system features that assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.

6.B.3.b **The following assurances shall be provided for a system operating at a High Level-of-Concern for Availability:**

6.B.3.b(1) [Cont1] Contingency Planning that includes a Contingency/Disaster Recovery Plan.

6.B.3.b(2) **[Cont2] Contingency Planning, including:**

6.B.3.b(2)(a) **Adequate hardware, firmware, software, power, and cooling to accomplish the mission when the operational equipment is unavailable. Consideration shall be given to fault-tolerant or "hotbackup" operations. The decision whether or not to use these techniques shall be explicit.**

6.B.3.b(2)(b) **Regular exercising and testing of the contingency plans. The plans for the tests shall be documented in the Contingency/Disaster Recovery Plan.**

6.B.3.b(3) **[Verif2] Verification by the DAA Rep that the necessary security procedures and mechanisms are in place; testing by the DAA Rep to ensure that they work appropriately.**

7 REQUIREMENTS FOR INTERCONNECTED ISs AND ADVANCED TECHNOLOGY

7.A Overview

This chapter discusses the security requirements for safeguarding interconnected information systems, and for safeguarding information systems that employ advanced technologies such as such as World Wide Web servers, mobile code, electronic mail, or collaborative computing.

7.A.1 An interconnected IS is composed of *separately accredited* ISs. Each self-contained IS maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating IS has its own ISSO.

7.A.1.a Interconnected ISs shall have a mechanism capable of adjudicating the different security policy implementations of the participating ISs.

7.A.1.b Interconnected ISs require accreditation that explicitly addresses their interconnectivity (see Chapter 9 for discussion and definition of accreditation).

7.A.2 When connecting two or more ISs, the DAA(s) shall review the security attributes of each system to determine whether the combination of data or the combination of users who have access to the interconnected ISs necessitates a higher level of security requirements. DAA(s) shall explicitly make this determination, even if the systems are accredited at the same level of technical requirements.

7.A.3 The characteristics and capabilities of interconnected ISs require special security considerations (e.g., controlling the flow of information into or out of an interconnected IS). This chapter introduces *additional* requirements for interconnected ISs and expands on the security requirements stated in Chapters 4, 5, and 6 as they apply to interconnected ISs.

7.A.4 Many environments employ technologies such as World Wide Web servers, mobile code, electronic mail, or collaborative computing to accomplish their mission. Such technologies may be employed across interconnected ISs to enhance inter-system services, or within an IS to enhance intra-system services. These technologies have security ramifications that are not always readily handled by the requirements provided in Chapters 4, 5, and 6. This chapter introduces *additional* security requirements for such technology and expands upon the security requirements in Chapters 4, 5, and 6 as they apply to such technologies.

7.B Controlled Interface

7.B.1 Controlled Interface Overview

7.B.1.a A *Controlled Interface* is a mechanism that facilitates adjudicating the security policies of different interconnected ISs (e.g., controlling the flow of information into or out of an interconnected IS). Controlling the flow of information into an interconnected IS helps preserve the integrity of the IS, and the integrity and confidentiality of the information maintained and processed by the IS. Controlling the flow of information out of the IS* helps preserve the confidentiality of the information leaving the IS, and may protect the integrity of the receiving ISs. The

adjudication of integrity and confidentiality policies may be handled in a variety of ways. For example:

[*Controlled Interfaces that control the flow of information out of an IS are often employed to facilitate push technology, where the goal is to push information to an indirect user residing outside of the IS perimeter, but within the IS boundary.]

7.B.1.a(1) A single Controlled Interface may perform all of the confidentiality and integrity adjudication; or

7.B.1.a(2) One Controlled Interface may be employed for adjudicating confidentiality policies while another adjudicates integrity policies; or

7.B.1.a(3) The adjudication of confidentiality and integrity policies may be distributed across a set of Controlled Interfaces where each performs some subset of confidentiality and integrity policy adjudication. In this instance, the set of Controlled Interfaces adjudicates all of the required integrity and confidentiality policies.

7.B.1.b While a Controlled Interface is often implemented as a mechanism (or a set of mechanisms) separate from the ISs it is intended to protect, this need not be the case. A Controlled Interface can be constructed so that some of its functionality resides in the ISs themselves. Regardless of its implementation, the Controlled Interface must conform to the requirements provided below.

7.B.2 Common Controlled Interface Requirements

7.B.2.a The DAA shall ensure that:

7.B.2.a(1) Mechanisms or procedures exist to prohibit general users from modifying the functional capabilities of the Controlled Interface.

7.B.2.a(2) Automated mechanisms are employed that can monitor the Controlled Interface for symptoms of failure or compromise. The mechanisms shall be protected against failure or compromise.

7.B.2.a(3) The Controlled Interface is physically protected.

7.B.2.b Routing information, employed for either controlling the release of outgoing information or the delivery of incoming information, shall be supplied or alterable only by the Security Support Structure of the Controlled Interface.

7.B.2.c Each Controlled Interface shall be configured and located to facilitate its ability to provide controlled communication between the interconnected systems.

7.B.2.d Each Controlled Interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited.

7.B.2.e Each Controlled Interface shall be tested to ensure that it satisfies all of the appropriate Controlled Interface criteria listed in this chapter.

7.B.2.f The Controlled Interface shall be included in a configuration management program. Security policies, procedures, etc., shall be documented.

7.B.2.g Recovery procedures and technical system procedures will be in place to assure that recovery of the Controlled Interface is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.

7.B.2.h The Controlled Interface shall implement data and software storage integrity, to include to the use of strong storage integrity mechanisms (e.g. controls that track and report changes to security configurations files).

7.B.2.i Safeguards shall be provided to assure that users cannot circumvent technical controls.

7.B.2.j All direct user access to the Controlled Interface shall be audited.

7.B.2.k Remote administration of the Controlled Interface is discouraged. All remote administration of Controlled Interfaces requires written approval of the DAA. If remote administration is employed, the session must be protected through the use of the following techniques:

7.B.2.k(1) Strong authentication, *and either*

7.B.2.k(2) Physically separate communications paths, *or*

7.B.2.k(3) Logically separated communications paths based upon either

7.B.2.k(3)(a) NSA-approved encryption; *or*

7.B.2.k(3)(b) NSA-approved encryption and DAA-approved privacy encryption to provide privacy of the remote administration session.

7.B.2.k(4) Direct user access to the Controlled Interface shall require strong authentication.

7.B.2.k(5) The requirements imposed upon Controlled Interfaces do not release the DAA, ISSO, or ISSM of the obligation to ensure that the ISs comprising the interconnected IS provide the required security functionality.

7.B.2.k(6) The introduction of a Controlled Interface does not impact the determination of the Protection Level or Levels-of-Concern of the ISs comprising the interconnected IS.

7.B.3 Controlled Interface Confidentiality Requirements

7.B.3.a A Controlled Interface shall be *required* for facilitating the adjudication of confidentiality policies if:

7.B.3.a(1) The two interconnected ISs are approved to process information of different classifications; and

7.B.3.a(2) Neither interconnected IS is operating at Protection Level 4 or 5.

7.B.3.b A Controlled Interface shall be *required* for facilitating the adjudication of confidentiality policies if:

7.B.3.b(1) The compartments, sub-compartments, caveats, control markings, or special handling of information processed by one interconnected IS is different than the compartments, sub-compartments, caveats, control markings, or special handling of information processed by the other interconnected IS; and

7.B.3.b(2) Neither interconnected IS is operating at Protection Levels 3, 4, or 5.

7.B.3.c At a minimum,* the following confidentiality policy adjudication features shall be provided:

[*One circumstance in which additional security requirements should be considered involves the IS receiving information via the Controlled Interface, which in turn is directly connected to another system accessible by a user holding a lower clearance. This topic is further discussed in paragraph 9.D.3.c(1).]

7.B.3.c(1) Traffic Review. Review the classification of all outgoing (i.e., going outside of the interconnected IS perimeter) traffic based on associated security labels (where provided) or data content (if applicable) before being released. If labels are used, the Controlled Interface must maintain the integrity of the labels.

7.B.3.c(2) Controlled Release. Ensure that only traffic that is explicitly permitted (based on traffic review) is released from the perimeter of the interconnected IS.

7.B.3.c(3) Encryption. Encrypt (as needed) all outgoing communication (including the body and attachment of the communication) with the appropriate level of encryption for the information, transmission medium, and target system.

7.B.3.c(4) Protection. Ensure that users and processes in a lower protection domain are prevented from accessing information for which they are not authorized that resides in a higher domain. In addition, when information at a higher security level is made available to a lower security level, the information shall be protected and maintained at the higher security level until it satisfies the traffic review and controlled release requirements described above.

7.B.3.c(5) Audit/Logging. Log all data release activities, to include identity of releaser, identity of recipient, identity of data released, device identifier (id) (e.g., port id), time, and date of release, modification, or application of security labels.

7.B.3.c(6) Fail-secure. Ensure that the operational failure of the Controlled Interface does not result in any unauthorized release of information outside of the IS perimeter.

7.B.3.d The Availability Level-of-Concern of each Confidentiality Controlled Interface shall be at least as high as the lowest Availability Level-of-Concern level of the interconnected ISs.

7.B.3.e In addition to the requirements imposed upon the Controlled Interface, each interconnected IS that is receiving information shall:

7.B.3.e(1) Be accredited to process the level(s) and compartment(s) of information that it receives.

7.B.3.e(2) Provide the features and assurances necessary to ensure that information received is made available only to those authorized to receive the information.

7.B.3.f The security requirements imposed upon Confidentiality Controlled Interfaces are less stringent than those imposed upon PL4 or PL5 systems because Confidentiality Controlled Interfaces are more constrained in their operation and function than complete ISs. The information that flows through the Controlled Interface is generally push only or pull only. In those instances where the Controlled Interface supports both push and pull capabilities, some other constraint limits the bandwidth or format of information flowing through (e.g., information may be limited to a fixed format, or users may be limited to a set of fixed-format queries). Where information is flowing between systems approved to process different security levels or compartments and the information flow is not constrained in some manner similar to that described above, then the requirements of PL3, PL4, or PL5 as appropriate shall be applied.

7.B.4 Controlled Interface Integrity Requirements

7.B.4.a A Controlled Interface facilitating the adjudication of integrity policies shall control all information flows into an interconnected IS. The Controlled Interface shall be required regardless of (1) the Protection Level of the systems comprising the IS; or (2) the Protection Level of the systems comprising the interconnected systems with which it communicates.

7.B.4.b At a minimum,* the following integrity policy adjudication features shall be provided:

[*One circumstance in which additional security requirements should be considered involves the IS sending information to the Controlled Interface, which in turn is directly connected to another system accessible by users holding a lower clearance. This topic is further discussed in paragraph 9.D.3.c(1).]

7.B.4.b(1) Malicious code screening.* Review incoming information for viruses and other malicious code as feasible.

[*Having the Controlled Interface review incoming information for malicious code does not relieve the receiving IS from the responsibility of also checking for malicious code.]

7.B.4.b(2) Delivery. Ensure that incoming communications have an authorized user (and, as applicable, authorized addresses) as a destination.

7.B.4.b(3) Filtering. Support and filter communications protocols/services from outside the perimeter of the interconnected IS according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications).

7.B.4.b(4) Proxies. Support, as appropriate, protocol-mediation software (i.e., proxies) that are able to understand and take protective action based on applicationlevel protocols and associated data streams (e.g., filtering FTP connections to deny the use of the put command, effectively prohibiting the ability to write to an anonymous FTP server).

7.B.4.b(5) Extensibility. Where appropriate, provide security support for the incorporation of additional system services as they become available.

7.B.4.b(6) Auditing/Logging. Log data communications into the interconnected IS, to include identity of sender (e.g., person, end-system), identity of recipient (e.g., IP address, host and user), device id (e.g., port id), data, time, and event.

7.B.4.b(7) Fail-secure. Ensure that in the event of the operational failure of the Controlled Interface, no information external to the interconnected IS shall enter the IS.

7.B.4.c The Availability Level-of-Concern of each Integrity Controlled Interface shall be at least as high as the Availability Level-of-Concern of the IS into which the information flows are directed.

7.B.5 Controlled Interface Platform Protection Requirements. Unless the DAA provides a written exemption, the platform underlying the Controlled Interface mechanism must be able to isolate and protect the Controlled Interface application.

7.C Web Security

7.C.1 Overview

7.C.1.a Web technology is that part of network communications in which the parties communicate through the use of the HyperText Transfer Protocol (HTTP) (or some variant).

7.C.1.b Many organizations are employing Web technology (i.e., HTTP Web servers and clients) to establish *intranets* and *extranets*. An *intranet* is a Web communications system established within limited confines of a given enterprise (e.g., internal to a given business or agency). An *extranet* is private network using Web technology to share part of an enterprise's information or operations with suppliers, vendors, partners, customers or other enterprises. The technology employed in intranets and extranets is the same as that employed in the larger World Wide Web, but is confined (usually by controlled interfaces such as firewalls) to a limited audience.

7.C.1.c Because the Web technology is an enhanced form of network communications, many of the security requirements stated elsewhere in this manual apply directly to the use of Web technology. For example, NSA-approved encryption technology would be required to prevent the exposure of classified information to individuals who are not cleared for the information (see paragraphs 1.G.1 and 1.G.2).

7.C.2 Securing Web Clients

7.C.2.a Because of the power of Web technology, the Web client and associated workstation must be appropriately configured and secured. It is particularly important to be sensitive to combinations of unclassified data that in aggregate reveal classified information, and to combinations of information classified at one level that in aggregate reveal more highly classified information.

7.C.2.a(1) All certificates* shall be protected via passwords that adhere to DAA guidelines or some DAA-approved biometric mechanism.

[*A certificate is an association between an identity and a public key. Certificates are used as a way to verify the authenticity of an organization or individual.]

7.C.2.a(2) Only DAA-approved certification authorities* shall issue certificates that are installed on ISs that process SAP information.

[*A Certification Authority is an organization that issues public key certificates.]

7.C.2.a(3) If the Web client supports other capabilities (e.g., e-mail, collaborative computing, mobile code) in addition to traditional browser capabilities, then the use of these other capabilities shall be consistent with the appropriate guidelines stated elsewhere in this manual or as called for by the DAA.

7.C.2.b In addition, as Web client updates that address known security flaws become available, the ISSO shall ensure that they are implemented as soon as possible.

7.D Securing Servers

7.D.1 Various technologies such as Web or file transfer protocol (FTP) provide a convenient means for sharing information. Such technologies are examples of push/pull technology, which allow one entity to push information into a location and another entity to pull it from that location. Documents that an organization wishes to share with other organizations could be placed on (pushed out to) an external Web or FTP server (i.e., outside of the organization's IS), and then anyone able to access the server could access (pull off) the information. Documents that an organization wishes to share internally could be placed on an internal Web or FTP server (i.e., within an organization's IS) and then anyone within the organization able to access the server could obtain (pull off) the information.

7.D.2 Because such servers are by their nature relatively accessible, they are potentially subject to attacks that could result in modification or destruction of the operating system, or insertion of malicious code. To address these concerns, unless the DAA provides written permission to do otherwise:

7.D.2.a External servers shall be located external to a site's Controlled Interface (e.g., firewall) or shall be on a network separate from the site's intranet.

7.D.2.b The operating services and programs on servers (external and internal) shall be kept to a minimum, and services that are security risks (e.g., tftp, rlogin, rshell) or not required shall be disabled.

7.D.2.c The system that supports the server functionality shall, as much as possible, be dedicated to that purpose.

7.D.2.d All operating system, protocol and application (e.g., FTP and Web) security patches shall be implemented as soon as possible after they become known and their functionality has been tested.

7.D.2.e Remote access to servers by privileged users requires the use of a strong authentication mechanism, and all such accesses shall be audited.

7.D.3 Servers can be delineated into two broad categories: public (i.e., general access) servers and restricted access servers, described below.

7.D.3.a Public Servers. The information that is placed on a public server shall be limited to general access holdings that can be accessed by anyone who has authorized access to the inter/intranet/LAN on which the server resides. Servers employed as public servers shall implement all of the requirements stated in paragraph 7.D.2, above, and no general user accounts shall be permitted on the server.

7.D.3.b Restricted Access Servers. The information that is placed on a restricted access server is information which should only be accessed by authorized, authenticated users. In addition to the requirements stated in paragraph 7.D.2, above, restricted access servers shall implement the following security requirements:

7.D.3.b(1) The underlying operating system shall satisfy the confidentiality requirements of Protection Level 2 or higher, integrity requirements for Basic Level-of- Concern or higher, and availability requirements for Basic Level-of-Concern or higher.

7.D.3.b(2) Web servers shall implement secure Web technology (e.g., Secure Sockets Layer, Secure HTTP) where capable.

7.D.3.b(3) Strong authentication shall be required for all users accessing the restricted servers, and all such accesses shall be audited.

7.E Mobile Code and Executable Content

7.E.1 *Mobile code* is code obtained from remote systems,* transmitted across a network, and then downloaded onto and executed on a local system. In recent years mobile code has come to refer to Web-based code downloaded onto a user's client and run by the user's browser. Examples of such Web-based mobile code include Java, JavaScript, and ActiveX. The larger set of mobile code normally involves an explicit decision to execute – either by the user or by an application. Examples of mobile code that are directly executed by the user include Perl, Tcl/TK, REXX, Python, Java, and platform-specific executables (e.g., *.com, *.exe). Examples of mobile code that are executed by an application with little or no explicit user action include macros, ActiveX, PostScript and Java.

[*In this instance, a remote system would include any system which is physically separate from another IS, but is able to communicate via some data link. This would include systems connected via internets, intranets, client-server local area networks (LANs), etc.]

7.E.2 *Executable content* is the subset of mobile code that is largely invisible to the user and that operates without a user decision. Executable content consists of code that is referenced or embedded in HyperText Markup Language (HTML) and eXtensible Markup Language (XML) page, or an e-mail message. Typically, executable content is automatically activated upon viewing or loading the containing document, without any specific user interaction. The user may be unaware that a separate executable has been downloaded on the user's machine. Examples of executable content include Java Applets, ActiveX Controls, JavaScript, and VBScript.

7.E.3 Hostile mobile code or executable content could be used to introduce viruses or other malicious code, modify programs and allow unauthorized access to a system, corrupt data, or deny service.

7.E.4 Hostile mobile code or executable content is completely different from more traditional malicious code such as viruses and worms and is not currently detectable by conventional anti-viral software.

7.E.5 Until reliable executable content scanning detection technology* is available (as determined by the DAA) to address the security concerns with regard to mobile code or executable content obtained via the Web, the following requirements apply:

[*Anticipated security enhancements to Web-based mobile code or executable content include mobile code or executable content that is digitally signed (so as to identify the author) and constrained by the browser so that the privileges granted to the mobile code or executable content would be based on who signed the code/content, from where it was downloaded and other factors which could be tailored by an ISSO/M to the needs of the specific environment. Also under development are tools that would search for the signatures of known malicious mobile code or executable content, in a manner analogous to the way current antiviral software detects viruses.]

7.E.5.a All mobile code or executable content employed within an intelligence intranet enclave shall be registered within that enclave unless the DAA authorizes otherwise.

7.E.5.b As feasible, organizations shall implement a code review and quality control process for deployed mobile code or executable content and shall be responsible for the mobile code or executable content that they deploy.

7.E.5.c For those instances where there is no operational need to download mobile code or executable content, the ISSO or appropriate privileged user shall configure the IS or Controlled Interface to prevent the downloading of mobile code or executable content.

7.E.5.d Unless a written exception is granted by the DAA, organizations shall *not* run mobile code or executable content on mission-critical information systems.

7.E.5.e Downloading of mobile code or executable content from a system that processes information of a different classification level shall only be permitted if a Controlled Interface appropriately configured to handle such a download is in place, and with the written approval of the DAA.

7.F Electronic Mail (E-mail)

7.F.1 Encryption and E-Mail. E-mail shall conform to the electronic communications and transmission requirements regarding confidentiality stated elsewhere in this manual. In particular, an e-mail message (and associated attachments) shall be appropriately encrypted if during its transmission it may be accessible to individuals who lack either clearance or formal access approval for the information contained in the e-mail (and associated attachments).

7.F.2 Viruses and E-mail

7.F.2.a The DAA shall ensure that the threat of viruses in e-mail or attachments is addressed.

7.F.2.b Where technically feasible the DAA shall require the use of anti-viral mechanisms to detect and eradicate viruses in incoming and outgoing e-mail and attachments.

7.F.2.c The means employed to address the virus threat shall be stated in the SSP.

7.F.2.d The use of anti-viral procedures and mechanisms to detect and eradicate viruses transported by e-mail or attachments does not relieve the ISSO of ensuring that there are procedures and mechanisms (e.g., central choke points where diskettes are scanned for viruses prior to distribution within the IS) in place to safeguard against virus infection of the IS from other sources.

7.G Collaborative Computing

7.G.1 Collaborative computing allows members of a work group to share electronically any information, applications, and hardware to accomplish group assignments. Examples of collaborative computing mechanisms include shared white boards, application sharing, LAN-based video and audio conferencing, screen sharing, and text chatter. Collaborative computing may be done in either a peer-to-peer manner, in which user workstations act as servers to other group users, or in a client-server manner, in which user workstations connect to a common server where the data sharing is handled.

7.G.2 If not correctly configured, collaborative computing technologies can allow a user to see and hear everything happening at another user's workstation area, or to read, modify, and delete any information on or accessible to a user's workstation.

7.G.3 Until collaborative computing technologies incorporate security capabilities (e.g., I&A, access control, auditing) to the satisfaction of the DAA, the following requirements apply:

7.G.3.a Collaborative computing mechanisms shall be hosted only on systems operating at Protection Levels 1, 2, and 3, and between systems that process information of the same classifications. But hosting collaborative computing mechanisms on systems operating at Protection Level 3 requires the explicit, written approval of the DAA, and the DAA may impose additional technical or other security safeguards as needed.

7.G.3.b Collaborative computing mechanisms shall not be remotely activated. Activation requires an explicit action by the workstation user (e.g., in the case of a desktop video teleconference, the user of the desktop shall be required to take an explicit action to turn on the camera and microphone, remote users shall not be allowed to activate a user's camera or microphone remotely).

7.G.3.c Peer-to-peer collaborative computing mechanisms between systems operating at Protection Level 2 shall be configured to ensure that only the information on the screen is observable to the remote user. Information located elsewhere on the workstation shall not be observable, nor shall the remote user be able to modify or delete any information on the workstation. These restrictions also apply to any other IS to which the user's workstation is logically connected (e.g., any logically mounted disks).

7.G.3.d Collaborative computing mechanisms that provide video and/or audio conference capabilities shall provide some explicit indication that the video and audio mechanisms are operating.

7.G.3.e Running collaborative computing mechanisms on mission-critical systems is discouraged and shall require explicit, written DAA approval.

7.G.3.f The server portion of the client-server collaborative computing mechanism shall authenticate all users or processes acting on their behalf.

7.G.3.g While conducting a collaborative computing session, the user shall take all reasonable measures to ensure that no sensitive information is inadvertently made either audibly or visually accessible to the collaborative computing mechanism. This includes advising all personnel in the immediate area that the collaborative computing mechanism will be operating.

7.G.3.h Once the collaborative session is completed, the user shall immediately take an explicit action to disconnect/terminate the collaborative computing mechanism.

7.G.3.i Users shall not leave the workstation unattended while a peer-to-peer collaborative computing mechanism is in progress.

7.H Distributed Processing

Distributed processing systems can be considered single or network systems, and can be handled in accordance with the guidelines provided in Chapters 4, 5, 6, and 8. Distributed parallel processing occurs when an application on one IS divides a task into two or more parts and then sends the parts to the other ISs on the network for processing. This allows the idle CPU cycles on many ISs to be used for CPU intensive calculations. The results are then sent back to the originating IS for final processing. Distributed parallel processing should be restricted to Protection Level 1 and Basic Level of concern networks, and not be permitted on mission critical systems.

8 ADMINISTRATIVE SECURITY REQUIREMENTS

8.A Overview

The security requirements specified in this chapter are in addition to those identified in Chapters 4, 5, 6, and 7.

8.B Procedural Security

8.B.1 Security Training, Education, and Awareness

8.B.1.a Security education, training, and awareness are essential to a successful IS security program. Employees who are informed of applicable organizational policies and procedures can be expected to act effectively to ensure the security of system resources. Instruction is more effective when targeted to a specific audience. General users require different training than those employees with specialized responsibilities.

8.B.1.b *All* individuals involved in the Certification and Accreditation (C&A) process shall be trained in that process and in its documentation requirements.

8.B.1.b(1) As a minimum, training shall include the following:

8.B.1.b(1)(a) System security regulations and policies (individuals shall have the ability to implement and interpret national and agency/department regulations and policies).

8.B.1.b(1)(b) Common information security technologies and practices.

8.B.1.b(1)(c) Testing and evaluation techniques.

8.B.1.b(1)(d) Risk management concepts.

8.B.1.b(1)(e) Interconnected systems security concepts.

8.B.1.b(1)(f) Procedures for incident handling.

8.B.1.b(1)(g) C&A concepts, policies, and procedures.

8.B.1.b(1)(h) Audit analysis procedures and tools.

8.B.1.b(2) In addition to the requirements specified in 8.B.1.b(1), above, DAAs and DAA Reps shall have the following training:

8.B.1.b(2)(a) General information security orientation. An overview of what is expected of the person in this position, to include: infrastructure, risk management, the responsibility for accepting risks and the consequences, residual risks, basic security requirements, Protection Levels and Levels-of-Concern, C&A process.

8.B.1.b(2)(b) Software protection and validation techniques.

8.B.1.b(3) In addition to the requirements specified in 8.B.1.b(1) above, ISSMs shall have training in the destruction and release procedures for systems, components, and media.

8.B.1.b(4) In addition to the requirements specified in 8.B.1.b(1) above, ISSOs shall have the following training:

8.B.1.b(4)(a) How to implement common information systems security practices and technologies. This training shall include information on support infrastructures, help teams, and organizations that could assist the ISSO.

8.B.1.b(4)(b) How to implement testing and evaluation procedures.

8.B.1.b(4)(c) How to implement configuration management concepts.

8.B.1.b(4)(d) Destruction and release procedures for systems, components, and media.

8.B.1.b(4)(e) Other security disciplines that affect the ISSO's operations.

8.B.1.c The following individuals shall be trained in their responsibilities and those of their subordinates:

8.B.1.c(1) Privileged Users, with training to include:

8.B.1.c(1)(a) How to protect the physical area, media, and equipment (e.g., locking doors, care of diskettes).

8.B.1.c(1)(b) How to protect authenticators and operate the applicable system security features.

8.B.1.c(1)(c) Security consequences and costs so that security can be factored into their decisions (manager).

8.B.1.c(1)(d) How to implement and use specific access control products (system administrators).

8.B.1.c(1)(e) How to recognize and report potential security vulnerabilities, threats, security violations, or incidents.

8.B.1.c(1)(f) The organization's policy for protecting information and systems and the roles and responsibilities of various organizational units with which they may have to interact.

8.B.1.c(1)(g) The system security regulations and policies.

8.B.1.c(1)(h) What constitutes misuse or abuse of system privileges.

8.B.1.c(2) General Users, with training to include:

8.B.1.c(2)(a) How to protect the physical area, media, and equipment (e.g., locking doors, care of diskettes).

8.B.1.c(2)(b) How to protect authenticators and operate the applicable system security features.

8.B.1.c(2)(c) How to recognize and report security violations and incidents.

8.B.1.c(2)(d) The organization's policy for protecting information and systems.

8.B.2 Marking and Labeling. This subsection sets forth the policy and procedures for use of security markings and labels of system media that may contain classified information under the purview of the signatories of this manual. It implements Information Security Oversight Office (ISOO) Directive 1. It specifies the use of standard external labels for identifying the security classification of removable IS media. Any downgrading or

declassification of media shall be clearly reflected in its markings and shall be documented.

8.B.2.a Marking Storage Media

8.B.2.a(1) Removable information storage media shall bear external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. SSPs shall identify the removable storage media to be used with a system. Classified removable media shall be controlled and protected in a manner similar to that used for classified paper materials. Removable media shall be marked as classified if the media has ever been used on the classified system and during any use on the system, was writeable (i.e. the write-protect feature could not be verified).

8.B.2.a(1)(a) In those areas, designated in the SSP, where classified information is processed, unmarked media that are not in factory-sealed packages shall be protected at the highest level of classification processed within the facility, until the media has been reviewed and appropriately labeled.

8.B.2.a(1)(b) In those areas, designated in the SSP, where both classified and unclassified information are processed or stored, UNCLASSIFIED media labels (SF 710) shall be used to identify media that contain only unclassified information.

8.B.2.a(2) Non-removable information storage media shall bear external labels indicating the security classification of the information and applicable associated security markings, such as handling caveats and dissemination control labels. If it is difficult to mark the non-removable media itself, the labels described below may be placed in a readily visible position on the cabinet enclosing the media.

8.B.2.a(3) External Labels

8.B.2.a(3)(a) For a system operating at Protection Level 1, 2, or 3, storage media shall bear external labels indicating the highest classification level and applicable associated security markings of information ever processed on the system, unless a reliable human review of the media's entire contents is performed.

8.B.2.a(3)(b) For a system operating at Protection Level 4 or 5, storage media shall be labeled with the classification level and applicable associated security markings of information on the media.

8.B.2.b Marking Hardware Components. Procedures identified in the SSP shall be implemented to ensure that all components of an IS, including input/output devices that have the potential for retaining information,* terminals, standalone microprocessors, and word processors used as terminals, bear a conspicuous, external label stating the highest classification level and most restrictive classification category of the information accessible to the component in the IS. This labeling may consist of permanent markings on the component or a sign placed on the terminal.

[*For example, mice and trackballs do not normally retain information.]

8.B.2.c Marking Human-Readable Output. Human-readable output shall be marked appropriately, on each human-readable page, screen, or equivalent (e.g., the proper

classification must appear on each classified microfiche *and* on each page of text on the fiche).

8.B.2.c(1) Adding a Banner Page. Except as provided by the DAA, the first page of the output (the banner page) shall include a warning message reminding the person receiving the output to control every page according to the markings on the banner page until a reliable human review has determined that the output is marked appropriately.

8.B.2.c(1)(a) If the capability to provide automatic banner pages does not exist, procedures shall be developed to mark manually or otherwise assure review of printed output, as appropriate.

8.B.2.c(1)(b) Using procedures approved by the Data Owner or responsible official, explicit approval shall be obtained from the DAA or his designee before forwarding output, which has not had a reliable human review for appropriate security classification and marking, to recipients who do not have system access. Such approval(s) can be for a specific release, for the overall release procedure(s), or for both.

8.B.2.c(2) Marking Printed Output. Individual pages of output shall be marked as appropriate either (a) to reflect the classification and applicable associated security markings of the data that is printed on each page, or (b) with the highest classification and all applicable associated security markings of the data that is to be printed.

8.B.2.c(3) Marking Output From Shared Printers

8.B.2.c(3)(a) At the DAA's discretion, systems operating at Protection Level 1, 2, or 3 shall mark the beginning (banner) page of all human-readable, paged, hardcopy output (printer output) with a human-readable representation of the system's security parameter, which is the highest classification and all appropriate associated security markings of the information processed by the system. For Protection Level 3, procedures shall be implemented to ensure output is given only to authorized users.

8.B.2.c(3)(b) For systems that operate at Protection Level 4 or 5, the banner page of output shall be marked with the appropriate level of classification contained in the document produced.

8.B.2.d Variations. DAAs or their designees may identify specific types of media or hardware components that need not be marked in accordance with this policy so long as they remain within a single, secure environment, and:

8.B.2.d(1) All systems are operating at the same classification level and access authorizations;

8.B.2.d(2) The media or hardware components are documented in the SSP;

8.B.2.d(3) Mechanisms or procedures have been established to provide the security protection intended by this policy; and

8.B.2.d(4) If removed from the single, secure environment, the media are either appropriately marked or sanitized or declassified in accordance with paragraph 8.B.5, below.

8.B.2.e Removable system media shall be externally marked with the established classification label (or a facsimile of it), specified in Table 8.1 and published by the Information Security Oversight Office (ISOO).

8.B.2.f Definition. For the purposes of this subsection, the term *portable system media* means cassette tapes, floppy disks, cartridge disks, reel tapes, hard disks, compact disks, optical disks, and other removable system devices that store non-volatile data.

Table 8.1 - Classification Labeling

Label	Color[1]	Form Number	Size[2]
CLASSIFIED SCI	Yellow(101)	SF 712 (10-87)	2.500" by 1.375"
TOP SECRET	Orange(165)	SF 706 (1-87)	2.125" by 1.250"
SECRET	Red(186)	SF 707 (1-87)	2.125" by 1.250"
CONFIDENTIAL	Blue(286)	SF 708 (1-87)	2.125" by 1.250"
UNCLASSIFIED	Green(356)	SF 710 (1-87)	1.938" by 1.183"

Notes

1. Color tones should be similar to the industry standard Pantone Matching System (PMS) ink colors that correspond to the listed PMS reference numbers.
2. ISOO is considering publishing classification labels that are half of the size of the current labels while continuing publication of the current labels. The half-size classification labels would be developed to accommodate new types of portable IS media that have been introduced since October 1987.

8.B.2.g Implementation. Security labels shall be conspicuously placed on media; however, their placement must not adversely affect the operation of the equipment on which the media is used. A security label may be placed on the protective cover rather than on the media only if labeling the media would impair operation or if the media is too small to accommodate a label. The intent of marking is to provide a visible indicator of content to support proper handling and storage of the media.

8.B.2.h The security marking does not replace internal classification control detail. DAAs or their designees shall approve any other identifying marking (e.g., library retrieval number/locator) to be placed externally on the media.

8.B.2.i The downgrading or declassification instructions applicable to the data contained on the portable system media shall accompany the data when it is transferred from one security control point to another. These instructions may be internal to the media.

8.B.3 Manual Review of Human-Readable Output. Before human-readable output is released outside the security boundary, an appropriately authorized individual shall provide a reliable human review of the output to determine whether it is accurately marked with the appropriate classification and applicable associated security markings. The authorized reviewer shall be knowledgeable enough about the data to determine the presence of improper data in the information being reviewed, and shall be cleared for and have formal access approval for he information being reviewed. The review shall be

at a level of detail, as set forth by the DAA, to allow the reviewer to accept security responsibility for releasing the data to its recipient.

8.B.3.a The electronic output (i.e., softcopy) to be released outside the security boundary shall be verified by a review (in human-readable form) of all data including embedded text (e.g., headers and footers, hidden text, notes, edited text, control characters) before being released.

8.B.3.b Information on media that is not in human-readable form (e.g., embedded graphics, sound, video, imagery) shall be examined for content with the appropriate software, hardware, and firmware. Care is required to ensure that all layers or levels of the graphics or image are reviewed.

8.B.3.c Random or representative sampling techniques may be used to verify the proper marking of large volumes of output.

8.B.3.d If available, automated techniques approved by the DAA may be used to verify the proper output marking of data.

8.B.4 Media Accountability. Media accountability shall be implemented that provides a set of protection mechanisms comparable to those required for equivalent paper documents. Additional guidance appears in Chapter 5 of the DoD Overprint to the NISPOMSUP.

8.B.5 Media Clearing and Sanitization. Storage media shall be physically controlled and safeguarded in the manner prescribed for the most-sensitive designation, or highest classification level, and category of data ever recorded on it until destroyed or sanitized using approved procedures. The SSP shall specify the approved release procedure for the media of a given system. Procedures to be used for the sanitization, declassification, and reuse of storage media are described below:

8.B.5.a Clearing vs. Sanitizing vs. Destroying Media.

8.B.5.a(1) *Clearing* is the process of eradicating the data on the media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval. *Purging* or *sanitizing* is the process of removing the data from the media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before purging or sanitizing. In general, laboratory techniques cannot retrieve data that has been purged or sanitized. *Destroying* is the process of physically damaging the media so that it is not usable as media, and so that no known method can retrieve data from it.

8.B.5.a(2) Overwriting, clearing, purging, degaussing, and sanitizing are not synonymous with *declassification*. Declassification is the separate administrative process resulting in a determination that given media no longer requires protection as classified information. Procedures for declassifying media require DAA approval.

8.B.5.a(2)(a) Overwriting Media

8.B.5.a(2)(a)(1) Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing.

8.B.5.a(2)(a)(2) Several factors can reduce the effectiveness of overwriting. These include ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), and inability to overwrite bad sectors or tracks or information in inter-record gaps.

8.B.5.a(2)(a)(3) To clear magnetic disks, overwrite all locations three times (the first time with a random character, the second time with a specified character, and the third time with the complement of that specified character).

8.B.5.a(2)(b) Degaussing Media

8.B.5.a(2)(b)(1) Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

8.B.5.a(2)(b)(2) Magnetic media are divided into three types based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. Type I degaussers are used to degauss Type I media (i.e., media whose coercivity is no greater than 350 Oersteds [Oe]). Type IIa degaussers are used to degauss Type IIa media (i.e., media whose coercivity is no greater than 900 Oe). Currently, no degaussers can effectively degauss all Type III media (i.e., media whose coercivity is over 900 Oe). Some degaussers are rated up to 1700 Oe, but their specific approved rating must be determined prior to use. The correct use of degaussing products improves assurance that data is no longer retrievable and that inadvertent disclosure will not occur.

8.B.5.a(2)(b)(3) Refer to the current issue of NSA's *Information Systems Security Products and Services Catalogue* (Degausser Products List Section) for the identification of degaussers acceptable for the procedures specified in this manual. The vendor will provide test procedures to verify continued compliance. The ISSM, using these vendor-supplied test procedures, shall ensure testing at least annually of these products to verify that they continue to meet their manufacturers' specifications.

8.B.5.a(3) Sanitizing Media. Sanitization removes information from media or equipment so that data recovery using any known technique or analysis is prevented. Sanitizing is a two-step process that includes removing data from the media by effectively degaussing the media and removing all sensitivity labels, markings, and activity logs. After magnetic media are properly degaussed in accordance with NSA/CSSM 130-2, and all identifying labels removed, they are considered to be sanitized.

8.B.5.a(4) Destroying Media. Data storage media will be destroyed in accordance with PAA-approved methods.

8.B.5.b Media containing classified information

8.B.5.b(1) Reuse of media. Cleared or sanitized media that has previously contained classified information may be reused at the same classification level (e.g., TS → TS), or at a higher level (e.g., S → TS). Sanitized media may be downgraded or declassified with the DAA's and, as applicable, the Data Owner's approval as specified in the SSP. Only approved equipment and software shall be used to overwrite and degauss magnetic media containing classified information. Each action or procedure taken to overwrite or degauss such media shall be verified.

8.B.5.b(2) Clearing. Only approved equipment and overwriting software that is compatible with the specific hardware for overwriting shall be used to clear media that have contained classified information. Use of such software shall be coordinated in advance with the DAA. The success of the overwrite procedure shall be verified through random sampling of the overwritten media. Items that have been cleared (i.e., not sanitized) shall remain at the previous level of classification and remain in a secure, controlled environment.

8.B.5.b(3) Sanitizing

8.B.5.b(3)(a) Magnetic media containing classified information can be sanitized by use of an approved degaussing procedure. The DAA, with the Data Owner's approval (if applicable), can allow overwriting of some types of classified information as a sanitizing procedure.

8.B.5.b(3)(b) Media that have ever contained Sensitive Compartmented Information, other intelligence information, TOP SECRET SAP information, or Restricted Data cannot be sanitized by overwriting; such media shall be degaussed before release. Media that has ever contained COMSEC material cannot be sanitized at all; it shall be destroyed before release.

8.B.5.b(4) Optical Disks. Optical disks (including compact disk/read only memory, write once/read many, Digital Versatile Disk, and writeable compact discs) offer no mechanism for sanitization and must be destroyed via incineration or any other NSA-approved method. They should be placed in a classified trash bag labeled "non-soluble" and disposed as classified waste.

8.B.5.c Malfunctioning Media. Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing shall be reported to the ISSO, who will coordinate repair or destruction with the responsible DAA.

8.B.5.d Release of Memory Components and Boards

8.B.5.d(1) Before the release of any components or boards from an area used to process or store classified information, whether because they are malfunctioning or because they are no longer needed, the requirements of subsections (2) and (3), below, shall be met. This section applies only to components identified by the vendor or other technically-knowledgeable individual as having the capability of retaining user-addressable data and does not apply to other items (e.g., cabinets, covers, electrical components not associated with data), which may be released without reservation. For the purposes of this document, a memory component is the Lowest Replaceable Unit (LRU) in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies. Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing components for release (see NSA/CSSM 130-2). Memory components are specifically handled as either *volatile* or *nonvolatile*, as described below.

8.B.5.d(2) Volatile Memory Components. Memory components that *do* not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual data, are considered volatile memory components. Volatile components that have contained classified information may be released only in accordance with procedures developed by the ISSO and stated in the SSP. A record shall be maintained of the equipment release indicating that, per a best engineering assessment, all component memory is volatile and that no data remains in or on the component when power is removed.

8.B.5.d(3) Nonvolatile Memory Components. Components that do retain data when all power sources are discontinued are nonvolatile memory components; these include read-only memory (ROM), programmable ROM (PROM), or erasable PROM (EPROM), and their variants. Those that have been programmed at the vendor's commercial manufacturing facility, and are considered to be unalterable in the field, may be released. All other nonvolatile components may be released after successful completion of the procedures outlined in NSA/CSSM 130-2. Failure to accomplish these procedures shall require the ISSO to coordinate with the DAA for a determination of releasability.

8.B.5.e Release of Systems and Components. The ISSO shall develop equipment removal procedures for systems and components that have processed or contained classified or extremely sensitive information; these procedures shall be stated in the SSP. When such equipment is no longer needed, it can be released after:

8.B.5.e(1) Inspection of the system equipment by the ISSO or designee. This review shall assure that all media, including internal disks, have been removed or sanitized.

8.B.5.e(2) Creation of a record of the equipment release indicating the procedure used for sanitization, and to whom the equipment was released. This record shall be retained for a period prescribed by the DAA.

8.B.5.e(3) Using procedures specified by the DAA, notification to the DAA of the release of the equipment.

8.B.5.f Disposal of Printer Cartridges and Ribbons

8.B.5.f(1) Disposal of laser cartridges will be in accordance with DCID 6/9, Annex D, Part II.

8.B.5.f(2) Disposal of thermal ribbons and impact-type ribbons will be in accordance with the DoD Overprint to the NISPOMSUP, Chapter 5, Section 7.

8.B.6 Co-Location

8.B.6.a DAA approval is necessary to co-locate classified and unclassified ISs in a Special Access Program Facility (SAPF).

8.B.6.b The following conditions shall be adhered to:

8.B.6.b(1) An IS approved for processing unclassified information must be clearly marked as such when located within a SAPF.

8.B.6.b(2) An IS approved for processing unclassified information must be physically separated from any classified IS.

8.B.6.b(3) An IS approved for processing unclassified information must not be connected to any classified IS without the PAA's written approval.

8.B.6.b(4) Users must be provided with co-location process and procedures as part of their required security and awareness training.

8.B.6.b(5) The ISSO must document in the SSP the procedures and technical safeguards to ensure the protection of classified information.

8.B.6.b(6) All unmarked media must be treated as classified at the highest level processed by the facility until reviewed and verified.

8.B.6.c An unclassified portable IS (including personally owned ISs) is prohibited in a SAPF unless the DAA specifically permits its use. If permitted, all personnel shall adhere to the following procedures:

8.B.6.c(1) Connection of an unclassified portable IS to a classified IS is prohibited.

8.B.6.c(2) Connection of an unclassified IS to another unclassified IS may be done only with the DAA's written approval.

8.B.6.c(3) Use of an internal or external modem with the IS device is prohibited within the SAPF without the DAA's written approval.

8.B.6.c(4) The portable ISs and the contained data are subject to random reviews and inspections by the ISSO/ISSM. If classified information is found on the portable IS it shall be handled in accordance with the incident handling policy.

8.B.7 Incident Reporting and Response

8.B.7.a A formal incident-reporting program shall be put in place, and it shall be evaluated on a regular basis by the DAA. All security incidents shall be reported to the DAA and the Data Owner through the incident-reporting system. All incidents that may affect (or have affected) systems under more than one DAA shall be reported to the DAA responsible for the affected system. As appropriate, the information shall be forwarded to other involved DAAs and Data Owners. Additionally, organizational investigative agencies shall be immediately apprised of all security incidents and, if deemed necessary and appropriate, shall participate in their resolution.

8.B.7.b Procedures shall be developed by the ISSM and approved by the DAA to provide the appropriate responses to incidents.

8.B.7.c PAAs shall ensure the establishment of an incident reporting and response capability in the components under their purview. Notification to the PAA shall made within 24 hours of incidents involving intelligence information which, if compromised, could affect the safety of human life or could cause exceptionally grave damage to the national security. The PAA shall be notified within 4 days after the determination of:

8.B.7.c(1) The compromise of SAP information resulting from the failure of systems covered by this manual; or

8.B.7.c(2) Attempts by hostile elements (e.g., agents of a foreign intelligence service, recruited insiders, hostile outsiders) to penetrate any of these systems; or

8.B.7.c(3) The discovery of flaws or vulnerabilities that could result in the compromise of DoD SAP information.

8.B.7.d In the case of interconnected systems or systems that involve two or more PAAs:

8.B.7.d(1) Each DAA with responsibility for the affected system shall report all security-relevant events to affected parties, Data Owners, and all involved PAAs.

8.B.7.d(2) Each system's audit information shall be made available for investigations of security-relevant events.

8.B.8 Maintenance. An IS is 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 and unclassified information and facilities. System maintenance requirements and vulnerabilities shall be addressed during all phases of the system life cycle. Specifically, contract negotiations shall consider the security implications of system maintenance. This subsection details requirements necessary for maintaining system security during maintenance.

8.B.8.a Cleared Maintenance Personnel

8.B.8.a(1) Except as authorized by the DAA, personnel who perform maintenance on systems shall 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 an IS do not require an escort, unless need-to-know controls must be enforced. However, an appropriately cleared and, when possible, technically knowledgeable, facility employee shall be present

within the area where the maintenance is being performed to assure that the proper security and safety procedures are being followed.

8.B.8.a(2) Cleared foreign nationals may be utilized as maintenance personnel for those systems jointly owned and operated by the US and a foreign allied government, or those owned and operated by foreign allied governments. Approvals, consents, and detailed operational conditions must be fully documented within a Memorandum of Agreement and approved by the DAA.

8.B.8.b Uncleared (or Lower Cleared) Maintenance Personnel

8.B.8.b(1) If appropriately cleared personnel are unavailable to perform maintenance, an uncleared person, or one cleared to a lower level, may be used provided a fully cleared and technically qualified escort monitors and records that person's activities in a maintenance log.

8.B.8.b(2) For US-owned and operated ISs, uncleared/lower-cleared maintenance personnel must be US citizens. For systems jointly owned and operated by the US and a foreign allied government, or those owned and operated by foreign allied governments, uncleared/lower-cleared foreign nationals may be used. Approvals, consents, and detailed operational conditions must be fully documented within a Memorandum of Agreement and approved by the DAA.

8.B.8.b(3) Prior to maintenance by uncleared/lower-cleared personnel, the IS shall be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured. When a system cannot be cleared, DAA-approved procedures shall be enforced to deny the uncleared/lower-cleared individual visual and electronic access to any classified or sensitive data that is contained on the system.

8.B.8.b(4) A separate, unclassified copy of the operating system and application software, including any micro-coded floppy disks, cassettes, or optical disks that are integral to the IS, shall be used for all maintenance operations performed by uncleared/lower-cleared personnel. The copy shall be labeled "UNCLASSIFIED—FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSP. The ISSM must consider on a case-by-case basis maintenance procedures for an information system whose operating system resides on a non-removable storage device.

8.B.8.c General Maintenance Requirements

8.B.8.c(1) A maintenance log shall be maintained. The maintenance log shall include the date and time of maintenance, name of the individual performing the maintenance, name of escort, and a description of the type of maintenance performed, to include identification of replacement parts.

8.B.8.c(2) Maintenance of systems shall 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.

8.B.8.c(3) If systems or system components are to be removed from the facility for repair, they shall first be purged, and downgraded to an appropriate level, or sanitized of

all classified data and declassified in accordance with DAA-approved procedures. The ISSO or designee shall approve the release of all systems and all parts removed from the system (see section on Release of Memory Components and Boards).

8.B.8.c(4) Introduction of network analyzers (e.g., sniffers) that would allow the maintenance personnel the capability to do promiscuous mode (real time) monitoring shall be approved by the ISSM or designee prior to being introduced into an IS.

8.B.8.c(5) If maintenance personnel bring diagnostic test programs (e.g., software/firmware used for maintenance or diagnostics) into a facility, the media containing the programs (1) shall be checked for malicious code before the media is connected to the system, (2) shall remain within the facility, and (3) shall be stored and controlled at the level of the IS. Prior to entering the facility, the maintenance personnel shall be advised that they will not be allowed to remove media from the facility. If deviation from this procedure is required under special circumstances, then each time the diagnostic test media is introduced into a facility, the media shall undergo stringent integrity checks (e.g., virus scanning, checksum) prior to being used on the IS and, before leaving the facility, the media shall be checked to assure that no classified information has been written on it. Such a deviation requires approval by the ISSM.

8.B.8.c(6) All diagnostic equipment and other devices carried into a facility by maintenance personnel shall be handled as follows:

8.B.8.c(6)(a) Systems and system components being brought into the facility shall be inspected for obvious improper modification.

8.B.8.c(6)(b) Maintenance equipment that has the capability of retaining information shall be appropriately sanitized by procedures outlined in paragraph 8.B.5 before being released. If the equipment cannot be sanitized, the equipment shall remain within the facility, be destroyed, or be released under procedures approved by the DAA and the Data Owner(s) or responsible official(s).

8.B.8.c(6)(c) Replacement components that are brought into the facility for the purpose of swapping with facility components are allowed. However, any component placed into an IS shall remain in the facility until proper release procedures are completed. Any component that is not placed in an IS may be released from the facility.

8.B.8.c(6)(d) Communication devices with transmit capability (e.g., pagers, [RF] LAN connections) belonging to the maintenance personnel or any data storage media not required for the maintenance visit shall remain outside the system facility for return to the maintenance personnel upon departure from the facility.

8.B.8.c(7) Maintenance changes that impact the security of the system shall receive a configuration management review.

8.B.8.c(8) After maintenance has been performed, the security features on the IS shall be checked to assure that the IS is still functioning properly.

8.B.8.d Remote Maintenance (To be used on SAP systems only as approved by the DAA)

8.B.8.d(1) Remote diagnostic or maintenance services are acceptable if performed by a service or organization that provides the same level and category(ies) of security as the IS. The communications links connecting the components of the systems, associated data communications, and networks shall be protected in accordance with national policies and procedures applicable to the sensitivity level of the data that may be transmitted over the link.

8.B.8.d(2) If remote diagnostic or maintenance services are required from a service or organization that does not provide the same level of security required for the system being maintained, the IS shall be sanitized and physically separated from other information systems prior to the connection of the remote access line. If the system cannot be sanitized (e.g., due to a system failure), remote maintenance shall not be allowed.

8.B.8.d(3) Initiation and termination of the remote access shall be performed by the ISSO or designee. Keystroke monitoring shall be performed on all remote diagnostic or maintenance services. A technically qualified person shall review the maintenance log, and if appropriate, the audit log to assure the detection of unauthorized changes. The ISSM/ISSO shall assure that maintenance technicians responsible for performing remote diagnosis/maintenance are advised (e.g., contractually, verbally, or by banner) prior to remote diagnostics/maintenance activities that keystroke monitoring will be performed. Unless an exception has been granted by the DAA, maintenance personnel accessing the information systems at the remote site shall be cleared to the highest level of information processed on that system, even if the system was downgraded/sanitized prior to remote access. Installation and use of remote diagnostic links shall be specifically addressed in the SSP and agreed to by the DAA. An audit log shall be maintained of all remote maintenance, diagnostic, and service transactions including all commands performed and all responses. The log shall be periodically reviewed by the ISSO.

8.B.8.d(4) In addition, other techniques to consider for improving the security of remote maintenance include encryption and decryption of diagnostic communications, strong identification and authentication techniques, such as tokens, and remote disconnect verification. Where possible remote sessions should involve an interactive window for coordination with the information system's ISSM or ISSO. When the work has been completed, the sessions are terminated and the remote connection is physically broken.

8.B.8.d(5) Passwords used during the maintenance process shall be changed following each remote diagnostic maintenance service. All passwords are assigned and controlled by the information system's ISSM or ISSO.

8.B.9 Records Management. Records management for information stored in a system or on external media shall be governed by the records management policies of the appropriate agency, based on the guidelines from the National Archives and Records Agency.

8.C Environmental Security

8.C.1 Communications Security. The communications links connecting the components of the systems, associated data communications, and networks shall be protected in accordance with national policies and procedures applicable to the sensitivity level of the data being transmitted.

8.C.2 Protected Hardware, Software, and Firmware

8.C.2.a All hardware, software, firmware, documentation, and sensitive data handled by the system shall be protected throughout its life cycle to prevent intentional or unintentional disclosure, destruction, or modification (i.e., data integrity shall be maintained). This includes having appropriate personnel, physical, administrative, and configuration controls. Such controls shall be provided for unclassified hardware, software, or firmware, or documentation that may be used to eliminate, circumvent, or otherwise render ineffective the security safeguards for classified information. Unless otherwise specified by the accrediting authority, the degree of control and protection for all IS components shall be at least equal to the highest classification and most restrictive control measures required for the processed data.

8.C.2.b Uncleared personnel developing hardware, firmware, software, or data files shall not, to the maximum extent possible, have any knowledge that the software, hardware, firmware or data files will be used in a classified area. Before hardware, firmware, software, or data files that are developed or modified by uncleared personnel can be used in a classified processing period, appropriately cleared, technically knowledgeable personnel shall review them to ensure that no security vulnerabilities or malicious code exist. Software, hardware, and firmware used for maintenance or diagnostics shall be maintained within the secure computing facility and, even though unclassified, shall be separately controlled.

8.C.2.c Personnel responsible for installing modifications to system- or security-related software, hardware, and firmware or data files on a classified IS shall be cleared to the highest level of information processed or stored. Software, hardware, and firmware that contains security-relevant functions (e.g., sanitization, access control, auditing) shall be validated by the ISSO to confirm that security-related features are fully functional, protected from modification, and effective.

8.C.3 EMSEC/TEMPEST. The components of the systems, associated data communications, and networks shall be protected in accordance with national EMSEC/TEMPEST policies and procedures applicable to the sensitivity level of the data being transmitted.

8.C.4 Technical Surveillance Countermeasures (TSCM). The components of the systems, associated data communications, and networks shall be protected in accordance with national TSCM policies and procedures applicable to the sensitivity level of the data being transmitted.

8.D Physical Security

(JAFAN 6/9 and Section 8, Chapter 5 of the DoD Overprint to the NISPOMSUP also apply).

8.D.1 All technical security safeguards base their effectiveness on the assumption, either explicit or implicit, that all segments of the Security Support Structure have adequate physical security protection.

8.D.2 All systems shall comply with the applicable standards for physical protection of the data processed, stored, or transported therein. For facilities housing ISs processing SAP information, the applicable standard is JAFAN 6/9, *Physical Security Standards for Special Access Program Facilities (SAPF)*. Unencrypted SAP information shall be processed only in a SAPF. A Temporary SAPF (TSAPF), set up and formally accredited, is an approved SAPF that may be used to process SAP information for a limited time period.

8.E Personnel Security

Eligibility requirements for personnel requiring access to systems processing SAP information shall be as specified by the DoD standards and procedures applicable to the specific SAP. Because of the potential for damage to the national security interests of the United States inherent in the depth and sensitivity of access to intelligence programs by privileged users, agencies and organizations must provide strong security measures for such users. These measures must ensure that privileged users have no serious unresolved personnel security or counterintelligence issues prior to obtaining such access, and they must identify and resolve such issues as long as a person remains a privileged user.

8.E.1 Access by Foreign Nationals to Systems Processing Classified Information. US Government classified information is not releasable to foreign nationals except as authorized by the US Government. Data Owners can designate their information as releasable to individuals of specific nationalities. PAAs/DAAs shall obtain the written permission of all applicable Data Owners before allowing access by foreign nationals to a system that contains information not releasable to individuals of those nationalities. The decision to allow access by foreign nationals to systems that process classified information shall be explicit and shall be in writing.

8.F Handling Caveats and Handling Restrictions

Some SAP information has handling caveats that specify control or releasability restrictions on the information. Such information shall be controlled by agreement with the Data Owner, or under procedures established by the Data Owner, or by statute.

9 RISK MANAGEMENT, CERTIFICATION, AND ACCREDITATION

9.A Overview

This chapter discusses risk management, the certification process, the accreditation process, and the interrelationship of the three activities.

9.A.1 Risk management is the discipline of identifying and measuring security risks associated with an IS, and controlling and reducing those risks to an acceptable level. The goal of risk management is to invest organizational resources to mitigate security risks in a cost-effective manner, while enabling timely and effective mission accomplishment.

9.A.2 The risk management process identifies assets to be protected, potential threats and vulnerabilities, and countermeasures and safeguards that can eliminate vulnerabilities or reduce them to levels acceptable for IS accreditation. Risk management is based on careful identification and evaluation of the threats and vulnerabilities that apply to a given IS and its operational environment.

9.A.3 The certification process validates that appropriate Levels-of-Concern for integrity and availability and an appropriate Protection Level for confidentiality have been selected from the tables and descriptions (Chapters 3, 4, 5, 6, 7, and 8, and Appendix D) in this manual, and that the required safeguards have been implemented on the system as described in the SSP. This process culminates in the accreditation (permission for the system to operate processing specific classification and compartments of information at the approved Protection Level for confidentiality and approved Levels-of-Concern for integrity and availability) by the DAA.

9.A.4 The certification and accreditation process, from initial certification and accreditation to the withdrawal of accreditation, covers the entire life cycle of an IS.

9.B Risk Management

9.B.1 Risk management is relevant to the entire life cycle of an IS. During IS development, security countermeasures are chosen. During IS implementation and operation, the effectiveness of in-place countermeasures is reconfirmed, and the effect of current threat conditions on system security is assessed to determine if additional countermeasures are needed to sustain the accredited IS's security. In scheduling risk management activities and designating resources, careful consideration should be given to Certification and Accreditation (C&A) goals and milestones. Associated risks can then be assessed and corrective action taken for unacceptable risks. Risk management requires the routine tracking and evaluation of the security state of an IS.

9.B.2 The risk management process includes:

9.B.2.a Analysis of the threats to and vulnerabilities of an information system, as well as of the potential impact that losing the system's information or capabilities would have on national security. This analysis forms a basis for identifying appropriate and cost-effective countermeasures.

9.B.2.b Risk mitigation. Analysis of trade-offs among alternative sets of possible safeguards.

9.B.2.c Residual risk determination. Identification of the risk remaining after applying safeguards.

9.B.2.d Acceptable level of risk. Judicious and carefully considered assessment by the appropriate DAA that the residual risk inherent in operating the IS after implementing all proposed security features is acceptable.

9.B.2.e A reactive or responsive risk management process. To facilitate investigation of, and response to, incidents.

9.B.3 For interconnected systems, all of the requirements stated in paragraph 9.B.2, above, shall be applied to connections, including any changes or requested changes to, and exploitation (potential or real) of, connections.

9.B.4 Initial information gathering for the risk management process determines mission requirements (e.g., requirements for timeliness, confidentiality, availability, and correctness of information), resources available to mitigate risks (e.g., financial, staffing), constraints (e.g., commitment to use specific information technologies, architectures, or products), and applicable policies and requirements. This information should be made available and updated as necessary throughout the IS life cycle. Risk management activities provide important information for DAAs and typically include:

9.B.4.a Risk analysis. The analysis and assessment of information regarding threats, vulnerabilities and assets.

9.B.4.b Cost/benefit analysis. An analysis of the costs of providing and maintaining a safeguard versus the cost of losing or compromising the information or IS resource, including the operational impact of implementing a security safeguard.

9.B.4.c Security test and evaluation. An analysis of the safeguards protecting an IS in a given operational environment, for the purpose of determining the security posture of that system.

9.B.4.d Countermeasure implementation. The implementation of any action, device, procedure, technique, or other measure that reduces risk.

9.B.4.e Penetration testing. Security testing in which the testers attempt to circumvent the security features of an IS based on their understanding of the system design and implementation.

9.B.4.f IS review. A periodic review of the security posture of an IS, done at regular intervals and whenever there are any major changes to the IS.

9.B.5 Chapters 3, 4, 5, and 6 provide guidance for determining the correct safeguards to employ at the selected Integrity and Availability Levels-of-Concern and the Confidentiality Protection Level. Chapter 7 provides guidance regarding the appropriate safeguards to employ when interconnecting information systems and using advanced technology. This guidance is generic, and addresses only minimum security requirements. Specific threats, vulnerabilities, or constraints associated with an IS and its environment may impose additional security requirements on an IS or the substitution of safeguards from different security disciplines.

9.B.6 The following, additional risk management considerations apply when systems are interconnected:

9.B.6.a The risk management process must address new risks encountered by individual systems and the interconnected infrastructures to which they will connect.

9.B.6.b The risk management process must address the concerns and requirements of the organizations and elements (e.g., Data Owners) that are part of the information infrastructure being used to achieve interconnectivity.

9.B.6.c Additional constraints can arise due to organizational commitments to specific technologies or architectures, variations in policies or treaty agreements.

9.B.6.d Risk management responsibilities may be shared by multiple DAAs.

9.C Certification

9.C.1 Certification is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

9.C.2 The certification process validates that appropriate Levels-of-Concern for integrity and availability and an appropriate Confidentiality Protection Level have been selected from the tables and descriptions (Chapters 3, 4, 5, 6, and 7, and Appendix D) in this manual, and that the required safeguards have been implemented on the system as described in the SSP.

9.C.3 The ISSM shall provide a package of certification documentation to the DAA. This certification package shall include (1) the SSP; (2) the test plans, if system testing is required; (3) the test results (or, at the DAA's discretion, a summary of the test results); (4) a statement that the system implements the required security safeguards as described in the SSP; (5) an identification of any additional safeguards required by the DAA; (6) an identification of factors mitigating potential risk; and (7) a recommendation for DAA approval or disapproval.

9.C.4 The certification process culminates in an accreditation decision by the DAA.

9.D Accreditation

9.D.1 Overview

9.D.1.a The accreditation of an IS is the official management decision to operate an IS in a specified environment. The certification findings for the IS are the principal technical inputs to the accreditation decision. Therefore, the DAA is involved from the start of the system to ensure that accreditation goals are clearly defined. A DAA assumes responsibility for the decision to allow an IS to operate and therefore must be satisfied that the certification can support an informed decision. The accreditation statement is the DAA’s acceptance of responsibility for the appropriateness of IS security as implemented.

9.D.1.b An IS accreditation provides formal approval for an IS to operate, and identifies the following:

9.D.1.b(1) Stated operational concept and environment, including mission criticality and characterization of user communities (i.e., approximate number of users, clearance, formal access approvals, need-to-know, privileges).

9.D.1.b(2) Classification and sensitivity of the information on the IS, including specific applicable classifications, compartments, caveats, control markings, and special handling instructions that may be handled by the IS.

9.D.1.b(3) A given Confidentiality Protection Level.

9.D.1.b(4) A given Integrity Level-of-Concern.

9.D.1.b(5) A given Availability Level-of-Concern.

9.D.1.b(6) Specified operating conditions, including prescribed safeguards.

9.D.1.b(7) Stated interconnections with other ISs, when applicable.

9.D.1.b(8) A specified period of time.

9.D.1.c A DAA's accreditation of an IS and its environment is an assertion of an acceptable level of security risk. Acceptable security risk is the expectation that an IS will adequately protect against unauthorized access, alteration, or use of an IS's resources, and against denial of the IS's services to authorized users. This expectation is based on the assumption of continuous employment of administrative, procedural, physical, personnel, communications security, emanations security, and IS security controls. IS security controls can be features of the software, hardware, or firmware of an IS, or associated security-specific devices.

9.D.1.d Both ISs under development and ISs in operation can be accredited. ISs in operation shall be re-accredited whenever security-relevant changes occur in an IS or its operational environment. Even if no security-relevant changes occur, the accreditations shall be re-evaluated every three years.

9.D.2 Accreditation Authority

9.D.2.a SAP System Accreditations

9.D.2.a(1) For the Department of the Air Force, Special Access Program Information Systems or components of such systems (e.g., automated guards, security filters, or controlled interfaces) that operate at Protection Levels 4 and 5 may be accredited only by their respective PAA, who is the Director, Security and Special Programs Oversight, Administrative Assistant to the Secretary of the Air Force. The PAA may delegate, in writing, to the extent the PAA considers appropriate, the authority to accredit systems operating at Protection Levels 1, 2, or 3; but the PAA retains the ultimate responsibility for the security for the information processed in those systems.

9.D.2.a(2) For the Department of the Army, Special Access Program Information Systems or components of such systems (e.g., automated guards, security filters, or controlled interfaces) that operate at Protection Levels 4 and 5 may only be accredited by

their respective PAA, who is US Army Technology Management Office, DACS-DMP. The PAA may delegate, in writing, to the extent the PAA considers appropriate, the authority to accredit systems operating at Protection Levels 1, 2, or 3; but the PAA retains the ultimate responsibility for the security for the information processed in those systems.

9.D.2.a(3) For the Department of the Navy, Special Access Program Information Systems or components of such systems (e.g., automated guards, security filters, or controlled interfaces) that operate at Protection Levels 4 and 5 may only be accredited by their respective PAA, who is the Director of Special Programs (N7SP), Department of Navy. The PAA may delegate, in writing, to the extent the PAA considers appropriate, the authority to accredit systems operating at Protection Levels 1, 2, or 3; but the PAA retains the ultimate responsibility for the security for the information processed in those systems.

9.D.2.b Joint Accreditations

9.D.2.b(1) For systems operating under the purview of more than one PAA, the following guidelines shall be followed:

9.D.2.b(1)(a) For systems processing DoD SAP data:

9.D.2.b(1)(a)(1) Systems operating at Protection Levels 4 or 5 that are under the purview of three or more PAAs *shall* be jointly certified by a panel or board consisting of representatives of the affected parties.

9.D.2.b(1)(a)(2) Systems operating at Protection Level 3 that are under the purview of three or more PAAs *shall* be jointly certified by a panel or board consisting of representatives of the affected parties, and accredited by a single accrediting authority by mutual agreement.

9.D.2.b(1)(a)(3) Systems operating at Protection Level 2 that are under the purview of three or more PAAs *may* be jointly certified by a panel or board consisting of representatives of the affected parties, and accredited by a single accrediting authority by mutual agreement.

9.D.2.b(1)(b) For systems processing intelligence and DoD SAP data. Systems shall be accredited *separately* (i.e., via two separate accreditations) *or jointly* by the cognizant intelligence DAA and SAP DAA as per the guidance in paragraph 9.D.2.a, above, and in DCID 6/3.

9.D.2.b(2) For systems processing DoD SAP information, operating under the purview of more than one PAA, and that are not jointly certified by a panel or board:

9.D.2.b(2)(a) A Memorandum of Agreement (MOA) shall be required between the cognizant PAAs; the MOA should name a lead PAA, who will be responsible for the system certification. If no lead PAA is named, then both parties shall share responsibility.

9.D.2.b(2)(b) The MOA shall be included in the SSP.

9.D.3 Accreditation Process. Before accrediting a system to operate, the DAA shall (1) determine the IS's Confidentiality Protection Levels, and the Integrity and Availability Levels-of Concern, (2) inform the ISSM/ISSO of the DAA determination, (3) ensure that satisfactory safeguards (i.e., those requirements specified in Chapters 4, 5, and 6 for the Confidentiality Protection Level, and the Integrity and Availability Levels-of-Concern, respectively) have been implemented, (4) ensure that the applicable requirements specified in Chapter 7 ("Requirements for Interconnected Systems and Advanced Technology") and Chapter 8 ("Administrative Security Requirements") have been implemented, and (5) ensure that the residual risk is within acceptable limits. An impartial party selected by the DAA shall determine the level of residual risk. The impartial party may not be the system developer(s). However, the ultimate responsibility for accepting the residual risk rests with the DAA. While the DAA assumes formal responsibility for operating a system (and accepting the risk of such operation), the Data Owner has statutory responsibility for the information processed on the system. As such, the Data Owner has the authority to revoke permission to process information on the system if unsatisfied with the protection provided by the system. The Data Owner shall notify the PAA/DAA of any decision to revoke access to information.

9.D.3.a Accreditation of Similar Systems

9.D.3.a(1) At the DAA's discretion, the DAA can determine that systems in a group are, for accreditation purposes, essentially the same. Systems can be considered as "essentially the same" if (1) the Protection Levels and the Levels-of-Concern are the same; (2) the users have at least the required clearances and access approvals for all information on the systems; (3) the systems are processing the same level(s) and specific set(s) of information; (4) the system configurations are essentially the same; and (5) the environments of the systems are essentially the same. If the DAA chooses to accredit this set of systems as a unit, then an SSP may be written and approved by the DAA, to cover all of the similar systems. This type of approval applies only to systems operating at Protection Levels 1 and 2 (Chapter 3), and under the purview of a single DAA. The SSP for these systems shall specify the information required for certification of each system to be accredited under this procedure. The DAA shall accredit the first system under the SSP. All of the other individual systems to be operated under such an SSP shall be tested by the ISSO and certified by the ISSM as meeting the conditions of the approved SSP. This certification, in effect, accredits the individual system to operate under the SSP. The ISSM shall retain a copy of each certification report with the approved copy of the SSP and make a copy available to the DAA.

9.D.3.a(2) In determining whether two sets of systems are "similar" for the purposes of this section, consideration must be given to any required changes to the SSP. Adding similar systems requires changes only in identification, such as location, internal system configuration, and so forth. Any other required changes, such as administrative control outside the purview of a single DAA, indicate that the systems are not "similar" within the meaning of this section.

9.D.3.a(3) A Master System Security Plan (MSSP) may also be used to refer to and identify common security information for "similar systems" at a given site or facility as specified above. In this case, the MSSP shall include the identity of all systems covered. Such a listing can be as simple as a reference to a particular database containing the identifying information and locations of applicable systems.

9.D.3.b Site-Based Accreditation

9.D.3.b(1) The DAA may choose an alternate accreditation approach that consolidates all systems at a location into a single management entity called a "Site". The size and bounds of each site are determined by the relationship of each system (component) to the infrastructure, command lines of authority, and the span of control of the site's ISSM. Site accreditation begins with all systems at the site being evaluated and certified. The site is then accredited as a single entity, and the ISSM may be delegated the authority to add more systems to the site.

9.D.3.b(2) A Site Security CONOPS and a Site Security Architecture are required for site-based accreditation and shall contain a listing of all systems covered under the site-based accreditation, a description of how the site complies with the requirements of this manual, and a wiring diagram showing external connections.

9.D.3.c Interconnected Systems

9.D.3.c(1) The accreditor for a system that is to be connected to another system shall consider the security characteristics of the other system, as well as the security characteristics of all systems directly connected to the other systems. This has been described as considering connections "one layer further." If any of the systems that are "one layer further" are considered a greater security risk (e.g., having users of a lower security level), then the accreditor should consider increasing the Protection Level or Integrity Level-of-Concern, or both.

9.D.3.c(2) The DAA for each interconnected system is responsible for ensuring that all data is properly protected by each system that is directly connected to the DAA's system.

9.D.3.c(3) The security requirements applicable to the interconnected systems are determined by (a) the Confidentiality Protection Level and the Integrity and Availability Levels-of-Concern of the interconnected systems (Chapters 4, 5, and 6, and Appendix D), (b) their interface characteristics (Chapter 7), and (c) their operational environment.

9.D.3.c(4) An Interconnection Security Agreement (ISA) is required whenever an accredited system is connected to a system accredited by a different DAA*. The contents of such an ISA are specified in Appendix A.

[*Some types of interconnected networks, particularly those that are community wide, do not require a formal ISA. In this case, the function of the ISA is handled with a list of requirements to be satisfied prior to connection. Upon verification that the list has been satisfied, the interconnection is made.]

9.D.3.c(5) Chapter 7 of this manual contains further requirements for interconnected systems.

9.D.4 Accreditation Decision. Based on all available documentation and mitigating factors, the DAA shall decide whether to grant:

9.D.4.a Accreditation approval for the system to operate as certified.

9.D.4.b Accreditation disapproval, including recommendations and time lines for correcting specified deficiencies.

9.D.4.c Interim approval to operate, identifying the steps and any additional controls to be completed prior to full accreditation.

9.D.4.c(1) The DAA may grant interim approval to operate a system to meet written validated requirements or to permit a major conversion of a system. This interim accreditation may be granted for up to 180 days and can be renewed once for an additional 180 days. By the end of the second 180-day period, the system shall either be accredited or cease operation.

9.D.4.c(2) Protection measures specified by the DAA shall be in place and functioning during the period of interim approval.

9.D.4.c(3) A system that is under development or major modification, and is expected to be under development or major modification for an extended period, can be accredited to operate in such an environment. Such an accreditation shall include detailed descriptions of changes (or types of changes) that would not require additional DAA approvals, and changes (or types of changes) that would require additional DAA approvals.

9.D.5 Invalidation of an Accreditation. An accreditation immediately becomes invalid whenever detrimental, security-relevant changes occur to any of the following: the required Protection Level, the operational environment, the operational concept, or the interconnections. Any non-DAA-approved security-relevant changes to the IS may result in the invalidation of the accreditation.

9.D.6 Withdrawal of Accreditation

9.D.6.a The DAA shall withdraw accreditation and suspend operation if the security measures and controls established and approved for the system do not remain effective.

9.D.6.b The DAA shall withdraw accreditation when the system is no longer required to process SAP information, or if the operational need for the system no longer outweighs the risk of operating the system.

9.D.7 Re-evaluation of an Accreditation

9.D.7.a An accreditation shall be re-evaluated within three years after it is issued or whenever any security-relevant change occurs. An accreditation shall immediately be re-evaluated upon a detrimental, security-relevant change in the threat to, or vulnerability of the system; a change to the technical or non-technical security requirements; or a significant increase in the level of residual risk.

9.D.7.b Re-evaluation of an accreditation involves a determination by the DAA, based on a recommendation by the ISSM, whether the original accreditation is still valid. The DAA can re-accredit the system or require further action.

9.E The Certification and Accreditation (C&A) Process

9.E.1 The C&A process (from initial certification and accreditation to the withdrawal of accreditation) covers the entire life cycle of an IS. The C&A process depends upon careful identification of the security-relevant aspects of an IS. A complete IS certification considers a large number of factors associated with the IS and its operational environment. These factors include identification of the DAA; mission criticality; functional requirements; IS security boundaries; applicable security policies; security CONOPS; IS configuration; IS components; user characteristics and authorizations (e.g., includes foreign nationals, integrees, contractors); IS applications; site/facility locations; external interfaces and interconnections; Protection Level; Levels of Concern; classification of the data and associated caveats; IS and data ownership; risk analysis, including threat and vulnerability assessments and countermeasure implications; and counterintelligence aspects.

9.E.2 This section discusses the points in the IS life cycle (both development and operation) at which the requirements of this document are usually applied.

9.E.2.a Systems Under Development. The various phases of system development are described below and depicted in Table 9.1.

9.E.2.a(1) Design and Development Phase

9.E.2.a(1)(a) The Confidentiality Protection Level and the Availability and Integrity Levels-of-Concern are determined. See Chapters 4, 5, and 6 for specific requirements.

9.E.2.a(1)(b) The security requirements are defined using the matrices and requirements tables in this document.

9.E.2.a(1)(c) The threats to an IS and its vulnerabilities to the threats are identified. All known hardware, software, firmware, operational, and environmental vulnerabilities are identified. A determination is made whether or not the requirements of this manual satisfactorily mitigate the vulnerabilities. If they do not, it may be necessary to specify additional security requirements.

9.E.2.a(1)(d) The SSP for the IS is developed and submitted to the DAA (or a DAA representative) for approval. This step is a prerequisite for starting the IS's Fabrication and Production Phase.

9.E.2.a(2) First Test and Evaluation (T&E I) Phase. During T&E I, the Certification Test Plan and Test Procedures are developed. The Certification Test Plan outlines the IS certification test. It describes the test sets needed to demonstrate that the IS implements its security requirements. The plan also gives specific guidelines for conducting the tests. Certification test procedures expand the test set descriptions into step-by-step descriptions of the security requirement tests.

9.E.2.a(3) Second Test and Evaluation (T&E II) Phase

9.E.2.a(3)(a) Most of the C&A process is conducted during T&E II. Once functional testing is complete, the security test and evaluation is conducted based on the Certification Test Plan and Test Procedures. Shortfalls and vulnerabilities are

identified, and risks are analyzed. The outcome of the risk analysis is used to develop a plan to address shortfalls. The plan includes actions required to fix or work around particular shortfalls. The Certification Package (see paragraph 9.C, above) is then prepared and submitted to the DAA.

9.E.2.a(3)(b) The DAA reviews the Certification Package and uses its information as the basis for the accreditation decision. The DAA considers all relevant factors in determining whether to accredit a system. These factors include security environment, system mission, availability and cost of alternative countermeasures, and residual risks. The DAA may also consider factors that transcend security, such as program and schedule risks.

9.E.2.a(4) Operations and Maintenance (O&M) Phase. Changes to the IS's security structure may require recertification and reaccreditation (see paragraphs 9.C and 9.D, above).

9.E.2.a(5) Disposal Phase. When the IS is no longer required, the process ends with its secure disposal.

9.E.2.b Operational Systems. These systems shall be accredited under the requirements of this document. All of the steps listed in paragraph 9.E.2.a, above, will be conducted. Except for disposal, this process will be conducted under the O&M Phase. Prudent risk management dictates that careful consideration be given before adding expensive additional safeguards to a system that has an extensive history of operation with effective security. DAAs accrediting existing systems are strongly encouraged to give appropriate weight to the system's operating history.

9.F C&A Process: Exceptions

9.F.1 Limitations in resources and technical capabilities may prevent the satisfaction of all security requirements without introducing unacceptable delay in achieving the operational requirements that the system was intended to satisfy. Therefore, DAAs are authorized to grant written exceptions* to some security requirements identified in this manual under the following conditions:

[*For the purposes of this manual, an *exception* indicates that the implementation of one or more security requirements is temporarily postponed and that satisfactory substitutes for the requirement(s) may be used for a specified period of time. This is in contrast to a *waiver* that implies a security requirement has been set aside and need not be implemented at all.]

Table 9.1 - Developing a System

Design & Development	T&E-I	T&E- II	O&M	Disposal
Determine Levels-of-Concern Determine Protection Levels Define Security Requirements Define Threats, Vulnerabilities, Risks, and Counter-measures Revise Security Requirements (Information Matrix and Requirements Table) Develop SSP Approve SSP	Develop Certification Test Plan and Procedures	Perform Certification Evaluation Perform Security Testing Identify Shortfalls Define Vulnerabilities Conduct Risk Analysis — Identify and Prioritize Risks Identify additional Counter-measures Make risk assessment recommendations Develop Certification Package Obtain interim approval to operate if applicable Obtain Accreditation	IS is Recertified and IS is Reaccredited	Perform Secure Disposal

9.F.1.a The written request for an exception shall state explicitly:

9.F.1.a(1) The requirements that are to be excepted and for what duration. The request shall include evidence stating why the identified requirements cannot be implemented, and indicate the countermeasures that are to be substituted.

9.F.1.a(2) What aspect of the threat or associated vulnerabilities is related to the proposed request. The request shall include evidence that the consequent risk to the system and to the information it processes, stores, or transmits will be acceptable based on other countermeasures that will be employed over the specified period.

9.F.1.a(3) A plan for implementing the “excepted” security requirements later in the life cycle of the system shall be developed.

9.F.1.a(4) Approval of the exception will make it incumbent upon the accrediting authority responsible for the system to ensure that the necessary programmatic, planning, and funding steps are taken to ensure implementation of any security requirements that are temporarily postponed as a consequence of approval of the exception.

9.F.2 There shall be no exceptions to the following requirements:

9.F.2.a Development of a System Security Plan (including a User's Security Guide when applicable).

9.F.2.b Implementation of a security training and awareness program.

9.F.2.c Compliance with all applicable physical, personnel, and communications security requirements.

9.F.2.d The appointment of an ISSO.

9.F.2.e Completion of risk management requirements described in paragraph 9.B, above, the certification process described in paragraph 9.C, above, and the formal acceptance of the risk of operation by the designated accrediting authority as specified in paragraph 2.B.4, above.

9.G Special Categories of ISs

9.G.1 General

9.G.1.a This subsection describes several categories (e.g., dedicated servers, embedded systems, tactical systems) of ISs that can often be adequately secured without implementation of all the technical features specified in Chapters 4, 5, and 6. These systems are *not* exceptions or special cases of the requirements specified in Chapters 4, 5, and 6.

9.G.1.b Unthinkingly applying the technical security requirements specified in Chapters 4, 5, and 6 to these ISs could result in unnecessary costs and operational impacts. In general, the technical question is *where*, *when*, and *how* to apply a given set of safeguards, rather than *whether* to apply the safeguards. For many of these special ISs (such as dedicated servers, and tactical, data acquisition, and embedded systems), the physical security protections for the IS provide the required access control, while the application running on the platform provides the required user separation.

9.G.1.c These special systems still must undergo the C&A process (including risk management) described earlier in this chapter. A key part of that C&A process for these systems is determining whether all of the technical features specified in Chapters 4, 5, and 6 are applicable.

9.G.2 Dedicated Servers

9.G.2.a Certain specialized ISs, when acting as part of a network as dedicated servers, may need fewer technical security countermeasures. These ISs have the characteristics listed below:

9.G.2.a(1) No user code is present on the IS.

9.G.2.a(2) Only IS administrators and maintainers can access the system.

9.G.2.a(3) The IS provides non-interactive services to clients (e.g., packet routing or messaging services).

9.G.2.a(4) The hardware and/or application providing network services otherwise meets the security requirements of the network.

9.G.2.a(5) The risk of attack against the Security Support Structure using network communications paths is low.

9.G.2.a(6) The risk of attack against the Security Support Structure using physical access to the system itself is sufficiently low.

9.G.2.b The platform (i.e., hardware and operating system) on which the dedicated server runs usually needs meet no more than Protection Level 2 security requirements. The dedicated server may have a large number of clients (i.e., individuals who use the server's functional capabilities in a severely constrained way). The server application itself will have to provide the more stringent technical protections appropriate for the system's Protection Level and operational environment. Assurances appropriate to the Protection Level and Levels-of-Concern for the IS shall be implemented.

9.G.2.c An IS that *does have general users or does execute general user code* is not a dedicated server within the meaning of this section, and so shall meet all security requirements specified for its Protection Level and operational environment.

9.G.2.d The term "dedicated 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 implemented on a general-purpose computer platform could be accredited under this manual and, if such a system meets the specifications in a., above, the system's technical requirements could be characterized by this section.

9.G.2.e The use of the above technical security 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 IS. Changes to technical requirements are predicated upon adequate application of physical security and other appropriate security disciplines.

9.G.3 Embedded and Special-Purpose ISs. Some ISs have no general users, are incapable of alteration by users, and are designed and implemented to provide a very limited set of predetermined functions. For such ISs, if the DAA determines that the applications running on the IS provide an adequate level of security, then the security requirements specified in Chapters 4, 5, and 6 do not apply.

9.G.4 Tactical or Deployable Systems. A tactical system may be part of a fixed location or maintained in a deployable configuration so that it can be moved quickly to another location to support operational mission requirements. The system can operate in a stand-alone mode or be attached via communications to a mobile or fixed facility under an extended LAN or WAN configuration. Tactical systems shall provide the appropriate Protection Level and Levels-of-Concern based upon the operating environment, network connection requirements, portability, and degree of access to other systems. The Protection Level and Levels-of-Concern shall be applied while the system is in-garrison,

in-transit, and/or deployed. The DAA may require additional security requirements or safeguards for tactical systems while in-transit or in the deployed environment.

9.G.5 ISs With Group Authenticators

9.G.5.a Many of the security measures specified in this manual assume that an IS includes an acceptable level of individual accountability. This is normally assured by the use of unique user identifiers and authenticators. Operationally, the design of some ISs necessitates more than one individual using the same identifier/authenticator combination. Such situations are often referred to as requiring the use of group authenticators.

9.G.5.b 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. DAAs shall avoid situations in which the group authenticator is effectively the sole access control mechanism for the system. Use of group authenticators for broader access *after* the use of a unique authenticator for initial identification and authentication carries much less risk. The use of group authenticators shall be explicitly authorized by the DAA.

9.G.5.c Positions and applications requiring the use of group authenticators shall be discussed in the SSP.

9.G.6 Information Systems Using Periods Processing

9.G.6.a An IS is said to operate in a periods processing environment if it is appropriately sanitized between operations in differing Protection Level periods, or with differing user communities or data.

9.G.6.b As long as the sanitization procedures between each Protection Level segment have been approved by the DAA based on guidelines from the Data Owner(s) or responsible official(s), the IS need meet only the security requirements of each processing period, while in that period. If the sanitization procedures for use between periods are approved by the DAA(s), the security requirements for a given period are considered in isolation, without consideration of other processing periods. Such sanitization procedures shall be detailed in the SSP.

9.G.6.c Under periods processing, the highest sensitivity level and the most restrictive data processed on the system will determine the DAA. The DAA shall coordinate authorizations for using the system at lower or less restrictive levels.

9.G.7 Single-User, Standalone ISs. Extensive technical safeguards are normally inappropriate and inordinately expensive for single-user, standalone ISs. DAAs can approve administrative and environmental protections for such ISs, in lieu of technical safeguards. Except for systems that operate in a periods processing environment as specified above, ISs that have one user at a time, but have a total of more than one user, are multi-user ISs, and the DAA shall consider the systems as such in determining the Protection Level and the resulting security requirements.

Appendix A

CONTENTS OF AN INTERCONNECTION SECURITY AGREEMENT

A.A Policy Basis

An Interconnection Security Agreement (ISA) is required whenever a system accredited by one DAA is connected to another system accredited by a different DAA. It documents and formalizes the interconnection arrangement and stipulates specific requirements for it. This appendix provides general guidance regarding the ISA's contents, but individual ISAs may be tailored by mutual consent.

A.B Contents of an ISA

A.B.1 An ISA shall include the following items:

A.B.1.a A general description of the information to be offered to the interconnected system by each participating system.

A.B.1.b A description of the kinds of information services to be offered to the interconnected system by each participating system.

A.B.1.c A discussion of all security details pertinent to the exchange of information between the systems in question.

A.B.1.d A summary discussion of the aspects of trusted behavior expected by and from each system in the interconnected system.

A.B.1.e The detailed discussion of new or additional security awareness and training requirements, including assignment of responsibility for providing the training to all users of the interconnected system and, if appropriate, for developing new awareness and training materials.

A.B.2 The ISA shall address the following aspects of security:

A.B.2.a The security policies that each system's Security Support Structure is designed to enforce along with the security policies of the resultant interconnected system.

A.B.2.b The classifications, categories, and sensitivities of the information to be exchanged, in particular, the highest classification and sensitivity and the most restrictive protection requirements for information to be handled through the interconnection.

A.B.2.c The nature of the services (e.g., individual user, consumer, file query, general computational services) that each system is to provide.

A.B.2.d A careful and thorough description of the user community and/or information recipients to be served by the interconnected systems. The description must specify all formal access approvals required.

A.B.2.e The clearance circumstances and nationalities of the defined user communities, including the lowest clearance of any individual who will have access to the interconnected system.

A.B.2.f The Confidentiality Protection Level, Integrity and Availability Levels-of-Concern, and levels of technical requirements for all participating systems; a description of any revised or new restrictions to be placed on terminals, including their usage, location, and physical accessibility.

A.B.2.g Any special considerations for dial-up connections to any system in the proposed interconnection, including the security threats that such arrangements imply and the safeguards to protect against them.

A.B.2.h A specification of the security parameters to be transmitted by each system to others with which it wishes to exchange information or from which it solicits information or other services.

A.B.2.h(1) The nature of the security parameters may depend on, and be different for, various classes of service.

A.B.2.h(2) The security parameters to be exchanged between systems shall be sufficient for each system involved to ascertain the following information:

A.B.2.h(2)(a) Whether the requesting system is a legitimate requester.

A.B.2.h(2)(b) Whether the class of service requested falls within that prescribed by the ISA.

A.B.2.h(3) Transmission of user identification and its associated authentication could satisfy the requirement for these security parameters.

A.B.2.i Any required security parameters that are to be exchanged and that go beyond the established requirements of this document.

A.B.2.i(1) For example, sufficient security parameters may be required under some circumstances (e.g., personal accountability) to allow the respondent system to determine the following information:

A.B.2.i(1)(a) Whether a requesting individual user is authorized to receive the information and/or system services requested.

A.B.2.i(1)(b) Whether all details of the transaction fall within the individual-user services described in the ISA.

A.B.2.i(2) Transmission of some additional identifying parameter such as employee identification number or secondary authenticator could satisfy such an additional requirement.

A.B.2.j A description of the security protections in the data communications arrangements, both local to each participating system as well as the long-haul connections between them.

A.B.2.k A description of how participating systems will share the audit trail responsibilities and what events each will log. The information collected in the several audit trails when taken together constitutes the audit trail for the interconnected system; it must be adequate to meet the general purposes intended for audit trails.

A.B.2.l The details of an overall security plan for the interconnected system and assignment of responsibilities for producing and accepting the plan. This plan shall be an addendum to the security plans of each participating system.

A.B.2.m A description of the agreements made concerning the reporting of and responses to information security incidents.

Appendix B

GLOSSARY OF TERMS AND DEFINITIONS

Accountability. The property that allows auditing of information system activities to be traced to persons or processes that may then be held responsible for their actions.

Accreditation. The official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Administrative Security. The management constraints, operational, administrative, and accountability procedures and supporting control established to provide an acceptable level of protection for data.

Attack. Attempt to gain unauthorized access to an IS's services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality.

Authenticator. Means used to confirm the identity of a station, originator, or individual. For example, a password is often used to authenticate the individual using a particular user identifier.

Availability. Timely, reliable access to data and information services for authorized users.

Biometrics. Identification or recognition of a person based on distinguishing characteristics or traits (e.g., fingerprint, retinal pattern).

Blacklisting. Blacklisting is the process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to logon to the system, even with the "correct" authenticator. Blacklisting can be permanent (i.e., until lifted by administrative action), or temporary (i.e., until lifted by the system, without administrative action, usually after a time has elapsed). Blacklisting and lifting of a blacklisting are both security-relevant events.

Boundary. For purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system without a reliable human review by an appropriate authority. The location of such a review is commonly referred to as an "air gap."

Certification. The comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

Clearance. Formal certification of authorization to have access to classified information other than that protected in a special access program (including SCI). Clearances are of three types: CONFIDENTIAL, SECRET, and TOP SECRET. A TOP SECRET clearance permits access to TOP SECRET, SECRET, and CONFIDENTIAL material; a SECRET clearance, to SECRET and CONFIDENTIAL material; and a CONFIDENTIAL clearance, to CONFIDENTIAL material.

Clearing. Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

Client. An individual or a process acting on behalf of an individual who makes requests of a guard or dedicated server. The client's requests to the guard or dedicated server can involve data transfer to, from, or through the guard or dedicated server.

Collaborative Computing. The applications and technology (e.g., whiteboarding, group conferencing) that allow two or more individuals to share information in an inter- or intra-enterprise environment enabling them to work together toward a common goal.

Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes.

Controlled Interface. A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).

Counterintelligence. That phase of intelligence covering all activity devoted to neutralizing the effectiveness of hostile foreign intelligence collection activities.

Cryptanalysis. Operations performed in converting encrypted messages to plain text without initial knowledge of the cryptoalgorithm and/or key employed in the encryption.

Cryptographic Information. All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial.

Cryptographic System. The documents, devices, equipment, and associated techniques that are used as a unit to provide a means of encryption (enciphering or encoding).

Cryptography. Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Cryptologic Data. Information relating to cryptography and cryptanalysis.

Data Owner. The organization that has final statutory and operational authority for specified information.

Declassification (Media). An administrative action following sanitization of the IS or the storage media that the owner of the IS or media takes when the classification is lowered to unclassified. Declassification allows release of the media from the controlled environment if approved by the appropriate authorities.

Dedicated Server. A specialized IS in which there is no user code present, which can only be accessed by IS administrators and maintainers, and which provides non-interactive services to clients (e.g., packet routing or messaging services).

Degauss. (1) To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force, commonly referred to as demagnetizing, or (2) to reduce the correlation between previous and present data to a point that there is no known technique for recovery of the previous data.

Degausser. An electrical device or hand-held permanent magnet assembly that generates a coercive magnetic force for the purpose of degaussing magnetic storage media or other magnetic material.

Degaussing. A procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field.

Designated Accreditation Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Direct User. A user who is electronically connected to an IS typically via an interactive link and whose access is automatically limited in real-time by the IS on some basis (e.g., security clearance, authorization, need-to-know).

Disaster Recovery Plan. A plan that provides for the continuity of system operations after a disaster that makes normal system operation infeasible.

Discretionary Access Control (DAC). A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

Dominates. Security level S1 is said to dominate security level S2 if the hierarchical classification (confidential, secret, or top secret) of S1 is greater than or equal to that of S2 and the non-hierarchical categories (e.g., specific SCI or SAP controls) of S1 include all of those of S2 as a subset.

EMSEC/TEMPEST. The short name referring to investigation, study, and control of compromising emanations from IS equipment.

EPROM. The acronym for Erasable, Programmable, Read-Only Memory—a field-programmable read-only memory that can have the data content of each memory cell altered more than once. Sometimes referred to as a re-programmable read-only memory.

Extranet. A private network that uses Web technology, permitting the sharing of part of an enterprise's information or operations with suppliers, vendors, partners, customers, or other enterprises.

Formal Access Approval. Documented approval by a Data Owner to allow access to a particular category of information. Such access generally requires signing of an appropriate non-disclosure agreement, and entry of the individual's name on an access roster.

Group Authenticator. An authenticator that is used (sometimes in addition to a sign-on authenticator) to allow access to specific data or functions by members of a particular group, and that may be shared among all members of a group.

Indirect User. In contrast to a direct user, indirect users receive system output produced outside their control, either: (a) by an automated mechanism within the IS, or (b) from a process initiated by a direct user. An indirect user is precluded from initiating a process on the IS and receiving the output there from. An indirect user is one who is electronically connected to an IS by other than a direct, interactive link. An IS supporting indirect users does not have to withstand direct attacks against the system's security controls because an intervening processor(s) between the

user and the IS affords some protection and control. The processing capabilities of the IS must protect the data being processed from inadvertent control. The processing capabilities of the IS must protect the data being processed from inadvertent system spillage and misroutes; generally, the IS provides control over indirectly connected users who may attempt to gain unauthorized access to its protection facilities. While a wide range of security risks associated with this type of user exists, such risks are not considered to be as significant as those associated with directly connected users. There are no geographic restrictions on how far an indirectly connected user may be from an IS.

Information. The intelligence derived from the data on or about a system, or the intelligence obtained from the structure or organization of that data.

Information Assurance. Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Operations. Action taken to affect adversary information and information systems while defending one's own information and information systems.

Information System (IS). 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 (digital or analog); includes software, firmware, and hardware.

Information System Security Manager (ISSM). The manager responsible for an organization's information system security program.

Information System Security Officer (ISSO). The person responsible to the ISSM for ensuring that operational security is maintained for a specific IS, sometimes referred to as a Network Security Officer.

Integrity. Protection against unauthorized modification or destruction of information.

Integrity Lock. A cryptographic checksum designed and implemented so that the order of difficulty in undetectably modifying the item check summed (e.g., file, message) is comparable to the order of difficulty in breaking the cryptographic algorithm used.

Interconnected System. A set of separately-accredited systems that are connected together.

Intranet. A private network using Web technology that is employed within the confines of a given enterprise (e.g., internal to a business or agency).

Joint Accreditation. An accreditation process that is required when an IS is not under the sole jurisdiction of a single accrediting authority.

Least Privilege. The principle requiring that each subject is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

Level-of-Concern. A rating assigned to an IS by the DAA. A separate Level-of-Concern is assigned to each IS for confidentiality, integrity, and availability. The Level-of-Concern for confidentiality, integrity, and availability can be Basic, Medium, or High. The Level-of-Concern assigned to an IS for confidentiality is based on the sensitivity of the information it maintains, processes, and transmits. The Level-of-Concern assigned to an IS for integrity is based on the

degree of resistance to unauthorized modifications. The Level-of-Concern assigned to an IS for availability is based on the needed availability of the information maintained, processed and transmitted by the system for mission accomplishment, and how much tolerance for delay is allowed.

Malicious Code. Software or firmware that is designed with the intent of having some adverse impact on the confidentiality, integrity, or availability of an IS.

Mandatory Access Control (MAC). A means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity.

Master System Security Plan (MSSP). An identification of common security information for "similar systems" at a given site or facility. The MSSP, which is required for all site-based accreditations, contains the site CONOPS and architecture and includes a listing of all systems covered under the site based accreditation, a description of how the site complies with the requirements of this manual, and a "wiring diagram" showing external connections.

Media. All forms of storage (e.g., disks, memory, or paper output).

Memorandum of Agreement (MOA). A written agreement among the DAAs responsible for the information processed and maintained by an IS (or collection of ISs). The MOA stipulates all of the terms and conditions of the security arrangements that will govern the operation of the IS(s). The MOA shall include at least: (1) a general description of the information to be offered by each participating DAA; and (2) a discussion of all of the security details pertinent to the exchange of information between the DAAs. In addition, where the MOA is to cover an interconnected network of ISs of under the purview of different DAAs, then the MOA shall also include a description of the types of information services each participating IS will provide, and identify a lead DAA. If no lead DAA is named, then both parties share responsibility.

Mission-Critical [Information]. Any information processed, transmitted, stored, or displayed within or over a DoD SAP information system that is determined to be essential to the operational readiness or mission effectiveness of the DoD SAP community or its components, where essential refers to information related to any function, the loss of which would slow, impede, or stop the basic operations of the DoD SAP community.

Mission-Critical Information System. Any information system (or components thereof) that is used to process, store, or display mission-critical information.

Mobile Code. The code obtained from remote systems, transmitted across a network, and then downloaded onto and executed on a local system.

Multi-User System. A system that under normal operation has more than one user accessing it simultaneously. Systems that are accessed by more than one user sequentially (i.e., by one user at a time) without clearing or sanitization between users, are also considered to be multi-user systems; but the DAA can explicitly choose to protect such systems as if they were singleuser systems.

Non-Repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Named Object. An object that is sharable between users.

Need-to-Know. A determination made by an authorized holder of classified information that a prospective recipient of information requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Object. A passive entity that contains or receives information. Access to an object potentially implies access to the information that it contains.

Perimeter. Encompasses all those components of the system that are to be accredited by the DAA, and excludes separately accredited systems to which the system is connected.

Periods Processing. The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be purged of all information from one processing period before transitioning to the next.

Principal Accrediting Authority (PAA). The senior official having the authority and responsibility for all SAP information systems within an agency.

Privileged User. A user who has access to system control, monitoring, or administration functions (e.g., system administrator, system ISSO, maintainers, system programmers, etc.). See also Client.

Procedural Security. The management constraints, operational, administrative, and accountability procedures, and supplemental controls established to provide protection for sensitive information.

Processing. The state that exists when information is being accessed or acted-upon by one or more steps proceeding in a predetermined sequence or method.

Protected Distribution System (PDS). A wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control.

Protection Level. An indication of the implicit level of trust that is placed in a system's technical capabilities. A Protection Level is based on the classification and sensitivity of information processed on the system relative to the clearance(s), formal access approval(s), and need-to-know of all direct and indirect users that receive information from the IS without manual intervention and reliable human review. Protection Levels replace modes of operation defined in the 1988 DCID 1/16.

Purging. See Sanitizing.

Push Only Technology. The means by which data is presented to a user without a specific action initiated by that user. In client-server terminology, the server initiates, or "pushes," the data to the client, usually in accordance with a pre-established user profile. This interest profile typically contains information categories of interests, e.g., weather forecasts, stock quotes.

Push/Pull Technology. A combination of technologies for information dissemination and retrieval. Traditionally, data is retrieved by a user request, such as by a Web user. In this case, the user "pulls" information. Alternatively, an information server may "push" information to the client without client intervention, usually by applying a predefined profile that filters information.

Records Management. The policy for the tagging of information for records keeping requirements as mandated in the Federal Records Act and the National Archival and Records Requirements.

Remote Access. Any communication over a non-direct data link, including internets, intranets, client-server LANs, telephone lines, etc.

Remote Diagnostics/Maintenance. The operational procedure that involves connection of a system to an external (i.e., outside of the facility securing the system) remote service for analysis or maintenance.

Replay Attacks. An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

Residual Risk. Portion of risk that remains after security measures have been applied.

Responsible Official. The individual—approved in writing by the Data Owner—who has final statutory or operational responsibility for establishing protection requirements for a given piece of information within the responsible official's agency. Operationally, the responsible official makes decisions regarding protection of the Data Owner's information within the responsible official's agency.

Restricted Data (RD). All data concerning the following, but not including data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act:

- Design, manufacture, or utilization of atomic weapons;
- Production of special nuclear material; or
- Use of special nuclear material in the production of energy.

Risk. The expected loss from a given attack or incident. For an attack/defense scenario, risk is assessed as a combination of threat (expressed as the probability that a given action, attack or incident will occur, but may also be expressed as frequency of occurrence), vulnerability (expressed as the probability that the given action, attack, or incident will succeed, given that the action, attack or incident occurs) and consequence (expressed as some measure of loss, such as dollar cost, resources cost, programmatic impact, etc.). The total risk of operating a system is assessed as a combination of the risks associated with all possible threat scenarios. Risk is reduced by countermeasures.

Risk Analysis. Synonymous with risk assessment.

Risk Assessment. The process of analyzing the threats to and vulnerabilities of an information system, analyzing the potential impact that the loss of information or capabilities of a system would have on national security, and, based upon these analyses, identifying appropriate and cost-effective counter-measures.

Risk Management. The discipline of identifying and measuring security risks associated with an IS, and controlling and reducing those risks to an acceptable level.

Sanitizing. The removal of information from media or equipment such that data recovery using any known technique or analysis is prevented, as well as the removal of all classified labels and markings.

Security Concept of Operations (Security CONOPS). The guidance provided to those associated with a system concerning the standard operating procedures relating to security protection.

Security Incident. An act or circumstance in which there is a deviation from the requirements of the governing security regulations. Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of security incidents.

Security Label. A piece of information that represents the hierarchical classification (CONFIDENTIAL, SECRET, or TOP SECRET) and non-hierarchical compartments (e.g., specific SCI or SAP controls) of a subject or object and that thus describes the sensitivity of the data in the subject or object. Security labels are used as the basis for mandatory access control.

Security Markings. Indicators applied to a document, storage media, or hardware component to designate categorization and handling restrictions applicable to the information in the document.

Security Parameters. The highest classification and all appropriate associated security markings of the information processed.

Security Penetration Testing. System testing designed to evaluate the relative vulnerability of the system to hostile attacks. Penetration testers often try to obtain unauthorized privileges (especially attempts to obtain "root" or "superuser" privileges) by exploiting flaws in system design or implementation.

Security-Relevant Event. An event that an experienced ISSO would consider to require noting, investigation, or prevention (e.g., the discovery of malicious code in an IS, the discovery of an attempt to introduce malicious code into an IS). Security-relevant events include any event that would cause a deleterious change in the system or its environment.

Security Support Structure. Those components of a system (hardware, firmware, software, data, interfaces, storage media, and communications media) that are essential to the enforcement of the system's security policies.

Sensitive Compartmented Information. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCID 1/19).

Sensitive Compartmented Information Facility (SCIF). An accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or processed (DCID 6/9).

Special Access Program (SAP). A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level (EO 12958).

Special Access Program Facility (SAPF). A facility formally accredited by an appropriate agency in accordance with JAFAN 6/9 in which SAP information may be processed.

Storage. The state that exists when information is being held for use until needed for processing.

Storage Object. An object that supports both read and write accesses.

Strong Authentication. A form of authentication whereby it is very difficult or impossible for a hostile user to successfully intercept and employ a transmitted authenticator (i.e., highly resistant to replay attack).

Subject. An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or that changes the system state.

System. An Information System (IS).

System Security Plan (SSP). The description of the necessary protections to allow the system to operate securely. A sample SSP is described in Appendix C.

TEMPEST. See EMSEC

Threat. Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Transmission. The state that exists when information is being sent from one location to one or more other locations.

Trusted Facility Manual. The document containing the operational requirements; security environment; hardware and software configurations and interfaces; and all security procedures, measures, and contingency plans.

Trusted Path. A mechanism by which a person at a terminal can communicate directly with the Security Support Structure. This mechanism can be activated only by the person or the Security Support Structure and cannot be imitated by untrusted software, hardware, and firmware.

User. An individual who can receive information from, input information to, or modify information on, a system without a reliable human review. In a processing context, this also includes a process acting on behalf of a user. It is often convenient to refer to a user who is NOT a privileged user as a General User.

User Code. Executable software or firmware selected, controlled, or generated by a general user and not under the explicit control of a privileged user.

Vulnerability. A weakness in an IS, or cryptographic system, or component (e.g., system security procedures, hardware design, internal controls) that could be exploited.

Appendix C

SAMPLE SYSTEM SECURITY PLAN

C.A This appendix provides ISSOs an annotated outline for preparing System Security Plans (SSP) that include the necessary overviews, descriptions, listings, and procedures and that help meet the requirements contained in this document. ISSOs may modify the outline as necessary to address the unique characteristics of specific systems, including creating additional subtitles to accommodate any information that does not appropriately fit under one of those provided. This outline is not directive in nature; the contents and format of the SSP are at the discretion of the DAA.

C.B Where the information exists in another document, it need not be included in the SPP, but can be referenced and provided as required.

C.C To amend an existing plan when there is no need to revise it in its entirety, an ISSO may issue revisions as either a separate document with instructions to make pen-and-ink changes in the original plan or as amended pages. In either case, the revisions will clearly indicate the name and date of the plan being modified and the date of the revision. When issuing amended pages, the changed material must be clearly marked as such.

OUTLINE

ANNOTATED OUTLINE

1.0 INTRODUCTION

Describe the purpose and scope of the SSP, provide an overview of its contents, and explain its format. The Introduction may include any topic intended to help the reader understand and appreciate the purpose of the SSP. Pertinent background information may also be presented to provide clarity.

1.1 Security Administration

Provide the name of the system and the date of the plan, and indicate whether it is an original or revised plan. Identify the system owner whose activity it will support and any applicable contract numbers.

Provide the system owner's name and address. Identify the location of the system equipment (including the building and room number [s]).

Provide the names, telephone numbers (including secure numbers, if appropriate), and normal office hours of the ISSM, ISSO, and their alternates, if any. If there are multiple DAAs for the system, provide the agreements under which the system will operate. Provide an organizational structure showing the name and title of all security management levels above the ISSO.

Provide joint-use information, if applicable.

1.2 Mission

Describe how the security of the system will be managed. State the purpose or mission and scope of the system. Identify the projects the system supports.

2.0 SECURE FACILITY DESCRIPTION

Provide a physical overview of the facility (including its surroundings) housing the system. Include information about the secure environment required to protect the system equipment, software, hardware, and firmware, media, and output.

2.1 Physical Environment

State whether the secure facility is accredited or approved to process and store information at the level covered by the SSP, who accredited or approved it, the maximum level of information allowed, and when approved. State whether the secure facility is approved for open or closed storage.

State whether the approval includes unattended processing.

Specify whether the storage approval is for systems, hard disk drives, diskettes, tapes, printouts, or other items.

2.2 Floor Layout

Provide a floor plan showing the location of system equipment and any protected distribution systems. (This may be included in a referenced appendix.) The building and room number(s) must match the information provided in the hardware listing (see 4.0).

2.3 Secure Facility Access

Describe procedures for controlling access to the system, including personnel access controls, after-hours access, and procedures for providing access to uncleared visitors (e.g., admitting, area sanitizing, escorting).

2.4 TEMPEST

If applicable, describe TEMPEST requirements.

3.0 SYSTEM DESCRIPTION

Provide a detailed description of the system.

3.1 General Information

Provide a system overview and description.

Specify clearance level, any formal access requirements, and need-to-know requirements that are being supported.

Identify the data to be processed, including classification levels and any relevant compartments and special handling restrictions.

State the Protection Level for confidentiality.

State the Levels-of-Concern for confidentiality, integrity, and availability for all information on the system.

Indicate the percentage of the system's usage that will be dedicated to the Government's activity (e.g., periods processing).

Identify any system users who are not US citizens.

3.2 Interconnection Interface Description

Describe how the system is configured. Describe the security support structure and identify any specialized security components and their role.

Identify and describe procedures for any connectivity to the system. Indicate whether the connections are to be classified or unclassified systems.

Provide a simplified block diagram that shows the logical connectivity of the major components. (This may be shown on the floor layout if necessary [see 2.2].) For systems operating at Protection Levels 3, 4, or 5, provide an information flow diagram.

If applicable, discuss the separations of classified and unclassified systems within the secure facility.

3.3 Residual Risk

Provide a description of the residual risk of operating the system after the security requirements specified in this document have been implemented.

4.0 SYSTEM HARDWARE

Provide a complete listing of the major hardware. This list may be in tabular form located either in this section or a referenced appendix. The following information is required for all

major system hardware: nomenclature, model, location (i.e., building/room number), and manufacturer.

Provide a description of any custom-built system hardware.

Indicate whether the system hardware has volatile or nonvolatile memory components. Identify the nonvolatile components.

Describe the procedures for the secure control, operation, and maintenance of the hardware. If they have been authorized, describe the procedures for using readily transportable systems for unclassified processing in the secure facility.

5.0 SYSTEM SOFTWARE

Provide a complete listing of system software, including security software (e.g., audit software, anti-virus software), special-purpose software (e.g., in-house, custom, commercial utilities), and operating system software. This list may be in tabular form and may be located either in the section or in a referenced appendix. The following information is required for security-relevant software: software name, version, manufacturer, and intended use or function.

6.0 DATA STORAGE MEDIA

Provide a description of the types of data storage media. Discuss their controls. Indicate whether the system is configured with removable or non-removable hard disk drives.

7.0 SECURITY REQUIREMENTS

7.1 System-Specific Threats

Discuss any system-specific threats to the security of the information on the system.

7.2 User Access and Operation

Describe the system operation start-up and shut-down (mode termination). Provide any unique equipment clearing procedures.

Discuss all system user access controls (e.g., log-on ID, authenticators, file protections).

Identify the number of privileged users and the criteria used to determine privileged access.

If DAC or MAC is required, discuss those mechanisms that implement the DAC and MAC controls.

Discuss procedures for the assignment and distribution of authenticators, their frequency of change, and the granting of access to information and/or files.

Indicate whether system operation is required 24 hours per day.

Discuss procedures for after-hours processing.

7.3 Protection of the Security Support Structure

Discuss the protections provided to the Security Support Structure.

7.4 Security Features and Assurances

Discuss procedures for incident reporting.

Discuss remote access and operations requiring specific approval by the Government security authority.

Describe the configuration management program. Describe the procedures to ensure that changes to the system are coordinated with the ISSO before being implemented.

Discuss any security features unique to the system.

Discuss the auditing procedures used to monitor user access and operation of the system and the information that is to be recorded in the audit trail. State whether user access audit trails are manual or automatic.

Identify the individual responsible for ensuring the review of audit trails and how often the reviews must be performed.

Describe procedures for handling discrepancies found during audit trail reviews.

Describe all system hardware maintenance logs, the information recorded on them, the individual responsible for reviewing them, and how often they are reviewed.

7.5 Marking and Labeling

Describe how the system hardware will be labeled to identify its classification level, if applicable, for example, when classified and unclassified systems are co-located in the same secure area.

Describe how the data storage media will be labeled (identify the classification level and contents).

Discuss how classified and unclassified data storage media is handled and secured in the secure facility (e.g., safes, vaults, locked desk).

Discuss procedures for marking and controlling system printouts.

7.6 Maintenance Procedures

Describe the procedures to be used for maintenance or repair of defective systems.

7.7 Sanitization and Destruction

Describe the procedures or methods used to sanitize and or destroy software and hardware (volatile or nonvolatile components).

Describe the procedures or methods used to clear, sanitize, and destroy the data storage media.

7.8 Software Procedures

Indicate whether a separate version of the operating system software will be used for maintenance.

Describe the procedures for procuring and introducing new system software to support program activities.

Describe the procedures for evaluating system software for security impacts.

Describe procedures for protecting software from computer viruses and malicious code and for reporting incidents.

7.9 Media Movement

Describe the procedures or receipting methods for moving data storage media into and out of the secure facility.

Describe the procedures for copying, reviewing, and releasing information on data storage media.

Describe the procedures or receipting methods used to release and transport the system hardware from the secure facility.

Describe the procedures or receipting methods for temporarily or permanently relocating the system hardware within the secure facility.

Describe the procedures for introducing hardware into the secure facility.

8.0 SECURITY AWARENESS PROGRAM

Discuss the security awareness program.

9.0 INTERCONNECTION SECURITY AGREEMENT

Discuss any Interconnection Security Agreements or other agreements that are in place.

10.0 MEMORANDUM OF AGREEMENT/UNDERSTANDING (MOA/MOU)

Identify the MOA/MOU for those jointly accredited systems which require an MOA/MOU; include a copy of the document in an appendix.

11.0 EXCEPTIONS

Discuss any exceptions granted to the system operation.

12.0 GLOSSARY OF TERMS

List all special terms used in the SSP, including acronyms, with their meaning.

Appendix D

REQUIRED SYSTEM SECURITY FEATURES AND ASSURANCES TABLES

The following pages restate in tabular form the requirements established Chapters 4, 5, and 6. It is also necessary to implement the requirements from Chapter 7 ("Requirements for ISs and Advanced Technology") and Chapter 8 ("Administrative Security Requirements").

To use these tables, find the column representing the Protection Level for confidentiality or, for the integrity and availability tables, the Level-of-Concern. An "X" in the column indicates the requirement is mandatory, and an "A/R" indicates the requirement is optional (i.e., as required by the DAA).

The requirements themselves are spelled out following the tables, beginning on page D-2.

Table D.1 - Confidentiality Protection Level (PL)

Confidentiality	PL1	PL2	PL3	PL4	PL5
Access1	X	X	X	X	X
Access2		X	X	X	X
Access3			X		
Access4				X	X
Access5				X	X
AcctMan	A/R	X	X	X	X
Audit1	A/R	X	X	X	X
Audit2		X			
Audit3		A/R	X	X	X
Audit4			X		
Audit5			X	X	
Audit6				X	X
Audit7				X	
Audit8					X
Audit9					X
CCA				A/R	X
Doc1	X	X	X	X	X
Doc2		X	X	X	X
Doc3		A/R	X		
Doc4				X	X
I&A1	X				
I&A2	A/R	X	X	X	X
I&A3	A/R	X			
I&A4		X	X	X	X
I&A5			X	X	X
I&A6				X	X
Label1				X	X
Label2				X	X
LeastPrv		X	X	X	X
Marking		X	X		

Confidentiality	PL1	PL2	PL3	PL4	PL5
ParamTrans	X	X	X	X	X
Recovery	X	X	X	X	X
ResrcCtrl		X	X	X	X
ScrnLck	X	X	X	X	X
Separation			X	X	X
SessCtrl1	X	X	X	X	X
SessCtrl2		X	X	X	X
Storage	X	X	X	X	X
SysAssur1	X	X	X	X	X
SysAssur2		X	X	X	X
SysAssur3			X	X	X
SysAssur4				X	X
Test1	X				
Test2		X	X	X	X
Test3		A/R	X	X	X
Test4			A/R	X	
Test5					X
Trans1	X	X	X	X	X
TranSep				X	X

Table D.2 - Integrity Level-of-Concern

Integrity	Basic	Medium	High
Backup1	X		
Backup2		X	
Backup3		X	
Backup4			X
Change1		X	X
Change2			X
CM1	X	X	X
CM2		X	X
CM3			X
Integrty1	X		
Integrty2		X	X
Integrty3		X	X
MalCode	X	X	X
Recovery			X
SysIntgr1			X
SysIntgr2			X
Trans2			X
Validate		X	X
Verif1	X	X	
Verif2			X

Table D.3 - Availability Level-of-Concern

Integrity	Basic	Medium	High
Avail	X	X	X
Backup1	X		
Backup2			
Backup3		X	
Backup4			X
Backup5		X	X
Backup6			X
Commun		X	X
Cont1		X	X
Cont2			X
DOS			X
Maint		X	X
Monit			X
Power1		X	X
Power2		A/R	X
Priority			X
Recovery		X	X
Verif1	X	X	
Verif2			X

SYSTEM SECURITY FEATURES AND ASSURANCES

This section presents the requirements from Chapters 4, 5, and 6 in an alphabetic list.

[Access1]	Access control, including: Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel. Procedures controlling access by users and maintainers to IS resources, including those that are at remote locations.
[Access2]	Access Control including a Discretionary Access Control (DAC) Policy. A system has implemented DAC when the Security Support Structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The DAC policy includes administrative procedures to support the policy and its mechanisms. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest [COIs], encryption) shall allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The DAC mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.
[Access3]	Access Control, including: • Some process or mechanism(s) that allows users (or processes acting on their behalf) to determine the formal access approvals (e.g., compartments into which users are briefed) granted to another user. This process or mechanism is intended to aid the user in determining the appropriateness of information exchange. • Some process or mechanism(s) that allow users for (or processes acting on their behalf) to determine the sensitivity level (i.e., classification level, classification category, and handling caveats) of data. This process or mechanism is intended to aid the user in determining the appropriateness of information exchange.
[Access4]	Access Control, including assurance that each user shall receive from the system only that information to which the user is authorized access.

[Access5]	Access Control, including a Mandatory Access Control (MAC) Policy that shall require: • The Security Support Structure to enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices). • These subjects and objects to be assigned sensitivity labels that combine hierarchical classification levels and non-hierarchical categories; the labels shall be used as the basis for mandatory access control decisions. • The Security Support Structure to be able to support two or more such security levels. • Identification and authentication data to be used by the Security Support Structure to authenticate the user's identity and to assure that the security level and authorization of subjects external to the Security Support Structure that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user. • Application of the following restrictions to all accesses between subjects and objects controlled by the Security Support Structure: o A subject can read an object only if the security level of the subject dominates* the security level of the object (i.e., a subject can "read down"). [*Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the non-hierarchical categories of S1 include all those of S2.] o A subject can write to an object only if two conditions are met: the security level of the object must dominate the security level of the subject, and the security level of the *user's clearance** must dominate the security level of the object (i.e., a subject can "write up," but no higher than the user's clearance). [*In those instances where a subject is an electronic entity (e.g., a process), then the subject is generally acting on the behalf of a user.]
[AcctMan]	Account Management procedures that include: • Identifying types of accounts (individual and group, conditions for group membership, associated privileges). • Establishing an account (i.e., required paperwork and processes). • Activating an account. • Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators). • Terminating an account (i.e., processes and assurances).

[Audit1]	Auditing procedures, including: • Providing the capability to ensure that all audit records include enough information to allow the ISSO to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved. • Protecting the contents of audit trails against unauthorized access, modification, or deletion. • Maintaining collected audit data at least 12 months or one security review cycle, whichever is longer, and reviewing at least weekly. • The system's creating and maintaining an audit trail that includes selected records of: • Successful and unsuccessful logons and logoffs. • Accesses to security-relevant objects and directories, including opens, closes, modifications, and deletions. • Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.
[Audit2]	Auditing procedures, including: • Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual) shall be enforced. • Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or detection.
[Audit3]	Audit procedures that include the existence and use of audit reduction and analysis tools.
[Audit4]	An audit trail, created and maintained by the IS, that is capable of recording changes to mechanism's list of user formal access permissions. (NOTE: Applicable only if the **[Access3]** access control mechanism is automated.)

[Audit5]	Auditing procedures, including: • Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual). • Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion. These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.
[Audit6]	Auditing procedures, including: • Enforcement of the capability to audit changes in security labels. • Enforcement of the capability to audit accesses or attempted accesses to objects or data whose labels are inconsistent with user privileges. • Enforcement of the capability to audit all program initiations, information downgrades and overrides, and all other security-relevant events (specifically including identified events that may be used in the exploitation of covert channels). In the event of an audit failure, system shutdown unless an alternative audit capacity exists.
[Audit7]	Auditing procedures, including: • The capability of the system to monitor occurrences of, or accumulation of, auditable events that may indicate an imminent violation of security policies. • The capability of the system to notify the ISSO of suspicious events and taking the least-disruptive action to terminate the suspicious events.

[Audit8]	Auditing procedures, including: • Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual). • At least monthly testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion. These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.
[Audit9]	Auditing procedures, including: • The capability of the system to monitor, in real-time, occurrences of, or accumulation of, auditable events that may indicate an imminent violation of security policies. • The capability of the system to notify the ISSO of suspicious events and taking the least-disruptive action to terminate the suspicious event.
[Avail]	Processes and procedures to allow for the restoration* of the system. [*Restoration of service is a necessary function to guard against both natural disasters and denial-of-service attacks.]
[Backup1]	Backup procedures, including good engineering practice with regard to backup policies and procedures.
[Backup2]	Backup procedures to ensure both the existence of sufficient backup storage capability and effective restoration* of the backup data. [*In this context, restoration includes both incremental and complete replacement of the system's contents from the contents of the backup media.]
[Backup3]	Backup storage that is located to allow the prompt restoration of data. If required by the DAA, there shall additionally be off-site backup storage of the data, as per approved SSP; such storage is intended to enable recovery if a single event eliminates both the original data and the on-site backup data. If regular off-site backup is not feasible, such as on a ship at sea, alternative procedures, such as secure transmission of the data to an appropriate off-site location, should be considered.

[Backup4]	Backup procedures, including: • A capability to conduct backup storage and restoration of data and access controls. Frequent backups of data.* [*In this context, frequent means after any significant system hardware, software, or firmware change, and, in any case, no less often than once per year.] • At least annual restoration of backup data. • Backup storage that is located to allow the immediate restoration of data. There shall additionally be off-site backup storage of the data, as per approved SSP; such storage is intended to enable recovery if a single event eliminates both the original data and the on-site backup data. If regular off-site backup is not feasible, such as on a ship at sea, alternative procedures, such as secure transmission of the data to an appropriate offsite location, should be considered.
[Backup5]	Backup procedures to allow the restoration of operational capabilities with minimal loss of service or data. These procedures shall require: • Frequent backups of data. • To the extent deemed necessary by the DAA, assurance that system state after the restore will reflect the security-relevant changes to the system between the backup and the restore. • Assurance that the availability of information in storage is adequate for all operational situations and that catastrophic damage to any single storage entity will not result in system-wide loss of information. These policies shall include, among others, procedures for ensuring the physical protection of operational and backup media and equipment, and for ensuring the continued functionality of the operational and backup media and equipment. • Restoration of any security-relevant segment of the system state (e.g., access control lists, cryptologic keys, deleted system status information) without requiring destruction of other system data.
[Backup6]	Backup procedures, including: • Assurance that the system state after the restore will reflect security-relevant changes to the system between the backup and the restore. • Consideration to the use of technical features that enhance data integrity and availability including, among others, remote journaling, Redundant Array of Inexpensive Disks (RAID) 1 and above, and similar techniques.

[CCA]	At the discretion of the DAA, a thorough search for covert channels shall be conducted, and a determination shall be made of the maximum bandwidth of each identified channel.
[Change1]	Change Control that includes: • Mechanisms that notify users of the time and date of the last change in data content. • Procedures and technical system features to assure that changes to the data or to security-related items are: • Executed only by authorized personnel. • Properly implemented.
[Change2]	Change Control that includes: • A secure, unchangeable audit trail that will facilitate the correction of improper data changes. • Transaction-based systems (e.g., database management systems, transaction processing systems) shall implement transaction roll-back and transaction journaling, or technical equivalents.
[Commun]	Communications capability that provides adequate communications to accomplish the mission when the primary operations communications capabilities are unavailable.
[CM1]	Configuration Management (CM) that includes: • Policies that assure the effectiveness of storage integrity. • Procedures to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.
[CM2]	Configuration Management that includes: • A CM Plan, including: o Policies that assure storage integrity. o Procedures for identifying and documenting system connectivity, including any software, hardware, and firmware used for all communications (including, but not limited to wireless, IR, etc.). o Procedures for identifying and documenting the type, model, and brand of system or component, security relevant software, hardware, and firmware product names and version or release numbers, and physical locations. • A CM process to implement the CM Plan.

[CM3]	Configuration Management that includes: • A CM process to test, and verify the CM Plan periodically. • A CM control board, which includes the ISSM/ISSO as a member. • A verification process that assures it is neither technically nor procedurally feasible to make changes to the Security Support Structure outside of the CM process.
[Cont1]	Contingency Planning that includes a Contingency/Disaster Recovery Plan.
[Cont2]	Contingency Planning, including: • Adequate hardware, firmware, software, power, and cooling to accomplish the mission when the operational equipment is unavailable. Consideration shall be given to fault-tolerant or "hot-backup" operations. The decision whether or not to use these techniques must be explicit. • Regular exercising and testing of the contingency plans. The plans for the tests shall be documented in the Contingency/Disaster Recovery Plan.
[Doc1]	Documentation shall include: • A System Security Plan (see Appendix C). • A Security Concept of Operations (CONOPS) (the Security CONOPS may be included in the System Security Plan). The CONOPS shall at a minimum include a description of the purpose of the system, a description of the system architecture, the system's accreditation schedule, the system's Protection Level, integrity Level-of-Concern, availability Level-of-Concern, and a description of the factors that determine the system's Protection Level, integrity Level-of-Concern, and availability Level-of-Concern.
[Doc2]	Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.

[Doc3]	The DAA may direct that documentation also shall include: • Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level. • Reports of test results. • A general user's guide which describes the protection mechanisms provided, guidelines on how the mechanisms are to be used, and how the mechanisms interact.
[Doc4]	Documentation shall include: • Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level. • Reports of test results. • A general user's guide that describes the protection mechanisms provided, and that supplies guidelines on how the mechanisms are to be used, and how they interact. • Documentation, including System Design Documentation, if applicable.
[DOS]	Prevention of Denial of Service Attacks.* Where technically feasible, procedures and mechanisms shall be in place to curtail or prevent well-known, detectable, and preventable denial of service attacks (e.g., SYN attack). [*Only a limited number of denial-of-service attacks are detectable and preventable. Often, prevention of such attacks is handled by a controlled interface (see Chapter 7 for a discussion on controlled interfaces).]
[I&A1]	Identification and Authentication (I&A) procedures that include provisions for uniquely identifying and authenticating the users. Procedures can be external to the system (e.g., procedural or physical controls) or internal to the system (i.e., technical). Electronic means shall be employed where technically feasible.

[I&A2]	An Identification and Authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified:* [*Alternative controls, such as biometrics or smart cards, may be used at the discretion of the DAA. These alternative methods may have similar requirements. For example, the electronically stored version of biometric authentication patterns needs to be protected, as do password authenticators.] • Initial authenticator content and administrative procedures for initial authenticator distribution. • Individual and Group authenticators. (Group authenticators may only be used in conjunction with an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator). • Length, composition, and generation of authenticators. • Change Processes (periodic and in case of compromise). • Aging of static authenticators (i.e., not one-time passwords or biometric patterns). • History of authenticator changes, with assurance of non-replication of individual authenticators, per direction in approved SSP. • Protection of authenticators to preserve confidentiality and integrity.
[I&A3]	Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links (extranets, Internet, phone lines) that are outside of the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks).
[I&A4]	Identification and Authentication. In those instances where the means of authentication is user-specified passwords, the ISSO or ISSM may employ (under the auspices of the DAA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover a user's password.
[I&A5]	Identification and Authentication. In those instances where the users are remotely accessing the system, the users shall employ a strong authentication mechanism (i.e., an I&A technique that is resistant to replay attacks).
[I&A6]	Identification and Authentication management mechanisms that include: Implementation and support of a trusted communications path between the user and the Security Support Structure of the desktop for login and authentication. Communication via this path shall be initiated exclusively by the user and shall be unmistakably distinguishable from other paths. In the case of communication between two or more systems (e.g. client server architecture), bi-directional authentication between the two systems.

[Integrty1]	Good engineering practice with regard to COTS integrity mechanisms, such as parity checks and Cyclical Redundancy Checks (CRCs).
[Integrty2]	Data and software storage integrity protection, including the use of strong storage integrity mechanisms (e.g., integrity locks, encryption).
[Integrty3]	Integrity, including the implementation of specific non-repudiation capabilities (e.g., digital signatures), if mission accomplishment requires non-repudiation.
[Label1]	Labeling procedures, including: • Internal security labels that are an integral part of the electronic data or media. • Procedures for managing content, generation, attachment, and persistence of internal labels that are documented in the SSP. • Security labels that reflect the sensitivity (i.e., classification level, classification category, and handling caveats) of the information. • Maintenance by the Security Support Structure of a record of the kind(s) of data allowed on each communications channel. • A means for the system to ensure that labels that a user associates with information provided to the system are consistent with the sensitivity levels that the user is allowed to access.
[Label2]	Labeling procedures, including internal and external labeling such as label integrity, exportation, subject-sensitivity labels, and device labels, as applicable.
[LeastPrv]	Least Privilege procedures, including the assurance that each user or process is granted the most restrictive set of privileges or accesses needed for the performance of authorized tasks shall be employed.
[Maint]	Maintenance procedures that include preventive maintenance, scheduled to maximize the availability of the system, and thus to minimize interference with the operation of the system. Planning for maintenance shall include at least: • On-call maintenance. • On-site diagnostics. • Control of Remote Diagnostics, where applicable.
[MalCode]	Procedures to prevent the introduction of malicious code into the system, including the timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).

[Marking]	Marking procedures and mechanisms to ensure that either the user or the system itself marks all data transmitted or stored by the system to reflect the sensitivity of the data. This marking shall reflect the sensitivity (i.e., classification level, classification category, and handling caveats). Markings shall be retained with the data.
[Monit]	Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and concurrence of legal counsel. The monitoring tools shall be used for the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.
[ParamTrans]	Parameter Transmission. Security parameters (e.g., labels, markings) shall be reliably associated (either explicitly or implicitly) with information exchanged between systems.
[Power1]	System Availability, including, by default for a multi-user system, conditioned, battery-backed power adequate to allow the system to be fail-soft. If the system is multi-user, the decision not to use an Uninterruptible Power Supply (UPS) for the system shall be explicit.
[Power2]	System Availability, including, as required by the DAA, procedures for graceful transfer of the system to an alternate power source; these procedures shall ensure that the transfer is completed within the timing requirements of the application(s) on the system.
[Priority]	Priority protection that includes no "Deny Up" (i.e., a lower-priority process shall not be able to interfere with the system's servicing of any higher-priority process).
[Recovery]	Recovery procedures and technical system features to assure that system recovery is done in a trusted and secure manner. If any circumstances can cause an untrusted recovery, such circumstances shall be documented and appropriate mitigating procedures shall be put in place.
[ResrcCtrl]	Resource Control. All authorizations to the information contained within an object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the Security Support Structure's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system. There must be no residual data from the former object.

[ScrnLck]	Screen Lock. Unless there is an overriding technical or operational problem, a terminal/desktop/laptop screen-lock functionality shall be associated with each terminal/desktop/laptop computer. When activated, a screen-lock function shall place an unclassified pattern onto the entire screen of the terminal/desktop/laptop, totally hiding what was previously visible on the screen. Such a capability shall: • Be enabled either by explicit user action or if the desktop/terminal/laptop is left idle for a specified period of time (e.g., 15 minutes or more). • Ensure that once the desktop/laptop/terminal security/screen-lock software is activated, access to the desktop/terminal/laptop requires knowledge of a unique authenticator. • Not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).
[Separation]	Separation of Roles. The functions of the ISSO and the system manager/system administrator shall not be performed by the same person.
[SessCtrl1]	Session Controls, including: • Notification to all users prior to gaining access to a system that system usage may be monitored, recorded, and subject to audit. Electronic means shall be employed where technically feasible. • Notification to all users that use of the system indicates (1) the consent of the user to such monitoring and recording and (2) that unauthorized use is prohibited and subject to criminal and civil penalties. Electronic means shall be employed where technically feasible.
[SessCtrl2]	Enforcement of Session Controls, including: • Procedures for controlling and auditing concurrent logons from different workstations. • Station or session time-outs, as applicable. • Limited retry on logon as technically feasible. • System actions on unsuccessful logons (e.g., blacklisting of the terminal or user identifier).

[Storage]	Data Storage, implementing at least one of the following: • Information stored in an area approved for open storage* of the information. [*In the context of storage confidentiality, "approval for open storage" must include consideration of the possibility of access by all users who have direct access to the system or network, wherever physically located.] • Information stored in an area approved for continuous personnel access control (when continuous personnel access control is in effect), i.e., a 24-hour, 7-day-a-week operational area. • Information secured as appropriate for closed storage. • Information encrypted using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of the stored data.
[SysAssur1]	System Assurance shall include: • Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware. • Features or procedures for protection of the operating system from improper changes.
[SysAssur2]	System Assurance shall include: • Control of access to the Security Support Structure (i.e., the hardware, software, and firmware that perform operating system or security functions). • Assurance of the integrity of the Security Support Structure.
[SysAssur3]	System Assurance shall include: • Isolating the Security Support Structure, by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. • Using up-to-date vulnerability assessment tools to validate the continued integrity of the Security Support Structure by ensuring that the system configuration does not contain any well-known security vulnerabilities.
[SysAssur4]	System Assurance. The Security Support Structure shall maintain separate execution domains (e.g., address spaces) for each executing process.
[SysIntgr1]	System Integrity that includes isolation of the Security Support Structure, by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions.

[SysIntgr2]	System Integrity, such that the Security Support Structure maintains separate execution domains (e.g., address spaces) for each executing process.
[Test1]	Assurance shall be provided by the ISSM to the DAA that the system operates in accordance with the approved SSP, and that the security features, including access controls and configuration management, are implemented and operational.
[Test2]	The ISSM shall provide written verification to the DAA that the system operates in accordance with the approved SSP, and that the security features, including access controls, configuration management, and discretionary access controls, are implemented and operational.
[Test3]	Additional testing, at the discretion of the DAA. Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional. A test plan and procedures shall be developed and shall include: • A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability. • A detailed description of the assurances that have been implemented, and how this implementation will be verified. • An outline of the inspection and test procedures used to verify this compliance.
[Test4]	Testing, including: • Security Penetration Testing shall be conducted to determine the level of difficulty in penetrating the security countermeasures of the system. • An Independent Validation and Verification team shall be formed to assist in the security testing and to perform validation and verification testing of the system.
[Test5]	Testing shall include: • Security Penetration Testing to determine the level of difficulty in penetrating the security countermeasures of the system. • Formation of an Independent Verification and Validation team that at least annually assists in security testing and performing validation and verification testing of the system.

[Trans1]	Data Transmission. Data transmission that implements at least one of the following: • Information distributed only within an area approved for open storage of the information. • Information distributed via a Protected Distribution System* (PDS). [*A PDS provides physical protection or intrusion detection for communications lines. A PDS can also provide need-to-know isolation for communications lines.] • Information distributed using NSA-approved encryption mechanisms appropriate (see paragraph 1.G.1) for the classification of the information. • Information distributed using a trusted courier. • Dial-up lines, other than those that are protected with nationally certified cryptographic devices or PDSs, shall not be used for gaining access to system resources that process SAP information unless the DAA provides specific written authorization for a system to operate in this manner.
[Trans2]	Data Transmission, including: • Integrity mechanisms adequate to assure the integrity of transmitted information (including labels and security parameters). • Mechanisms to detect or prevent the hijacking of a communication session (e.g., encrypted communication channels).
[TranSep]	Separation of Data. Information transmissions of different security levels shall be segregated from each other (e.g., encryption, physical separation).
[Validate]	Security Support Structure Validation, including procedures or features to validate, periodically, the correct operation of the hardware, software, and firmware elements of the Security Support Structure.
[Verif1]	Verification by the ISSM that the necessary security procedures and mechanisms are in place; testing of them to verify that they work appropriately.
[Verif2]	Verification by the DAA Rep that the necessary security procedures and mechanisms are in place; testing of them by the DAA Rep to ensure that they work appropriately.

Appendix E

ACCESS BY FOREIGN NATIONALS TO SYSTEMS PROCESSING SPECIAL ACCESS INFORMATION

Appendix E, Access by Foreign Nationals to Systems Processing Special Access Information, is published under separate cover.

Appendix F

BIBLIOGRAPHY

1. Atomic Energy Act of 1954, as amended.
2. Common Criteria for Information Technology Security Evaluation, CCEB-96/011, Version 2.0, May 1998.
3. DCID 1/7, *Security Controls on the Dissemination of Intelligence Information*, 30 June 1998.
4. DCID 1/14, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)*, 2 July 1998.
5. DCID 1/19, *Security Policy for Sensitive Compartmented Information*, 1 March 1995.
6. DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, 18 November 2002.
7. DCID 3/1, *National Foreign Intelligence Board*, 14 January 1997.
8. DCID 3/14, Annex B, *Intelligence Community Standards for Security Labeling of Removable ADP Storage Media*, 22 January 1988.
9. DCID 5/6, *Intelligence Disclosure Policy*, dated 30 June 1998.
10. DIAM 50-4, *Department of Defense (DoD) Intelligence Information System (DODIIS) Information Systems Security (INFOSEC) Program*, 30 April 1997.
11. DoD 5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual*, August 1998.
12. DoD 5200.1-R, *Information Security Policy Regulations*, April 20, 1995.
13. DoD 5200.28, *Security Requirements for Automated Information Systems*, 21 March 1988.
14. DoD 5220.22-M, *National Industrial Security Program Operating Manual*, dated January 1995.
15. DoD 5220.22-M-Sup 1, *DoD Overprint to the National Industrial Security Program Operating Manual*, dated February 1995.
16. DoD Directive 0-5205.7, *Special Access Program (SAP) Policy*, 13 January 1997.
17. DoD Directive S-5210.36, *Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the US Government*, 10 June 1986.
18. DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, dated 16 June 1992.
19. DoD Directive 5530.3, *International Agreements*, dated 11 June 1987.
20. DoD Directive 8500.1, *Information Assurance (IA)*, dated 24 October 2002.
21. DoD Directive 8520.1, *Protection of Sensitive Compartmented Information (SCI)*, dated 20 December 2001.

22. DoD Directive 8530.1, *Computer Network Defense (CND)*, dated 8 January 2001.

23. DoD Instruction 8500.2, *Information Assurance (IA) Implementation*, dated 6 February 2003.

24. Executive Order 12333, *United States Intelligence Activities*, dated 4 December 1981.

25. Executive Order 12829, *National Industrial Security Program*, dated 6 January 1993.

26. Executive Order 12958, *Classified National Security Information*, as amended dated 25 March 2003

27. Executive Order 12968, *Access to Classified Information*, 4 August 1995.

28. Freedom of Information Act, The Privacy Act, 5 USC 552.

29. 32 CFR Part 2001, "Classified National Security Information, ISOO Directive No. 1" dated 22 September 2003.

30. *International Programs Security Handbook*, dated 1 May 2002.

31. Joint Air Force-Army-Navy (JAFAN) 6/9, *Physical Security Standards for Special Access Program Facilities*, 23 March 2004.

32. Joint Chiefs of Staff Instruction, 6510.01B *Defensive Information Operations Implementation*, 27 August 1997.

33. NACSIM no. 7002, *COMSEC Guidance for ADP Systems*, September 1975.

34. National Security Act of 1947, Section 102.

35. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated 5 July 1990.

36. NDP-1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*, dated 1 October 1988.

37. NSA/CSS Directive No. 130-1, *NSA/CSS Operational Information Systems and Networks Security Policy*, 13 March 1995.

38. NSDD-145, *National Policy of Telecommunications and Automated Information Systems Security*, 17 September 1984.

39. NSTISSI 4009, *National Information Systems Security (INFOSEC) Glossary*, dated August 1997.

40. NSTISSP #11, *National Security Telecommunications and Information Systems Security Policy*, dated 1 February 2000.

41. OMB Circular A-130, *Management of Federal Information Resources*, dated 15 July 1994, and principally, Appendix 3, *Security of Federal Automated Information*, dated 20 February 1996.

42. OMB Circular A-71, Transmittal Memorandum No. 1, *Security of Federal Automated Information Systems*, dated 27 July 1978.

43. Public Law 100-235, *The Computer Security Act of 1987*, dated 8 January 1988.

Appendix G

LIST OF ACRONYMS

C&A	Certification and Accreditation
CM	Configuration Management
CONOPS	Concept of Operations
COTS	Commercial off-the-Shelf
CRC	Cyclical Redundancy Check
DAA	Designated Accrediting Authority
DAC	Discretionary Access Control
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DoD	Department of Defense
DOE	Department of Energy
DOS	Denial of Service
E-mail	Electronic Mail
EPROM	Erasable PROM
HTTP	HyperText Transfer Protocol
I&A	Identification and Authentication
IC	Intelligence Community
IS	Information System
ISA	Interconnection Security Agreement
ISOO	Information Security Oversight Office
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISSO/M	Information System Security Officer/Manager

JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LRU	Lowest Replaceable Unit
MAC	Mandatory Access Control
MOA	Memorandum of Agreement
MSSP	Master System Security Plan
NFIB	National Foreign Intelligence Board
NOFORN	Not Releasable to Foreign Nationals
NSA	National Security Agency
NSO	Network Security Officer
O&M	Operations and Maintenance
Oe	Oersted
PAA	Principal Accrediting Authority
PAA	Principal Approving Authority
PDS	Protected Distribution System
PL	Protection Level
PM	Program Manager
PROM	Programmable ROM
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RF	Radio Frequency
ROM	Read-only Memory
SAP	Special Access Program
SAPF	SAP Facility
SAS	Special Assistant to the Secretary of Treasury

SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SIOP	Single Integrated Operational Plan
SSP	System Security Plan
T&E I	First Test and Evaluation Phase
T&E II	Second Test and Evaluation Phase
TCB	Trusted Computing Base
TSCM	Technical Surveillance Countermeasures
US	United States
UPS	Uninterruptible Power Supply
WAN	Wide Area Network