*UNCLASSIFIED*

# DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 6/3 PROTECTING SENSITIVE COMPARTMENTED INFORMATION WITHIN INFORMATION SYSTEMS

***APPENDICES***

## APPENDIX A - CONTENTS OF AN INTERCONNECTION SECURITY AGREEMENT (ISA)

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

**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.

**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.

**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 Accrediting Authority (DAA)**

The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

**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**

A formalization of a security determination that an individual is authorized access, on a need-to-know basis, to a specific type of classified information, such as Sensitive compartmented Information (SCI), that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

**Group Authenticator**

See **Authenticator**.

**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 checksummed (e.g., file, message) is comparable to the order of difficulty in breaking the cryptographic algorithm used.

**Intelligence Information**

For purposes of this manual, *intelligence information* refers to Sensitive Compartmented Information and special access programs for intelligence under the purview of the DCI.

**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**

The Level-of-Concern is 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 an intelligence information system that is determined to be essential to the operational readiness or mission effectiveness of the intelligence 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 intelligence 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 single-user systems.

**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.

**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.

**Object**

A passive entity that contains or receives information. Access to an object potentially implies access to the information that it contains.

**Named Object**

An object that is sharable between users.

**Storage Object**

An object that supports both read and write accesses.

**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 intelligence systems within an agency. Within the Intelligence Community, the PAAs are the DCI, EXDIR/CIA, AS/DOS (Intelligence & Research), DIRNSA, DIRDIA, ADIC/FBI (National Security Div), D/Office of Intelligence/DOE, SAS/Treasury (National Security), D/NIMA, and the D/NRO.

**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.

**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.

**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.

**Residual Risk**

Portion of risk that remains after security measures have been applied.

**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. For intelligence information, these could include compartment and sub-compartment indicators and handling restrictions. For DOE information, these could include indicators of information type (such as Restricted Data), and Sigma categories.

**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 1/19).

**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 DCID 1/21 in which SAP information may be processed.

**Storage**

The state that exists when information is being held for use until needed for processing.

**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.

**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).

**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 therefrom.

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.

**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.

**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.

## OVERVIEW

**1.0 INTRODUCTION**

1.1 Security Administration

1.2 Mission

**2.0 SECURE FACILITY DESCRIPTION**

2.1 Physical Environment

2.2 Floor Layout

2.3 Secure Facility Access

2.4 TEMPEST

**3.0 SYSTEM DESCRIPTION**

3.1 General Information

3.2 Interconnection Interface Description

3.3 Residual Risk

**4.0 SYSTEM HARDWARE**

**5.0 SYSTEM SOFTWARE**

**6.0 DATA STORAGE MEDIA**

**7.0 SECURITY REQUIREMENTS**

7.1 System-Specific Threats

7.2 User Access and Operation

7.3 Protection of the Security Support Structure

7.4 Security Features

---

## 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 (IN TABULAR FORM)<br>REQUIREMENTS 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-6.

TABLE D.1 Confidentiality Protection Level (PL) Table

| *Confidentiality* | *PL 1* | *PL 2* | *PL 3* | *PL 4* | *PL 5* |
|---|---|---|---|---|---|
| Access1 | X | X | X | X | X |
| Access2 |  | X | X | X | X |
| Access3 |  |  | X | X | X |
| Access4 |  |  |  | X | X |
| Access5 |  |  |  |  |  |
| AcctMan | A/R | X | X | X | X |
| Audit1 | A/R | X | X | X | X |

| | | | | | |
|---|---|---|---|---|---|
| Audit2 | | X | X | X | X |
| Audit3 | | A/R | X | X | X |
| Audit4 | | | X | X | X |
| Audit5 | | | | X | X |
| Audit6 | | | | | |
| Audit7 | | | | | |
| Audit8 | | | | | |
| Audit9 | | | | | |
| CCA | | | | A/R | X |
| Doc1 | X | X | X | X | X |
| Doc2 | | X | X | X | X |
| Doc3 | | A/R | X | X | X |
| Doc4 | | | | | |
| I&A1 | X | X | X | X | X |
| I&A2 | A/R | X | X | X | X |
| I&A3 | A/R | X | X | X | X |
| I&A4 | | | | X | X |
| I&A5 | | | | | |
| I&A6 | | | | | |
| Label1 | | | | X | X |
| Label2 | | | | X | X |
| LeastPrv | | X | X | X | X |
| Marking | | | X | | |
| ParamTrans | X | X | X | X | X |

| | | | | | |
|---|---|---|---|---|---|
| Recovery | X | X | X | X | X |
| ResrcCtrl | | X | X | X | X |
| ScrnLck | X | X | X | X | X |

| *Confidentiality* | *PL 1* | *PL 2* | *PL 3* | *PL 4* | *PL 5* |
|---|---|---|---|---|---|
| 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 | X | | X | X |
| Test2 | | A/R | X | X | X |
| Test3 | | | X | X | X |
| Test4 | | | A/R | | |
| Test5 | | | | | |
| Trans1 | X | X | X | X | X |
| TranSep | | | | X | X |

TABLE D.2 Integrity Level-of-Concern Table

| *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 | X | X |
| Integrty2 |  | X | X |
| Integrty3 |  |  |  |
| 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 Table

| *Availability* | *Basic* | *Medium* | *High* |
|---|---|---|---|
| Avail | X | X | X |
| Backup1 | X |  |  |
| Backup2 |  | X |  |
| Backup3 |  | X |  |
| Backup4 |  |  | X |

| | | | |
|---|---|---|---|
| Backup5<br>Backup6 | | | X<br>X |
| Commun | | X | X |
| Cont1<br>Cont2 | | X | X<br>X |
| DOS | | | X |
| Maint | | X | X |
| Monit | | | X |
| Power1<br>Power2 | | X<br>A/R | X<br>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:
>
> > 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.]

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 5 years 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 off-site 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:
>
> > Policies that assure storage integrity.
> >
> > 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.).
> >
> > 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 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 intelligence 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 - 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 1/21, *Physical Security Standards for Sensitive Compartmented Information Facilities*, 29 July 1994.
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 and its Supplement, dated February 1995.
15. DoD Directive 0-202-7, *Special Access Program*, 13 January 1997.
16. 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.
17. Executive Order 12333, *United States Intelligence Activities*, dated 4 December 1981.
18. Executive Order 12829, *National Industrial Security Program*, dated 6 January 1993.
19. Executive Order 12958, *Classified National Security Information*, dated 20 April 1995.
20. Implementing Directive for Executive Order 12958, 32 CFR Part 2001, 13 October 1995.
21. Joint Chiefs of Staff Instruction, 6510.01B *Defensive Information Operations Implementation*, 27 August 1997.
22. Executive Order 12968, *Access to Classified Information*, 4 August 1995.
23. Freedom of Information Act, The Privacy Act, 5 USC 552.
24. NACSIM no. 7002*, COMSEC Guidance for ADP Systems*, September 1975.
25. National Security Act of 1947, Section 102.
26. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated 5 July 1990.
27. NSA/CSS Directive No. 130-1, *NSA/CSS Operational Information Systems and Networks Security Policy*, 13 March 1995.
28. NSDD-145, *National Policy of Telecommunications and Automated Information Systems Security*, 17 September 1984.

29. NSTISSI 4009, *National Information Systems Security (INFOSEC) Glossary*, dated August 1997.
30. 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.
31. OMB Circular A-71, Transmittal Memorandum No. 1, *Security of Federal Automated Information Systems*, 27 July 1978.
32. Public Law 100-235, *The Computer Security Act of 1987*, dated 8 January 1988.

---

## APPENDIX F – LIST OF ACRONYMS

| | |
|---|---|
| ADIC/FBI | Assistant Director in Charge, Federal Bureau of Investigation |
| AS/DOS | Assistant Secretary, Department of State |
| C&A | Certification and Accreditation |
| CM | Configuration Management |
| CONOPS | Concept of Operations |
| COTS | Commercial off-the-Shelf |
| CRC | Cyclical Redundancy Check |
| D/NIMA | Director, National Imagery and Mapping Agency |
| D/NRO | Director, National Reconnaissance Office |
| DAA | Designated Accrediting Authority |
| DAC | Discretionary Access Control |
| DCI | Director of Central Intelligence |
| DCID | Director of Central Intelligence Directive |
| DDCI | Deputy Director of Central Intelligence |
| DDCI/CM | Deputy Director of Central Intelligence for Community Management |
| DIRDIA | Director, Defense Intelligence Agency |
| DIRNSA | Director, National Security Agency |
| 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 |
| 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 |
| 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 |