

Chapter 8.

Automated Information System Security

Section 1. Responsibilities

8-100. General.

- a. Computer and networking systems (collectively referred to as Automated Information Systems (AISs)) used to capture, create, store, processor distribute classified information must be operated so that the information is protected against unauthorized disclosure or modification.
- b. Protection requires a balanced approach that includes AIS features as well as administrative, operational, physical, and personnel controls. Protection is commensurate with the classification level and category of the information, the threat, and the operational requirements associated with the environment of the AIS.

8-101. Scope. This Chapter describes the minimum security requirements for an AIS processing classified information.

8-102. Responsibilities.

- a. The CSA shall establish a line of authority for oversight, review, inspection, certification, and accreditation of AISS used by its contractors.
- b. The contractor shall publish and promulgate an AIS Security Policy that addresses the classified processing environment. The contractor shall appoint an Information Systems Security Representative (ISSR) whose responsibilities are to:
 - (1) Maintain liaison with the CSA.
 - (2) Implement and administer the contractor's AIS Security Policy.
 - (3) Ensure the preparation of an AIS Security Plan (AISSP).
 - (4) Ensure the establishment and maintenance of security safeguards and access controls.

- (5) Ensure that users have the security clearance, special access authorizations, and **need-to-know** for the information that they can access.
- (6) Ensure that all AIS security related documentation is current.
- (7) Advise the CSA of any abnormal event that effects the security of the AIS.
- (8) Ensure that secure maintenance procedures are followed.
- (9) Ensure that security audit records are maintained, accessible, and reviewed and analyzed at least weekly.
- (10) Designate Security Custodians in facilities with multiple AIS or multiple shifts.
- (11) Ensure the development and implementation of an ongoing AIS security education program.
- (12) Perform threat based, aperiodic inspections pursuant to the AISSP. The frequency of inspections may be adjusted for sufficient cause.
- (13) Ensure that Memoranda of Agreement are in place for AIS supporting multiple CSAS.
- (14) Approve and document the movement of AIS equipment.
- (15) Approve the release of sanitized equipment and components in accordance with the **sanitization** matrix.
- (16) Approve and document additional AIS operated in dedicated security mode that is substantially the same as described in the AISSP.

The classification level of the additional AIS must be the same as that of the approved AIS.

- (17) Approve and document additional or replacement components of a dedicated or system high AIS that are identical in functionality and do not affect the security of the AIS.
- (18) Document in the security plan and administer any procedures necessary to prevent classified information from migrating to unclassified AISS and leaving the security area.

Section 2. Accreditation and Security Modes

8-200. AIS Accreditation

- a. The contractor shall obtain written accreditation from the CSA prior to processing classified information on **AISs**. To obtain accreditation, the contractor shall submit a formal request to the CSA and an **AISSP**. Where similar AIS are located within the same facility, a single security plan is permitted.
- b. Accreditation is the CSAS approval for an AIS to process classified information in an operational environment. The accreditation is based on documentation, analysis, and evaluation of AIS operations with respect to security risks and also on the safeguards associated with operation of the AIS.
- c. Interim accreditation may be granted in order for a contractor to start processing classified information. This interim action shall be for a specific period and shall specify the contractor actions to be completed and the minimum security requirements to be met during this period.
- d. AIS accreditation may be withdrawn by the CSA should procedures and controls established in the **AISSP** be assessed ineffective by the CSA. Accreditation may also be withdrawn by the CSA when there has been an unacceptable change in system or security configuration.
- e. The contractor can self-approve **AISS** that are similar to previously accredited AIS security profile and components provided the self-approval plan and procedures are included in the **AISSP**. **In the event of discrepancies, or determination** by the CSA that the self-approval plan is not administered effectively, the CSA may withdraw the contractor's self-approval authority.
- f. An AIS may be reaccredited or self-approval authority can be reinstated by the CSA after review, analysis, and approval of an updated **AISSP**. An accredited **AIS** may be reaccredited when significant changes to the original accreditation or baseline occur.

8-201. Equipment not Requiring Accreditation.

Some equipment/components, to include test equipment, fits the definition of an AIS, whereas others may

not. The ISSR will determine and document the capability of such equipment in the context of the equipment components ability to collect and process information. As a general rule, equipment composed of volatile memory with no other storage media would not require accreditation. AIS components that need not be included in the system accreditation include but are not limited to:

- a. Electronic typewriters, basic function calculators, and test equipment.
- b. Security requirements for **AISs** that are embedded as an integral element of a **larger** system that is used to perform or control a function, such as test stands, **simulators**, control systems or weapons systems should be established concurrently with the design and development of the system. If not provided, the contractor shall request them from the appropriate GCA. In the absence of such requirements, the security requirements and procedures of this Manual will be applied to the extent appropriate as determined by the CSA.

8-202. The AIS Security Plan.

- a. **User Operational Procedures.** These procedures describe how **access** to an AIS and classified information is authorized and revoked; the protection mechanisms provided by the AIS, guidelines on their use, and how they interact with one another, procedures for screening and preventing the introduction of malicious code, and the like.
- b. **System Configuration Management Procedures.** These procedures describe the documenting, controlling, changing, and maintaining of the accountability of AIS hardware, firmware, software, communications interfaces, operating procedures, and installation structures.
- c. **Audit Features and Controls.** These describe:
 - (1) A chronological record of AIS usage and system support activities.
 - (2) Maintenance and repair of AIS hardware, including installation or removal of equipment, devices or components.

- (3) Transaction receipts, equipment sanitization, declassification and release records.

d. **Concept of Operations (CONOP).** The CONOP describes what the AIS will be used for and how it will operate.

e. **Continuity of Operations Procedures (COOP).** The COOP describes procedures to ensure continuous operations of AISS in the event of a disaster resulting from fire, flood, malicious act, human error, or any other occurrence. When the GCA determines a COOP to be necessary, the requirements will be contractually imposed. Costs directly related to the COOP requirements when in addition to safeguards required by this Manual, will be charged to the specific contract for which the requirements are imposed. At a minimum, the COOP must include:

- (1) Identification of mission-essential resources, including AIS components, key response and recovery personnel, and alternate site processing requirements.
- (2) Identification of mission-essential applications.
- (3) The type of response necessary to continue the mission, based on the projected recovery time.
- (4) Frequency of performing backups to ensure, at a minimum, that current back-up copies of mission essential software and data exist.
- (5) An estimate of the cost of exercising the plan, software, or alternate site.

f. **System Administration and Maintenance Procedures.** These describe maintenance and repair procedures, including adding, changing, and removing components, and the use of maintenance devices and utilities.

g. **Training Procedures.** Security awareness training must be provided prior to assigning the individual access to the AIS and updated as needed. An individual receiving the training may be required to sign an agreement to abide by the security requirements specified in the AISSP.

h. **Startup and Shut-down Procedures.** These include system upgrading and downgrading, handling of user data and output, access controls to the

AIS and remote AIS areas during, between, and after classified processing; and the declassification, release and destruction of storage media and AIS.

i. **Certification Test Plan.** This plan outlines the inspection and test procedures to demonstrate compliance with the security requirements associated with the mode of operation. It must include a detailed description of how the implementation of the operating system software, data management software, firmware, and related security software packages will enable the AIS to meet the compartmented or multilevel mode requirements. Products, subsystems, and systems that have been endorsed through formal evaluation programs (e.g., the Evaluated Products List supporting the TCSEC) must be evaluated as part of the AIS in the certification and accreditation process. In lieu of a certification test plan for the dedicated and system high mode, the ISSR will:

- (1) Verify that system access controls and/or procedures are functional for the dedicated mode.
- (2) Provide test results that verify that need to know controls are implemented for the system high mode.

8-203. Security Modes-General.

a. A(SS that process classified information must operate in the dedicated, system-high, compartmented, or multilevel mode. Security modes are authorized variations in security environments, requirements, and methods of operating. In all modes, the integration of automated and conventional security measures shall, with reasonable dependability, prevent unauthorized access to classified information during, or resulting from the processing of such information, and prevent unauthorized manipulation of the AIS that could result in the compromise of classified information.

b. In determining the mode of operation, three elements must be addressed:

- (1) The boundary of an AIS includes all users that are directly or indirectly connected, and who can receive data from the system without a reliable human review by a cleared authority. The perimeter is the extent of the system that is to be accredited as a single system.

(2) The nature of data is defined in terms of its classification levels, compartments, **subcompartments**, and sensitivities.

(3) The level and diversity of access privileges of its users are defined as their clearance levels, need-to-know, and formal access approvals.

8-204. **Dedicated Security Mode.**

a. **An AIS** is operating in the dedicated mode when each user with direct-or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

(1) A PCL and need-to-know for all information stored or processed.

(2) If applicable, has all formal access approvals and has executed all appropriate nondisclosure agreements for all the information stored and/or processed (including all compartments and sub-compartments).

b. The following security requirements are established for AISs operating in the dedicated mode:

(1) Enforce system access procedures.

(2) All hardcopy output and media removed will be handled at the level for which the system is accredited until reviewed by a knowledgeable individual.

8-205. **Security Features for Dedicated Security Mode.** Since the system is not required to provide technical security features, it is up to the user to protect the information on the system.

8-206. **Security Assurances for Dedicated Security Mode.** Configuration management procedures must be employed to maintain the ability of the AIS to protect the customer's classified information. Configuration management procedures must be conducted in coordination with the ISSR. The systems configuration management procedures shall include an approach for specifying, documenting, controlling, and maintaining the visibility and accountability of all appropriate AIS hardware, firmware, software, communications interfaces, operating procedures, installation structures and changes thereto.

8-207. **System High Security Mode.** An AIS is operating in the system-high mode when each user with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts has all of the following:

a. A PCL for all information on the AIS.

b. Access approval and has signed nondisclosure agreements for all the information stored and/or processed.

c. A need-to-know for some of the information contained within the system.

8-208. **Security Features for System High Mode.**

AISS operating in the system high mode, in addition to meeting all of the security standards established for the dedicated mode, will:

a. Define and control access between system users and named objects (e.g., files and programs). The enforcement mechanism must allow system users to specify and control the sharing of those objects by named individuals and/or explicitly defined groups of individuals. The access control mechanism must either, by explicit user action or by default, provide that all objects are protected from unauthorized access (discretionary access control). Access permission to an object by users not already possessing access permission must only be assigned by authorized users of the object.

b. When feasible, as determined by the CSA, provide a time lockout in an interactive session after an interval of user inactivity. The time interval and restart requirements shall be specified in the **AISSP**.

c. Provide an audit trail capability that records time, date user ID, terminal ID (if applicable), and file name for the following events:

(1) System log on and log off.

(2) Unsuccessful access attempts.

d. Protect the audit, identification, and authentication mechanisms from unauthorized access modification, access or deletion.

- e. Require that storage contain no residual data from the previously contained object before being assigned, allocated, or reallocated to another subject.
- f. Ensure that each person having access to a multi-user AIS have the proper security clearances and authorizations and be uniquely identified and authenticated before access to the AIS is permitted. The identification and authentication methods used shall be specified and approved in the **AISSP**. User access controls in multi-user AISS shall include authorization, user identification, and authentication; administrative controls for assigning these shall be covered in the **AISSP**.
 - (1) **User Authorizations.** The manager or supervisor of each user of an AIS shall determine the required authorizations, such as **need-to-know** for that user.
 - (2) User Identification. Each system user shall have a unique user identifier and authenticator.
 - (a) **User ID Reuse.** Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) shall be removed from the AIS.
 - (b) **User ID Removal.** The ISSR shall ensure the development and implementation of procedures for the prompt removal of access from the AIS when the need for access no longer exists.
 - (c) **User ID Revalidation.** The ISSR shall ensure that all user ID's are **revalidated** at least annually, and information such as sponsor and means of off-line contact (e.g., phone number, mailing address) are updated as necessary.
- g. **Authentication.** Each user of a multi-user AIS shall be authenticated before access is permitted. This authentication can be based on any one of three types of information: something the person knows (e.g., a password); something the person possesses (e.g., a card or key); something about the person (e.g., fingerprints or voiceprints); or some combination of these three. Authenticators that are passwords shall be changed at least every 6 months. Multi-user AISs shall ensure that each user of the AIS is authenticated before access is permitted.

- (1) **Logon.** Users shall be required to authenticate their identities at "logon" time by supplying their authenticator (e.g., password, smart card, or fingerprints) in conjunction with their user ID.
- (2) **Protection of Authenticator.** An authenticator that is in the form of knowledge or possession (password, smart card, keys,) shall not be shared with anyone. Authenticators shall be protected at a level commensurate with the accreditation level of the AIS.
- (3) **Additional Authentication Countermeasures.** Where the operating system provides the capability, the following features shall be implemented:
 - (a) **Logon Attempt Rate.** Successive logon attempts shall be controlled by denying access after multiple (maximum of five) unsuccessful attempts on the same user ID, by limiting the number of access attempts in a specified time period, by the use of a time delay control system, or other such methods, subject to approval by the CSA.
 - (b) **Notification to the User.** The user shall be notified upon successful logon of the date and time of the user's last logon; the ID of the terminal used at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

8-209. Security Assurances for System High Mode.

- a. **Examination of Hardware and Software.** AIS hardware and software shall be examined when received from the vendor and before being placed into use.
 - (1) **AIS Hardware.** An examination shall result in assurance that the equipment appears to be in good working order and have no elements that might be detrimental to the secure operation of the resource. Subsequent changes and developments which affect security may require additional examination.

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

(3) **Custom Software or Hardware Systems. New or significantly changed** security relevant software and hardware developed specifically for the system shall be subject to testing and review at appropriate stages of development.

b. **Security Testing.** The system security features for need-to-know controls will be tested and verified. Identified flaws **will** be corrected.

8-210. Compartmented Security Mode. An AIS is operating in the compartmented mode when users with direct or indirect access to the AIS, its peripherals, or remote terminals have all of the following:

- a. A PCL for the most restricted information processed.
- b. Formal access approval and has signed nondisclosure agreements for that information to which he or she is to have access (some users do not have formal access approval for all compartments or subcompartments processed by the AIS).
- c. A valid need-to-know for that information for which he/she is to have access.

8-211. Security Features for Compartmented Mode.

In addition to all security features and security assurances required for the system high mode of operation, AIS operating in the compartmented mode of operation shall also include:

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

b. **Export of Security Labels.** Security labels exported from the AIS shall be accurate representations of the corresponding security labels on the information in the originating AIS.

c. **Mandatory Access Controls.** Mandatory access controls shall provide a means of restricting access to files based on the sensitivity (as represented by the label) of the information contained in the files and the formal authorization (i.e. security clearance) of users to access information of such sensitivity.

d. No information shall be accessed whose compartment is inconsistent with the session log on.

e. Support a trusted communications path between itself and each user for initial logon and verification for AIS processing TOP SECRET information.

f. Enforce, under system control, a system-generated, printed, and human-readable security classification level banner at the top and bottom of each physical page of system hard-copy output.

g. Audit these additional events: the routing of all system jobs and output, and changes to security labels.

8-212. Security Assurances for Compartmented Mode.

a. **Confidence in Software Source.** In acquiring resources to be used as part of an AIS, consideration shall be given to the level of confidence placed in the vendor to provide a quality product, to support the security features of the product, and to assist in the correction of any flaws.

b. **Flaw Discovery.** The vendor shall have implemented a method for ensuring the discovery of flaws in the system (hardware, firmware, or software) that may have an effect on the security.

c. **Description of Security Enforcement Mechanisms (often referred to as the Trusted Computing Base).** The protections and provisions of the security enforcement mechanisms shall be documented in such a manner to show the underlying planning for the security. The security enforcement mechanisms shall be isolated and protected from any user *or* unauthorized process interference or modification. Hardware and software features shall be provided that can be used to periodically validate the correct operation of the elements of the security enforcement mechanisms.

- d. **Independent Validation and Verification.** An independent validation and verification team shall assist in the certification testing of an AIS and shall perform validation and verification testing of the system as required by the CSA.
- e. **Security Label Integrity. The methodology shall ensure, (1) Integrity** of the security labels; (2) The association of a security label with the transmitted data; and (3) Enforcement of the control features of the security labels.
- f. **Detailed Design of Security Enforcement Mechanisms.** An **informal** description of the security policy model enforced by the system shall be available.

8-213. Multilevel Security Mode. An AIS is operating in the multilevel mode when all of the following statements are satisfied concerning the users with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts:

- a. All users of the multilevel system must have a PCL but some users may not have a PCL for all levels of the classified information residing on the system.
- b. All users are cleared, have a need-to-know, and the appropriate access approval (i.e., signed nondisclosure agreements) for information to be accessed.

8-214. Security Features for Multilevel Mode. In addition to all security features and security assurances required for the compartmented mode of operation, AIS operating in the multilevel mode shall also include:

- a. A mechanism that is able to monitor the occurrence or accumulation of security **auditable** events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when thresholds are exceeded and, if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event.
- b. Access controls that are capable of specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object. It will be possible to specify for each named object a list of named individuals and a list of groups of named individuals for which no access to the object is to be given.

- c. Support a trusted communication path between the AIS and users for *use* **when** a positive **AIS-to-user** connection is required (i.e., logon, change subject security level). Communications via this trusted path shall be activated exclusively by a user or the AIS and shall be logically isolated and unmistakably **distinguishable** from other paths.
- d. Support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. The AIS system administrative personnel shall only be able to perform security administrator functions after taking a distinct **auditable** action to assume the security administrative role of the AIS system. Non-security functions that can be performed in the security administrative role shall be limited strictly to those essential to performing the security role effectively.
- e. Provide procedures **and/or** mechanisms to assure that, after an AIS system failure or other discontinuity, recovery without a protection compromise is obtained.
- f. Immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A user shall be able to query the system as desired for a display of the user's complete sensitivity label.
- g. Enforce an upgrade or downgrade principle where all users processing have a system-maintained classification; no data is read that is classified higher than the processing session authorized; and no data is written unless its security classification level is equal to the user's authorized processing security classification.

8-215. Security Assurances for Multilevel Mode.

- a. **Flaw Tracking and Remediation.** The vendor shall provide evidence that all discovered flaws have **been** tracked and remedied.
- b. **Life-Cycle Assurance.** The development of the AIS hardware, firmware, and software shall be under life-cycle control and management (i.e., **control** of the AIS from the earliest design stage through decommissioning).
- c. **Separation of Functions.** The functions of the ISSR and the AIS manager shall not be performed by the same person.

- d. Device Labels.** The methodology shall ensure that the originating and destination device labels are a part of each message header and enforce the control features of the data flow between originator and destination.
- e. Trusted Path.** The system shall support a trusted communication path between the user and system security mechanisms.
- f. Security Isolation.** The security enforcement mechanism shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures). The protection of the security enforcement mechanism shall provide isolation and non circumvention of isolation functions.
- g. Security Penetration Testing.** In addition to testing the performance of the AIS for certification, there shall be testing to attempt to penetrate the security countermeasures of the system. The test procedures shall be documented in the test plan for certification and also in the test plan for ongoing testing.

Section 3. Controls and Maintenance

8-300. Physical Security.

- a. Physical security safeguards shall be established that prevent or detect unauthorized access to accredited system entry points and unauthorized modification of the AIS hardware and software. Hardware integrity of the AIS, including remote equipment, shall be maintained at **all** times, even when the AIS is not processing or storing classified information.
 - b. Attended classified processing **shall** take place in an area, normally a Restricted Area, where authorized persons can exercise constant surveillance and control of the AIS. All unescorted personnel to the area must have a government granted PCL and controls must be in place to restrict visual and aural access to classified information.
 - c. When the AIS is processing classified information unattended, or when classified information remains on an unattended AIS, a Closed Area is required.
 - d. When the AIS is not in use, all classified information has been removed and properly secured, and the AIS has been downgraded, continuous physical protection, to prevent or detect unauthorized modification of the AIS hardware and software, shall be implemented **through** one or more of the following methods:
 - (1) Continuous supervision by authorized personnel.
 - (2) Use of approved cabinets, enclosures, seals, **locks** or Closed Areas.
 - (3) Use of area controls that prevent or detect tampering or theft of the **hardware** and software. These controls will vary depending on **the** overall physical security controls in effect in the immediate secure area.
- uncleared persons is used in a classified processing period, it must be reviewed or tested by authorized and knowledgeable contractor personnel to provide reasonable assurance that security **vulnerabilities** do not exist.
- b. The **AISSP** must provide procedures for approval of installation of any software on the AIS.
 - c. Software provided on media that may be written to (e.g., magnetic media) must be safeguarded commensurate with the accreditation level unless a physical write-protect mechanism is used. (Mechanisms shall be tested and verified by attempting to write to the media.) The write protection mechanism must be verified once during each session when it is used to process classified information.
 - d. Unclassified software provided on media that cannot be changed (e.g., **CD** read-only media) may be loaded onto the classified system without being labeled or classified provided it is immediately removed from the security area upon completion of the loading procedure. If the media is to be retained in the security **area**, it may be controlled and stored as unclassified **media**.
 - e. The contractor shall validate the functionality of security-related software (e.g., access control, auditing, purge, etc.) before the AIS is accredited. The software shall be revalidated when changed.
 - f. Use of software of unknown or suspect origin is strongly discouraged.
 - g. The contractor must verify that all software is free of malicious code prior to installation.
 - h. Unclassified vendor-supplied software used for maintenance or diagnostics must be controlled as though classified.
 - i. Incidents involving malicious software will be investigated by the **ISSR**. If the incident affects the integrity of classified information, the CSA will be notified immediately and a written report detailing the findings of this investigation will be submitted to the CSA in accordance with the **AISSP**.

8-301. Software Controls.

- a. Contractor personnel that design, develop, test, install, or make modifications to systems, or use security software, shall be cleared to the level of the AIS. Non-system or applications software that will be used during classified processing periods can be developed or modified by personnel without a clearance. However, before software developed by

8-302. Media Controls.

- a. In general, media that contains classified information will be handled in a manner consistent with the handling of **classified** documents.
- b. All storage media used for classified data on dedicated and system high AIS must be labeled and controlled to the highest level of the information on the AIS. However, information not at the highest level may be written to appropriately **classified/unclassified** media using authorized procedures and/or methods.
- c. All data storage media for compartmented and **multi-level** AIS must be labeled and controlled to the highest level of the information contained on the media.
- d. When two or more AISS are collocated in the same security area and processing at different levels or compartments, procedures described in the system security plan will be used to distinguish among them.
- e. Authorized sanitization procedures for the most commonly used memory and storage media are defined in the sanitization matrix.
- f. Media must be sanitized and **all** markings and labels removed before media can be declassified. **Sanitization** actions must be verified and a record must be annotated to show the date, the particular sanitization action taken, and the person taking the action.
- g. Media must be sanitized and declassified prior to release from continuous protection.
- h. **All** printed output from an AIS processing in the dedicated or system high mode must be treated as though classified until verified to **be** unclassified.

8-303. Security Audits

- a. In addition to the audits required under security modes, the following logs are required regardless of mode of operation. The logs must include **the** date, the event, and the person responsible.
 - (1) Maintenance, repair, installation, or removal of hardware components. Log must include the component involved, and action taken.
 - (2) Installation, testing, and modification of operating system and security-related software. Log must include the software involved and action taken.

- (3) Upgrading and downgrading actions.
 - (4) Sanitization and declassifying media and devices.
 - (5) Application and reapplication of seals.
- b. At intervals specified in the **AISSP**, the ISSR (**or** designee) shall review, analyze, and annotate audit records created during classified processing periods to ensure that all pertinent activity is properly recorded and appropriate action has been taken to correct anomalies.
 - c. Audit trail records shall be retained until reviewed and released by the contractor or CSA but not more than 12 months.

8-304. AIS Operations

- a. **Security Level Upgrading.** To increase the level of processing on an AIS the following procedures must be implemented:
 - (1) Adjust the area controls to the level of information to be processed.
 - (2) Configure the AIS as described in the AISSP. The use of logical disconnects is prohibited for AIS processing TOP SECRET information.
 - (3) Remove and store removable data storage media not to be used during the processing period.
 - (4) Clear all memory including buffer storage.
 - (5) Initialize the system for processing at the approved level of operation with a dedicated copy of the operating system. This copy of the operating system must be protected commensurate with the security classification and access levels of the information to be processed during the period.
- b. **Security Level Downgrading.** To lower the level of processing, the following procedures must be implemented:
 - (1) Remove and store removable data storage media not to be used during the lower processing period.

- (2) Clear the memory and buffer storage of the equipment to be downgraded, for collateral SECRET and below; sanitize for TOP SECRET.
- (3) Sanitize printers.
- (4) For classified processing, configure the AIS as described in the AISSP.
- (5) Adjust the area controls to the level of **information** to be processed.
- (6) Initialize the system for processing at the lower level with a dedicated copy of the operating system. This copy of the operating system must be protected commensurate with the security classification and access levels of the information to be processed during the period.

8-305. Identification and Authentication Techniques. When the AIS is processing classified information, access to any unattended hardware must conform to those required in this document for the highest level of classified material processed on the AIS. Specific user identification and authentication techniques and procedures will be included in the AISSP. Examples of identification and authentication techniques include, but are not limited to: user IDs and passwords, tokens, biometrics and smartcards.

- a. User IDs identify users in the system and are used in conjunction with authentication techniques to gain access to the system. User IDs will be disabled whenever a user no longer has a need-to-know or proper clearance. The user ID will be deleted from the system only after review of programs and data associated with the ID. Disabled accounts will be removed from the system as soon as practical. Access attempts will be limited to five tries. Users who fail to access the system within the established limits will be denied access until the user's ID is reactivated.
- b. When used, system logon passwords will be randomly selected and will be at least six characters in length.
 - (1) Appropriate guidance must be provided by the ISSR or contractor to users prior to their choosing *their* own logon passwords. When

an automated system logon-password generation routine is used, it must be described in the AISSP.

- (2) Passwords must be validated by the system each time the user accesses the system.
 - (3) System logon passwords must not be displayed at any terminal or printed on any printer.
 - (4) Passwords will not be shared by any user.
 - (5) Passwords will be classified and controlled at the highest level of the information accessed.
 - (6) Passwords must be changed at least every 6 months.
 - (7) Immediately following a suspected or known compromise of a password, the ISSR will be notified and a new password issued.
- c. Master data files containing the user population system logon passwords will be encrypted when practical. Access to the files will be limited to the ISSR and a designee identified in the AISSP.
 - d. When classified and unclassified AIS are collocated the following requirements apply:
 - (1) The LSSR must document procedures to ensure the protection of classified information.
 - (2) The unclassified AIS cannot be connected to the classified AIS.
 - (3) Users shall be provided a special awareness briefing.
 - e. When two or more AISS are collocated in the same security area and processing at different levels or compartments, procedures described in the AISSP will be used to distinguish among them.
- 8-304. Maintenance**
- a. Cleared personnel who perform maintenance or diagnostics do not normally require an escort. Need-to-know for access to classified information must be

enforced. Uncleared maintenance personnel must always be escorted by a cleared and technically knowledgeable individual. The ISSR must ensure that escorts of uncleared maintenance personnel are trained and sufficiently knowledgeable concerning the **AISSP**, established security policies and practices, and escorting procedures.

- b. If maintenance is being conducted by appropriately cleared personnel, system sanitizing or component isolation are a **local** option. If maintenance is being performed by uncleared personnel, steps must be taken to effectively deny access to classified information by the uncleared person and any maintenance equipment or software used; these procedures should be documented in the **AISSP**. A technically knowledgeable escort is preferred. If access to classified data cannot be precluded by the escort, either the component under maintenance must be physically disconnected from the classified **AIS** (and sanitized before and after maintenance) or the entire **AIS** must be sanitized before and after maintenance.
- c. The dedicated copy of the system software with a direct security function shall not be used for maintenance purposes by uncleared personnel.
- d. When a system failure prevents sanitization of the system prior to maintenance by uncleared vendor personnel, **AISSP** procedures must be enforced to

deny the uncleared person visual and electronic access to any classified data that may be contained on the system.

- e. When practical, all maintenance and diagnostics will be performed in the contractor's facility. Any **AIS** components or equipment released from secure control is no longer part of an accredited system.
- f. Vendor-supplied software/firmware used for maintenance or diagnostics must be protected at the level of the accredited **AIS**. The **CSA** may **allow**, on a **case-by-case** basis, the release of certain types of costly magnetic media for maintenance, such as disk head-alignment.
- g. All maintenance tools, diagnostic equipment, and other devices used to service an accredited **AIS** must be approved by the contractor.
- h. Any component board placed into an accredited **AIS** must remain in the security area until proper release procedures are completed.
- i. Remote diagnostic or maintenance services are strongly discouraged. If remote diagnostic or maintenance services become necessary, the **AIS** shall be sanitized and disconnected from any communication links to network, prior to the connection of any non-secured communication line.

Clearing and Sanitization Matrix

Media	Clear	Sanitize
Magnetic Tape¹		
Type I	s o r b	a, b, or m
Type II	a o r b	b e r m
Type III	a o r b	m
Magnetic Disk		
Bernoulli	a, b, or c	m
Floppies	a, b, or c	m
Non-Removable Rigid Disk	c	a, b, d, or m
Removable Rigid Disk	a, b, or c	a, b, d, or m
Optical Disk		
Read Many, Write Many	c	m
Read Only		m, n
Write Once, Read Many (Worm)		m, n
Memory		
Dynamic Random Access Memory (DRAM)	c o r g	c, g, or m
Electrically Alterable PROM (EAPROM)	i	j o r m
Electrically Erasable PROM (EEPROM)	i	h o r m
Erasable Programmable ROM (EPROM)	k	I then c, or m
Flash EPROM (FEPROM)	i	c then i, or m
Programmable ROM (PROM)	c	m
Magnetic Bubble Memory	c	a, b, c, or m
Magnetic Core Memory	c	a, b, e, or m
Magnetic Plated Wire	c	c and f, or m
Magnetic Resistive Memory	c	m
Nonvolatile RAM (NOVRAM)	c o r g	c, g, or m
Read Only Memory ROM		m
Static Random Access Memory (SRAM)	c o r g	c and f, g, or m
Equipment		
Cathode Ray Tube (CRT)	g	q
Printers		
Impact	g	p then g
Laser	g	o then g

¹ Type I and Type H magnetic tape can only be sanitized for reuse by using approved degaussing equipment. Type III tape cannot be sanitized by degaussing. The CSA will advise the contractor of currently approved Type I and Type II degaussers. If the contractor uses more than one type of tape (i.e., Type I, Type II, or Type III) and has an approved degausser, then all magnetic tapes must be labeled as to their "Type." to ensure that each is sanitized by appropriate means. Type I magnetic tape has a **coercivity** of 350 **oersted**s or less; Type II has a **coercivity** between 351 and 750 **oersted**s; and Type III has a **coercivity** greater than 750 **oersted**s.

Clearing and Sanitization Matrix

- a. **Degauss** with a Type I degausser
- b. **Degauss** with a Type II degausser.
- c. Overwrite all addressable locations with a single character.
- d. Overwrite all addressable locations with a character, its complement, then a random character and verify. **THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAINS TOP SECRET INFORMATION.**
- e. Overwrite all addressable locations with a character, its complement, then a random character.
- f. Each overwrite must reside in memory for a period longer than the classified data resided.
- g. Remove ail power to include **battery** power.
- h. Overwrite all locations with a random pattern, all locations with **binary** zeros, all locations with binary ones.
- i. Perform a full chip erase as per manufacturer's data sheets.
- j. Perform i above, then c above, a total of three times.
- k. Perform an ultraviolet erase according to manufacturer's recommendation.
- l. Perform k above, but increase time by a factor of three.
- m. Destroy - Disintegrate, incinerate, pulverize, shred, or smelt.
- n. Destruction required only if classified information is contained.
- o. Run five pages of unclassified text (font test acceptable).
- p. Ribbons must be destroyed. Platens must be cleaned.
- q. Inspect **and/or** test screen surface for evidence of burned-in information. If present, the cathode ray tube must be destroyed.

Section 4. Networks

8-400. Networks. This Section identifies basic security requirements for protecting classified information processed on accredited networks. Network operations shall maintain the integrity of the security features and assurances of its mode of operation. A “Reference Guide for Security in Networks” can be obtained from the CSA.

8-401. Types of Networks.

- a. A Unified Network is a collection of AIS’s or network systems that are accredited as a single entity by a single CSA. A unified network may be as simple as a small standalone LAN operating in dedicated mode, following a single security policy, accredited as a single entity, and administered by a single ISSR. The perimeter of such a network encompasses all its hardware, software, and attached devices. Its boundary extends to all its users. A unified network has a single mode of operation based on the clearance levels, access, and need-to-know. This mode of operation will be mapped to the level of trust required and will address the risk of the least trusted user obtaining the most sensitive information processed or stored on the network.
- b. An interconnected network is comprised of separately accredited AISS and/or unified networks. Each self-contained AIS maintains its own intra-AIS services and controls, protects its own resources, and retains its individual accreditation. Each participating AIS or unified network has its own ISSR. The interconnected network must have a security support structure capable of adjudicating the different security policy (implementations) of the participating AISS or unified networks. An interconnected network requires accreditation, which may be as simple as an addendum to a Memorandum of Agreement (MOA) between the accrediting authorities.

8-402. Methods of Interconnection.

- a. Security support structure (SSS) is the hardware, software, and firmware required to adjudicate security policy and implementation differences between and among connecting unified networks and/or AISs. The SSS must be accredited. The following requirements must be satisfied as part of the SSS accreditation:

- (1) Document the security policy enforced by the SSS.

- (2) Identify a single mode of operation,

- (3) Document the network security architecture and design.

- (4) Document minimum contents of MOA’s required for connection to the SSS.

- b. Separately accredited network (SAN) is a medium of interconnection of convenience. Networks and/or AISS that are interconnected through a SAN must meet the connection rules of the SAN.

- c. The interconnection of previously accredited systems into an accredited network may require a re-examination of the security features and assurances of the contributing systems to ensure their accreditations remain valid.

- (1) Once an interconnected network is defined and accredited, additional networks or separate AISS (separately accredited) may only be connected through the accredited SSS.

- (2) The addition of components to contributing unified networks that are members of an accredited interconnected network are allowed provided these additions do not change the accreditation of the contributing system.

8-403. Network Requirements.

- a. **Network Security Management.** The contractor shall designate an ISSR for each accredited network to oversee security. The ISSR is responsible for ensuring compliance with the network security requirements as described in the AISSP.

- b. **Network Security Coordination.**

- (1) Every network must have a security plan.

- (2) When different CSAS are involved, a single network security manager (NSM) may be named that will be responsible for network security (including the network AISSP). The NSM will

ensure a comprehensive approach to enforce the overall security policy required by the network security plan.

c. Specific network requirements must be determined on a case-by-case basis by the CSAS involved; however, as a minimum, the **AISSP** for the network must address the following additional requirements:

(1) Description of security services and mechanisms protecting against network specific threats. Consistent with its mode of operation, the network must provide the following security services:

(a) Access control.

(b) Data flow control.

(c) Data separation.

(d) Auditing.

(e) Communications integrity.

(2) Consistent implementation of security features across the network components.

(3) Configuration control of network interconnections.

(4) Protection and control of data transfers.

(5) Security features incorporated in communications protocols.

(6) Adequacy of any filtering bridge, secure gateway, or other similar security device in controlling access and data flow.

(7) Compatibility of the entire combination of operating modes when connecting a new system.

(8) Adequacy of the external system's features to support the local security policy.

S-404. Transmission Security. Protected Distribution Systems or National Security Agency approved encryption methodologies and devices shall be used to protect classified information when it is being transmitted between network components.