DoD 5220.22-M-Sup 1

NATIONAL INDUSTRIAL SECURITY PROGRAM

OPERATING MANUAL SUPPLEMENT

February 1995

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-2000

POLICY

December 29, 1994

FOREWORD

I am pleased to promulgate this inaugural edition of the Supplement to the National Industrial Security Program Operating Manual (NISPOMSUP). It provides the enhanced security requirements, procedures, and options to the National Industrial Security Program Operating Manual (NISPOM) for:

Critical Restricted Data (RD) classified at the Secret and Top Secret levels;

Special Access Programs (SAPS) and SAP-type compartmented efforts established and approved by the Executive Branch;

Sensitive Compartmented Information (SCI) or other DCI SAP-type compartmented programs under the Director of Central Intelligence which protect intelligence sources and methods; and

Acquisition, Intelligence, and Operations and Support SAPS.

This Supplement is applicable to contractor facilities located within the United States, its Trust Territories and Possessions. In cases of inconsistencies between the NISPOM (baseline) and this Supplement as imposed by a Cognizant Security Agency (CSA), as defined herein, the Supplement will take precedence.

The NISPOM Supplement has been written as a menu of options. Throughout this NISPOMSUP it is understood that whenever a security option is specified for a SAP by the Government Program Security Officer (PSO), his or her authority is strictly based on the security menu of options originally approved in writing by the CSA, or designee. CSAS may delegate such responsibility for the implementation of SAP security policies and procedures. Since SAPS have varying degrees of security based on sensitivity and threat, all programs may not have the same requirements. When a security option is selected as a contract requirement, it becomes a “shall” or “will” rather than a “may” in this document. Bold and italicized print denotes contractor security requirements, except in chapter titles and paragraphs.

The Director of Central Intelligence Directives (DCIDs), which prescribe procedures for the DCI Sensitive Compartmented Information (SCI) or other SAP-type DCI programs also set the upper standard of security measures for programs covered by this Supplement. DCIDs may be used by any SAP program manager with approval from the CSA. Specific security measures that are above the DCIDs (noted by asterisks) shall be approved by the CSA or designee.

The provisions of this NISPOMSUP apply to all contractors participating in the administration of programs covered by this Supplement. In cases of doubt over the specific provisions, the contractor should consult the PSO prior to taking any action or expending program-related funds. In cases of extreme emergency requiring immediate attention, the action taken should protect the Government’s interest and the security of the program from compromise.

This NISPOMSUP is intended to be a living document. Users are encouraged to submit changes through their CSA to the Executive Agent's designated representative at the following address:

Department of Defense
ODTUSD(P)PS
ATTN: Director Special Programs
The Pentagon, Room 3C285
Washington, D.C. 20301-2200

This NISPOMSUP will be reviewed and updated as necessary, but in any case no more than one year from the date of publication.

n

Waker B. Slocombe
Under Secretary of Defense (Policy)

TABLE OF CONTENTS

CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS

CHAPTER 2. SECURITY CLEARANCES

CHAPTER 3. SECURITY TRAINING AND BRIEFINGS

CHAPTER 4. CLASSIFICATION AND MARKING

CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION

CHAPTER 6. VISITS and MEETINGS

CHAPTER 7. SUBCONTRACTING

TABLE OF CONTENTS

CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS

CHAPTER 2 SECURITY CLEARANCES

CHAPTER 3. SECURITY TRAINING AND BRIEFINGS

CHAPTER 4. CLASSIFICATION AND MARKING

CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION

CHAPTER 6. VISITS and MEETINGS

CHAPTER 7. SUBCONTRACTING

Chapter 1
General Provisions and Requirements

Section 1. Introduction

1-1oo. Purpose.

a. This Supplement provides special security measures to ensure the integrity of SAPS, Critical SECRET Restricted Data (SRD), and TOP SECRET Restricted Data (TSRD) and imposes controls supplemental to security measures prescribed in the NISPOM for classified contracts. Supplemental measures fall under the cognizance of the DoD, DCI, DOE, NRC or other CSA as appropriate. See page 1-1-2 for Figure 1, SAP Government and Contractor Relationships. Additionally, specific contract provisions pertaining to these measures applicable to associated unacknowledged activities will be separately provided. Any Department, Agent y, or other organizational structure amplifying instructions will be inserted immediately following the applicable security options selected from the NISPOMSUP. This will facilitate providing a contractor with a supplement that is overprinted with the options selected.

b. **Security Options.** This Supplement contains security options from which specific security measures may be selected for individual programs. The options selected shall be specifically addressed in the Program Security Guide (PSG) and/or identified in the Contract. The PSG shall be endorsed by the CSA or his/her designee, establishing the program, although, as a rule, the DCIDs sets the upper limits. In some cases, security or sensitive factors may require security measures that exceed DCID standards. In such cases, the higher standards shall be listed separately and specifically endorsed by the CSA creating the program and maybe reflected as an overprint to this Supplement.

1-101. scope.

a. The policy and guidance contained herein and imposed by contract is binding upon all persons who arc granted access to SAP information. Acceptance of the contract security measures is a prerequisite to any negotiations leading to Program participation and accreditation of a Special Access Program Facility (SAPF).

b. The following is restated from the baseline for clarity. If a contractor determines that implementation of any provision of this Supplement is more costly than provisions imposed under previous U.S. Government policies, standards, or requirements, the contractor shall notify the Cognizant Security Agency. ***Contractors shall, however, implement any such provision within three years from the date of this Supplement, unless a written exception is granted by the CSA.***

c. The DCIDs apply to all SCI and DCI programs and any other SAP that selects them as the program security measures.

1-102. **Agency Agreement SAP Program Areas. The** Government Agency establishing a SAP will designate a Program Executive Agent for the administration, security, execution, and control of the SAP. The Program Security Officer (PSO), rather than the Facility CSA, will be responsible for security of the program and all program areas.

1-103. **Security Cognizance. Those** heads of Agencies authorized under E.O. 12356 or successor order to create SAPS may enter into agreements with the Secretary of Defense that establish the terms of the Secretary of Defense's responsibilities for the SAP. When a Department or Agency of the Executive Branch retains cognizant security responsibilities for its SAP, the provisions of this Supplement will apply.

1-104. Supplement Interpretations. ***AU contractor requests for interpretation of this Supplement will be forwarded to the PSO.***

1-105. **Supplement Changes.** Users of this Supplement are encouraged to submit recommended changes and comments through their PSO in concurrence with the baseline.

1-106. **Waivers and Exceptions.** The purpose of having a waiver and exception policy is to ensure that deviations from established SAP criteria are systematically and uniformly identified to the Government Program Manager (GPM). Every effort will be made to avoid

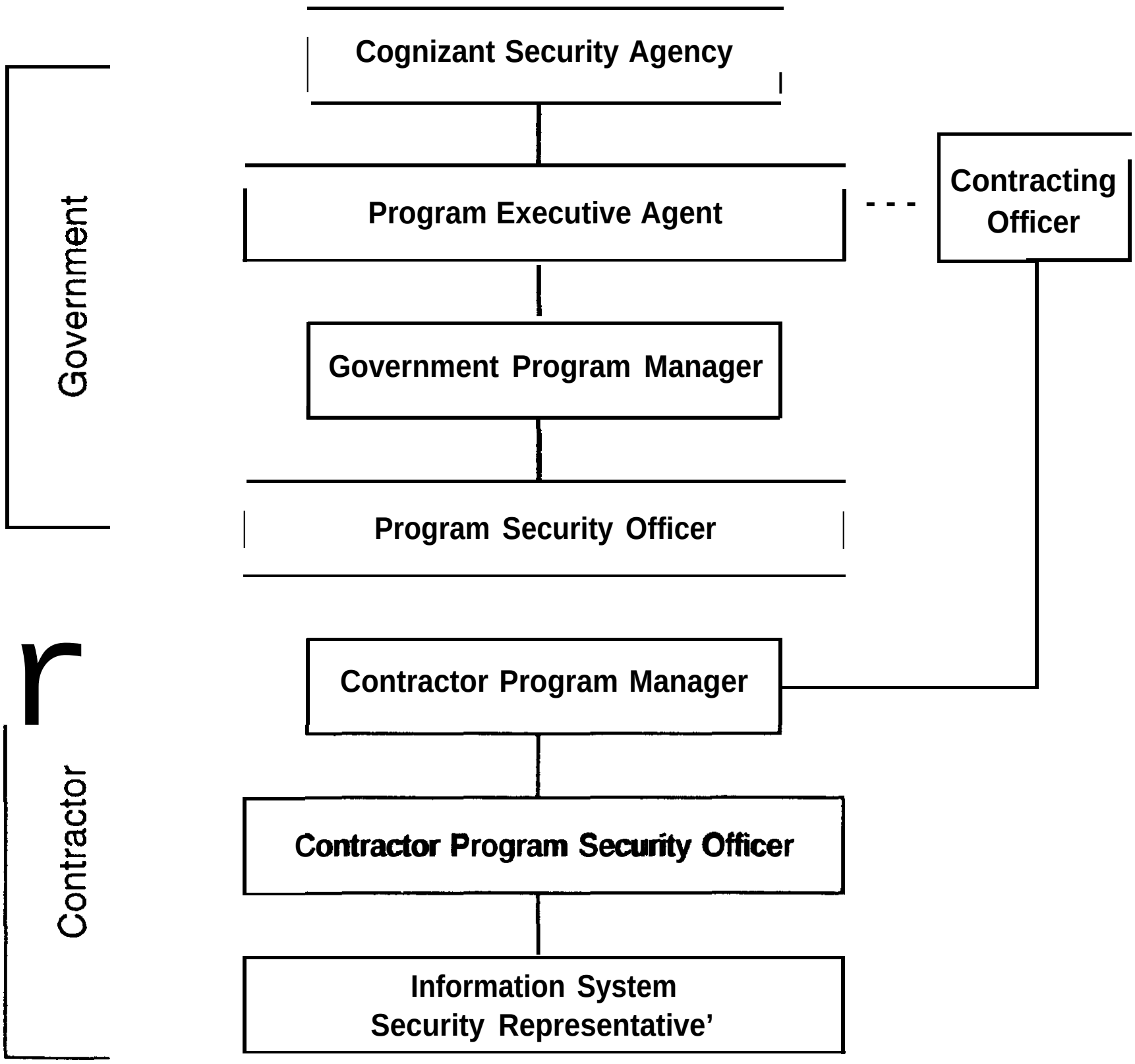
waivers to established SAP policies and procedures unless they are in the best interest of the Government. In those cases where waivers are required, a request will be submitted to the PSO. As appropriate, the PSO, and if necessary the GPM (if a different individual) will assess the request for waiver and provide written approval. If deemed necessary, other security measures which address the specific vulnerability may be implemented.

1-107. **Special Access Programs Categories and Types.**

a. There are four generic categories of SAPS: (1) Acquisition SAP (AQ-SAP); (2) Intelligence SAP (IN-SAP); (3) Operations and Support SAP (OS-SAP); and (4) SCI Programs (SCI - SAP) or other DCI programs which protect intelligence sources and methods.

b. There are two types of SAPS, acknowledged and unacknowledged. An acknowledged SAP is a program which may be openly recognized or known; however, specifics are classified within that SAP. The existence of an unacknowledged SAP or an unacknowledged portion of an acknowledged program, will not be made known to any person not authorized for this information.

SAP
Government/Contractor Relationships



[1] SSR may work for the CPSO, or work a.. a peer to the CPSO for A IS purposes, depending on Program Requirements.

Section 2. General Requirements

1-200. Responsibilities A *SAP Contractor program Manager (CPM) and Contractor Program Security Officer (CPSO) will be designated by the contractor. These* individuals are the primary focal points at the contractor facility who execute the contract. They are responsible for all Program matters. ***The initial nomination or appointment of the CPSO and any subsequent changes will be provided to the PSO in writing. The criteria necessary for an individual to be nominated as the CPSO will be provided in the Request for Proposal (RFP).*** For the purposes of SAPS, the following responsibilities are assigned:

a. The CPM is (sometimes the same as, or in addition to a Contract Project Manager) the contractor employee responsible for:

(1) Overall Program management.

(2) Execution of the statement of work, contract, task orders and all other contractual obligations.

b. The CPSO oversees compliance with SAP security requirements.

The CPSO will:

(1) ***Possess a personnel clearance and Program access at least equal to the highest level of Program classified information involved.***

(2) ***Provide security administration and management for his/her organization.***

(3) ***Ensure personnel processed for access to a SAP meet the prerequisite personnel clearance and/or investigative requirements specified.***

(4) ***Ensure adequate secure storage and work spaces.***

(5) ***Ensure strict adherence to the provisions of the NISPOM and its Supplement.***

(6) ***When required, establish and oversee a classified material control program for each SAP.***

(7) ***When required, conduct an annual inventory of accountable classified material***

(8) ***When required, establish a SAPF.***

(9) ***Establish and oversee visitor control program.***

(10) ***Monitor reproduction and/or duplication and destruction capability of SAP information.***

(11) ***Ensure adherence to special communications capabilities within the SAPF.***

(12) ***Provide for initial Program indoctrination of employees after their access is approved; rebrief and debrief personnel as required***

(13) ***Establish and oversee specialized procedures for the transmission of SAP material to and from Program elements.***

(14) ***When required, ensure contractual specific security requirements such as TEMPEST, Automated Information System (AIS), and Operations Security (OPSEC) are accomplished.***

(15) ***Establish security training and briefings specifically tailored to the unique requirements of the SAI?***

***1-201.* *Standard Operating Procedures (SOP). The** CPSO maybe required to prepare a comprehensive SOP to implement the security policies and requirements for each SAP. When required, SOPS will address and reflect the contractor's method of implementing the PSG. Forward proposed SOPS to the PSO for approval. SOPS may be a single plan or series of individual documents each addressing a security function. Changes to the SOP will be made in a timely fashion, and reported to the PSO as they occur.

1-202. Badging. Contractors performing on Programs where all individuals cannot be personally identified, may be required to implement a PSO-approved badging system.

1-203. **Communications Security (COMSEC).** ***Classified SAP information will be electronically transmitted only by approved secure communicating channels authorized by the PSO.***

***1-204.* *Two-Person Integrity (TPI) Requirement** **The** TPI rule may be required and exercised only with the Program CSA approval. This requirement does not

apply to those situations where one employee with access is left alone for brief periods of time, nor dictate that those employees will be in view of one another.

1-205. Contractors Questioning Perceived Excessive Security Requirements. All personnel are highly encouraged to identify excessive security measures that they believe have no added value or are cost excessive and should report this information to their industry contracting officer for subsequent reporting through contracting channels to the appropriate GPM/PSO. The GPM/PSO will respond through appropriate channels to the contractor questioning the security requirements.

1-206. Security Reviews.

a. **General. The** frequency of Industrial Security Reviews (e.g., Reviews, evaluations, and security surveys) is determined by the NISPOM and will be conducted by personnel designated by the CSA.

b. **Joint Efforts.** In certain cases, an individual Program may be a joint effort of more than one component of the U.S. Government or more than one element of the same component. In such a case, one element will, by memorandum of agreement, take the lead as the Cognizant Security Agency and may have security review responsibility for the Program facility. In order to ensure the most uniform and efficient application of security criteria, review activities at contractor facilities will be consolidated to the greatest extent possible.

c. **Prime Contractor Representative.** A security rep **resentative** from the prime contractor may be present and participate during reviews of subcontractors, but cannot be the individual appointed by the CSA to conduct security reviews specified in paragraph 1-206a.

d. **Review Reciprocity.** In order to ensure the most uniform and efficient application of security reviews, review **reciprocity** at contractor facilities will be considered whenever possible.

e. **Contractor Reviews.** When applicable, the U.S. Government may prescribe the intervals that the contractor **will** review their systems.

f. **Team Reviews.** Team Reviews maybe conducted by more than one PSO based on mutual consent and cooperation of both the Government and the contractor.

Section 3. Reporting Requirements

1-300. General. ***All reports required by the NISPOM will be made through the PSO.*** In those instances where the report affects the baseline facility clearance or the incident is of a personnel security clearance nature, the report will also be provided to the Facility CSA. In those rare instances where classified program information must be included in the report, the report will be provided only to the PSO, who will sanitize the report and provide the information to the CSA, if appropriate.

a. **Adverse Information.** ***Contractors will report to the PSO any information which may adversely reflect on the Program-briefed employee's ability to properly safeguard classified Program information.***

b. SAP **Non-Disclosure Agreement (NDA).** ***A report will be submitted to the PSO on an employee who refuses to sign a SAP NDA.***

c. **Change in Employee Status.** ***A written report of all changes in the personal status of SAP indoctrinated personnel will be provided to the PSO.*** In addition to those changes identified in NISPOM subparagraph 1-302c., include censure or probation arising from an adverse personnel action, and revocation, or suspension downgrading of a security clearance or Program access for reasons other than security administration purposes.

d. Employees Desiring Not to Perform **on SAP Classified Work.** ***A report will be made to the PSO upon notification by an accessed employee or an employee for whom access has been requested that they no longer wish to perform on the SAP. Pending further instructions from the PSO, the report will be destroyed in 30 days.***

e. ***Foreign Travel.** The PSO may require reports of all travel outside the continental United States, Hawaii, Alaska and the U.S. possessions (i.e., Puerto Rico) except same-day travel to border areas (i.e., Canada, Mexico) for Program-accessed personnel. Such travel is to be reported to the CPSO, and retained for the life of the Contract/Program travel. Travel by Program-briefed individuals into or through countries determined by the CSA as high-risk areas, should not be undertaken without prior notification. A supplement to the report outlining the type and extent of contact with foreign nationals, and any attempts to solicit information or establish a continuing relationship by a foreign national may be required upon completion of travel.

f. **Arms Control Treaty Visits.** ***The GPM and PSO will be notified in advance of any Arms Control Treaty Visits.*** Such reports permit the GPM and PSO to assess potential impact on the SAP activity and effectively provide guidance and assistance.

g. **Litigation.** ***Litigation or public proceedings which may involve a SAP will be reported. These*** include legal proceedings and/or administrative actions in which the prime contractor, subcontractors, or Government organizations and their Program-briefed individuals are a named party. ***The CPSO will report to the PSO any litigation actions that may pertain to the SAP, to include the physical environments, facilities or personnel or as otherwise directed by the GPM.***

1-301. Security Violations and Improper Handing of Classified Information. Requirements of the NISPOM baseline pertaining to security violation are applicable, except that all ***communications will be appropriately made through Program Security Channels within 24 hours of discovery to the PSO.*** The PSO must promptly advise the Facility CSA in all instances where national security concerns would impact on collateral security programs or clearances of individuals under the cognizant of the Facility CSA.

a. **Security Violations and Infractions**

(1) Security Violation. A security violation is any incident that involves the loss, compromise, or suspected compromise of classified information. ***Security violations will be immediately reported within 24 hours to the PSO.***

(2) **Security Infraction.** A security infraction is any other incident that is not in the best interest of security that does not involve the loss, compromise, or suspected compromise of classified information. ***Security infractions will be documented and made available for review by the PSO during visits.***

b. **Inadvertent Disclosure.** An inadvertent disclosure is the involuntary unauthorized access to classified SAP information by an individual without SAP access authorization. Personnel determined to have had unauthorized or inadvertent access to classified SAP information (1) should be interviewed to determine the extent of the exposing, and (2) maybe requested to complete an Inadvertent Disclosure Oath.

(1) If during emergency response situations, guard personnel or local emergency authorities (e.g., police, medical, fire, etc.) inadvertently gain access to Program material, they should be interviewed to determine the extent of **the exposure.** If circumstances **warrant,** a preliminary inquiry will be conducted. **When** in doubt, contact the PSO for advice.

(2) ***Refusal*** *to sign an* ***inadvertent*** *disclosure oath will be reported by the CPSO to the PSO.*

(3) *Contractors* ***shall*** *report* ***all*** *unauthorized* ***disclosures involving RD or Formerly Restricted Data (FRD) to Department of Energy (DOE) or Nuclear Regulatory Commission (NRC) through their CSA.***

Chapter 2
Security Clearances

Section 1. Facility Clearances

2-100. General. Contractors will possess a Facility Security Clearance to receive, generate, use, and store classified information that is protected in SAPs.

a. If a facility clearance has already been granted, the SAP Program Executive Agent may carve in the Facility CSA. The agreement entered into by the Secretary of Defense (SECDEF) with the other CSA's will determine the terms of responsibility for the Facility CSA with regard to SAP programs. Due to the sensitivity of some SAPS, the program may be carved out by the Executive Agent designated by the CSA.

b. The CPSO shall notify the PSO of any activity which affects the Facility Security Clearance, (FCL).

c. In certain instances, security and the sensitivity of the project may require the contract and the association of the contractor with the Program CSA be restricted and kept at a classified level. The existence of any unacknowledged effort, to include its SAPF, will not be released without prior approval of the PSO.

2-101. Co-Utilization of SAPF. If multiple SAPS are located within a SAPF, a Memorandum of Agreement (MOA) shall be written between government program offices defining areas of authorities and responsibilities. The first SAP in an area shall be considered to be the senior program and therefore the CSA for the zone unless authority or responsibility is specifically delegated in the MOA. The MOA shall be executed prior to the introduction of the second SAP into the SAPF.

2-102 Access **of Senior Management Officials.** *Only those Senior Management Officials requiring informatwn pertaining to the SAP shall be processed SAP access.*

2-103. **Facility Clearances for Multifacility Organizations.**

a. When cleared employees are located at uncleared locations, the CPSO may designate a cleared management official at the uncleared location who shall:

(1) Process classified visit requests, conduct initial or recurring briefings for cleared employees, and provide written confirmation of the briefing to the CPSO.

(2) Implement the reporting requirements of the NISPOM and this Supplement for all cleared employees and furnish reports to the CPSO for further submittal to the CSA.

(3) Ensure compliance with all applicable measures of the NISPOM and this Supplement by all cleared employees at that location.

b. If a cleared management official is not available at the uncleared location, the CPSO (or designee) shall conduct the required briefing during visits to the uncleared location or during employee visits to the location or establish an alternative procedure with CSA approval.

Section 2. Personnel Clearances and Access

2-200. General. This section establishes the requirements for the selection, processing, briefing, and debriefing of contractor personnel for SAPS.

2-201. Program **Accessing Requirements and Procedures.**

a. ***The individual will have a valid need-to-know (NTK) and will materially and directly contribute to the Program,***

b. ***The individual will possess a minimum of a current, final SECRET security clearance or meet the investigative criteria required for the level of access.*** If a person's periodic reinvestigation (PR) is outside the five-year scope and all other access processing is current and valid, the PSO may authorize access. However, the individual will be immediately processed for either a Single Scope Background Investigation (SSBI) or National Agency Check with Credit (NACC) as required by the level of clearance or as otherwise required by the contract.

c. ***The contractor will nominate the individual and provide a description of the NTK justification. The CPM will concur with the nomination and verify Program contribution by signature*** on ***the Program Access Request (PAR). The CPSO will complete the PAR and review it for accuracy ensuring all required signatures are present.*** The CPSO signature verifies that the security clearance and investigative criteria are accurate, and that these criteria satisfy the requirements of the Program. Information regarding the PAR may be electronically submitted. While basic information shall remain the same, signatures may not be required. The receipt of the PAR package via a preapproved channel shall be considered sufficient authentication that the required approvals have been authenticated by the CPSO and contractor program manager.

d. Access Criteria **and Evaluation Process.** In order to eliminate those candidates who clearly will not meet the scope for access and to complete the Personnel Security Questionnaire (PSQ), access evaluation may be required. In the absence of written instructions from the contracting activity, the evaluation process will conform to the following guidelines:

(1) Evaluation criteria will not be initiated at the contractor level unless both the employee and contractor agree.

(2) Contractors will not perform access evaluation for other contractors.

(3) Access evaluation criteria will be specific and will not require any analysis or interpretation by the contractor. Access evaluation criteria will be provided by the government as required.

(4) Those candidates eliminated during this process will be advised that access processing has terminated.

e. Submit a Letter of Compelling Need or other documentation when requested by the PSO.

f. Formats required for the processing of a SAP access fall into two categories: those required for the conduct of the investigation and review of the individual's eligibility, and those that explain or validate the individual's NTK. These constitute the PAR package. The PAR package used for the access approval and NTK verification will contain the following: the PAR and a recent (within 90 days) PSQ reflecting pen and ink changes, if any, signed and dated by the nominee.

g. Once the PAR package has been completed, the CPSO will forward the candidate's nomination package to the PSO for review:

(I) The PSO will review the PAR package and determine access eligibility.

(2) Access approval or denial will be determined by the GPM and/or access approval authority.

(3) The PSO will notify the contractor of access approval or denial.

(4) Subcontractors may submit the PAR package to the prime. The prime will review and concur on the PAR and forward the PAR and the unopened PSQ package to the PSO.

h. SCI access will follow guidelines established in DCID 1/14.

2-202. Supplementary Measures and Polygraph.

a. Due to the sensitivity of a Program or criticality of information or emerging technology, a polygraph may be required. The polygraph examination will be conducted by a properly trained, certified, U.S. Government Polygraph Specialist. If a PR is outside the 5-year investigative scope, a polygraph maybe used as an interim basis to grant access until completion of the PR.

b. There are three categories of polygraph: Counterintelligence (CI), Full Scope (CI and life style), and Special Issues Polygraph (SIP). The type of polygraph conducted will be determined by the CSA.

2-203. **Suspension and Revocation.** All PSO direction to contractors invoIving the suspension or revocation of an employee's access will be provided in writing and if appropriate, thru the contracting officer.

2-204. **Appeal Process. The** CSA will establish an appeal process.

2-205. **Agent of the Government- The** Government may designate a contractor-nominated employee as an Agent of the Government on a case-by-case basis. Applicable training and requirements will be provided by the Government to contractor designated as Agents of the Government.

2-206 **Access Roster or List.** ***Current access rosters of Program-briefed individuals are required at each contractor location. They*** should be properly protected and maintained in accordance with the PSG. The access roster should be continually reviewed and reconciled for any discrepancies. The data base or listing may contain the name of the individual organization, position, billet number (if applicable), level of access, social security number, military rank/grade or comparable civilian rating scheme, and security clearance information. ***Security personnel required for adequate security oversight will not count against the billet structure.***

Chapter 3
Security Training and Briefings

Section 1. Security Training and Briefings

3-100. General. *Every Special Access Program (SAP) will have u Security Training and Briefing Program.* **As** a minimum, SAP-indoetrinated personnel will be provided the same or similar training and briefings as outlined in the baseline **NISPOM.** *In addition, CPSOs responsible for SAPS at contractor facilities will establish a Security Education Program to meet any specific or unique requirements of individual special access programs.* Topics which will be addressed, if **appropriate** to the facility or the SAP(s), include:

a. Security requirements unique to SAPS;

b. Protection of classified relationships;

c. **Operations** Security **(OPSEC);**

d. Use of nicknames and code words;

e. Use of special transmission methods;

f. Special test-range security procedures;

g. Procedures for unacknowledged SAP security. An unacknowledged SAP **will** require additional security training and briefings, beyond that required in the baseline. Additional requirements will be specified in the Contract Security Classification Specification and will address steps necessary to protect sensitive relationships, locations, and activities.

h. Specific procedures to report fraud, waste, and abuse.

i. Computer security education that is to include operational procedures, threats, and **vulnerabil** ities.

j. Writing unclassified personnel appraisals and reviews.

k. Third-Party Introductions. The purpose of the Third-Party Introduction is to provide a clearance. and/or access verification to other cleared personnel. The introduction is accomplished by a briefed third party, who has knowledge of both individual's access.

3-101. Security Training. *The CPSO will ensure that the following security training measures are implemented:*

a. *Initial Program Security Indoctrination. Every individual accessed to a SAP will be given an initial indoctrination. The briefing will clearly identify the information to be protected, the reasons why this information requires protection, and the need to execute a NDA. The individual will be properly briefed concerning the security requirements for the Program, understand their particular security responsibilities, and will sign a NDA.* This indoctrination is in addition to any other briefing required for access to collateral classified or company proprietary information. It will be the responsibility of the PSO to provide to the contractor information as to what will be included in the initial indoctrination to include fraud, waste, and abuse reporting procedures.

b. Professionalized AIS training maybe required of all contractor Information Systems Security Representatives **(ISSRs)** to ensure that these individuals have the appropriate skills to perform their job functions in a competent and cost-effective manner. This training will be made available by the CSA. The training should consist of, but not be limited to, the following criteria:

(1) Working knowledge of all applicable and national CSA regulations and policies including those contained in this supplement;

(2) Use of common Information Security **(INFOSEC)** practices and technologies;

(3) AIS certification testing procedures;

(4) Use of a risk management methodology;

(5) Use of configuration management methodology.

3-102. Unacknowledged Special Access Programs (SAP). Unacknowledged SAPS require a significantly greater degree of protection than acknowledged SAPS. Special emphasis should be placed on:

a. Why the SAP is unacknowledged;

b. Classification of the SAP:

c. Approved communications system;

d. Approved transmission systems;

e. Visit procedures;

f. Specific program guidance.

3-103. Refresher Briefings. *Every accessed individual will receive an annual refresher briefing from the CPSO to include the following, as a minimum:*

a. Review of Program-unique security directives or guidance;

b. Review of those elements contained in the original NDA.

Note. The PSO may require a record to be maintained of this training.

3-104. **Debriefing and/or Access Termination.** *Persons briefed to SAPS will be debriefed by the CPSO or his designee. The debriefing will include as a minimum a reminder of each individual's responsibilities according to the NDA which states that the individual has no Program or Program-related material in his/her possession, and that he/she understands his/her responsibilities regarding the disclosure of classified Program information.*

a. Debriefings should be conducted in a SAPF, Sensitive Compartmented Information Facility (SCIF), or other secure area when possible, or as authorized by the PSO.

b. Procedures for debriefing will be amanged to allow each individual the opportunity to ask questions and receive substantive answers from the debriefer.

c. Debriefing Acknowledgments will be used and executed at the time of the debriefing and include the following:

(1) Remind the individual of his/her continuing obligations agreed to in the SAP NDA.

(2) Remind the individual that the NDA is a legal contract between the individual and the U.S. Government.

(3) Advise that all classified information to include Program information is now and forever the property of the U.S. Government.

(4) *Remind the individual of the penalties for espionage and unauthorized disclosure as contained in Tides 18 and 50 of the U.S. Code. The briefer should have these documents available for handout upon request. Require the individual to sign and agree that questions about the NDA have been answered and that Tides 18 and 50 (U.S. Codes) were made available and understood.*

(5) Remind the individual of his/her obligation not to discuss, publish, or otherwise reveal information about the Program. The appearance of Program information in the public domain does not constitute a de facto release from the continuing secrecy *agreement.*

(6) Advise that any future questions or concerns regarding the Program (e.g., solicitations for information, approval to publish material based on Program knowledge and/or experience) will be directed to the CPSO. The individual will be provided a telephone number for the CPSO or PSO.

(7) Advise that each provision of the agreement is severable, i.e., if one provision is declared unenforceable, all others remain in force.

(8) Emphasize that even though an individual signs a Debriefing Acknowledgment Statement, he/she is never released from the original NDA/secrecy agreement unless specifically notified in writing.

d. Verify the return of any and all SAP classified material and unclassified Program-sensitive material and identify all security containers to which the individual had access.

e. When debriefed **for cause, include a brief statement as to the reason** for termination of access and notify the PSO. In addition the CPSO will notify all agencies holding interest in that person's clearance/ accesses.

f. The debriefer will advise persons who refuse to sign a debriefing acknowledgment that such refusal could affect future access to special access programs and/ or continued clearance eligibility. It could be cause for administrative sanctions and it will be reported to the appropriate" Government Clearance Agency.

g. Provide a point of contact for debriefed employees to report any incident in the future which might affect the security of the Program.

3-105. Administrative Debriefings. Efforts to have all Program-briefed personnel sign a Debriefing Acknowledgment Statement may prove difficult. If attempts to locate an individual either by telephone or mail are not successful, the CPSO should prepare a Debriefing Acknowledgment Statement reflecting the individual was administratively debriefed. ***The Debriefing Acknowledgment Statement will be forwarded to the PSO. The CPSO will check*** to ***ensure that no Program material is charged out to, or in the possession of these persons.***

3-106. Recognition and Award Program. Recognition and award programs could be established to single out those employees making significant contributions to Program contractor security. If used, CPSOs will review award write-ups to ensure recommendations do not contain classified information.

Chapter 4
Classification and Markings

Section 1. Classification

Challenges to Classification. *AU challenges to SAP classified information and/or material shall be forwarded through the CPSO to the PSO to the appropriate Government contracting activity. AU such challenges shall remain in Program channels.*

Section 2. Marking Requirements

4-200. **General.** ***Classified material that is developed under a SAP will be marked and controlled in accordance with the NISPOM, this Supplement, the Program Security Classification Guide, and other Program guidance as directed by the PSO.***

4-201. **Additional Provisions and Controls. The** PSO may specify additional markings to be applied to SAP **working** papers based on the sensitivity and criticality of the Program, when approved by the CSA.

4-202. **Engineer's Notebook.** An engineer's notebook is a working record of continually changing Program technical data. It should NOT include drafts of correspondence, reports, or other materials. ***The outer cover and first page will be marked with the highest classification level contained in the notebook.*** Portion marking or numbering is not required. Other requirements pertaining to these notebooks may be imposed by the PSO.

4-203. **Cover Sheets.** ***Cover sheets will be applied to SAP documents when the documents are created or distributed. NOTE: CODE WORDS WILL NOT BE PRINTED ON THE COVER SHEETS.*** The unclassified nickname, digraph, or trigraph may be used.

4-204. **Warning Notices.** ***Generally, Program classified marking and transmission requirements will follow this Supplement. Transmission of Program or Program-related material will be determined by the PSO. Besides the classifications markings, inner containers will be marked:***

"TO BE OPENED ONLY **BY:"** ***followed by the name of the individual to whom the material is sent.*** A receipt may be required. Apply the following markings on the bottom center of the front of the inner container:

WARNING

THIS PACKAGE CONTAINS CLASSIFIED U.S. GOVERNMENT INFORMATION. TRANSMISSION OR REVELATION OF THIS INFORMATION IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY TITLE 18, U.S. CODE, SECTION 798 (OR TITLE 42, SECTION XX FOR RD OR FRD MATERIAL). IF FOUND, PLEASE DO NOT OPEN. "CALL COLLECT" THE FOLLOWING NUMBERS, (area code) (number) (PSO/CPSO work number) DURING WORKLNG HOURS OR (area code) (number) (PSO/CPSO) AFTER WORKING HOURS.

Chapter 5
Safeguarding Classified Information

Section 1. General Safeguarding Requirements

5-100. General. Classified and unclassified sensitive SAP material must be stored in SAP CSA approved facilities only. Any deviations must have prior approval of the SAP CSA or designee.

Section 2. Control and Accountability

5-200. **General.** ***Contractors shall develop and maintain a system that enables control of SAP classified information and unclassified Program sensitive information for which the contractor is responsible.***

5-24)1. **Accountability.** ***Accountability of classified SAP material shall be determined and approved in writing by the CSA or designee at the time the SAP is approved.*** A separate accountability control system may be required for each SAP.

5-202. Annual Inventory. An annual inventory of accountable SAP classified material may be required. The results of the inventory and any discrepancies may be required to be reported in writing to the PSO.

5-203. Collateral classified material required to support a SAP contract may be transferred within SAP controls. ***Transfer will be accomplished in a manner that will not compromise the SAP or any classified information. The PSO will provide oversight for collateral classified material maintained in the SAP.*** Collateral classified material generated during the performance of a SAP contract may be transferred from the SAP to the contractor's collateral classified system. The precautions required to prevent compromise will be approved by the PSO.

Section 3. Storage and Storage Equipment

(not further supplemented)

Section 4. Transmission

5-400. General. *SAP classified material shall be transmitted outside the contractor's facility in a manner that prevents loss or unauthorized access.*

5-401. **Preparation.** *AU classified SAP material will be prepared, reproduced, and packaged by Program-briefed personnel in approved Program facilities.*

5-402. **Couriers.** *The PSO through the CPSO will provide detailed courier instructions to couriers when hand-carrying SAP material The CPSO will provide the courier with an authorization letter.* Report any travel anomalies to the CPSO as soon as practical. The CPSO will notify the PSO.

5-403. **Secure Facsimile and/or Electronic Transmission.** Secure facsimile and/or electronic transmission encrypted communications equipment may be used for the transmission of Program classified information. *When secure facsimile and/or electronic transmission is permitted, the PSO or other Government cognizant security reviewing activity will approve the system in writing.* Transmission of classified Program material by this means may be receipted for by an automated system generated message that transmission and receipt has been accomplished. For TOP SECRET documents a receipt on the secure facsimile may be required by the PSO.

5-404. **U.S. Postal Mailing.** A U.S. Postal mailing channel, when approved by the PSO, may be established to ensure mail is received only by appropriately cleared and accessed personnel.

5-405. **TOP SECRET Transmission.** *TOP SECRET (TS) SAP will be transmitted via secure data transmission or via Defense Courier Service unless other means have been authorized by the PSO.*

Section 5. Disclosure

5-500. **Release of Information.** ***Public release of SAP information is not authorized without written authority from the Government as provided for in U.S. Code, Titles 10 and 42.*** Any attempt by unauthorized personnel to obtain Program information and sensitive data will be reported immediately to the Government Program Manager (GPM) through the PSO using approved secure communication channels.

Section 6. Reproduction

5-600. **General.** ***Program material will be reproduced on equipment specifically designated by the CPSO*** and may require approval by the PSO. The CPMS and CPSOs may be required to prepare written reproduction procedures.

5-601. The PSO or designee may approve reproduction of TS material.

Section 7. Disposition and Retention

5-700. Deposition. CPSOS may be required to inventory, dispose of, request retention, or return for disposition all classified SAP-related material (including AIS media) at contract completion and/or close-out. ***Request for proposal (RFP), solicitation, or bid and proposal collateral classified and unclassified material contained in Program files will be reviewed and screened to determine appropriate disposition (i.e., destruction, request for retention). Disposition recommendations by categories of information or by document control number, when required, will be submitted to the PSO for concurrence. Requests for retention of classified information (SAP and non-SAP) will be submitted to the Contracting Officer, through the PSO for review and approval. Requirements for storage and control of materials approved for retention will be approved by the PSO.***

5-701. Retention of SAP Material. The contractor may be required to submit a request to the Contracting Officer (CO), via the PSO, for authority to retain classified material beyond the end of the contract performance period. The request will also include any retention of Program-related material. ***The contractor will not retain any Program information unless specifically authorized in writing by the Contracting Officer. Storage and control requirements of SAP materials will be approved by the PSO.***

5-702. **Destruction.** ***Appropriately indoctrinated personnel shall ensure the destruction of classified SAP data.*** The CSA or designee may determine that two persons are required for destruction. Nonaccountable waste and unclassified SAP material may be destroyed by a single Program-briefed employee.

Section 8. Construction Requirements

5-800. General. Establishing a Special Access Program Facility (SAPF). Prior to commencing work on a SAP, the contractor may be required to establish an approved SAPF to afford protection for Program classified information and material. ***Memorandums of Agreement (MOA) are required prwr to allowing SAPS with different CSAS to share a SAPF.***

5-801. **Special Access Program Facility.**

a. A SAPF is a program area, room, group of rooms, building, or an enclosed facility accredited by the PSO where classified SAP Program business is conducted. ***SAPFs will be afforded personnel access control to preclude entry by unauthorized personnel. Non-accessed persons entering a SAPF will be escorted by an indoctrinated person.***

b. A Sensitive Compartmented Information Facility (SCIF) is an area, room, building, or installation that is accredited to store, use, discuss, or electronically process SCI. The standard and procedures for a SCIF are stated in DCIDs 1/19 and 1/21.

c. ***SAPFS accredited prior to implementation of this Supplement will retain accreditation until no longer required or recertification is required due to major modification of the external perimeter, or changes to the Intrusion Detection System (IDS), which affects the physical safeguarding capability of the facility.***

d. ***Physical security standards will be stated in the Government's RFP, RFQ, contract, or other precontract or contractual document.***

e. The need-to-know (NTK) of the SAP effort may warrant establishment of multi-compartments within the same SAPF.

f. *There may be other extraordinary or unique circumstances where existing physical security standards are inconsistent with facility operating requirements, for example, but not limited to, research and test facilities or production lines. ***Physical security requirements under these circumstances will be established on a case-by-case basis and approved by the PSO/Contracting Officer, as appropriate. (Note: as approved by the CSA at establishment of the SAP.)***

g. The PSO will determine the appropriate security countermeasures for discussion areas.

5-802. **Physical Security Criteria Standards.**

a. DCID 1/21 standards may apply to a SAPF when one or more of the following criteria are applicable:

(1) State-of-the-art technology as determined by CSAS to warrant enhanced protection.

(2) Contractor facility is known to be working on specific critical technology.

(3) Contractor facility is one of a few (3 or less) known facilities to have the capability to work on specific critical technology.

(4) TOP SECRET or SECRET material is maintained in open storage.

(5) A SAPF is located within a commercial building, and the contractor does not control all adjacent spaces.

(6) SCI or Intelligence Sources and methods are involved.

(7) Contractors or technologies known to be a target of foreign intelligence services (FIS).

b. The NISPOM baseline closed area construction requirements with Sound Transmission Class (STC) in accordance with DCID 1/21, Annex E and intrusion alarms in accordance with Annex B, DCID 1/21 may apply to a SAPF when one of the following criteria are applicable.

(1) Not state-of-the-art technology and the technology is known to exist outside U.S. Government control.

(2) The SAP is a large-scale weapon system production program.

(3) No open storage of Confidential SAP material in a secure working area unless permitted by the PSO on a case-by-case basis.

(4) A SAPF located within a controlled access area.

(5) Intelligence related activities.

c. The PSO may approve baseline closed area construction requirements as an additional option for some SAP program areas.

5-803. **SAP Secure Working Area.** The PSO may approve any facility as a SAP Secure Working Area. Visual and sound protection may be provided by a mix of physical construction, perimeter control, guards, and/or indoctrinated workers.

5-804. Temporary **SAPF.** The PSO may accredit a temporary SAPF.

5-S05. **Guard** Response.

a. ***Response to alarms will be*** in ***accordance with DCID 1/21, or***

b. ***The NISPOM***

c. ***Response personnel will remain at the scene until released by the CPSO or designated representative.***

NOTE: The CPSO will immediately provide notification to the PSO if there is evidence of forced entry, with a written report to follow within 72 hours.

5-806. **Facility Accreditation.**

a. Once a facility has been accredited to a stated level by a Government Agency, that accreditation should be accepted by any subsequent agency.

b. For purposes of co-utilization, costs associated with any security enhancements in a SCIF or SAPF above preexisting measures may be negotiated for reimbursement by the contractor's contracting officer or designated representative. Agreements will be negotiated between affected organizations.

c. ***If a previously accredited SAPF becomes inactive for a-period not to exceed one year, the SAP accreditation will be reinstated by the gaining accrediting agency provided the following is true:***

(1) The threat in the environment surrounding the SAPF has not changed;

(2) No modifications have been made to the SAPF which affect the level of safeguarding;

(3) The level of safeguarding for the new Program is comparable to the previous Program;

(4) The SAPF has not lost its SAP accreditation integrity and the contractor has maintained continuous control of the facility.

(5) A technical surveillance countermeasure survey (TSCM) maybe required.

NOTE: Previously granted waivers are subject to negotiation.

5-807. **Prohibited Items.** Items that constitute a threat to the security integrity of the SAPF (e.g., cameras or recording devices) are prohibited unless authorized by the PSO. All categories of storage media entering and leaving the SAPFS may require the PSO or his/her designated representative approval.

Chapter 6
Visits and Meetings

Section 1. Visits

6-100. General. ***A visit certification request for all Program visits will he made prior to a visit to a Program facility.*** When telephone requests are made, a secure telephone should be used whenever possible. Visit ***requests will be handled exclusively by the cognizant CPSO or designated representative. The*** GPM or PSO or his/her designated representative will approve all visits between Program activities. ***However, visits between a prime contractor and the prime's subcontractors and approved associates will be approved by the CPSO.*** Twelve-month visit requests are not authorized unless approved by the PSO.

6-101. ***Visit Request Procedures. All visit requests will be sent only via approved channels. In addition*** to ***the NISPOM, the follo wing additional information for visits to a SAPF will include:***

a. ***Name and telephone number of individual (not organization) to be visited;***

b. ***Designation of person as a Program courier when applicable; and***

c. Verification (e.g., signature) of the CPSO or designated representative that the visit request informatwn is correct.

6-102. Termination and/or Cancellation of a Visit Request. If a person is debriefed from the Program prior to expiration of a visit certification, or if cancellation of a current visit certification is otherwise appropriate, the CPSO/FSO or his/her designated representative will immediately notify all recipients of the cancellation or termination of the visit request.

6-103. **Viiit Procedures.**

a. **Identification of Visitors.** ***An official photograph if identification such as a valid driver's license is required***

b. **Extension.** When a visit extends past the date on the visit certification, a new visit request is not required if the purpose remains the same as that stated on the current visit request to a specific SAPF.

c. Rescheduling. When a rescheduled visit occurs after a visit request has been received, the visit certification will automatically apply if the visit is rescheduled within thirty days and the purpose remains the same.

d. **Hand-carrying.** It is the responsibility of the host CPSO to contact the visitor's CPSO should the visitor plan to hand-carry classified material. ***CPSOs will use secure means for notification.*** In emergency situations where secure communications are not available, contact the PSO for instructions. ***When persons return to their facility with SAP material, they will relinquish custody of the material to the CPSO or designated representative. Arrangements will be made to ensure appropriate overnight storage and protection for material returned after close of business.***

6-104. **Collateral Clearances and Special Access Program Visit Requests.** Collateral clearances and SAP accesses may be required in conjunction with the SAP visit. If access to collateral classified information is required outside the SAPF, then the CPSO can certify clearances and accesses as required within the facility. Certification will be based on the SAP visit request received by the CPSO. The CPSO will maintain the record copy of the visit certification. SCI visit certification will be forwarded through appropriate SCI channels.

6-105. Non-Program-Briefed Visitors. ***In instances where entry to a SAPF by non-Program-briefed personnel is required (e.g., maintenance, repair), they will complete and sign a visitor's record and will be escorted by a Program-briefed person at all times. Sanitization procedures will be implemented in advance to ensure that personnel terminate classified discussions and other actions and protect SAP information whenever a non-briefed visitor is in the area. If maintenance is required of a classified device, the uncleared maintenance person shall be escorted by a Program-briefed, technically knowledgeable individual Every effort should be made to have a technically knowledgeable Program-briefed person as an escort.***

6-106. Visitor Record. *The PSO may require the CPSO to establish a Program visitor's reeord. ***This record will be maintained inside the SAPF,*** and retention may be required.

Section 2. Meetings

(not further supplemented)

Chapter 7
Subcontracting

Section 1. Prime Contracting Responsibilities

7-100. General. This section addresses the responsibilities and authorities of prime contractors concerning the release of classified SAP information to subcontractors. Prior to any release of classified information to a prospective subcontractor, the prime contractor will determine the scope of the bid and procurement effort. Prime contractors will use extreme caution when conducting business with non-Program-briefed subcontractors to preclude the release of information that would divulge Program-related (classified or unclassified Program sensitive) information.

7-101. **Determining Clearance Status of Prospective Subcontractors.** ***AU prospective subcontractor personnel will have the appropriate security clearance and meet the investigative criteria as specified in this Supplement prior to being briefed into a SAP. The*** eligibility criteria will be determined in accordance with the NISPOM and this Supplement. For acknowledged Programs, in the event a prospective subcontractor does not have the appropriate security clearances, the prime contractor will request that the cognizant PSO initiate the appropriate security clearance action. A determination will be made in coordination with the PSO as to the levels of facility clearance a prospective subcontractor facility has for access to classified information and the storage capability level.

7-102. **Security Agreements and Briefings.** In the pre-contract phase, the prime contractor wil I fully advise the prospective subcontractor (prior to any release of SAP information) of the procurement's enhanced special security requirements. Arrangements for subcontractor Program access will be pre-coordinated with the PSO. When approved by the PSO, the prime contractor CPSO will provide Program indoctrinations and obtain NDAs from the subcontractors. A security requirements agreement will be prepared that specifically addresses those enhanced security requirements that apply to the subcontractor. The security requirements agreement may include the following elements, when applicable:

a. General Security Requirements.

b. Reporting Requirements.

c. Physical and/or Technical Security Requirements.

d. Release of Information.

e. Program Classified Control or Accountability.

f. Personnel Access Controls.

g. Security Classification Guidance.

h. Automated Information System.

i. Security Audits and Reviews.

j. Program Access Criteria.

k. Subcontracting.

1. Transmittal of Program Material.

m. Storage.

n. Testing and/or Manufacturing.

o. Program Travel.

p. Finances.

q. Sanitization of Classified Material.

r. Security Costs and Charging Policy.

s. Fraud, Waste, and Abuse Reporting.

t. Test Planning.

u. OPSEC.

v. TEMPEST.

7-103. Transmitting Security Requirements. *Contract Security Classification Specifications prepared by the prime contractor will be coordinated with the GPM/PSO and contracting officer prior to transmitting to the subcontractor. Contract Security Classification Specifications prepared by the prime contractor will be forwarded to the GPM/PSO and contracting officer for coordination and signature.*

Chapter 8
Automated Information Systems (AIS)

Section 1. Responsibilities

8-100. Introduction

a. **Purpose and Scope.** This chapter addresses the protection and control of information processed on AIS. ***This entire chapter is contractor required and is not an option. The type is not bold or italicized, because it would include the complete chapter.*** AISS typically consist of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information. This chapter specifies requirements and assurances for the implementation, operation, maintenance, and management of secure AIS used in support of SAP activities. Prior to using an AIS or AIS network for processing U.S. Government, Customer, or Program information, the Contractor/ Provider will develop an AIS Security Plan (AISSP) as described herein and receive written Customer authorization to process Customer information. Such authorization to process requires approval by the Customer. The Provider will also assign an Information System Security Representative (ISSR) to support the preparation of these documents and to subsequently manage AIS security on-site for the Customer's program. After the AISSP is approved by the Customer, the Provider will thereafter conform to the plan for all actions related to the Customer's program information. This information includes the selection, installation, test, operation, maintenance, and modification of AIS facilities, hardware, software, media, and output.

b. **Requirements.** The AISSP selected menu upgrades to the NISPOM baseline will be tailored to the Provider's individual AIS configuration and processing operations. Alternatives to the protective measures in this Supplement may be approved by the Customer after the Provider demonstrates that the alternatives are reasonable and necessary to accommodate the Customer's needs. Prior to implementation, the Provider will coordinate any envisioned changes or enhancements with the Customer. Approved changes will be included in the AISSP. Any verbal approvals will subsequently be documented in writing. The information and guidance needed to prepare and obtain approval for the AISSP is described herein.

c. Restrictions. No personally owned AISS will be used to process classified information.

8-101. Responsibilities.

The Customer is the Government organization responsible for sponsoring and approving the classified and/or unclassified processing. The Provider is the Contractor who is responsible for accomplishing the processing for the Customer. The Information System Security Representative (ISSR) is the Provider-assigned individual responsible for on-site AIS processing for the Customer in a secure manner.

a. **Provider Responsibilities.** The Provider will take those actions necessary to meet with the policies and requirements outlined in this document. The provider will:

(1) Publish and promulgate a corporate AIS Security Policy that addresses the classified processing environment.

(2) Designate an individual to act as the ISSR.

(3) Incorporate AISS processing Customer information as part of a configuration management program.

(4) Enforce the AIS Security Policy.

b. **ISSR Responsibilities.** The Provider-designated ISSR has the following responsibilities:

(1) AIS Security Policy. Implement the AIS Security Policy.

(2) AIS Security Program. Coordinate the establishment and maintenance of a formal AIS Security Program to ensure compliance with this document:

(a) AIS Security Plan (AISSP). Coordinate the preparation of an AISSP in accordance with the outline and instructions provided in this document. After Customer

approval, the AISSP becomes the controlling security document for AIS processing Customer information. Changes affecting the security of the AIS must be approved by the Customer prior to implementation and documented in the AISSP.

(b) AIS Technical Evaluation Test Plans. For systems operating in the compartmented or multi-level modes, prepare an AIS Technical Evaluation Test Plan in coordination with the Customer and applicable security documents.

(c) Certification. Conduct a certification test in accordance with 8-102, c. and provide a certification report.

(d) Continuity of Operations Plan (COOP). When contractually required, coordinate the development and maintenance of an AIS COOP to ensure the continuation of information processing capability in the event of an AIS-related disaster resulting from fire, flood, malicious act, human error, or any other occurrence that might adversely impact or threaten to impact the capability of the AIS to process information. This plan will be referenced in the AISSP.

(e) Documentation. Ensure that all AIS security-related documentation as required by this chapter is current and is accessible to properly authorized individuals.

(f) Customer Coordination. Coordinate all reviews, tests, and AIS security actions.

(g) Auditing. Ensure that the required audit trails are being collected and reviewed as stated in 8-303.

(h) Memorandum of Agreement. As applicable, ensure that Memoranda of Agreement are in place for AISS supporting multiple Customers.

(i) Compliance Monitoring. Ensure that the system is operating in compliance with the AISSP.

(j) AIS Security Education and Awareness. Develop an on-going AIS Security Education and Awareness Program.

(k) Abnormal Occurrence. Advise Customer in a timely manner of any abnormal event that affects the security of an approved AIS.

(1) Virus and malicious code. Advise Customer in a timely manner of any virus and malicious code on an approved AIS.

(3) Configuration Management. Participate in the configuration management process.

(4) Designation of Alternates. The ISSR may designate alternates to assist in meeting the requirements outlined in the chapter.

c. Special Approval Authority. In addition to the above responsibilities, the Customer may authorize in writing an ISSR to approve specific AIS security actions including:

(1) Equipment Movement. Approve and document the movement of AIS equipment.

(2) Component Release. Approve the release of sanitized components and equipment in accordance with Tables 1 and 2 in 8-501.

(3) Stand-alone Workstation and Portable AIS Approval. Approve and document new workstations in accordance with an approved AIS security plan and the procedures defined in this document for workstations with identical functionality. Approve and document portable AIS.

(4) Dedicated and System High Network Workstation Approval. Approve and document additional workstations identical in functionality to existing workstations on an approved Local Area Network (LAN) provided the workstations are not located outside of the previously defined boundary of the LAN.

(5) Other AIS Component Approval. Approve and document other AIS components identical in functionality to existing components on an approved LAN provided the components are not located outside of the previously defined boundary of the LAN.

8-102. Approval To Process.

Prior to using any AIS to process Customer information, approval will be obtained from the Customer. The following requirements will be met prior to approval.

a. **AIS Security Program.** The Provider will have an AIS security program that includes:

(1) An AIS security policy and a formal AIS security structure to ensure compliance with the guidelines specified in this document;

(2) An individual whose reporting functionalities are within the Provider's security organization formally named to act as the ISSR;

(3) The incorporation of AISs processing Customer information into the Provider's configuration management program. The Provider's configuration management program shall manage changes to an AIS throughout its life cycle. As a minimum the program will manage changes in an AIS's:

(a) Hardware components (data retentive only)

(b) Connectivity (external and internal)

(c) Firmware

(d) Software

(e) Security features and assurances

(f) AISSP

(g) Test Plan

(4) Control. Each AIS will be assigned to a designated custodian (and alternate custodian) who is responsible for monitoring the AIS on a continuing basis. The custodian will ensure that the hardware, installation, and maintenance as applicable conform to appropriate requirements. The custodian will also monitor access to each AIS. Before giving users access to any such AIS, the custodian will have them sign a statement indicating their awareness of the restrictions for using the AIS. These statements will be maintained on file and available for review by the ISSR.

b. **AIS Security Plan (AISSP). The** Provider will prepare and submit an AISSP covering AISS processing information in a Customer's Special Access Program Facility (SAPF), following the format in Appendix C. For RD, the Customer may modify the AISSP format.

c. AIS Certification and Accreditation.

(1) Certification. Certification is the comprehensive evaluation of technical and non-technical security features to establish the extent to which an AIS has met the security requirements necessary for it to process the Customer information. Certification precedes the accreditation. The certification is based upon an inspection and test to verify that the AISSP accurately describes the AIS configuration and operation (See Appendix C and D). A Certification Report summarizing the following will be provided to the Customer:

(a) For the dedicated mode of operation, the provider must verify that access controls, configuration management, and other AISSP procedures are functional.

(b) In addition, for System High AIS the ISSR will verify that discretionary controls are implemented.

(c) For compartmented and multilevel AIS, certification also involves testing to verify that technical security features required for the mode of operation are functional. Compartmented and multi-level AIS must have a Technical Evaluation Test Plan that includes a detailed description of how the implementation of the operating system software, data management system software, firmware, and related security software packages will enable the AIS to meet the Compartmented or Multilevel Mode requirements. The plan outlines the inspection and test procedures to be used to demonstrate this compliance.

(2) Accreditation. Accreditation is the formal declaration by the Customer that a classified AIS or network is approved to operate in a particular security mode; with a prescribed set of technical and non-technical security features; against a defined threat; in a given operational environment; u rider a stated operational concept; with stated interconnections to other AIS; and at an acceptable level of risk. The accreditation decision is subject to the certification process. Any changes to the accreditation criteria described above may require a new accreditation.

d. **Interim Approval.** The Customer may grant an interim approval to operate.

e. Withdrawal of Accreditation. The Customer may withdraw accreditation if:

(1) The security measures and controls established and approved for the AIS do not remain effective.

(2) The AIS is no longer required to process Customer information.

f. **Memorandum of Agreement.** A Memorandum of Agreement (MOA) is required whenever an accredited AIS is co-utilized, interfaced, or networked between two or more Customers. This document will be included, as required, by the Customer.

g. Procedures for Delegated Approvals. For AISS operating in the dedicated or system high modes, the Customer may delegate special approval authority to the ISSR for additional AISS that are identical in design and operation. That is: two or more AIS are identical in design and operate in the same security environment (same mode of operation, process information with the same sensitivities, and require the same accesses and clearances, etc). Under these conditions the AISSP in addition to containing the information required by Appendix C shall also include the certification requirements (inspection and tests) and procedures that will be used to accredit all AISs. The CSA will validate that the certification requirements are functional by accrediting the first AIS using these certification requirements and procedures. The ISSR may allow identical AIS to operate under that accreditation if the certification procedures are followed and the AIS meets all the certification requirements outline in the AISSP. The AISSP will be updated with the identification of the newly accredited AIS and a copy of each certification report will be kept on file.

8-103. Security Reviews.

a. **Purpose.** Customer AIS Security Reviews are conducted to verify that the Provider's AIS is operated in accordance with the approved AISSP.

b. **Scheduling.** Customer AIS Reviews are normally scheduled at least once every 24 months for Provider systems processing Customer program information. The Customer will establish specific review schedules.

c. Review Responsibilities. During the scheduled Customer AIS Security Review, the Provider will furnish the Customer representative conducting the Review with all requested AIS or network documentation. Appropriate Provider security, operations, and management representatives will be made available to answer questions that arise during the Customer AIS Review process.

d. **Review Reporting.** At the conclusion of the Customer AIS Review visit, the Customer will brief the Provider's appropriate security, operations, and management representatives on the results of the Review and of any discrepancies discovered and the recommend measures for correcting the security deficiencies. A formal report of the Customer AIS Review is provided to the Provider's security organization no later than 30 days after the Review.

e. Corrective Measures. The Provider will respond to the Customer in writing within 30 days of receipt of the formal report of deficiencies found in the Customer AIS Review process. The response will describe the actions taken to correct the deficiencies outlined in the formal report of Customer AIS Review findings. If proposed actions will require an expenditure in funds, approval will be obtained from the Contracting Officer prior to implementation.

Section 2. Security Modes

8-200. Security Modes-General.

a. AISs 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, storage, or transmission of such information, and prevent unauthorized manipulation of the AIS that could result in the compromise or loss of classified information.

b. In determining the mode of operation of an AIS, three elements must be addressed: the boundary and perimeter of the AIS, the nature of the data to be processed, and the level and diversity of access privileges of intended users. Specifically:

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

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

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

8-201. **Dedicated** Security **Mode.**

a. An AIS is operating in the dedicated mode (processing either full time or for a specified period) 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 valid personnel clearance for all information stored or processed on the AIS.

(2) Formal access approvals and **has** executed all appropriate non-disclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or SAPS).

(3) A valid need to know for all information stored on or processed within the AIS.

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

(1) Be **located** in a **SAPF.**

(2) Implement and **enforce** access procedures to the **AIs.**

(3) **All** hard copy output will be handled at the level for which the system is accredited until reviewed by a knowledgeable individual.

(4) **All** media removed from the system will **be** protected at the highest classification level of information stored or processed on the system until reviewed and properly marked according to procedures in the AIS **security** plan.

c. **Security Features for Dedicated Security Mode.**

(1) Since the system is not required to provide technical security features, it is up to the user to **protect** the information on the system. For networks operating in the dedicated mode, automated identification and authentication controls are required.

(2) For DoD, the Customer may require audit records of user access to the system. Such records will include: user ID, start date and time, and stop date and time. Logs will be maintained IAW 8-303.

d. **Security Assurances for Dedicated Security Mode.**

(1) AIS *security* assurances must *include* an approach for specifying, documenting, **controlling,** and maintaining the integrity of all appropriate AIS hardware, firmware, software, communicant ions interfaces, operating *procedures,* installation structures, security documentation, and changes thereto.

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

(a) Classified AIS Hardware. An examination shall result in assurance that the equipment appears to be in good working order and have no parts that might be detrimental to the secure operation of the resource. Subsequent changes and developments which affect security may require additional examination.

(b) Classified AIS Software.

1. Commercially procured software shall be examined to assure that the software contains no features which might be detrimental to the security of the classified AIS.

2. Security-related software shall be examined to assure that the security features function as specified.

(c) 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.

8-202. **System High Security Mode.**

a. An AIS is operating in the system high mode (processing either full time or for a specified period) 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 valid personnel clearance for ail information on the AIS.

(2) Formal access approval and has signed non-disclosure agreements for all the information stored and/or processed (including all compartments and subcompartments).

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

b. AISS operating in the system high mode, in addition to meeting all of the security requirements, features, and assurances established for the dedicated mode, will meet the following:

(1) Security Features for System High Mode

(a) Define and control access between system users and named objects (e.g., files and programs) ‘in the AIS. 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) Time Lockout. Where technically feasible, the AIS shall time lockout an interactive session after an interval of user inactivity. The time interval and restart requirements shall be specified in the AIS Security Plan.

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

1. Introduction of objects into a user’s address space (e.g., file open and program initiation as determined by the Customer and ISSR).

2. Deletion of objects (e.g., as determined by the Customer and ISSR).

3. System log-on and log-off

4. Unsuccessful access attempts.

(d) Require that memory and storage contain no residual data from the previously contained object before being assigned, allocated, or reallocated to another subject.

(e) Identification Controls. Each person having access to a classified AIS shall have the proper security clearances and authorizations and be uniquely identified and authenticated before access to the classified AIS is permitted. The identification and authentication methods used shall be specified and approved in the AIS Security Plan. User access controls in classified AISS shall include authorization, user

in the AIS Security Plan. User access controls in classified 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 a classified 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 Removal. The ISSR shall ensure the development and implementation of procedures for the prompt removal of access from the classified AIS when the need for access no longer exists.

   b. User ID Revalidation. The AIS ISSR shall ensure that all user IDs 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.

(f) Authentication. Each user of a classified AIS shall be authenticated before access is permitted. This authentication can be based on any one of three types of information: something the person knows (e.g., a password); something the person possesses (e.g., a card or key); something about the person (e.g., fingerprints or voiceprints); or some combination of these three. Authenticators that are passwords shall be changed at least every six months.

1. Requirements.

   a. Log-on. Users shall be required to authenticate their identities at "log-on" time by supplying their authenticator (e.g., password, smart card, or fingerprints) in conjunction with their user ID.

   b. 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 Classified AIS.

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

   a. Log-on Attempt Rate. Successive log-on 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 Customer.

   b. Notification to the User. The user shall be notified upon successful log-on of: the date and time of the user's last log-on; the ID of the terminal used at last log-on; and the number of unsuccessful log-on attempts using this user ID since the last successful log-on. This notice shall require positive action by the user to remove the notice from the screen.

(g) The audit, identification, and authentication mechanisms must be protected from unauthorized access, modification, or deletion.

   c. Security Assurances for System High Mode. The system security features for need-to-know controls will be tested and verified. Identified flaws will be corrected.

8-203. **Compartmented Security Mode.**

a. 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:

(1) A valid personnel clearance for access to the most restricted information processed in the AIs.

(2) Formal access approval and have signed nondisclosure agreements for that information to which he/she is to have access (some users do not have formal access approval for all compartments or subcompartments processed by the AIS.)

(3) A valid need-to-know for that information for which he/she is to have access.

b. **Security Features for Compartmented Mode. In** addition to all Security Features and Security Assurances required for the System High Mode of Operation, Classified AIS operating in the Compartmented Mode of Operation shall also include:

(1) Resource Access Controls,

(a) Security Labels. The Classified 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 Classified AIS shall be accurate representations of the corresponding security labels on the information in the originating Classified AIS.

(2) Mandatory Access Controls. Mandatory access controls shall be provided. These 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.

(3) No information shall be accessed whose compartment is inconsistent with the session log-on.

(4) Support a trusted communications path between itself and each user for initial log-on and verification.

(5) 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.

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

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

c. Security Assurances for Compartmented Mode.

(I) Confidence in Software Source. In acquiring resources to be used as part of a Classified 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.

(2) Flaw Discovery. The Provider shall ensure the vendor has implemented a method for the discovery of flaws in the system (hardware, firmware, or software) that may have an effect on the security of the AIS.

(3) No Read Up, No Write Down. 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 or lower than the user's authorized processing security classification and all non-hierarchical categories are the same.

(4) Description of the Security Support Structure (often referred to as the Trusted Computing Base). The protections and provisions of the security support structure shall be documented in such a manner to show the underlying planning for the security of a Classified AIS. 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.

(5) Independent Validation and Verification. An Independent Validation and Verification team shall assist in the technical evaluation testing of a classified AIS and shall perform validation and verification testing of the system as required by the Customer.

(6) Security Label Integrity. The methodology shall ensure the following:

(a) Integrity of the security labels;

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

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

(7) Detailed Design of security enforcement mechanisms. An informal description of the security policy model enforced by the system shall be available.

8-204. **Multilevel Security** Mode. NOTE: Multilevel Security Mode is not routinely -authorized for SCI or SAP applications. Exceptions for SCI may be made by the heads of CIA, DIA, or NSA on a case-by-case basis. Exceptions for SAP may be made by the Customer.

a. 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:

(1) Some users do not have a valid personnel clearance for all of the information processed in the AIS. (Users must possess a valid CONFIDENTIAL, SECRET, or TOP SECRET clearance.)

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

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

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

(1) Audit. Contain 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.

(2) Trusted Path. Support a trusted communication path between the AIS and users for use when a positive AIS-to-user connection is required (i.e., log-on, 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. For Restricted Data, this requirement is only applicable to multilevel AIS that have at least one uncleared user on the AIS.

(3) 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 on 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.

(4) Security Isolation. The AIS security enforcement mechanisms 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 mechanisms shall provide isolation and noncircumvention of isolation functions. For Restricted Data, this requirement is only applicable to multilevel AIS that have at least one uncleared user on the AIS.

(5) Protection of Authenticator. Authenticators shall be protected at the same level as the information they access.

c. Security Assurances for Multilevel Mode.

(1) Flaw Tracking and Remediation. The Provider shall ensure the vendor provides evidence that all discovered flaws have been tracked and remedied.

(2) Life-Cycle Assurance. The development of the Classified AIS hardware, firmware, and software shall be under life-cycle control and management (i.e., control of the Classified AIS from the earliest design stage through decommissioning).

(3) Separation of Functions. The functions of the AIS ISSR and the Classified AIS manager shall not be performed by the same person.

(4) 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.

(5) Security Penetration Testing. In addition to testing the performance of the classified AIS for certification and for ongoing testing, there shall be testing to attempt to penetrate the security countermeasures of the system. The test procedures shall be documented in the test plan for certification and for ongoing testing.

(6) Trusted Recovery. Provide procedures and/or mechanisms to assure that, after an AIS system failure or other discontinuity, recovery without a protection compromise is obtained.

(7) Covert Channels. A covert channel analysis shall be performed.

Section 3. System Access and Operation

8-300 System Access. Access to the system will be limited to authorized personnel. Assignment of AIS access and privileges will be coordinated with the ISSR. Authentication techniques must be used to provide control for information on the system. Examples of authentication techniques include, but are not limited to: passwords, tokens, biometrics, and smart cards. User authentication techniques and procedures will be described in the AISSP.

a. **User IDs.** User IDs identify users in the system and are used in conjunction with other authentication techniques to gain access to the system. User IDs will be disabled whenever a user no longer has a need-t-know. 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. Whenever possible, 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 ID is reactivated.

b. **Access Authentication.**

(1) Password. When used, system log-on passwords will be randomly selected and will be at least six characters in length. The system log-on password generation routine must be approved by the Customer.

(2) Validation. Authenticators must be validated by the system each time the user accesses the AIS.

(3) Display. System log-on passwords must not be displayed on any terminal or contained in the audit trail. When the AIS cannot prevent a password from being displayed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password.

(4) Sharing. Individual user authenticators (e.g., passwords) will not be shared by any user.

(5) Password Life. Passwords must be changed at least every six months.

(6) Compromise. Immediately following a suspetted or known compromise of a password or Personal Identification Number (PIN) the ISSR will be notified and a new password or PIN issued.

(7) Group Log-on Passwords. Use of group log-on passwords must be justified and approved by the Customer. After log-on, group passwords may be used for file access.

c. **Protection of Authenticators.** Master data files containing the user population system log-on authenticators will be encrypted when practical. Access to the files will be limited to the ISSR and designated alternate(s), who will be identified in writing.

d. **Modems.** Modems require Customer approval prior to connection to an AIS located in a Customer SAPF.

e. **User Warning Notice.** The Customer may require log-on warning banners be installed.

8-301. System Operation.

a. Processing initialization is the act of changing the AIS from unclassified to classified, from one classified processing level to another, or from one compartment to another or from one Customer to another. To begin processing classified information on an approved AIS the following procedures must be implemented:

(1) Verify that prior mode termination was properly performed.

(2) Adjust the area security controls to the level of information to be processed.

(3) Configure the AIS as described in the approved AISSP. The use of logical disconnects requires Customer approval.

(4) 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 labeled and controlled commensurate with the security classification and access levels of the information to be processed during the period.

b. **Unattended Processing.** Unattended processing will have open storage approval and concurrence from the customer. Prior to unattended processing,

all remote input and/or output (1/0) not in approved open storage areas will be physically or electrically disconnected from the host CPU. The disconnect will be made in an area approved for the open storage. Exceptions are on a case-by-case basis and will require Customer approval.

c. **Processing Termination.** Processing termination of any AIS will be accomplished according to the following requirements.

(1) Peripheral Device Clearing. Power down all connected peripheral devices to sanitize all volatile buffer memories. Overwriting of these buffer areas will be considered by the Customer on a case-by-case basis.

(2) Removable Storage Media. Remove and properly store removable storage media.

(3) Non-removable (Fixed) Storage Media. Disconnect (physically or electrical] y) all storage devices with nonremovable storage media not designated for use during the next processing period.

(4) CPU Memory. Clear or sanitize as appropriate all internal memory including buffer storage and other reusable storage devices (which are not disabled, disconnected, or removed) in accordance with 8-501, Table 2.

(5) Laser Printers. Unless laser printers operating in SAPFS will operate at the same classification level with the same access approval levels during the subsequent processing period, they will be cleared by running three pages of unclassified randomly generated text. For SCI, five pages of unclassified pages will be run to clear the printer. These pages will not include any blank spaces or solid black areas. Otherwise, no pages need be run through the printer at mode termination.

(6) Thermal printers. Thermal printers have a thermal film on a spool and take-up reel. Areas in which these types of laser printers are located will be either approved for open storage, or the spools and take-up reels will be removed and placed in secure storage. The printer must be sanitized prior to use at a different classification level.

(7) Impact-type Printers. Impact-type printers (e.g., dot-matrix) in areas not approved for open storage will be secured as follows: Remove and secure all printer ribbons or dispose of them as classified trash. Inspect all printer platens. If any indication' of printing is detected on the platen, then the platen will be either cleaned to remove such printing or removed and secured in an approved classified container.

(8) Adjust area security controls.

8-302. **Collocation of Classified and Unclassified AIS.**

a. Customer permission is required before a Provider may collocate unclassified AIS and classified AIS. This applies when:

(1) The unclassified information is to be processed on an AIS located in a SAPF, or

(2) The unclassified information is resident in a database located outside of a SAPF but accessed from terminals located within the SAPF.

b. AIS approved for processing unclassified information will be clearly marked for UNCLASSIFIED USE ONLY when located within a SAPF. In addition the following requirements apply:

(I) Must be physically separated from any classified AIS.

(2) Cannot be connected to the classified AIS.

(3) Users shall be provided a special awareness briefing.

(4) ISSR must document the procedures to ensure the protection of classified information.

(5) All unmarked media is assumed to be classified until reviewed and verified.

c. Unclassified portable AIS devices are prohibited in a SAPF unless Customer policy specifically permits their use. If permitted, the following procedures must be understood and followed by the owner and user:

(1) Connection of unclassified portable AIS to classified AIS is prohibited.

(2) Connection to other unclassified AISs may be allowed provided Customer approval is obtained.

(3) Use of an internal or external modem with the AIS device is prohibited within the SAPF.

(4) The Provider will incorporate these procedures in the owner's initial and annual security briefing.

(5) Procedures for monitoring portable AIS devices within the SAPF shall be outlined in either the AISSP or the Facility Security Plan. These devices and the data contained therein are subject to security inspection by the ISSR and the Customer. Procedures will include provisions for random reviews of such devices to ensure that no classified program-specific or program-sensitive data is allowed to leave the secure area. Use of such a device to store or process classified information may, at the discretion of the Customer, result in confiscation of the device. All persons using such devices within the secure area will be advised of this policy during security awareness briefings.

(6) Additionally, where Customer policy permits, personally owned portable AIS devices may be used for unclassified processing only and must follow the previous guidelines.

8-303. System **Auditing.**

a. **Audit Trails.** Audit trails provide a chronological record of AIS usage and system support activities related to classified or sensitive processing. In addition to the audit trails normally required for the operation of a stand-alone AIS, audit trails of network activities will also be maintained. Audit trails will provide records of significant events occurring in the AIS in sufficient detail to facilitate reconstruction, review, and examination of events involving possible compromise. Audit trails will be protected from unauthorized access, modification, and deletion. Audit trail requirements are described under mode of operation.

b. **Additional Records and Logs. The** following additional records or logs will be maintained by the Provider regardless of the mode of operation. These will include:

(1) Maintenance and repair of AIS hardware, including installation or removal of equipment, devices, or components.

(2) Transaction receipts, such as equipment sanitization, release records, etc.

(3) Significant AIS changes (e.g., disconnecting or connecting remote terminals or devices, AIS upgrading or downgrading actions, and applying seals to or removing them from equipment or device covers).

c. Audit Reviews. The audit trails, records, and logs created during the above activities will be reviewed and annotated by the ISSR (or designee) to be sure that all pertinent activity is proper] y recorded and appropriate action has been taken to correct anomalies. The Customer will be notified of all anomalies that have a direct impact on the security posture of the system. The review will be conducted at least week] y.

d. **Record Retention.** The Provider will retain the most current 6 to 12 months (Customer Option) of records derived from audits at all times. The Customer may approve the periodic use of data reduction techniques to record security exception conditions as a means of reducing the volume of audit data retained. Such reduction will not result in the loss of any significant audit trail data.

Section 4. Networks

8-400 Networks. This section addresses network-specific requirements that are in addition to the previously stated AIS requirements. Network operations must preserve the security requirements associated with the AIS's mode of operation.

a. Types of Networks.

(1) 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 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. 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.

(2) 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 net works. An interconnected network requires accreditation, which may be as simple as an addendum to a Memorandum of Agreement (MOA) between the accrediting authorities.

b. **Methods of Interconnection.**

(1) 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:

(a) Document the security policy enforced by the SSS.

(b) Identify a single mode of operation.

(c) Document the network security architecture and design.

(d) Document minimum contents of MOA's required for connection to the SSS.

(2) The interconnection of previously accredited systems into an accredited network may require a reexamination of the security features and assurances of the contributing systems to ensure their accreditations remain valid.

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

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

c. **Network Security Management. The** Provider will designate an ISSR for each Provider network. The ISSR may designate a Network Security Manager (NSM) to oversee the security of the Provider's network(s), or may assume that responsibility. The ISSR is responsible for coordinating the establishment and maintenance of a formal network security program based on an understanding of the overall security-relevant policies, objectives, and requirements of the Customer. The NSM is responsible for ensuring day-to-day compliance with the network security requirements as described in the AISSP (as covered below) and this Supplement.

d. **Network Security Coordination.** When different accrediting authorities are involved, a Memorandum of Agreement is required to define the cognizant authority and the security arrangements that will govern the operation of the overall network. When

two or more ISSRS are designated for a network, a lead ISSR will be named by the Provider(s) to ensure a comprehensive approach to enforce the Customer's overall security policy.

e. Network Security.

The AISSP must address:

(1) A description of the network services and mechanisms that implement the network security policy.

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

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

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

(c) Description of the network and any external connections.

(d) The network security policy including mode of operation, information sensitivities, and user clearances.

(e) Must address the internode transfer of information (e.g., sensitivity level, compartmentation, and any special access requirements), and how the information is protected.

(f) Communications protocols and their security features.

(g) Audit Trails and Monitoring.

1. If required by the mode of operation, the network shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of successful and unsuccessful accesses to the AIS network components within the perimeter of the accredited network. The audit data shall be protected so that access is limited to the ISSR or his/her designee.

2. For Restricted Data, methods of continuous on-line monitoring of network activities may be included in each network operating in the **Compartmented Securit** y Mode or higher. This monitoring may also include realtime notification to the ISSR of any system anomalies.

3. For Restricted Data networks operating in the Compartmented Mode or higher, the Customer may require the audit trail to include the changing of the configuration of the network (e.g., a component leaving the network or rejoining).

4. The audit trail records will allow association of the network activities with corresponding user audit trails and records.

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

6. For Restricted Data, the Customer may require alarm features that automatically terminate the data **flow** in case of a malfunction and then promptly notify the ISSR of the anomalous conditions.

(h) Secure Message Traffic. The communications methodology for the network shall ensure the detection of errors in traffic across the network links.

f. **Transmission Security.** Protected Distribution Systems or National Security Agency approved encryption methodologies shall be used to protect classified information on communication lines that leave the SAPF. Protected distribution systems shall be either constructed in accordance with the national standards or utilize National Security Agency approved protected distribution systems.

g. Records. The Customer may require records be maintained of electronic transfers of data between automated information systems when those systems are not components of the same unified network. Such records may include the identity of the sender, identity and location of the receiver, date/time of the transfer, and description of the data sent. Records are retained according to 8-303.d.

Section 5. Software and Data Files

8-500. Software and Data Files.

a. **Acquisition and Evaluation.** ISSR approval will be obtained before software or data files may be brought into the SAPF. All software must be acquired from reputable and/or authorized sources as determined by the ISSR. The Provider will check all newly-acquired software or data files, using the most current version and/or available of virus checking software and procedures identified in the AISSP to improve assurance that the software or data files are free from malicious code.

b. Protection. Media that may be written to (e.g., magnetic media) must be safeguarded commensurate with the level of accreditation of the dedicated or system high AIS. Media on compartmented or multilevel AISS will be protected commensurate with the level of the operating session. If a physical write-protect mechanism is utilized, media may be introduced to the AIS and subsequently removed without changing the original classification. The integrity of the write-protection mechanism must be verified at a minimum of once per day by attempting to write to the media. Media which cannot be changed (e.g., CD read-only media) may be loaded onto the classified system without labeling or classifying it provided it is immediately removed from the secure area. If this media is to be retained in the secure area, it must be labeled, controlled, and stored as unclassified media as required by the Customer.

(1) System Software. Provider personnel who are responsible for implementing modifications to system or security-related software or data files on classified AISS inside the SAPF will be appropriately cleared. Soft ware that contains security related functions (e.g., sanitization, access control, auditing) will be validated to confirm that security-related features are fully functional, protected from modification, and effective.

(2) Application Software. Application software or data files (e.g., general business software), that will be used by a Provider during classified processing, may be developed/modified by personnel outside the security area without the requisite security clearance with the concurrence of the Customer.

(3) Releasing Software. Software that has not been used on an AIS processing classified information may be returned to a vendor. If media containing software (e.g., applications) are used on a classified system and found to be defective, such media may not he removed from a SAPF for return to a vendor. When possible, software will be tested prior to its introduction into the secure facility.

c. Targetability. For SCI and SAP the software, whether obtained from sources outside the facility or developed by Provider personnel, must be safeguarded to protect its integrity from the time of acquisition or development through its life cycle at the Provider's facility (i.e., design, development, operational, and maintenance phases). Uncleared personnel will not have any knowledge that the software or data files will be used in a classified area, although this may not be possible in all cases. Before software or data files that are developed or modified by uncleared personnel can be used in a classified processing period, it must be reviewed by appropriately cleared and knowledgeable personnel to ensure that no security vulnerabilities or malicious code exists. Configuration management must be in place to ensure that the integrity of the software or data files is maintained.

d. **Maintenance Software.** Software used for maintenance or diagnostics will be maintained within the secure computing facility and, even though unclassified, will be separately controlled. The AISSP will detail the procedures to be used.

e. **Remote Diagnostics.** Customer approval will be obtained prior to using vendor-supplied remote diagnostic links for on-line use of diagnostic software. The AISSP will detail the procedures to be used.

8-501. **Data Storage Media.** Data storage media will be control led and labeled at the appropriate classification level and access controls of the AIS unless write-protected in accordance with 8-500.b. Open storage approval will be required for non-removable media.

a. **Labeling Media.** All data storage media will be labeled in human-readable form to indicate its classification level, access controls (if applicable), and other identifying information. Data storage media that is to be used solely for unclassified processing

and collocated with classified media will be marked as UNCLASSIFIED. Color coding (i e., media, labels) is recommended. If required by the Customer, all removable media will be labeled with a classification label immediately after removing it from its factory-sealed container.

b. **Reclassification.** When the classification of the media increases to a higher level, replace the classification label with a higher classification-level label. The label will reflect the highest classification level, and access controls (if applicable) of any information ever stored or processed on the AIS unless the media is write-protected by a Customer-approved mechanism. Media may never be downgraded in classification without the Customer's written approval.

c. **Copying Unclassified Information from a Classified AIS.**

(1) **The** unclassified data will be written to factory-fresh or verified unclassified media using approved copying routines and/or utilities and/or procedures as stated in the AISSP. For SCI and SAP, media to be released will be verified by reviewing all data on the media including embedded text (e.g., headers and footers). Data on media that is not in human readable form (e.g., imbedded graphs, sound, video) will be examined for content with the appropriate software applications. Data that cannot be reasonably observed in its entirety will be inspected by reviewing random samples of the data on the media.

(2) Moving Classified Data Storage Media Between Approved Areas. The ISSR w il I establish procedures to ensure that data will be written to factory-fresh or sanitized media. The media will be reviewed to ensure that only the data intended was actually written and that it is appropriately classified and labeled. Alternatives for special circumstances may be approved by the Customer. All procedures will be documented in the AISSP.

d. **Overwriting, Degaussing, Sanitizing, and Destroying Media.** Cleared and sanitized media may be reused within the same classification level (i.e., TS-TS) or to a higher level (i.e., SECRET-TS). Sanitized media may be downgraded or declassified with the Customer's approval. Only approved equipment and software may be used to overwrite and degauss magnetic media containing classified information. Each action or procedure taken to overwrite or degauss such media will be verified. Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing will be reported to the ISSR, who will coordinate repair or destruction with the Customer. (See Table 1.)

Caution: Overwriting, degaussing, and sanitizing are not synonymous with declassification. Declassification is a separate administrative function. Procedures for declassifying media require Customer approval.

(1) Overwriting Media. Overwriting is a software procedure that replaces the data previously stored on magnetic storage media with a predefine set of meaningless data. Overwriting is an acceptable method for clearing. Only approved overwriting software that is compatible with the specific hardware intended for overwriting will be used. Use of such software will be coordinated in advance with the Customer. The success of the overwrite procedure will be verified through random sampling of the overwritten media. The effectiveness of the overwrite procedure may be reduced by several factors: ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps. To clear magnetic disks, overwrite all locations three (3) times (first time with a character, second time with its complement, and the third time with a random character). Items which have been cleared must remain at the previous level of classification and remain in a secure, controlled environment.

(2) Degaussing Media. Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more reliable than overwriting magnetic media. Magnetic media are divided into three types. Type I degaussers are used to degauss Type I magnetic media (i.e., media whose coercivity is no greater than 350 Oersteds (Oe)). Type H degaussers are used to degauss Type 11 magnetic media (i.e., media whose coercivity is no greater than 750 Oe). Currently there are no degaussers that can effectively degauss all

Type HI magnetic media (i.e., media whose coercivity is over 750 Oe). Some degaussers are rated above 750 Oersteds and their specific approved rating will be determined prior to use. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically-saturated material's magnetization to zero. The correct use of degaussing products improves assurance that classified data is no longer retrievable and that inadvertent disclosure will not occur. Refer to the current issue of NSAS ***Information*** Systems ***Security Products and Services Catalogue*** (Degausser Products List Section) for the identification of degaussers acceptable for the procedures specified herein. These products will be periodically tested to ensure continued compliance with the specification NSA CSS ***Media Declassification and Destruction Manual NSA 130-2.***

(3) Sanitizing Media. Sanitization removes information from media such that data recovery using any known technique or analysis is prevented. Sanitizing is a two-step process that includes removing data from the media in accordance with Table 1 and removing all classified labels, markings, and activity logs.

(4) Destroying Media. Data storage media will be destroyed in accordance with Customer-approved methods.

(5) Releasing Media. Releasing sensitive or classified Customer data storage media is a three-step process. First, the Provider will sanitize the media and verify the sanitization in accordance with procedures in this chapter. Second, the media will be administratively downgraded or declassified either by the CSA or the ISSR, if such authority has been granted to the ISSR. Third, the sanitization process, downgrading or declassification, and the approval to release the media will be documented.

Table 1
Clearing and Sanitization Data Storage

Type Media	Clear	Sanitize
(a) Magnetic Tape		
Type I	s o r b	a, b, or destroy
Type II	a o r b	b or destroy
Type III	a o r b	Destroy
(b) Magnetic Disk Packs		
Type I		a, b, or c
Type II		b o r e
Type III		Destroy
(c) Magnetic Disk Packs		
Floppies	a, b, or c	Destroy
Bernoulli's	a, b, or c	Destroy
Removable Hard Disks	a, b, or c	a, b, c, or destroy
Non-Removable Hard Disks	c	a, b, c, or destroy
(d) Optical Disk		
Read Only		Destroy
Write Once, Read Many (Worm)		Destroy
Read Many, Write Many	c	Destroy

These procedures will be performed by or as directed by the ISSR.

a. Degauss with a Type I degausser

b. Degauss with a Type II degausser

c. Overwrite all locations with a character, its complement, then with a random character. Verify that all sectors have been overwritten and that no new bad sectors have occurred. If new bad sectors have occurred during classified processing, this disk must be sanitized by method a or b described above. Use of the overwrite for sanitization must be approved by the Customer.

Note: For hand-held devices (e.g., calculators or personal directories), sanitization is dependent upon the type and model of the device. If there is any question about the correct sanitization procedure, contact the manufacturer or the Customer. In general, sanitization is accomplished as follows: Depress the "CLEAR ENTRY" and the "CLEAR MEMORY" buttons, remove the battery for several hours, and remove all associated magnetic media and retain it in the SAPF or destroy. In some models there are special-purpose memories and key-numbered memories, as well as "register stacks." Caution will be taken to clear all such memories and registers. This may take several key-strokes and may require the use of the operator's manual. Test the hand held device to ensure that all data has been removed. If there is any question, the device will remain in the SAPF or be destroyed.

Table 2
Sanitizing AIS Components

TYPE	PROCEDURE
Magnetic Bubble Memory	a, b, or c
Magnetic Core Memory	a, b, or d
Magnetic Plated Wire	d o r e
Magnetic-Resistive Memory	Destroy
Solid State Memory Components	
Random Access Memory (RAM) (Volatile)	f, then j
Nonvolatile RAM (NOVRAM)	l
Read Only Memory (ROM)	Destroy (see k)
Programmable ROM (PROM)	Destroy (see k)
Erasable Programmable ROM (EPROM)	g, then d and j
Electronically Alterable PROM (EAPROM)	h, then d and j
Electronically Erasable PROM (EEPROM)	i, then d and j
Flash EPROM (FEPROM)	i, then d and j

These procedures will be performed by or as directed by the ISSR.

a. Degauss with a Type I degausser.

b. Degauss with a Type II degausser.

c. Overwrite all locations with any character.

d. Overwrite all locations with a character, its complement, then with a random character.

e. Each overwrite will reside in memory for a period longer than the classified data resided.

f. Remove all power, including batteries and capacitor power supplies, from RAM circuit board.

g. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.

h. Pulse all gates.

i. Perform a full chip erase. (See Manufacturer's data sheet.)

j. Check with Customer to see if additional procedures are required.

k. Destruction required only if ROM contained a classified algorithm or classified data.

l. Some NOVRAM are backed up by a battery or capacitor power source; removal of this source is sufficient for release following item f procedures. Other NOVRAM are backed up by EEPROM which requires application of the procedures for EEPROM (i.e., i, then d and j).

Section 6. AIS Acquisition, Maintenance, and Release

S-600. AIS Acquisition, Maintenance, and Release.

a. **Acquisition.** AISS and AIS components that will process classified information will be protected during the procurement process from direct association with the Customer's program, When required by the Customer, protective packaging methods and procedures will be used while such equipment is in transit to protect against disclosure of classified relationships that may exist between the Customer and the Provider.

b. **Maintenance Policy. The** Provider will discuss maintenance requirements with the vendor before signing a maintenance contract. The Customer may require that AISS and AIS components used for processing Customer information will be protected during maintenance from direct association with the Customer's program.

(1) Cleared maintenance personnel are those who have a valid security clearance and access approvals commensurate with the information being processed. Complete sanitization of the AIS is not required during maintenance by cleared personnel, but need-to-know will be enforced. However, an appropriately cleared Provider individual will be present within the SAPF while a vendor performs maintenance to ensure that proper security procedures are being followed. Maintenance personnel without the proper access authorization and security clearance will *always be* accompanied by an individual with proper security clearance and access authorization and never left alone in a SAPF. The escort shall be approved by the ISSR and be technically knowledgeable of the AIS to be repaired.

(2) Prior to maintenance by a person requiring escort, either the device under maintenance shall be physically disconnected from the classified AIS (and sanitized before and after maintenance) or the entire AIS shall be sanitized before and after maintenance. When a system failure prevents clearing of the system prior to maintenance by escorted maintenance personnel, Customer-approved procedures will be enforced to deny the escorted maintenance personnel visual and electronic access to any classified data that may be contained on the system.

(3) All maintenance and diagnostics should be performed in the Provider's secure facility. Any AIS component or equipment released from secure control for any reason may not be returned to the SAPF without the approval of the ISSR. The Customer may require that a permanent set of procedures be in place for the release and return of components. These procedures will be incorporated into the AISSP.

c. Maintenance Materials and Methods.

(1) Unclassified Copy of Operating System. A separate, unclassified, ***dedicated for maintenance*** copy of the operating system (i.e., a specific copy other than the copy(s) used in processing Customer information), including any microcode floppy disks or cassettes that are integral to the operating system, will be used whenever maintenance is done by uncleared personnel. This copy will be labeled "UNCLASSIFIED-FOR MAINTENANCE USE ONLY." Procedures for an AIS using a nonremovable storage device on which the operating system is resident will be considered by the Customer on a case-by-case basis.

(2) Vendor-supplied Software and/or Firmware. Vendor-supplied software and/or firmware used for maintenance or diagnostics will be maintained within the secure computing facility and stored and controlled as though classified. If permitted by the Customer, the ISSR may allow, on a case-by-case basis, the release of certain types of costly magnetic media for maintenance such as disk head-alignment packs.

(3) Maintenance Equipment and Components. All tools, diagnostic equipment, and other devices carried by the vendor to the Provider's facility will be controlled as follows:

(a) Tool boxes and materials belonging to a vendor representative will be inspected by the assigned escort before the vendor representative is permitted to enter the secure area.

(b) The ISSR will inspect any maintenance hardware (such as a data scope) and make a best technical assessment that the hardware cannot access classified data. The equipment will not be allowed in the

secure area without the approval of the ISSR.

(c) Maintenance personnel may bring kits containing component boards into the secure facility for the purpose of swapping out component boards that may be faulty. Any component board placed into an unsanitized AIS will remain in the security facility until proper release procedures are completed. Any component board that remains in the kit and is not placed in the AIS may be released from the secure facility.

(d) Any communication devices with transmit capability belonging to the vendor representative or any data storage media not required for the maintenance visit will be retained outside the SAPF for return to the vendor representative upon departure from the secure area.

(4) Remote Diagnostic Links. Remote diagnostic links require Customer approval. Permission for the installation and use of remote diagnostic links will be requested in advance and in writing. The detailed procedures for controlling the use of such a link or links will have the written approval of the Customer prior to implementation.

d. **Release of Memory Components and Boards.** Prior to the release of any component from an area used to process or store Customer information, the following requirements will be met in respect to coordination, documentation, and written approval. This section applies only to components identified by the vendor or other technically knowledgeable individual as having the capability of retaining user addressable data and does not apply to other items (e.g., cabinets, covers, electrical components not associated with data), which may be released without reservation. For the purposes of this document, a memory component is considered to be the ***Lowest Replaceable Unit*** (LRU) in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module or may consist of several modules and subassemblies. Unlike media sanitization, clearing may be an acceptable method of sanitizing components for release (see 8-501, Table 2). Memory components are specifically handled as either volatile or nonvolatile as described below.

(1) Volatile Memory Components. Memory components that *do not* retain data after removal of all electrical power sources, and when reinserted into a similarly configured AIS *do not* contain residual data, are considered volatile memory components. Volatile components may be released only after accomplishing the following steps:

(a) Maintain a record of the equipment release indicating that all component memory is volatile and that no data remains in/on the component when power is removed.

(b) Equipment release procedures shall be developed by the ISSR and stated in the AISSP.

(2) Nonvolatile Memory Components. Memory components that *do* retain data when all power sources are disconnected are nonvolatile memory components. Nonvolatile memory components defined as ***read only memory*** (ROM), ***programmable ROM*** (PROM), or ***erasable PROM*** (EPROM)that have been programmed at the vendor's commercial manufacturing facility are considered to be unalterable in the field and may be released. Customized components of this nature that have been programmed with a classified algorithm or classified data will be destroyed. All other nonvolatile components may be released after successful completion of the procedures outlined in 8-501, Table 2. Failure to accomplish these procedures will require the ISSR to coordinate with the Customer for a determination of releasability. Nonvolatile components shall be released only after accomplishing the following steps:

(a) Maintain a record of the equipment release indicating the procedure used for sanitizing the component, who performed the sanitization, and who it was released to.

(b) Equipment release procedures must be developed by the ISSR and stated in the AISSP. The record will be retained for 12 months.

(3) Inspecting AIS Equipment. All AIS equipment designated for release will be inspected by the ISSR. This review will ensure that all media including internal disks have been removed.

8-601. **Test Equipment.** The Provider will determine the capability of individual test instruments to collect and process information. If necessary, the manufacturer will be asked to provide this information. A description

of the capabilities of individual test equipment will be provided to the Customer. Security requirements are based on concerns about the capability of the equipment to retain sensitive or classified data. Test equipment with nonvolatile fixed or removable storage media will comply with the requirements of this Supplement and be approved by the Customer for introduction and use in the SAPF. Test equipment with no data retention and no secondary storage does not require Customer approval.

Section 7. Documentation and Training

8-700. Documentation and Training.

a. Provider Documentation. The Provider will develop, publish, and promulgate a corporate AIS security policy, which will be maintained on file by the ISSR.

b. Security Documentation. The Provider will develop and maintain security-related documentation which are subject to review by the Customer as follows:

(1) AISSP. Prepare and submit to the Customer for approval an AISSP in accordance with Customer guidance that covers each AIS which will process information for the Customer. This plan will appropriately reference all other applicable Provider security documentation. In many cases, an AISSP will include information that should not be provided to the general user population. In these cases, a separate **user security** guide will be prepared to include only the security procedures required by the users.

(2) Physical Security Accreditation. Maintain on file the physical security accreditation documentation that identifies the date(s) of accreditation, and classification level(s) for the system device locations identified in the AISSP, and any open storage approvals.

(3) Processing Approval. Maintain on file the Customer's processing approval (i.e., interim approval or accreditation) that specifies the date of approval, system, system location, mode of operation, and classification level for which the AIS is approved.

(4) Memorandum of Agreement. Maintain on file a formal memorandum of agreement signed by all Customers having data concurrently processed by an AIS or attached to the network.

(5) AIS Technical Evaluation Test Plan. As a prerequisite to processing in the compartmented or multilevel mode, develop and submit a ***technical evaluation test plan*** to the Customer for approval. The technical evaluation test plan will provide a detailed description of how the implementation of the operating system software, data management system software, and related security software packages will enable the AIS to meet the compartmented or multilevel mode requirements stated herein. The test plan will also outline the test procedures proposed to demonstrate this compliance. The results of the test will be maintained for the life of the system.

(6) Certification Report. The Certification Report will be maintained for the life of the system.

c. **System User Training and Awareness. All AIS** users, custodians, maintenance personnel, and others whose work is associated with the Customer will be briefed on their security responsibilities. These briefings will be conducted by the Provider. Each individual receiving the briefing will sign an agreement to abide by the security requirements specified in the AISSP and any additional requirements initiated by the Customer. This securit y awareness training will be provided prior to the individual being granted access to the classified AIS and at least annually thereafter. The awareness training will cover the following items and others as applicable:

(1) The security classifications and compartments accessible to the user and the protection responsibilities for each. If the user is a privileged user, discuss additional responsibilities commensurate with those privileges;

(2) Requirements for controlling access to AISS (e.g., ***user lDs, passwords and password security, the need-to-know principle, and protecting terminal screens and printer output from unauthorized access);***

(3) Methods of securing unattended AISs such as checking print routes, logging off the host system or network, and turning the ***A IS off,***

(4) Techniques for securing printers such as removing latent images from laser drums, cleaning platens, and locking up ribbons;

(5) Caution against the use of government-sponsored computer resources for unauthorized applications;

(6) The method of reporting security-related incidents such as misuse, violations of system security, unprotected media, improper labeling, network data spillage, etc.;

(7) Media labeling, including classification labels, data-descriptor labels, placement of labels on media, and maintenance of label integrity;

(8) Secure methods of copying and verifying media;

(9) Methods of safeguarding media, including write protection, removal from unattended AISs, and storage;

(10) Methods of safeguarding hard-copy output, including marking, protection during printing, and storage;

(11) Policy on the removal of media;

(12) Methods of clearing and sanitizing media;

(13) Procedures for destroying and disposing of media, printer ribbons, and AIS circuit boards and security aspects of disposing of AISs;

(14) Methods of avoiding viruses and other malicious code including authorized methods of acquiring software, examining systems regularly, controlling software and media, and planning for emergencies. Discuss the use of recommended software to protect against viruses and steps to be taken when a virus is suspected;

(15) AIS maintenance procedures including the steps to be taken prior to AIS maintenance and the user's point-of-contact for AIS maintenance matters;

(16) Any special security requirements with respect to the user's AIS environment including connections to other AIS equipment or networks;

(17) The use of personally owned electronic devices within the SAPF;

(18) Any other items needed to be covered for the specific Customer's program.

Chapter 9
Restricted Data

Section 1. Introduction

9-100. General. This chapter of the NISPOMSUP addresses those supplemental security requirements for SECRET Restricted Data (SRD) and TOP SECRET Restricted Data (TSRD) information which have been identified as being sufficiently sensitive to necessitate security standards above and beyond those mandated by the NISPOM baseline document. ***Hereafter these are referred to as Critical SRD or TSRD. CONFIDENTIAL RD and all classification levels of Formerly Restricted Data shall be protected in accordance with the requirements in the NISPOM baseline document.*** In addition to those requirements in Chapter 9 of the NISPOM, this chapter prescribes the supplemental requirements for the protection of Critical SRD and TSRD information. Neither the NISPOM nor the NISPOMSUP are to be construed to apply to the safeguarding requirements for Special Nuclear Material, Nuclear Explosive Like Assemblies, or Nuclear Weapons.

9-101. Requirements. Under the authority of the Atomic Energy Act of 1954, the Secretary of Energy, using his/her authority over Restricted Data, may issue orders, guides, and manuals concerning protection of Restricted Data. These issuances serve as the basis for government-wide implementation procedures. However, these procedures of other agencies have not been endorsed by DOE. As a result of changes in the world situation, these policy issuances are currently under review by the Joint DOE/DOD Nuclear Weapons Information Access Authorization Review Group. Until the Review Group's recommendations are approved as policy by the Secretary of Energy, DOD contractors will continue to protect Critical SRD and TSRD in accordance with established contractual provisions. A revision of this chapter will be developed and promulgated following the results of the Joint DOE/DOD Nuclear Weapons Information Access Authorization Review Group. Nothing in this paragraph alters or abridges the authority of the Secretary of Energy under the Atomic Energy Act of 1954, as amended. DOD contracts awarded in the interim period dealing with the physics of nuclear weapons design, as specified in 9-101 .a through 9-101.i, will be reviewed by technically qualified representatives to determine if the contract involves the above specified Critical SRD or TSRD information. ***If so, this chapter's requirements will be included in the contractual document.*** DOE technical experts will be available to provide advice and assistance upon request by contracting agency representative. Should the results of the Joint DOE/DOD Nuclear Weapons Information Access Authorization Review Group modify the information specified in 9-101 .a through 9-101 .i, the affected contracts may be amended. ***For DOE contractors, Restricted Data will continue*** to ***be protected in accordance with the Department of Energy's 5600 series Safeguards and Security orders until the Review Group's recommendations are approved as policy by the Secretary of Energy and this chapter is revised to conform to the new policy.***

a. Theory of operation (hydrodynamic and nuclear) or completed design of thermonuclear weapons or their unique components. This definition includes specific information about the relative placement of components and their functions with regard to initiating and sustaining the thermonuclear reaction.

b. Theory of operation or complete design of fission weapons or their unique components. This definition includes the high explosive system with its detonators and firing unit, pit system, and nuclear initiating system as they pertain to weapon design and theory.

c. Manufacturing and utilization information which reveals the theory of operation or design of the physics package.

d. Information concerning inertial confinement fusion which reveals or is indicative of weapon data.

e. Complete theory of operation, complete or partial design information revealing sensitive design features or information on energy conversion of a nuclear directed energy weapon. Sensitive information includes but is not limited to the nuclear energy converter, energy director, or other nuclear directed energy system or components outside the envelope of the nuclear source but within the envelope of the nuclear directed energy weapon.

f. Manufacturing and utilization information and output characteristics for **nuclear** energy converters, directors, or other nuclear directed energy weapon systems or components outside the envelope of the nuclear source and which do not comprehensively reveal the theory of operation, sensitive design features of the nuclear directed energy weapon or how the energy conversion takes place.

g. Nuclear weapon vulnerability assessment information concerning use control systems that reveals an exploitable design feature, or an exploitable system weakness or deficiency, **which** could be expected to permit the unauthorized use or detonation of a nuclear weapon.

h. Detailed design and functioning information of nuclear weapon use control systems and their components. Includes actual hardware and drawings that reveal design or theory of operation. This also includes use control information for passive and active systems as well as for disablement systems.

i. Access to specific categories of noise and quieting information, fuel manufacturing technology and broad policy or program direction associated with Naval Nuclear Propulsion Plants as approved by the Naval Nuclear Propulsion Program CSA.

9-102.

a. ***Contractors shall establish protective measures for the safeguarding of Critical SRD and TSRD in accordance with the requirements of this chapter. Where these requirements are not appropriate for protecting specific types or forms of material, compensatory provisions shall be developed and approved by the CSA, with the concurrence of DOE, as appropriate. Nothing in this NISPOMSUP shall be construed to contradict or inhibit compliance with the law or building codes.***

b. ***Access to Restricted Data shall be limited to persons who possess appropriate access authorization, or PCL, and who require such access (need-to-know) in the performance of official duties (i.e., have a verifiable need-to-know). For access to TOP SECRET Restricted Data, an individual must possess an active Q access authorization, or a final TOP SECRET PCL, based on a SSBI. For access to Critical SECRET Restricted Data, as defined in 9-101.a through 9-101.i, an individual must possess an active Q access authorization, or final TOP SECRET or SECRET PCL, based on a SSBI. Controls shall be established to detect and deter unauthorized access to Restricted Data.***

Section 2. Secure Working Areas

9-200. **Secure Working Areas.**

a. **General.** When not placed in approved storage, Critical SRI) and TSRD must be maintained in approved Secured Working Areas, and be constantly attended to by, or under the control of, a person or persons having the proper access authorization, or PCL, and a need-to-know, who are responsible for its protection.

b. **Requirements. Secure** Working Area boundaries shall be defined by physical barriers (e.g., fences, walls, doors). Protective personnel or other measures shall be used to control authorized access through designated entry portals and to deter unauthorized access to the area. A personnel identification system (e.g., security badge) shall be used as a control measure when there are more than 30 persons per shift. Entrance/Exit inspections for prohibited articles and/or Government property may be conducted by protective personnel. When access to a Secure Working Area is authorized for a person without appropriate access authorization or need-to-know, measures shall be taken to prevent compromise of classified matter. Access to safeguards and security interests within a Secure Working Area, when not in approved storage, is controlled by the custodian(s) or authorized **user(s).** Means shall be used to detect unauthorized intrusion appropriate to the classified matter under protection.

9-201. Barriers. ***Physical barriers shall be used to demarcate the boundaries of a Secure Working Area. Permanent barriers shall be used to enclose the area, except during construction or transient activities, when temporary barriers may be erected.*** Temporary barriers may be of any height and material that effectively impede access to the area.

a. **Walls.** ***Building materials shall offer penetration resistance to, and evidence of, unauthorized entry into the area. Construction shall meet local building codes. Walls that constitute exterior barriers of Security Areas shall extend from the floor to the structural ceiling, unless equivalent means are used.***

(1) ***When transparent glazing material is used, visual access to the classified material shall be prevented by the use of drapes, blinds, or other means.***

(2) Insert-type panels (if used) shall be such that they cannot be removed from outside the area being protected without showing visual evidence of tampering.

b. **Ceilings and Floors.** ***Ceilings and floors shall be constructed of building materials that offer penetration resistance to, and evidence of, unauthorized entry into the area. Construction shall meet local building codes.***

c. **Doors.** ***Doors and doorjambs shall provide the necessary barrier delay rating requi: by the applicable procedure. As a minimum, requirements shall include the following:***

(1) ***Doors with transparent glazing material may be used if visual access is not a security concern; however, they shall offer penetration resistance to, and evidence of, unauthorized entry into the area.***

(2) A sight baffle shall be used if visual access is a factor.

(3) An astragal shall be used where doors used in pairs meet.

(4) Door 10U vers, baffle plates, or astragals, when used, shall be reinforced and immovable from outside the area being protected.

d. **Windows.** ***The following requirements shall be applicable to windows:***

(1) When primary reliance is placed on windows as physical barriers, they shall offer penetration resistance to, and evidence of, unauthorized entry into the area.

(2) Frames shall be securely anchored in the walls, and windows shall be locked from the inside or installed in fixed (nonoperable) frames so the panes are not removable from outside the area being protected.

(3) ***Visual barriers shall be used if visual access is a factor.***

e. Unattended Openings.

(1) *Physical protection features shall be implemented at all locations where storm sewers, drainage swells, and site utilities intersect the fence perimeter.*

(2) *Unattended openings in security barriers, which meet the following criteria, must incorporate compensatory measures such as security bars: greater than 96 inches square* **(619.20** *square centimeters) in area and greater than 6 inches (15.24 centimeters) in the smallest dimension; and located within 18 feet (5.48 meters) of the ground, roof, or ledge of a lower Security Area; or located 14 feet (4.26 m) diagonally or directly opposite windows, fire escapes, roofs, or other openings in uncontrolled adjacent buildings; or located 6 feet (1.83 m) from uncontrolled openings in the same barrier.*

Section 3. Storage Requirements

9-300. General. *Custodians and authorized users of Critical SRD and TSRD are responsible for the protection and control of such matter.*

9-301. TSRD Storage. *TOP SECRET Restricted Data that is not under the personal control of an authorized person shall be stored within a security repository located within a Secure Working Area with CSA approved supplementary protection consistent with Chapter 5-307.a and 5-307.b of the NISPOM baseline. Authorized repositories are as follows:*

a. *In a locked, General Services Administration - approved security container.*

b. *In a vault or vault-type room.*

9-302. **Critical SRD Storage.** *Critical SRD shall be stored in a manner authorized for Top Secret Restricted Data matter or in one of the following ways:*

a. *In a locked General Services Administration-approved security container located within a Secure Working Area.*

b. *In a General Services Administration-approved security container, not located within a Secure Working Area, under supplemental protection (i.e., intrusion detection system protection or protective patrol).*

c. In a steel filing cabinet, not meeting General Services Administration requirements, but approved for use prior to the date of this NISPOMSUP, which may continue to be used until there is a need for replacement. It shall be equipped with a minimum of either an Underwriter Laboratories Group 1, built-in, changeable combination lock or a lock that meets Federal Specification FF-P-11O "Padlock, Changeable Combination. " Steel filing cabinets located within a Secure Working Area shall be under approved supplemental protection (i.e., intrusion detection system protection or protective patrol). If the steel filing cabinet is not located within a Secure Working Area, it shall be under intrusion detection system protection.

Chapter 10
International Security Requirements

International security information that is required by a SAP or is SAP-related will conform to the NISPOM as directed by the PSO.

Chapter 11
Miscellaneous

Section 1: TEMPEST

TEMPEST Requirements. When compliance with TEMPEST standards is required for a contract, the GPM/PSO will issue specific guidance in accordance with current national directives that afford consideration to realistic, validated, local threats, cost effectiveness, and zoning.

Section 2. Government Technical Libraries

SAP information will not be sent to the National Defense Technical Information Center or the U.S. Department of Energy Office of Scientific and Technical Information.

Section 3. Independent Research and Development

11-300. General. ***The use of SAP information for a contractor Independent Research and Development (IR&D) effort will occur only with the specific written permission of the Contracting Officer. Procedures and requirements necessary for safeguarding SAP classified information when it is incorporated in a contractor's IR&D effort will be coordinated with the PSO.***

11-301. **Retention of SAP Classified Documents Generated Under IR&D Efforts. With** the permission of the Contracting Officer, the contractor may be allowed to retain the classified material generated in connection with a classified IR&D effort. The classified documents may be required to be sanitized. If necessary, the Government agency will provide the contractor assistance in sanitizing the material to a collateral ***or*** unclassified level (i.e., by reviewing and approving the material for release).

11-302. Review **of Classified IR&D Efforts.** ***IR&D operations and documentation that contain SAP classified information will be subject to review in the same manner as other SAP classified information in the possession of the contractor.***

Section 4. Operations Security

Special Access Programs may require unique Operations Security (OPSEC) plans, surveys, and activities to be conducted as a method to identify, define, and provide countermeasures to vulnerabilities. These requirements may be made part of the contractual provisions.

Section 5. Counterintelligence (CI) Support

11-500. Counterintelligence (CI) Support. Analysis of foreign intelligence threats and risks to Program information, material, personnel, and activities may be undertaken by the Government Agency. Resulting information that may have a bearing on the security of a SAP will be provided by the Government to the contractor when circumstances permit. Contractors may use CI support to enhance or assist security planning and safeguarding in pursuit of satisfying contractual obligations. Requests should be made to the PSO.

11-501. **Countermeasures.** Security countermeasures may be required for SAPS to protect critical information, assets, and activities. When OPSEC countermeasures are necessary, they will be made a part of the contract provisions and cost implementation may be subject to negotiation. Countermeasures may be active or passive techniques, measures, systems, or procedures implemented to prevent or reduce the timely effective collection and/or analysis of information which would reveal intentions or capabilities (e.g., traditional security program measures, electronic countermeasures, signature modification, operational and/or procedural changes, direct attack against and neutralization of threat agents and/or platforms, etc.).

Section 6. Decompartmentation, Disposition, and Technology Transfer

11-600. *Every scientific paper, journal article, book, briefing, etc., pertaining to a SAP and prepared by personnel currently or previously briefed on the SAP that is proposed for publication or presentation outside of the SAP will be reviewed by the PSO and a Program-briefed Public Affairs Officer (PAO) if available. Any release will be by the GPM.* Often SAP-unique "tools" such as models, software, technology, and facilities may be valuable to other SAPS. Some information, material, technology, or components may not be individuall y sensitive. If information or materials can be segregated and disassociated from the SAP aspects of the Program, decompartmentation and release of the information and/or materials may be approved to support U.S. Government activities. *The information and materials proposed for release will remain within the Program Security Channels until authorized for release.*

11-601. Procedures. The following procedures apply to the partial or full decompartmentation, transfer (either to another SAP or collateral Program), and disposition of any classified information, data, material(s), and hardware or software developed under a SAP contract or subcontract (SCI information will be handled within **SCI** channels).

a. **Deeompartmentation.** *Prior to decompartmenting any classified SAP information or other material(s) developed within the Program, the CPSO will obtain the written approval of the CPM. Decom - partmentation initiatives at a Program activity will include completion of a Decompartmentation or Transfer Review Format Include supporting documentation that will be submitted through the PSO to the GPM. Changes, conditions and stipulations directed by the GPM will be adhered to. Approval of Program decompartmentation and all subsequent transfers will be in writing.*

b. **Technology Transfer.** Technologies may be transferred through established and approved channels in cases where there would be a net benefit to the U.S. Government and Program information is not exposed or compromised. The Contracting Officer is the approval authority for technology transfers.

(1) Contractor Responsibilities. *CPSOs will ensure that technologies proposed for transfer receive a thorough security review. The review will include a written certification that all classified items and unclassified Program-sensitive information have been redacted from the material in accordance with sanitization procedures authorized by the GPM. A description of the sanitization method used and identification of the official who accomplished the redaction will accompany the information or* material(s) *forwarded to the GPM for review and approval*

(2) Government Responsibilities. The contracting officer's representative (COR), PSO, and GPM will make every attempt to review requests expeditiously. ***Requests will be submitted at least thirty (30) working days prior to the requested release date.*** This is particularly important when requesting approval for Program-briefed personnel to make non-Program related presentations at conferences, symposia, etc.

Section 7. Other Topics

11-700. Close-out of a SAP. *At the initiation of a contract close-out, termination or completion of the contract effort, the CPSO will consider actions for disposition of residual hardware, software, documentation, facilities, and personnel accesses. Security actions to close-out Program activities will prevent compromise of classified Program elements or other SAP security objectives. The* contractor may be required to submit a termination plan to the Government. The master classified material accountability record (log or register) normally will be transferred to the PSO at Program close-out.

11-701. Special Access Program Secure Communications Network. SAPS may use a SAP secure communications and/or data network linking the GPM and/or contractors with associated technical, operational, and logistic support activities for secure communications.

11- 702. Patents. *Patents involving SAP information will be forwarded to the GPM/PSO for submission to the Patents Office. The PSO will coordinate with Government attorneys and the Patent Office for submission of the patent.*

11-703. Telephone Security. The PSO will determine the controls, active or inactive, to be placed on telecommunication lines. *SAPFs accredited for discussion or electronic processing will comply with DCID 1/21 and Telephone Security Group (TSG) standards as determined by the PSO.*

Appendix A
Definitions

Access Approval Authority. Individual responsible for final access approval and/or denial determination.

Access Roster. A database or listing of individuals briefed to a special access program.

Access Termination. The removal of an individual from access to SAP or other Program information.

Accrediting Authority. A Customer official who has the authority to decide on accepting the security safeguards prescribed or who is responsible for issuing an accreditation statement that records the decision to acccept those safeguards.

Acknowledged Special Access Program. A SAP whose existence is publicly acknowledged.

Acquisition Special Access Program (AQ-SAP). A special access program established primarily to protect sensitive research, development, testing, and evaluation (RDT&E) or procurement activities in support of sensitive military and intelligence requirements.

Agent of the Government. A contractor employee designated in writing by the Government Contracting Officer who is authorized to act on behalf of the Government.

Authentication. a. To establish the validity of a claimed identity. b. To provide protection against fraudulent transactions by establishing the validity of message, station, individual, or originator.

Automated Information System (AIS). A generic term applied to all electronic computing systems. AISS are composed of computer hardware (i.e., automated data processing (ADP) equipment and associated devices that may include communication equipment), firmware, operating systems, and other applicable software. AISS collect, store, process, create, disseminate, communicate, or control data or information.

Billets. A determination that in order to meet need-to-know criteria, certain SAPS may elect to limit access to a predetermined number of properly cleared employees. Security personnel do not count against the billet system.

Boundary. The boundary of an AIS or network includes all users that are directly or indirectly connected and who can receive data from the system without a reliable human review by an appropriately cleared authority.

Certification. A statement to an accrediting authority of the extent to which an AIS or network meets its security criteria. This statement is made as part of and in support of the accreditation process.

Clearing. The removal of information from the media to facilitate continued use and to prevent the AIS system from recovering previously stored data. However, the data may be recovered using laboratory techniques. Overwriting and degaussing are acceptable methods of clearing media.

Codeword. A single classified word assigned to represent a specific SAP or portions thereof.

Collateral Information. Collateral information is National Security Information created in parallel with Special Access Information under the Provisions of E.O. 12356 (et al) but which is not subject to the added formal security protection required for Special Access Information (stricter access controls, need-to-know, compartmentation, stricter physical security standards, etc).

Compelling Need. A requirement for immediate access to special program information to prevent failure of the mission or operation or other cogent reasons.

Contractor Program Security Officer (CPSO). An individual appointed by the contractor who performs the security duties and functions for Special Access Programs.

Contractor Program Manager (CPM). A contractor-designated individual who has overall responsibility for all aspects of a Program.

Counterintelligence Awareness. A state of being aware of the sensitivity of classified information one possesses, collaterally aware of the many modes of operation of hostile intelligence persons and others whose interests are inimical to the United States while

being able to recognize attempts to compromise one's information, and the actions one should take, when one suspects he has been approached, to impart the necessary facts to trained counterintelligence personnel.

Customer. The Government organization that sponsors the processing.

Data Integrity. a. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction. b. The property that data has not been exposed to accidental or malicious alteration or destruction.

Debriefing. The process of informing a person his need-to-know for access is terminated.

Declassification {Media). An administrative step that the owner of the media takes when the classification is lowered to UNCLASSIFIED. The media must be properly sanitized before it can be downgraded to UNCLASSIFIED.

Degauss. a. To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force, commonly referred to as demagnetizing, or b. 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 degaussing magnetic storage media or other magnetic material.

Degaussing (Demagnetizing). Procedure using an approved device to reduce the magnetization of a magnetic storage media to zero by applying a reverse (coercive) magnetizing force rendering any previously stored data unreadable and unintelligible.

Digraph and/or Trigraph. A two and/or three-letter acronym for the assigned Codeword or nickname.

Disclosure Record. A record of names and dates of initial access to any Program information.

e.g. For example (exempli gratia).

Eligibility. A determination that a person meets personnel security standards for access to Program material.

EPROM. A field-programmable read-only memory that can have the data content of each memory cell altered more than once. An EPROM is bulk-erased by exposure to a high-intensity ultraviolet light. Sometimes referred to as a reprogrammable read-only memory.

EEPROM. Abbreviation for electrically erasable programmable read-only memory. These devices are fabricated in much the same way as EPROMs and, therefore, benefit from the industry's accumulated quality and reliability experience. As the name implies, erasure is accomplished by introducing electrical signals in the form of pulses to the device, rather than by exposing the device to ultraviolet light. Similar products using a nitride NMOS process are termed EAROMS (for electrically alterable read-only memory).

Government Program Manager (GPM). The senior Government Program official who has ultimate responsibility for all aspects of the Program.

i.e. That is (id est).

Inadvertent Disclosure. A set of circumstances or a security incident in which a person has had involuntary access to classified information to which the individual was or is not normally authorized.

Indoctrination. An initial indoctrination and/or instruction provided each individual approved to a SAP prior to his exposure concerning the unique nature of Program information and the policies, procedures, and practices for its handling.

Information Systems Security Representative (ISSR). The Provider-assigned individual responsible for the on-site security of the AIS(S) processing information for the Customer.

Joint Use Agreement. A written agreement signed by two or more accrediting authorities whose responsibility includes information processed on a common AIS or network. Such an agreement defines a cognizant security authority and the security arrangements that will govern the operation of the network.

Memorandum of Agreement (MOA). An agreement, the terms of which are delineated and attested to by the signatories thereto. MOA & MOU (Memorandum of Understanding) are used interchangeably.

Network. A computing environment with more than one independent processor interconnected to permit communications and sharing of resources.

Nicknames. A combination of two separate unclassified words assigned to represent a specific SAP or portion thereof.

Nonvolatile Memory Components. Memory components that do retain data when all power sources are disconnected.

Object Reuse. The reassignment to some subject of a medium (e.g., page frame, disk sector, magnetic tape) that contained one or more objects. To be securely reassigned, such media will contain no residual data from the previously contained object(s).

Office Information System (01S). An 01S is a special purpose AIS oriented to word processing, electronic mail, and other similar office functions. An 01S is normally comprised of one or more central processing units, control units, storage devices, user terminals, and interfaces to connect these components.

Overwrite **(Re-recording) Verification.** An approved procedure to review, display, or check the success of an overwrite procedure, or b. The successful testing and documentation through hardware and random hard-copy readout of the actual overwritten memory sectors.

Perimeter. The perimeter of an AIS or network is the extent of the system that is to be accredited as a single system.

Peripheral Devices. Any device attached to the network that can store, print, display, or enhance data (e.g., disk and/or tape, printer and/or plotter, an optical scanner, a video camera, a punched-card reader, a monitor, or card punch).

Personal Computer System (PC). A PC is a system based on a microprocessor and comprised of internal memory (ROMs and RAMs), input and/or output, and associated circuitry. It typically includes one or more read/write device(s) for removable magnetic storage media (e.g., floppy diskettes, tape cassettes, hard disk cartridges), a keyboard, CRT or plasma display, and a printer. It is easily transported and is primarily used on desk tops for word processing, database management, or engineering analysis applications.

Program Access Request (PAR). A formal request used to nominate an individual for Program access.

Program Channels or Program Security Channels. A method or means expressly authorized for the handling or transmission of classified or unclassified SAP information whereby the information is provided to indoctrinated persons.

Program Executive Agent. The highest ranking military or civilian individual charged with direct responsibility for the Program and usually appoints the Government Program Manager.

Program Material. Program material and information describing the service(s) provided, the capabilities developed, or the item(s) produced under the SAP.

Program Security Officer (PSO). The Government official who administers the security policies for the SAP

Program Sensitive Information. Unclassified information that is associated with the Program. Material or information **that,** while not directly describing the Program or aspects of the Program, could indirectly disclose the actual nature of the Program to a non-Program-briefed individual.

Provider. The Contractor or Government-support organization (or both) that provides the process on behalf of the Customer.

Sanitizing. The removal of information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures.

Secure Working Area. An accredited facility or area that is used for handling, discussing and/or processing, but not storage of SAP information.

Security level. A clearance or classification and a set of designators of special access approvals; i.e., a clearance and a set of designators of special access approval or a classification and a set of such designators, the former applying to a user, the latter applying, for example, to a computer object.

Security **Policy.** The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. A complete security policy will necessarily address many concerns beyond the scope of computers and communications.

Security Profile. The approved aggregate of hardware/ software and administrative controls used to protect the system.

Security Testing. A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See also: Functional Testing, Penetration Testing, Verification.

Sensitivity Label. A collection of information that represents the security level of an object and that describes the sensitivity of the data in the object. A sensitivity label consists of a sensitivity level (classification and compartments) and other required security markings (e.g., Codewords, handling caveats) to be used for labeling data.

Sensitive Activities. Sensitive activities are special access or Codeword programs, critical research and development efforts, operations or intelligence activities, special plans, special activities, or sensitive support to the customer or customer contractors or clients.

Sensitive Compartmented Information (SCI). SCI is classified information concerning or derived from intelligence sources and methods or analytical processes that is required to be handled within a formal control system established by Director of Central Intelligence.

Sensitive Compartmented Information Facility (SCIF). SCIF is an area, room(s), building installation that is accredited to store, use, discuss, or electronically process Sensitive Compartmented Information (SCI). The standards and procedures for a SCIF are stated in DCIDs 1/19 and 1/21.

Special Access Program Facility (SAPF). A specific physical space that has been formally accredited in writing by the cognizant PSO which satisfies the criteria for generating, safeguarding, handling, discussing, and storing CLASSIFIED and/or UNCLASSIFIED Program information, hardware, and materials.

Special **Program Document Control Center. The** component's activity assigned responsibility by the ISSR for the management, control, and accounting of all documents and magnetic media received or generated as a result of the special program activity.

Stand-Alone AIS. A stand-alone AIS may include desktop, laptop, and notebook personal computers, and any other hand-held electronic device containing classified information. Stand-alone AISS by definition are *not* connected to any LAN or other type of network.

System. An assembly of computer and/or communications hardware, software, and firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

Trigraph. (See Digraph ruder Trigraph.)

Trojan Horse. A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security (for example, making a "blind copy" of a sensitive file for the creator of the Trojan horse).

Trusted Computer System. A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Path. A mechanism by which a person at a terminal can communicate directly with the trusted computing base. This mechanism can **only be activated by** the person or the trusted computing base and cannot be imitated by untrusted software.

Two-Person Integrity. A provision that prohibits one person from working alone.

Unacknowledged Special Access Program. A SAP with protective controls that ensures the existence of the Program is not acknowledged, affirmed, or made known to any person not authorized for such information. All aspects (e.g., technical, operational, logistical, etc.) are handled in an unacknowledged manner.

Users. Any person who interacts directly with an AIS or a network system. This includes both those persons who are authorized to interact with the system and those people who interact without authorization (e.g., active or passive wiretappers).

Vendor. The manufacturer or sellers of the AIS equipment and/or software used on the special program.

Virus. Malicious software. A form of Trojan horse that reproduces itself in other executable code.

Volatile Memory Components. Memory components that *do not* ***retain*** data after removal of all electrical power sources and when reinserted into a similarly configured AIS do not contain residual data.

Workstation. A high-performance, microprocessor-based platform that uses specialized software applicable to the work environment.

Appendix B
AIS Acronyms

Many computer security-related acronyms are used in this Supplement. These acronyms, after first being defined, are used throughout this document to reduce its length. The acronyms used in this document are defined below:

AIS	Automated Information System
AISSP	AIS Security Plan
CM	Configuration Management
CCB	Configuration Control Board
CPU	Central Processing Unit
CRT	Cathode Ray Tube (Monitor Screen Tube)
CSA	Cognizant Security Agency (Customer)
DAC	Discretionary Access Control
DCID	Director of Central Intelligence Directive
DoD	Department of Defense
E.O.	Executive Order
EPROM	Erasable Programmable Read-Only Memory
EAPROM	Electrically Alterable Programmable Read-Only Memory
EEPROM	Electrically Erasable Programmable Read-Only Memory
I/O	Input and/or Output
ISSR	Information System Security Representative
K	Thousand (kilo)
LAN	Local Area Network
LOOON	Log On
MAC	Mandatory Access Control
MODEM	Modulator and/or Demodulator
NCSC	National Computer Security Center
NSA	National Security Agency
OMB	Office of Management and Budget
PC	Personal Computer (i.e., desktop, laptop, notebook, or hand-held computer)
PL	Public Law
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
ROM	Read Only Memory
SAN	Separately Accredited Network
SAP	Special Access Program
SAPF	Special Access Program Facility

SCI	Sensitive Compartmented Information
STD	Standard
TS	Top Secret
USER ID	User Identification

Appendix C
AISSP Outline

This outline provides the basis for preparing an AIS Security Plan **(AISSP).** The annotated outline, with prompts and instructions, will assist **ISSRs** in preparing a plan that includes necessary overviews, descriptions, listings, and procedures. It will also assist in covering the requirements contained in this **NISPOM** Supplement. In preparing the **AISSP,** any information that does not appropriately fit under a subtitle may be placed under a main title. For example, a hardware list or references to a hardware list will be placed under the 4.0 AIS HARDWARE heading. For changes to an existing plan that do not require revision of the entire plan, provide name and date of the plan to be modified, date of changes on each page, and cross reference to the plan's applicable paragraph numbers. (For changes, only the change pages with the applicable plan name and date need to be sent to the **CSA.)**

Table Of Contents

1.0 INTRODUCTION

This section will describe the purpose and scope of the AISSP. It may include any topic intended to help the reader understand and appreciate the purpose of the AISSP. Pertinent background information may also be presented to provide clarity.

1.1 Security Administration.

Provide the name and date of this plan and indicate whether it is an original or revised plan.

Specify the cognizant Customer Program Office whose activity the AIS will support and the contract number(s), if applicable.

Specify the Provider's name and address. Identify the location of the AIS equipment (including the building and room numbers(s)).

Provide the names of the Provider's program manager, ISSR, alternate(s). Also provide their secure and unsecure telephone numbers and their normal office hours.

Provide an organizational structure showing the name and title of all security management levels above the ISSR.

Provide joint-use information if applicable.

1.2 Purpose and Scope.

The plan will describe how the Provider will manage the security of the system. Describe the purpose and scope of this AIS.

2.0 SAPF DESCRIPTION.

This section will provide a physical overview of the AIS SAPF (including its surroundings) that is used to secure the Customer's program activities. It will include information about the secure environment required to protect the AIS equipment, software, media, and output.

2.1 Physical Environment.

State whether the SAPF is accredited or approved to process and store classified information, who accredited or approved it, the security level, and when approved. State whether the SAPF is approved for open or closed storage.

Specify whether the storage approval is for hard disk drives, diskettes, tapes, printouts, or other items.

State whether the approval includes unattended processing.

2.2 Floor Layout.

Provide a floor plan showing the location of AIS equipment and any protected wire lines. (This may be included in a referenced appendix.) The building and room number(s) will match the information provided in the hardware listing (see 4.0).

2.3 SAPF Access.

Describe procedures for controlling access to the AIS(S) to include: after hours access, personnel access controls, and procedures for providing access to uncleared visitors (e.g., admitting, sanitizing area, escorting).

2.4 TEMPEST.

If applicable, describe TEMPEST countermeasures.

3.0 AIS DESCRIPTION

This section will provide a detailed description of the system and describe its security features and assurances.

Describe variances and exceptions.

3.1 General Information

Provide a system overview and description.

Specify clearance level, formal access (if appropriate), and need-to-know requirements that are being supported.

Identify the data to be processed including classification levels, compartments, and special handling restrictions that are relevant.

State the mode of operations.

Indicate the AIS's usage (in percent) that will be dedicated to the Customer's activity (e.g, periods processing).

3.2 Configuration and Connectivity.

Specify whether the AIS is to operate as a stand-alone system, as a terminal connected to a mainframe, or as a network.

Describe how the AIS or network is configured. If a network, specify whether it is a unified network or interconnected network. Describe the security support structure and identify any specialized security components and their role.

Identify and describe procedures for any connectivity to the AIS(S). 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 AISS operating in the compartmented or multilevel modes an information flow diagram will be provided.

If applicable, discuss the separations of classified and unclassified AISS within the SAPF.

Indicate whether the AIS is configured with removable or nonremovable hard disk drives.

Describe the configuration management program. Describe the procedures to ensure changes to the AIS require prior coordination with the ISSR.

3.3 User Access and Operation.

Describe the AIS operation start-up and shut-down (mode termination). Provide any unique equipment clearing procedures.

Discuss all AIS user access control (e.g., log-on ID, passwords, file protection, etc.).

Identify the number of system users and the criteria used to determine privileged access.

If the mode is other than dedicated, discuss those mechanisms that implement DAC and MAC controls.

Discuss procedures for the assignment and distribution of passwords, their frequency of change, and the granting of access to information and/or files.

Indicate whether AIS operation is required 24 hours per day.

Discuss procedures for after hours processing. State whether the AIS(S) are approved for unattended processing.

Discuss procedures for marking and controlling AIS printouts.

Discuss remote access and operations requiring specific approval by the CSA.

Discuss procedures for incident reporting.

3.4 Audit Trails.

If applicable, discuss the audit trails used to monitor user access and operation of the AIS and the information that is recorded in the audit (rail. State whether user access audit trails are manual or automatic.

Identify the individual who will review audit trails and how often.

Describe procedures for hand] ing discrepancies found during audit trails reviews.

4.0 AIS HARDWARE

This section will describe the AIS hardware that supports the Customer’s program. This section will provide a listing of the AIS hardware and procedures for its secure control, operation, and maintenance.

Provide a complete listing of the major hardware used to support the Customer’s program activities. This list may be in tabular form located either in this section or a referenced appendix. The following information is required for all major AIS hardware: nomenclature, model, location (i.e., building/room number), and manufacturer.

Provide a description of any custom-built AIS hardware,

Indicate whether the AIS hardware has volatile or nonvolatile memory components. Specifically, identify components that are nonvolatile.

If authorized, describe procedures for using portable devices for unclassified processing.

Identify the custodian(s) for AISs.

4.1 Labeling Hardware.

Describe how the AIS hardware will be labeled to identify its classification level (e.g., classified and unclassified AISS collocated in the same secure area).

4.2 Maintenance Procedures.

Describe the maintenance and sanitization procedures to be used for maintenance or repair of defective AIS hardware by inappropriately cleared personnel.

4.3 Hardware Sanitization and Destruction.

Describe the procedures or methods used to sanitize and or destroy AIS hardware (volatile or nonvolatile components).

4.4 Hardware Movement.

Describe the procedures or receipting methods used to release and transport the AIS hardware from the SAPF.

Describe the procedures or receipting methods for temporarily or permanently relocating the AIS hardware within the SAPF.

Describe the procedures for introducing hardware into the SAPF.

4.5 Hardware Control and Audit Trails.

Describe all AIS hardware maintenance logs, the information recorded on them, who is responsible for reviewing them, and how often.

5.0 AIS SOFTWARE

This section will provide a listing of all the software that supports the Customer's program. It will also provide procedures for protecting and using this software.

5.1 Authorized Software.

Provide a complete listing of all software used to support the Customer's program activities. This list may be in tabular form and may be located either in the section or in a referenced appendix. The listing will also include security software (e. g., audits software, anti-virus software), special-purpose software (e.g., in-house, custom, commercial utilities), and operating system software. The following information is required for AIS software: software name, version, manufacturer, and intended use or function.

5.2 Software Procedures.

Indicate whether a separate unclassified version of the operating system software will be used for maintenance.

Describe the procedures for procuring and introducing new AIS software to support program activities.

Describe the procedures for evaluating AIS software for security impacts.

Describe procedures for protecting software from computer viruses and malicious code and for reporting incidents.

6.0 DATA STORAGE MEDIA

This section provides a description of the types of data storage media to be used in the Customer's program and their control.

6.1 Labeling and Storing Media.

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 SAPF (e.g., safes, vaults, locked desk).

6.2 Media Clearing, Sanitization, and Destruction.

Describe the procedures or methods used to clear, sanitize, and destroy the data storage media.

6.3 Media Movement.

Describe the procedures (or receipting methods) for moving data storage media into and out of the SAPF.

Describe the procedures for copying, reviewing, and releasing information on data storage media.

6.4 Media Control.

Describe the method of controlling data storage media.

7.0 AIS SECURITY AWARENESS PROGRAM

Discuss the Provider's security awareness program.

Indicate that the AIS users are required to sign a statement acknowledging that they have been briefed on the AIS security requirements and their responsibilities.

8.0 GLOSSARY OF TERMS

Appendix D
AIS Certification and Accreditation

A. CERTIFICATION

The ISSR, working jointly with the Customer, is responsible for coordinating and supporting the certification process. The ISSR is responsible for certifying, or coordinating the certification of, the AIS or network. Certification, which is a prerequisite for accreditation, is accomplished as follows:

1. Identify operational requirements, define the *Mode of Operation,* and identify applicable security requirements, in accordance with this document and applicable documents referenced herein.

2. Conduct a *Risk Management Review* to identify risks and needed countermeasures and specify additional security requirements (countermeasures) based on the review.

3. Prepare an AISSP. Refine the plan throughout the certification process.

4. Conduct a test and inspection to establish the extent to which the AIS performs the security functions needed to support the mode of operation and security policy for the system as outlined in the AISSP. The Customer will require a written certification report.

5. Operating in the compartmented or multilevel mode requires the development of an AIS *Technical Evaluation Plan.* After Customer concurrence, accomplish testing as described herein. AIS security testing provides assurance to the Customer that the subject AIS(s) or network(s) meets the security requirements for operating in the compartmented or multilevel mode. Such testing is a prerequisite for Customer accreditation.

   a. Coordination Scheduling and Testing. The security test may be jointly conducted by the Provider and the Customer.

   b. Testing Prerequisite. The Provider-developed *A IS Technical Evaluation Test Plan will* be coordinated and/or approved by the customer.

B. ACCREDITATION

Accreditation is the Customer's authorization and approval for an AIS or network to process sensitive data in an operational environment. The Customer bases the accreditation on the results of the certification process. Following certification, the Customer reviews the risk assessment, employed safeguards, vulnerabilities, and statement of level of risk and makes the accreditation decision to accept risk and grant approval to operate; grant *interim approval to operate* (IATO) and fix deficiencies; or to shut-down, fix deficiencies, and recertify.

Appendix E
References

1. U.S. Government Publications

OMB Circular A- 130	Management of Federal Information Resources Appendix III, Security of Federal AISs
PL-99-474	Computer Fraud and Abuse Act of 1986
PL-100-235	Computer Security Act of 1987
EO 12333	United States Intelligence Activities
EO 12356	National Security Information
EO 12829	National Industrial Security Program

2. National Telecommunications & Information Systems Security (NTISS) Publications

COMPUSEC/1 -87	Security Guideline
NTISSAM	Advisory Memorandum on Office Automation
NTISSI 300	National Policy on Control of Compromising Emanations
NTISSI 7000	TEMPEST Countermeasures for Facilities
NTISSIC 4009	National Information Systems Security (INFOSEC) Glossary
NACSIM 5000	TEMPEST Fundamentals
NACSIM 5201	TEMPEST Guidelines for Equipment/System Design Standard
NACSIM 5203	Guidelines for Facility Design and Red/Black Installation
NACSIM 7002	COMSEC Guidance for ADP Systems

3. National Computer Security Center (NCSC) Publications (The Rainbow Series)

NCSC-WA-002-85	Personal Computer Security Considerations
NCSC-TG-001	A Guide to Understanding Audit in Trusted Systems [Tan Book]
NCSC-TG-002	Trusted Product Evaluation - A Guide for Vendors [Bright Blue Book]
NCSC-TG-003	A Guide to Understanding Discretionary Access Control in Trusted Systems [Orange Book]
NCSC-TG-004	Glossary of Computer Security Terms [Aqua Book]

NCSC-TG-005	Trusted Network Interpretation [Red Book]
NCSC-TG-006	A Guide to Understanding Configuration Management in Trusted Systems [Orange Book]
NCSC-TG-007	A Guide to Understanding Design Documentation in Trusted Systems [Burgundy Book]
NCSC-TG-008	A Guide to Understanding Trusted Distribution in Trusted Systems [Lavender Book]
NCSC-TG-009	Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria [Venice Blue Book]
NCSC-TG-011	Trusted Network Interpretation Environments Guideline-Guidance for Applying the Trusted Network Interpretation [Red Book]
NCSC-TG-013	Rating Maintenance Phase Program Document [Pink Book]
NCSC-TG-O 14	Guidelines for Formal Verification Systems [Purple Book]
NCSC-TG-0 15	A Guide to Understanding Trusted Facility Management [Brown Book]
NCSC-TG-017	A Guide to Understanding Identification and Authentication in Trusted Systems [Lt. Blue Book]
NCSC-TG-018	A Guide to Understanding Object Reuse in Trusted Systems [Lt. Blue Book]
NCSC-TG-019	Trusted Product Evaluation Questionnaire [Blue Book]
NCSC-TG-020A	Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System [Gray Book]
NCSC-TG-02 1	Trusted Database Management System Interpretation [Lavender Book]
NCSC-TG-022	A Guide to Understanding Trusted Recovery [Yellow Book]
NCSC-TG-025	A Guide to Understanding Data Remanence in Automated Information Systems [Green Book]
NCSC-TG-026	A Guide to Writing the Security Features User's Guide for Trusted Systems [Peach Book]
NCSC-TG-027	A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems [Turquoise Book]
NCSC-TG-028	Assessing Controlled Access Protection [Violet Book]
NCSC C-Technical	Computer Viruses: Prevention, Detection, and Treatment Report-001
NCSC C-Technical	Integrity in Automated Information Systems (Sept. 91) Report 79-9 i
NCSC C-Technical	The Design and Evaluation of INFOSEC Systems: The Report 32-92 Computer Security Contribution to the Composition Discussion

4. Department of Defense Publications

NSA/CSS	Media Declassification and Destruction Manual
	Manual 130-2 Contractor Guidelines for AIS Processing of NSA SCI
DoD 5200.28-M	Automated Information System Security Manual
DoD 5200.28	DoD Trusted Computer System Evaluation Criteria
DoD 5220.22-M	National Industrial Security Program Operating Manual
CSC-STD-002-85	DoD Password Management Guidelines [Green Book]
CSC-STD-003-85	Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments [Yellow Book]
CSC-STD-004-85	Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements [Yellow Book]
CSC-STD-005-85	DoD Magnetic Remanence Security Guideline [NSA] Information Systems Security Products and Services Catalogue
NSA/CSS -	Section 5, Degaussing Level Performance Test Procedures Spec. L14-4-A55

5. Director of Central Intelligence Directives

DCID 1/7	Security Controls on the Dissemination of Intelligence Information, [For Official Use Only]
DCID 1/14	Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information [Unclassified]
DCID l/16	Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks [SECRET]
DCID 1/16	Security Manual for Uniform Protection of Intelligence (Supplement) Processed in Automated Information Systems and Networks [SECRET] (Supplement to DCID 1/16)
DCID l/19	DCI Security Policy Manual for SCI Control Systems [UNCLASSIFIED]
DCID 1/20	Security Policy Concerning Travel and Assignment of Personnel With Access to Sensitive Compartmented Information (SCI) [UNCLASSIFIED]
DCID 1/21	Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs) [For Official Use Only]
DCID I /22	Technical Surveillance Countermeasures [CONFIDENTIAL]
DCID 3/14-1	Information Handling Committee [Unclassified]
DCID 3/14-5	Annex B, Intelligence Community Standards for Security Labeling of Removable ADP Storage Media [Unclassified]

6. Legislation, Directive, and Standards

Atomic Energy Act of 1954, as amended

National Security Act of 1947

National Security Decision Directive 298, “Operations Security”

Telephone Security Group standards