

DoD 5220.22-M-Sup 1.



NATIONAL INDUSTRIAL SECURITY PROGRAM

OPERATING
MANUAL
SUPPLEMENT

February 1995



Department of Defense Overprint

to the

NATIONAL INDUSTRIAL SECURITY PROGRAM

OPERATING MANUAL SUPPLEMENT

This document is issued as guidance to all DoD SAPs.

**This document contains information
EXEMPT FROM MANDATORY DISCLOSURE
under the FOIA. Exemption 5 applies. Key lock
protection by authorized personnel required.**

FOR OFFICIAL USE ONLY



POLICY

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D C 20301-2000

January 14, 1998

**Department of Defense National Industrial Security Program Supplement
Overprint**

FOREWORD

In December 1994, the Under Secretary of Defense (Policy) signed the first National Industrial Security Program (NISP) Operating Manual Supplement (NISPOMSUP). The document outlined enhanced security requirements, procedures, and options to the National Industrial Security Program Operating Manual (NISPOM) Baseline for certain types of activities that require protection beyond the Baseline, including:

Acquisition, Intelligence and Operations and Support Special Access Programs (SAPs) and SAP-type compartmented efforts approved by the Executive Branch;

Secret and Top Secret critical Restricted Data (RD); and

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

The NISPOMSUP is an interagency document applicable to the entire Executive Branch -- not just the Department of Defense (DoD). At the time of its publication, DoD Components were authorized to issue separate implementers to refine, explain, and codify the unique requirements of formally established SAPs. With this document, the DoD is issuing a single Overprint for the entire Department. Publishing this NISPOMSUP Overprint represents the culmination of the efforts of industry representatives, the interagency SAP Security Standards Working Group, and the Military Services. It does not add requirements; it clarifies existing ones and provides for uniform implementation of standards across the Department.

The provisions of the NISPOMSUP and this Overprint apply to all DoD agencies, organizations, and contractors participating in the administration or performance of DoD SAPs covered by the NISPOMSUP. It also applies to other Government organizations that, by agreement, operate DoD SAPs. This NISPOMSUP Overprint will not be further supplemented with additional security requirements in security classification or procedures guides, security plans, or similar procedural documents. Individual written OPSEC security measures for specific SAPs may be negotiated.

The Overprint text, shown in bold Arial font, provides information that did not appear in the original NISPOMSUP, but has been added to clarify or explain a given requirement. If doubt exists concerning a specific provision of the document, contractors should consult the Program Security Officer (PSO) to resolve the issue before taking action or expending program-related funds.

To facilitate reciprocity, standards within this Overprint are categorized to be consistent with the three SAP protection levels: Waived, Unacknowledged and Acknowledged. Major NISPOMSUP options in this Overprint are annotated with a "√" for each category to which a particular option applies, changing that option to a standard. These protection standards may be waived through the following procedures:

Waivers "down" to lessen or decrease the SAP standards contained in this NISPOMSUP Overprint must be approved by the appropriate SAP Central Office or designated flag-level

official (e.g., general, admiral, member of the senior executive service (SES) or senior intelligence service (SIS)). Waivers "down" must be registered with the organization's SAP central office during the time the waiver is in force. The Director, DoD SAP Coordination Office (SAPCO) must be notified in writing of the exact content of the waiver.

Waivers "up" to increase or expand individual SAP protective measures must be approved by the DoD SAPCO acting for the SAP Oversight Committee (SAPOC). In an emergency, a flag-level official may authorize a waiver "up." The Director or Deputy Director of the DoD SAPCO must be informed of this action within ten working days. All waivers ("up" and "down"), to include those temporarily imposed, will be reported to the SAPOC during the annual SAP revalidation.

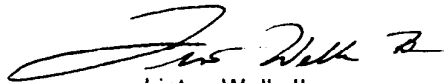
Applying "commensurate protective measures" to a particular SAP means that equivalent protections are being used rather than following the exact wording of the NISPOMSUP Overprint. An example might be using a "commensurate protective measure" for the requirement in 9-201a, which states, in part, that for secure working area walls, "Building materials shall offer penetration resistance to, and evidence of, unauthorized entry... Construction shall meet local building codes." A SAP located in an underground facility chiseled from solid rock may not meet "local building codes;" however, after considering the penetration resistance provided by the rock, a cognizant authority could approve the facility construction as providing protection commensurate with the requirement described in paragraph 9-201a. The use of "commensurate protective measures" is a risk-management decision, which is delegated to Component-level security professionals in the grade of GS-14 or above, or military equivalent.

Appendix F provides formats which are designed for use by SAPs to (1) facilitate standardization under the NISP; (2) eliminate redundant requirements as mandated by E.O. 12829; and (3) standardize procedures as stated in Recommendation # 2 of the Commission on Protecting and Reducing Government Secrecy. These formats should serve as guides until appropriate forms are developed. The formats are not intended to replace forms, which are currently approved under the Paperwork Reduction Act.

Submit comments and suggestions for improvement to

Richard F. Williams, CPP
Director, Special Programs, OUSD(P)
The Pentagon, Room 3C285
Washington, D.C. 20301

Adherence to the standards set forth in this NISPOMSUP Overprint will ensure compliance with national-level policy; serve to implement Recommendation # 2 of the Commission on Protecting and Reducing Government Secrecy; and allow for general and specific reciprocity among and between SAPs of the same sensitivity level. General reciprocity applies if a SAP operates at the full levels of protection of the Overprint. Specific reciprocity allows specifically identified areas of reciprocity for those programs which operate with waivers, or programs which have exercised "commensurate protective measures." Specific reciprocity requires mutual agreement.



Linton Wells II
Deputy to USD(P)
for Policy Support

NISPOM Supplement (NISPOMSUP) Overprint

A key to understanding the Overprint

There are a number of different fonts and typefaces used within the NISPOMSUP Overprint. This page provides a key to understanding the Overprint. If you are not thoroughly familiar with the style and layout of the Overprint, please study the example provided below prior to proceeding. NOTE: As you read the Overprint remember that since the NISPOMSUP was coordinated and approved as an interagency document, all language in the original NISPOMSUP remains unchanged. Also, since the NISPOMSUP is a supplement to the Baseline NISP Operating Manual (NISPOM), any section that has not been supplemented within the Overprint remains governed by Baseline NISPOM requirements.

This example is clipped from a page of the NISPOMSUP Overprint. It illustrates the use of the various fonts and type faces to promote understanding of the requirements in the Overprint. The example also aids in identifying the origin of the specific requirement.

5-201. 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.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

a. The following types of classified information requires accountability (personal signature or other identifiers). This material will be entered into a document accountability system whenever it is received, generated, or...

The use of Times New Roman font indicates that this text came directly from the NISPOMSUP. The ***bold italics*** indicates that all SAPs must comply with the requirement in the text. The standard Times New Roman text following the ***bold italics*** is also verbatim from the NISPOMSUP.

This text block indicates to which level of SAP the NISPOMSUP option applies. It is written in **bold Arial** font to show it has been added to the original language of the NISPOMSUP. This block appears in the Overprint immediately after each identified NISPOMSUP option.

The use of **bold Arial** font indicates that this text was added to the NISPOM Supplement to promote understanding and further explain the requirement.

On the following page is a table listing each NISPOMSUP option, where the option is found in the NISPOMSUP Overprint, and the level of SAP to which the individual option applies.

**SECURITY REQUIREMENTS
MENU OF OPTIONS**

OPTION No.	NISPOM-SUP	OVERPRINT PAGE NO.	TITLE	REMARKS	LEVELS
1.	1-201	1-2-2	Standard Operating Procedures (SOP)	Prepare a comprehensive program SOP	W,U,A
2.	1-202	1-2-3	Badging	PSO approved badging system for program areas	W,U,A
3.	1-204	1-2-4	Two Person Integrity (TPI)	Two Person Integrity with PSO approval	W
4.	1-206.c.	1-2-5	Prime Contractor Representative	Prime contractor may be present and participate in subcontractor reviews	W,U
5.	1-206.e.	1-2-5	Contractor Reviews	Government prescribed contractor review intervals	W,U,A
6.	1-206.f.	1-2-5	Team Reviews	Reviews by more than one PSO with consent of Government and contractor	W,U,A
7.	1-300.e.	1-3-1	Foreign Travel	PSO may require reporting of all travel outside the U.S.; supplemental report may be required.	W,U,A
8.	2-100.a.	2-1-1	Facility Clearance - CSA	Program Executive Agent may carve-in or carve-out CSA	W,U
9.	2-100.c.	2-1-1	Contract Association with CSA	Association may be restricted and classified	W,U
10.	2-201.b.	2-2-1	Program Access Requirements	PSO may authorize access if PR is outside the 5 year scope	W,U,A
11.	2-201.d.	2-2-2	Access Criteria and Evaluation Process	PSQ completion and access evaluation may be required at the activity	W,U,A
12.	2-202.a.	2-2-4	Supplemental Measures and Polygraph	Polygraph may be required for access or interim access pending PR completion	W,U,A
13.	2-205	2-2-5	Agent of the Government	Government may designate a contractor nominated as an Agent of the Government	W,U,A
14.	3-101.b.	3-1-2	Security Training	Professional AIS training may be required of all contractor ISSRs	W,U,A
15.	3-103	3-1-4	Refresher Briefings	PSO may require a record be kept of briefings	W,U,A
16.	4-200	4-2-1	SAP Markings	SAP material will be marked and controlled as specified by the PSO	W,U,A
17.	4-202	4-2-2	Engineer's Notebooks	PSO may impose additional requirements	W,U,A
18.	5-201	5-2-1	Accountability	A separate control system may be required for each SAP	W,U,A
19.	5-202	5-2-2	Annual Inventory	May be required for classified SAP material with a written report of discrepancies	W,U,A
20.	5-203	5-2-2	Collateral Material	May be transferred in or out of a SAP	W,U,A
21.	5-403	5-4-2	Secure Facsimile and/or Electronic Transmission	May be used for SAP as approved by PSO; may require receipting	W,U,A
22.	5-404	5-4-2	U.S. Postal Mailing	Mailing channels may be established as approved by the PSO	W,U,A
23.	5-600	5-6-1	Reproduction	Equipment may require PSO approval; written procedures may be required; PSO approval may be required for TS	W,U,A
24.	5-700	5-7-1	Disposition	CPSOs may be required to inventory, dispose of, request retention, or return for disposition all SAP-related material	W,U,A
25.	5-701	5-7-1	Retention	Contractor may be required to submit a retention request to the CO via the PSO.	W,U,A
26.	5-702	5-7-1	Destruction	Two Person Destruction of classified may be required; non-accountable waste may be destroyed by a single person	W,U,A

**SECURITY REQUIREMENTS
MENU OF OPTIONS**

OPTION No.	NISPOM-SUP	OVERPRINT PAGE NO.	TITLE	REMARKS	LEVELS
27.	5-800	5-8-1	Special Access Program Facility	Contractor may be required to establish approved SAPF prior to commencing work	W,U,A
28.	5-801.f.	5-8-1	SAPF Physical Security	Unique physical security requirements may be established on a case-by-case basis	W,U,A
29.	5-802.a.	5-8-2	SAPF Physical Security Standards	DCID 1/21-like standards may be required for a SAPF	W,U,A
30.	5-802.b.	5-8-2	SAPF Physical Security Standards	NISPOM closed area standards may be applied with DCID 1/21-like STC standards	W,U,A
31.	5-802.c.	5-8-2	SAPF Physical Security Standards	PSO may approve baseline construction as additional option for some areas	W,U,A
32.	5-803	5-8-2	SAP Secure Working Areas	PSO may approve any area with options for providing sound protection	W,U,A
33.	5-804	5-8-2	Temporary SAPF	PSO may accredit a temporary SAPF	W,U,A
34.	5-806.c	5-8-3	Technical Surveillance Countermeasures survey	TSCM may be required for a reinstatement of previously accredited SAPF	W,U,A
35.	5-807	5-8-3	Prohibited Items	Magnetic media entering or leaving SAPF may require PSO approval	W,U,A
36.	6-106	6-1-2	Visitor Record	Separate program visitor record may be required; retention may be required	W,U,A
37.	7-102	7-1-2	Security Agreements	Requirements for subcontracting security requirements agreements	W,U,A
38.	11-301	11-3-1	Independent Research and Development document retention	Contractor may be allowed to retain classified material; sanitization may be required	W,U,A
39.	11-400	11-4-1	Operations Security	Employing OPSEC cover techniques may be required	W,U,A
40.	11-500	11-5-1	Counterintelligence Support	Analysis of foreign intelligence threats and risks to programs	W,U,A
41.	11-501	11-5-1	Countermeasures	Security countermeasures for SAPs may be required	W,U,A
42.	11-700	11-7-1	Close-out of a SAP	Contractor may be required to submit a termination plan	W,U,A
43.	11-701	11-7-1	SAP Secure Communications	Secure communications network and/or data network linking may be used	W,U,A
44.	DCIDs 1-100	1-1-1	DCID-like Standards	Director of Central Intelligence Directives (DCID) may be imposed for SCI within a DoD SAP	W,U,A
45.	DCIDs 1-101	1-1-2	DCID-like standards	DCID-like standards may be applied to a DoD SAP only with SAPOC approval	W,U,A

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. **NOTE: For DoD this is specified in this Overprint.**

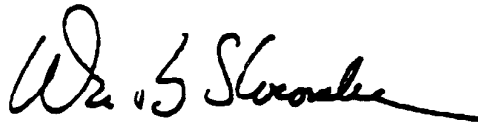
The provisions of this NISPOMSUP apply to all contractors participating in the administration of

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.

A handwritten signature in black ink, appearing to read "W. B. Slocombe", with a long horizontal flourish extending to the right.

Walter B. Slocombe
Under Secretary of Defense
(Policy)

TABLE OF CONTENTS

CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS

	<i>Page</i>
Section 1. Introduction	1-1-1
Section 2. General Requirements	1-2-1
Section 3. Reporting Requirements	1-3-1

CHAPTER 2. SECURITY CLEARANCES

Section 1. Facility Clearances	2-1-1
Section 2. Personnel Clearances and Access.....	2-2-1

CHAPTER 3. SECURITY TRAINING AND BRIEFINGS

Section 1. Security Training and Briefings	3-1-1
--	-------

CHAPTER 4. CLASSIFICATION AND MARKING

Section 1. Classification	4-1-1
Section 2. Marking Requirements	4-2-1

CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION

Section 1. General Safeguarding Requirements	5-1-1
Section 2. Control and Accountability	5-2-1
Section 3. Storage and Storage Equipment	5-3-1
Section 4. Transmission	5-4-1
Section 5. Disclosure	5-5-1
Section 6. Reproduction	5-6-1
Section 7. Disposition and Retention	5-7-1
Section 8. Construction Requirements	5-8-1

CHAPTER 6. VISITS AND MEETINGS

Section 1. Visits	6-1-1
Section 2. Meetings	6-2-1

TABLE OF CONTENTS

CHAPTER 7. SUBCONTRACTING

	<i>Page</i>
Section 1. Prime Contractor Responsibilities	7-1-1

CHAPTER 8. AUTOMATED INFORMATION SYSTEMS

Section 1. Responsibilities	8-1-1
Section 2. Security Modes	8-2-1
Section 3. System Access and Operation	8-3-1
Section 4. Networks	8-4-1
Section 5. Software and Data Files	8-5-1
Section 6. AIS Acquisition, Maintenance, and Release	8-6-1
Section 7. Documentation and Training	8-7-1

CHAPTER 9. RESTRICTED DATA

Section 1. Introduction	9-1-1
Section 2. Secure Working Areas.....	9-2-1
Section 3. Storage Requirements	9-3-1

CHAPTER 10. INTERNATIONAL SECURITY REQUIREMENTS

Section 1. International Security	10-1-1
---	--------

CHAPTER 11. MISCELLANEOUS

Section 1. TEMPEST	11-1-1
Section 2. Government Technical Libraries.....	11-2-1
Section 3. Independent Research and Development	11-3-1
Section 4. Operations Security	11-4-1
Section 5. Counterintelligence (CI) Support.....	11-5-1
Section 6. Decompartmentation, Disposition, and Technology Transfer	11-6-1
Section 7. Other Topics.....	11-7-1

APPENDICES

Appendix A. Definitions	A-1
Appendix B. AIS Acronyms	B-1
Appendix C. AISSP Outline	C-1
Appendix D. AIS Certification and Accreditation	D-1
Appendix E. References	E-1

Appendix F. Special Access Program FormatsF-1
Appendix G Security Documentation Retention G-1

FIGURES

Figure 1. SAP Government and Contractor Relationships1-1-4

TABLES

Table 1. Training Requirements3-1-2
Table 2. Clearing and Sanitization Data Storage8-5-5
Table 3. Sanitizing AIS Components8-5-7

Chapter 1

General Provisions and Requirements

Section 1. Introduction

1-100. 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 Cognizant Security Agency (CSA) as appropriate. See page 1-1-4 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, Agency, 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 may be reflected as an overprint to this Supplement.

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

NOTE: Within DoD, the available options for DoD Waived, Unacknowledged, and Acknowledged DoD SAPs are specified herein as standards (requirements). The material appearing in bold Arial font is DoD implementing language for SAPs. It does not apply to sensitive compartmented information, which is governed by the NISPOM Supplement as implemented by the DCIDs. The DCIDs (e.g., DCID 1-21) will be imposed on the SCI information within a DoD SAP.

1-101. Scope.

a. **The policy and guidance contained herein and imposed by contract is binding upon all persons who are 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):**

1. This document will be applicable to the following SAP activities: all Government offices participating in DoD SAPs, SAPs for which a DoD organization is the Executive Agent, and all

contractor locations performing work on DoD SAPs or SAPs for which the DoD is the Executive Agent. This document is applicable to SAP activities located within the United States, its Trust Territories and Possessions, and at overseas locations.

2. At Government locations, the Government Program Manager (GPM), or equivalent Senior Government Manager, may fulfill the role of the GPM and Contractor Program Manager (CPM) (this applies to government employees conducting the work) as specified in this document. The terminology “activity security officer” and Contractor Program Security Officer (CPSO) shall be applied to the responsible security officer or manager at a Government location.

3. Certain Government and contractor locations supporting multiple SAPs may be assigned a single, cognizant PSO or Security Representative. This single, cognizant PSO shall be responsible for the implementation of policy contained in this document. This responsibility shall include area approval, approval of Standard Operation Procedures, Automated Information System Security Plans (AISSP), approval of individuals selected as Information System Security Representatives (ISSR), and overseeing ISSR activities specified in Chapter 8 of this

document.

- 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 CSA. *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.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

DCID like standards will be applied to DoD SAPs only with SAPOC approval.

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. *All contractor requests for interpretation of this Supplement will be forwarded to the PSO. Within DoD, the PSO will submit all policy interpretations to the cognizant Central Office for review and any action deemed appropriate.*

1-105. Supplement Changes. Users of this Supplement are encouraged to submit recommended changes and comments through their PSO in concurrence with the baseline. **Within DoD, the PSO will forward all change proposals to the Director, Special Programs, OUSD (P) via the cognizant Central Office.**

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.

Use SAP Format 12 to submit waiver requests to these and other security directives in SAPs. Security Officers at all levels maintain a file of approved waivers. Attach maps, photos, or drawings when necessary. Subcontractors submit SAP Format

12 through their prime contractor, who will annotate the REVIEWING OFFICIAL block. The requester ensures adequate compensatory measures are taken for each waiver. Submit completed SAP Format 12 to the PSO, who will process the waiver as provided for in the Foreword to the NISPOM Overprint.

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. **Within DoD, three levels of SAP protection apply. The three levels are:**

- 1. Waived SAP**
- 2. Unacknowledged SAP**
- 3. Acknowledged SAP.**

These SAP levels are further explained in DoD Directive 0-5205.7 and DoD Instruction 0-5205.11.

SAP

Government/Contractor Relationships

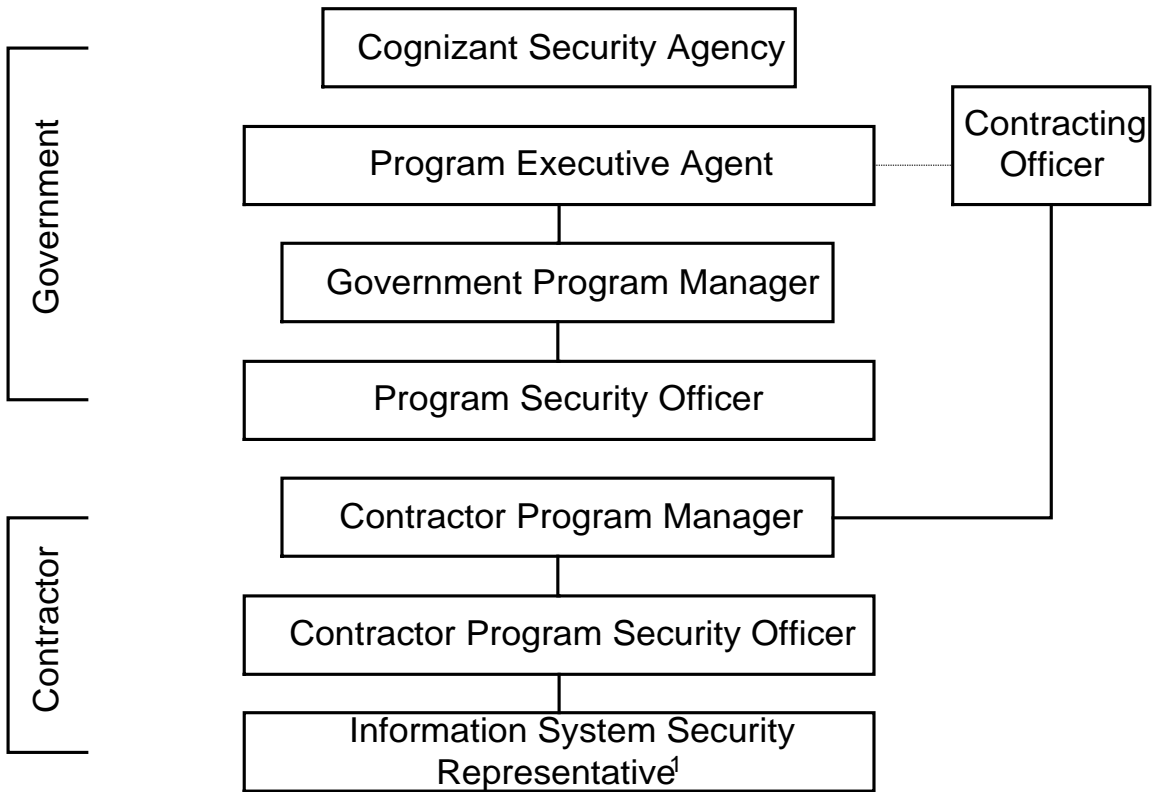


Figure 1

¹ISSR may work for the CPSO, or work as a peer to the CPSO for AIS 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:

Unless circumstances (size and involvement) dictate otherwise, each organization associated with a SAP must designate one or more knowledgeable Security Officers to be responsible for implementing program security policies within its activity. Security Officers must have the position, responsibility, and authority commensurate with the degree of security support required for that organization. The PSO must approve or reject the appointment of all CPSOs.

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, its Supplement, and this Overprint .*
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 (within DoD this is known as EMSEC), Automated Information System (AIS), and Operations Security (OPSEC) are accomplished.*

15. *Establish security training and briefings specifically tailored to the unique requirements of the SAP.*

1-201. *Standard Operating Procedures (SOP). The CPSO may be 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.

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

a. SOPs are similar to Standard Practice Procedures (SPPs) formerly required prior to the National Industrial Security Program (NISP). Prepare SOPs only if revision of the current SPP is required to implement new guidance contained in this or program-specific security directives/guidance.

b. Refrain from including repetitious, word-for-word verbiage from any other security directives. Instead, address the

local and “nuts-and-bolts” implementation of applicable security directives (including the NISPOM, NISPOMSUP, and this Overprint). Care should be taken not to add to requirements in such a way that would increase program costs. The following subjects, as applicable, should be considered for inclusion:

- **Secure communications device instructions.**
- **Annual self-reviews.**
- **Handling classified material (marking, storing, access, working papers, distribution, mailing, hand-carrying, etc.).**
- **Reproduction.**
- **Destruction.**
- **Top Secret control procedures (if applicable).**
- **Safe or vault custodian duties and end-of-day security checks.**
- **Emergency protection.**
- **Entry and exit reviews and briefcase and parcel searches.**
- **Security incidents.**
- **Document control (e.g., accountability of SAP classified material) and audit procedures.**
- **Subcontracting, handling of vendors and consultants.**
- **Personnel selection and program access procedures.**
- **Security organization and**

management.

- Operations security (OPSEC).
- Security education.
- Unique security procedures.

c. Prepare and forward SOPs for specific program activities (i.e., test, transportation, and handling) to the PSO at least 30 days in advance of the planned activity. When the activity occurs frequently or throughout the contract, develop generic or “boiler plate” plans and omit dates and other specifics. Submit dates and plans under separate cover.

d. Automated Information Systems (AISs). Prepare and maintain a computer SOP to implement the security policies contained in Chapter 8. Do not necessarily write a specific SOP for each system. Instead, write a generic SOP and prepare attachments showing unique details for each specific system using SAP Format 16.

e. Contractors are not required to prepare an SOP for pre-solicitation activity (PSA), a Program Research and Development Announcement (PRDA), Request for Information (RFI), or Request for Proposal (RFP) when there is no contractual relationship established for that effort. Classification guidance and special security rules reflected on the DD Form 254 and in the PSG suffice for a SOP. If a formal contract is not executed, one of the following three actions (or

combination of the three actions) will be taken:

- The material will be returned to the Government.

- The material will be destroyed and a copy of the destruction certificate will be forwarded to the Government.

- Documentation will be retained by the contractor. If information is retained, written procedures which establish protective measures, will be in place.

f. Subcontractors are not required to prepare SOPs when all work by that subcontractor is performed at a prime contractor facility. Storage normally is not authorized at the subcontractor location under these circumstances. Keep program access records and other program documentation at the prime contractor facility.

g. Fabrication. Fabrication of program-related classified hardware or models may require a specific security plan. Consult the PSO to determine when security plans are required.

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

WAIVED - ✓

UNACKNOWLEDGED - ✓

ACKNOWLEDGED - ✓

The best form of entry control is

personal introduction and identification. Use this procedure to the maximum extent. Use a badge system unless the program area is small enough (normally less than 25 people) to permit total personal identification and access level determination.

When a badging system is considered necessary, the security officer will document the badge approach in the SOP, addressing topics such as badge accountability, storage, inventory, disposition, destruction, format and use (i.e. magnetic stripes, photographs, biometrics, and so on).

If card readers are used in conjunction with badges and a means exist to lock out lost, unused, and relinquished badges, the PSO may negate the requirements stated above for badge inventory, accountability and destruction.

1-203. Communications Security (COMSEC). *Classified SAP information will be electronically transmitted only by approved secure communications 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.

**WAIVED - ✓
UNACKNOWLEDGED -
ACKNOWLEDGED -**

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.

When required, reports of this type will be routed through a newly created organization established to assist in resolution of disputes: Committee for Special Access Program Process Improvement, c/o Department of the Air Force, The Pentagon, Room 5D972, Washington, D.C. 20330-1720.

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 CSA 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.

Individual SAPs managed by a joint organization (one or more components of the Government or more than one element of the same component) will identify one organization having security review responsibility for each SAPF.

c. **Prime Contractor Representative.** A security representative 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.

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED –

Contractor personnel will not serve as review team chiefs, assign ratings, conduct in/out briefings, or be responsible for completing the security review report.

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.

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

Contractors will conduct self-reviews annually. Normally, conduct this review halfway between Government reviews. Unless the contractor's review reveals a significant security weakness or potential compromise condition, reports of self-reviews need not be submitted to the PSO.

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

WAIVED - √

UNACKNOWLEDGED - √
ACKNOWLEDGED - √

1-208. (Baseline). Government and industry fraud, waste, and abuse (FWA) reporting is encouraged through channels designated by the PSO. Do not use other advertised FWA hotlines when program or SAP information (also refers to SAR information) may be revealed. Therefore, normal FWA reporting channels (e.g., DoD-advertised FWA hotline) must not be used for SAPs and associated SAR marked information.

a. **When requested, confidentiality may be granted. Individuals may be assured that they can report FWA instances without fear of reprisal or unauthorized release of their identity.**

b. **The PSO will provide the name and telephone number for the current FWA manager or monitor and a poster reflecting this information.**

c. **Disclosures received by SAP channels that are deemed inappropriate (e.g., Inspector General (IG) complaints, grievances, suggestions, discrimination complaints), will not be accepted. Instead, the individual making the disclosure will be referred to the appropriate agency or reporting system. Assistance will be provided to ensure that adequate program security is maintained for these referrals.**

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.*

If an NDA is not signed, access will not be granted.

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.

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

Report all foreign travel to the CPSO (preferably within 30 days). (Use SAP Format 6.) The CPSO will maintain a record of foreign travel in the individual's personnel file. Personnel must:

- **Notify the CPSO before travel to any country identified on the National Security Threat List provided by the PSO. This is required so that appropriate defensive travel briefings can be provided. Report travel to all other countries to the CPSO.**

- **CPSOs will ensure that**

personnel are given a foreign travel briefing (required by paragraph 3-107), review the proposed itinerary, and follow-up on security-related issues.

Reporting Foreign Contacts.

Foreign contacts meeting the following criteria must be reported to the CPSOs. The CPSO provides the information to the PSO. Report any of the following:

- **Contact with personnel from foreign diplomatic establishments.**
- **Recurring contact with a non-US citizen when financial ties are established or involved.**
- **A request by anyone for illegal or unauthorized access to classified or controlled information.**
- **Contact with an individual (regardless of nationality) under circumstances that suggest the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.**

f. **Arms Control Treaty Visits.** *The GPM and PSO will be notified in advance of any Arms Control Treaty Visits (see also para 11-704).* 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.* For DoD this applies to component level SAP Central Office as appropriate.

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) may be 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.

1-302. (Baseline). Social Contact Reporting (foreign or otherwise). Report social contact when:

- **The individual is questioned regarding the specifics of his or her job, organization, mission, etc.**
- **Questioning is persistent regarding social obligations, family situations, etc.**
- **Frequent or continuing contact is anticipated (e.g., pen pals, ham operators, INTERNET).**
- **Any unusual incident with a citizen or other entity of any country.**

FOR OFFICIAL USE ONLY

1-3-4

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 CSAs will determine the terms of responsibility for the Facility CSA with regard to SAP programs. Due to the sensitivity of some SAPs, the program shall be carved out by the Executive Agent designated by the CSA.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED -

- 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.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED -

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 information pertaining to the SAP shall be processed for 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.

All briefings and indoctrinations must be accomplished in a SAPF or other working facility (e.g., temporary SAPF as designated by the PSO).

FOR OFFICIAL USE ONLY

2-1-3

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.

Access to SAP information is neither a right nor an entitlement; it is a wholly discretionary security determination granted only to those individuals who meet stringent background and security standards. Program Security Guides will list approved access approval authorities. See the limitation in paragraph 2-201d.

When approved by the PSO, a transfer in status may occur, providing the transfer is to a location where the security procedures do not differ unless approved by the PSO and there is a valid need to know. Grant special access to no one merely by reason of federal service, contracting status, as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

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.

**WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓**

PSOs, whenever possible, will accept the SSBI or a National Agency Check with Local Agencies Check and Credit (NACLCL) of another Federal agency if current within five years. When another Federal agency conducts an individual's Personnel Security Investigation (PSI), the adjudicative authority must review any disqualifying information, including, when available, access denial by another agency and the reasons therefore, before granting special access.

- 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.

Use SAP Format 1, Program Access Request, to request special access.

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.

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

As part of the PAR processing procedure, the CPSO must check local record and file repositories, when available and accessible, before submitting a PAR. The query must reveal the existence of any local adverse information files concerning the nominee.

- 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.

Unless the employee has exercised the privacy option, CPSOs must review employee SF 86 for accuracy and completeness unless the employee seals the information in an envelope. Forward the sealed envelope to the PSO.

- g. Once the PAR package has been completed, the CPSO will forward the candidate's nomination package to the PSO for review:
 1. 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.

SAP access will follow guidelines established by the Security Policy Board and published in DoD 5200.2R with the following clarifications:

- 1. The individual's immediate family or cohabitant(s), must also be U.S. citizens. An exception to this requirement may be granted when a compelling need exists. Submit letters of compelling need to the PSO.**
- 2. Anytime a candidate acquires immediate family members (to include spouse's parents) or other persons to whom he or she is bound by affection or obligation and who are not U.S. citizens, he or she must report it to their security officer. SAP Format 20, Foreign Relative or Associate Interview, will be used to conduct an interview as determined by the PSO.**
- 3. For the purpose of SAP access eligibility determinations, marijuana or any other form of cannabis sativa is considered a "drug" (e.g., as described in DCID 1/14).**
- 4. Adjudication Authorities are established to uniformly apply the adjudication standards in this supplement and to ensure equitable and consistent access decisions that are neither capricious nor arbitrary and that conform to existing statutes and Executive Orders.**

i. Briefings

- 1. Complete a SAP Format 2, Special Access Program Indoctrination Agreement for personnel being accessed. If a program requires a polygraph agreement, also complete SAP Format 2a, Special Access Program Indoctrination Agreement (Polygraph Supplement).**
- 2. Have the individual approved for access sign the nondisclosure (SAP Format 2) and prebriefing (Format 2a if polygraph is authorized for the program) acknowledgment sections before briefing. Then, conduct the program or project briefing and have the individual sign the briefing acknowledgment portion of SAP Format 2. Prepare a new SAP Format 2 (and Format 2a, if appropriate) each time an individual is briefed to a higher level or reindoctrinated after being debriefed. A single SAP Format 2 (and Format 2a, if appropriate) may be executed for subcompartments of the same program, to include access to multiple projects or independent research and development (IRAD).**
- 3. If the program or project requires a polygraph agreement, as approved by the OSD SAPOC, and the individual has previously signed a briefing statement reflecting that he or she was not subject to a random polygraph, the individual must sign a SAP Format 2a, or be exempted by the component SAP Central**

Office. This may be accomplished during annual refresher training (see paragraph 3-103).

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

j. Periodic Reinvestigations (PRs). A current investigation is defined as an investigation not older than five years.

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

1. For outdated PSIs, request a PR when initial access is involved.

When time is of the essence, the ADJUDICATION Authorities and the PSOs are empowered to verbally suspend a person's special access. Unless unusual conditions prevail, written confirmation of the verbal direction is provided to the contractor no later than the close of business on the next working day.

2. Do not place SAP points of contact (POCs), program names, or other program identifiers on the DD Form 1879. Instead annotate these forms in accordance with PSO guidance.

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

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 may be used as an interim basis to grant access until completion of the PR.

Whenever possible, all accessed persons or candidates for access are guaranteed the opportunity to appeal decisions to deny or limit their special access. They may appeal to a higher authority. Denial, revocation, or limitation of a candidate's SAP access is an access decision only and may not be the basis for further unfavorable administrative actions. Such a decision does not reflect on any other aspect of the candidate's loyalty, trustworthiness, or reliability.

**WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √**

In all cases where the polygraph is used for SAP screening purposes, the SAPOC will be notified as part of the annual review process.

The appropriate Adjudication Authority notifies the employer's CPSO of a decision to deny, revoke, warn, or limit its employee's special access. The CPSO, in turn, notifies the employee, who has 30 days from the date of receipt of the letter in which to appeal the decision. He or

b. There are three categories of polygraph:

she must sign the request and provide a mailing address for the written reply.

On appeal, the appropriate Adjudication Authority provides any additional information from the candidate and the rationale behind the decision to the next higher review authority.

The Appeals Board/Authority makes final SAP access determinations. On occasion, overriding national security interests will not allow full disclosure of pertinent information.

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 contractors designated as Agents of the Government.

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

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.*

Submit an updated access list to the Government Program Office semiannually. If there is no change, send a negative report.

2-213. Consultants (Baseline).

a. A consultant is an individual

whose services are retained by a company to provide specialized, professional services to accomplish a specific task. Services are retained through a professional service agreement and/or statement of work between the individual and the sponsoring company.

A consultant to a SAP activity must have the appropriate personnel security clearance on file with the sponsoring company and be approved for Program Access by the GPM and PSO. The consultant will perform classified work at an approved SAPF in accordance with the DD Form 254. In addition, before the consultant can be considered to perform his specialized service, the company sponsoring the consultant must submit to the PSO, a copy of the professional service agreement and/or Statement of Work detailing what specific tasks he/she will be performing. Once consultant status is approved, the consultant's Program Access Request package, which will also include an executed Consultant Security Agreement, can be adjudicated for access to the program. A Consultant Security Agreement can be obtained from the PSO.

Upon access approval, the consultant will be escorted into the SAP area and given a thorough and in-depth security and technical briefing outlining the policies and procedures on how the program facility operates in a Special Access environment.

Any change in the consultant's status, (i.e., he/she is hired by the sponsoring entity to work in their organization or any other deviation to the existing professional services agreement which would negate his/her consultant status), must be reported immediately to the GPM and PSO.

- b. Job Shopper/Temporary Help.
Contact the PSO for further guidance.**

Chapter 3 Security Training and Briefings

Section 1. Security Training and Briefings

3-100. General. *Every Special Access Program (SAP) will have a Security Training and Briefing Program.* As a minimum, SAP-indoctrinated 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:

The security education program applies to all program-accessed individuals. Tailor specific security education programs to the mission and function of the activity. Gear individual training to the current specific job. Table 1 summarizes training requirements

- 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 vulnerabilities.

Ensure that all persons who are responsible for and access computers are aware of proper operational and security-related procedures. Conduct computer security refresher training at least annually (along with, or separately from, other refresher training [paragraph 3-103]).

- 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 accesses.

The CPSO or other security education manager who provides overall management and direction for security education programs. The PSO exercises responsibility for

individual SAP programs. Appointed Security Officers at all levels supervise security education, determine specific training requirements, and provide assistance and guidance as required. Supervisors ensure completion of

required training. The Program Director and other management officials are responsible to implement a security education program and emphasize their support by individual example.

Table 1. Training Requirements

Type	Frequency	Documentation	Remarks
Indoctrination	One Time	SAP Format 2/2a	Gear Toward Job Involved
Specialized	Ongoing	Any Method	Use Any Method
Refresher	Annual	Format 17/Data Base	Mandatory Subjects
Foreign Travel	Event-Driven/Annually	SAP Format 17	Mandatory Subjects
Termination	One Time	SAP Format 2/2a	Mandatory Subjects

(NOTE: other types of training are addressed on a case by case basis.)

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 may be 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:

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

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.

Industrial security education and training materials are frequently developed and issued by the Defense Security Service (DSS), defense contractors, and other Government agencies. Such materials are available by purchase, on loan, or free of charge. All Security Officers are encouraged to obtain, tailor, and use these materials to enhance their security education program. A word of caution: Before use, closely review these materials and ensure that they do not contain guidance that contradicts established SAP procedures. Additionally, use of these materials by themselves does not fully satisfy SAP security education requirements (SAP security education programs must include program-unique and SAP items).

The PSO may distribute SAP-specific materials through each CPSO. Materials include the Security Action Report, posters, FWA items, and counterintelligence items of interest. Retain these materials within approved SAPFs.

Ensure that each individual to be

program accessed understands his or her obligations and responsibilities for security. Include a combination of written and verbal briefings. Use excerpts from the espionage laws and explain the agreement and laws to each individual. Include actions persons may take to defeat Foreign Intelligence Service (FIS) efforts.

If appropriate, design a separate briefing for each level of access, compartment, and project. Include local procedures as well as items from the specific PSD document. If appropriate, cover the potential requirement for a polygraph examination and state that such examination is limited to counterintelligence and counterespionage questions. Brief each individual based on function and specific to the role and function the individual will be accessed. Do not solely use the “read-and-sign” method to satisfy this training requirement.

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:

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

- 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.

This refresher training replaces what used to be called indoctrination training. The name change was made to emphasize that the purpose of this training is to present new and applicable training rather than a reaccomplishment of the indoctrination briefing. There is no need to re-sign the initial briefing statement (SAP Format 2) once it has been initially authenticated. This training should be conducted on a face-to-face basis and must include all non-full-time employees regardless of their work location. Refresher training may be conducted throughout the calendar year or accomplished at one session. Individuals accessed to multiple SAPs need only attend one briefing or training session. If approved by the PSO (or higher authority), similar training conducted by security personnel from other agencies or departments may also satisfy refresher training. Topics to cover include:

- Foreign intelligence

techniques and threat reporting (information that must be reported to the PSO).

- **Discussing program information over unsecured telephones and use of STU IIIs. Ensure that personnel are briefed on the use of STU IIIs before use and annually thereafter. As a minimum, discuss the protection of information transmitted, specific STU III security requirements, STU III security incident identification, and reporting requirements. Pay particular attention to, and expand the training for, personnel who operate fax machines connected to STU IIIs.**

- **Information concerning actual or potential terrorism, terrorist groups, espionage, or sabotage of any U.S. facility, activity, person, or resource.**

- **Adverse affects to national security resulting from unauthorized disclosure.**

- **Derivative classification and marking requirements.**

- **Adverse reporting (Continuing Evaluation of Personnel Program).**

- **Reporting FWA (through SAP channels).**

- **Program vulnerabilities, program threat, and OPSEC.**

- **Computer security (applicable for computer users only), to include computer operating procedures, audit trails, logs, forms, receipts, media protection, use of system, copyright laws, and licensing agreements.**

- **Common security deficiencies discovered during recent security self-reviews; usually, self-reviews or other security reviews identify security weaknesses and are an excellent tool to identify additional training needs.**

- **Other security education topics such as document control, TEMPEST, reproduction, etc., may be included in refresher training.**

Personal Status Changes. During refresher training, give personnel the opportunity to report any previously unreported personal status changes. Optionally, require persons to review their SF Form 86, update as necessary, and authenticate its currency in block 18 on the original form.

NOTE: Pursuant to the training matrix on page 3-1-2, document all security education training and file the documentation in individual's folder. Use SAP Formats 2/2A to document briefings and debriefings. Use SAP Format 17 to record refresher or foreign travel training. If multiple SAPs are involved, a centralized record system may be used. A computer database to reflect training conducted may be substituted for filing training records in individual folders.

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.

Design a formal debriefing program which appropriately addresses the following:

- **How to obtain a release before publishing.**

- **What can and cannot be discussed or placed in resumes and applications for security clearances.**

- **Turning in all holdings.**

- **Applicability of, and penalties for, engaging in espionage.**

- **Who (the POC) to report suspected FIS contacts or any attempt by unauthorized persons to solicit program data. The priority (top to bottom) for reporting this information is as follows:**

- **Servicing SAP Security Officer.**

- **CPSO or member of CPSO's organization.**

- **Nearest FBI office.**

(NOTE: Contact the PSO/CPSO before discussing classified or program information with the FBI).

- **Ensure that appropriate espionage laws and codes are available (as an optional handout) and provide the same on request.**

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 arranged 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 Titles 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 Titles 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/secretcy 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.

Because the CPSO may not be aware of all programs an individual is accessed to, the PSO will notify service counterparts known to have activity at a particular location. The PSO will ensure that the adjudication authority is notified as well when such notification is required.

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.

If an individual refuses to execute a debriefing form, administer an oral debriefing in the presence of a witness and annotate the debriefing form: "ORAL DEBRIEFING CONDUCTED; INDIVIDUAL REFUSED TO SIGN." The briefer and witness

sign beneath the statement attesting to this action. Immediately report this fact to the PSO. The PSO will contact other organizations as required.

- 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.*

- a. **If an individual is not available to complete the debriefing form, send an unclassified debriefing form to the individual via certified mail (return receipt requested) and request that he or she complete the form and return it to the activity.**
- b. **If the individual does not respond or return the completed debriefing form. Follow the procedures in para C.**
- c. **If the whereabouts of the individual cannot be determined in 6 months, administratively debrief the individual by completing a debriefing form, annotating the form with, INDIVIDUAL NOT AVAILABLE; ADMINISTRATIVELY**

DEBRIEFED. The SO (Security Officer) signs the debriefing form and attaches a narrative explanation.

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.

3-107. Foreign Travel. Training is provided to all accessed personnel annually or before travel, whichever is earlier. Include both general and country-specific information and threat advisories, when appropriate. See paragraph 1-300e for additional information on reporting foreign travel and contacts.

a. Recommended Topics.

Depending on destination include:

- **Foreign intelligence techniques, terrorist activities, civil situations, or other hazards to personal safety for the region being visited.**
- **Reporting foreign travel and foreign contacts of significance (information that must be reported to the PSO as listed in paragraph 1-300e).**

- b. **Reciprocity. Individuals accessed to multiple SAPs need only attend one foreign travel briefing.**

3-108. Specialized Training. Training is given periodically throughout the period of time an individual has program access. It is designed for a category of individual job

assignment, (e.g., security specialist, administrative, document handler, engineer). It also may be designed to cover specific items of interest, e.g., review result, new test, or change in program status.

a. Security Officers must develop an aggressive, on-going security education program. Conduct this training when special events are scheduled.

b. Provide a defensive briefing on elicitation techniques used by FIS to persons attending international conferences and symposia, regardless of location. On their return, provide the PSO a report when FIS contact was made or suspected. Information in this briefing is normally provided by the Government.

c. Brief couriers as specified in paragraph 5-402b.

Chapter 4 Classification and Markings

Section 1. Classification

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

4-100. Program Directors (PDs) and Contractor Program managers (CPMs) share responsibility for accuracy, currency, and necessity of classifications applied to documents and material.

4-101. Program Classification. See each Program or Project Security Classification Guide (PSCG) for program specific, operational and technical security classification guidance.

4-102. Nicknames, Codewords, and other Identifiers (See Appendix A for definitions).

- a. Coordinate and request nicknames and project names through the PSO.
- b. Request a change of nicknames, codewords, and other program identifiers immediately when compromised or suspected of compromise.
- c. There is no established timeframe to change program

identifiers. After continuous use, however, they become synonymous with the program. This defeats their purpose and they become ineffective from an OPSEC viewpoint. The PD or PSO makes this determination and requests a nickname or codeword change through the Security Director.

- d. Codewords will be used within program channels by properly indoctrinated personnel. The use of a codeword, its meaning, and classification guidance must be placed in the program security classification guide.

4-103. DD Form 254 Requirements.

- a. Prepare DD Form 254, DoD Contract Security Classification Specification, for each contractor, subcontractor, or consultant. Use DD Form 254 to transmit the PSCG, Program Security Guide (PSG), and other documents containing security classification guidance.
- b. The contractor will maintain a current listing of the location of containers, rooms, and completely dedicated buildings that contain SAP materials and are carved out

from DSS cognizance. Provide this list to the PSO, who will include this information in the program data base.

- c. Do not attach lengthy attachments to DD Forms 254 that merely repeat information, policy, and procedures contained in any other security directive (e.g., TEMPEST policy).

- d. The PSO will prepare and forward to the Contracting Officer an approved DD Form 254 for each prime contract. For subcontracts, the prime CPSO will prepare a proposed DD Form 254 and forward it to the PSO for approval before release to subcontractors.

- e. The PSO provides detailed guidance pertaining to DD Forms 254 on classification, release to the DSS, carve-out status, etc. This guidance is based on the specific PSCG.

FOR OFFICIAL USE ONLY

4-1-2

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.*

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

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.

a. All program-classified documents, media, and materials will contain the following markings on the top and bottom of each page:

SECRET/CODEWORD or NICKNAME or SPECIAL ACCESS REQUIRED

b. Government Original Classification: The Original Classification Authority has four choices for determining the declassification date. That date depends on the sensitivity of the information involved. A date or event that does not exceed 10 years; example: completion of a test.

Ten years from the date of the original decision (not the date the document was originated); this date does not change; example: budget information.

Extension of a 10 year classification; example: technology remains unknown to other nations, X(1-8).

Information is exempt from automatic declassification; example: Top Secret RCS Data Normally 25X(1-9) (not a date) would appear on the declassification line.

Classified By: (Name of the person {a designated Original Classification Authority} signing the guide or document).

Reason: E.O. 12958 Section 1.5a,c,e,g,d.

Declassify On: Specific Date or Event, 10-Year Date, X-3 (see EO 12958, Section 1.6(a)), or 25X-4 (see EO 12958, Section 3.4 (b)).

c. Government/Contractor Derivative Classification.

1. For derived classification (single source):

Derived From: SRPSCG, 1 Oct 95

2. Declassify On: (Varies-See examples in paragraph b). If multiple sources are used, show "Multiple Sources" on the classification line and show the longest duration of any of the sources on the declassification line.

Derived From: Multiple Sources (list each source on originator's file copy).

Declassify On: (longest period of any source).

d. Unless the classification is based on a compilation of information, portion markings are required for each document. Identify classified as well as unclassified paragraphs. Mark SAP classified paragraphs with the classification abbreviations.

e. When marking documents containing a specific SAP's information, the following paragraph or portion markings are required: (a) The classification of the paragraph, (i.e. CONFIDENTIAL, SECRET or TOP SECRET), and (b) an appropriate program identifier. For example: S/ABC or C/SE. For information involving multiple programs, include all applicable di/trigraphs.

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.

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

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 classification 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 WORKING HOURS OR (area code) (number) (PSO/CPSO) AFTER WORKING HOURS.

The protective marking Handle Via Special Access Channels Only (HVSACO) may be imposed by the PSO to identify information which must remain in SAP controlled protective channels. See Appendix A for a detailed definition. When applicable, a separate procedural document is issued by the services which explains control, dissemination, transmission, etc., of HVSACO.

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. **DoD will strive for consistent applications of physical security safeguards.**

FOR OFFICIAL USE ONLY

5-1-2

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.*

5-201. 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.

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

a. The following types of classified information requires accountability (personal signature or other identifiers). This material will be entered into a document accountability system whenever it is received, generated, or dispatched, either internal or external to the command or contractor.

1. All TOP SECRET information requires accountability. Assign a document control number and specific copy number to each Top Secret document generated in, received by or dispatched from the SAPF.

2. Maintain a disclosure (access) record for each Top Secret document maintained in the SAPF. Use a cover sheet and attach it to each TOP SECRET document. Record the identity of persons given access to the information and the date of

disclosure on the cover sheet. Record the name only once regardless of the number of times subsequent access occurs.

3. All COMSEC material will be accounted for in accordance with published COMSEC guidelines.

4. Vendor software shall be accounted for in accordance with paragraph 8-500.

5. At the direction of the CSA, full accountability may be required for SECRET/SAR material.

b. (NOTE: refers to NISPOM Baseline.) Unless otherwise stipulated by the CSA, only receipt and dispatch records are required for Confidential and Secret SAP material (individual receipting is not required). The SO will establish a dedicated document log, classified at the appropriate level, for record dispatch and receipt transactions involving SAP classified documents. Although document titles may be unclassified, the compilation of information may require the document log to be classified. Consult the program classification guide and the PSO for guidance. Refer to paragraph 5-202 of the NISPOM baseline for further information on the receipt and dispatch log.

c. To minimize proliferation of multiple document logs and accountability systems in the SAPF, the SO may elect to log all Confidential and Secret SAR receipt and dispatch transitions in the Top Secret document accountability system rather than create separate documents logs.

(classified and unclassified) is adequately protected to avert the unauthorized use, duplication or removal of the media. The media must be secured in limited access containers or labeled with the identity of the individual responsible for maintaining the material.

d. The accountability system will require individual responsibility for all TOP SECRET information, COMSEC material, and vendor software in the SAPF. It will be approved by the PSO prior to implementation. The document accountability system will be able to produce a Master Document Listing that reflects all transactions within 30 day of generation, receipt, or dispatch. If an automated system is used, a backup duplicate record (manual or automated) will be retained to permit recall in even of loss (system crash).

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.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

e. Specific format, retention requirements, and disposition instructions for custodial logs will be incorporated in the agency and contractor's SOP. After PSO approval, the control log will be maintained in accordance with the SOP.

If specifically instructed by the PSO, a 100-percent annual inventory will be conducted for Top Secret material. If the CSA approves accountability requirements for other levels of classified material, the PSO may specify the frequency of inventories.

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.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

f. AIS Media Control System. A system of procedures, approved by the PSO, which provides controls over use, possession, and movement of magnetic media in SAPFs. These procedures must insure all magnetic media

5-204. TOP SECRET/SAR WORKING PAPERS ACCOUNTABILITY, MARKING AND DESTRUCTION.

a. TOP SECRET/SAR working papers may be created for short-term material development within the SAPF.

b. TOP SECRET/SAR working papers shall be properly classified, program marked and protected in an approved SAPF. Attach a cover sheet and plainly mark the date of origin and annotate "WORKING PAPER" on the cover sheet.

c. TOP SECRET/SAR working papers shall either be entered into the accountability system or destroyed within 30 calendar days from the date of origin or as stipulated in other Defense directives. Thereafter, the document must be assigned a document accountability number and copy designation. It will be formally entered into the accountability system.

d. A TOP SECRET/SAR working paper will be reconfigured to display the appropriate document accountability and copy designation and all applicable cover, page, paragraph, portion markings, and declassification instructions prior to removal from the SAPF.

5-205. Secret Working Papers.

a. If the CSA established accountability requirement for program SECRET/SAP material, then the instructions in 5-204 shall apply to all SECRET/SAP working

papers and 5-206 Working Notebooks.

5-206. Top Secret Working Notebooks. Working notebooks are authorized only as a special category of working papers for which the retention limitation does not apply.

a. Consider only materials that undergo frequent change and revision in this category. Do not include in these notebooks verbatim drafts of final correspondence or other materials that transition from notes to draft to formal documentation.

b. Working notebooks (loose-leaf) are exempt from normal document accountability for each page or document within the notebook. Instead, assign and control the notebook as one document. A table of contents is required to ensure completeness.

c. Before using bound notebooks, prenumber each page consecutively and place the notebook document control number on each page. Do not remove pages from these notebooks. As an optional method to a bound notebook, three ring or loose-leaf binders can be used.

d. Mark the outer cover or first page with the highest anticipated classification. Date entries when they are created. Mark each page with the highest classification contained therein, but portion marking is not required.

e. Do not reproduce working notebooks or transfer material from a notebook to any location unless the material is entered into formal document accountability.

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.*

Establish a focal point to oversee transmission of program material. Use the following order of precedence:

- **Cryptographic communications systems (secure fax/AIS).**
- **Courier (PSO approval required for commercial courier).**
- **United States Postal Service (USPS) registered mail (return receipt requested); limit to S/SAP and below materials.**

(Baseline) Hardware. Before any hardware movement of program assets, develop a transportation plan and obtain the PSO's approval. Develop the plan early in the program development to facilitate required coordination between various entities. Appoint a program-accessed individual, knowledgeable about program security requirements, to serve as the focal point for transportation issues. Ensure that the planning includes priority of transportation modes (Government surface/air, commercial surface/air) and inventory of classified hardware to ensure program integrity. Also, make sure that transportation methods maintain a continuous chain of custody between the origination and destination, and comply with all

Department of Transportation laws and PSGs.

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

Do not include or require a receipt (other than the receipt and dispatch records) for Secret/Confidential/SAP or Unclassified HVSAO material. Include a listing of materials contained in the package which the recipient will acknowledge. Do not normally classify receipts. Show an unclassified address on the TO and FROM blocks. Classify material only when the compilation of subjects requires classification. Security Officers make these determinations based on their judgment.

When a receipt or acknowledgment is not returned within 30 days, immediately initiate tracer action. Reproduce a copy of the receipt held in suspense control files; mark it TRACER – ORIGINAL RECEIPT NOT RECEIVED – PLEASE RESPOND WITHIN 7 DAYS. Send the receipt to the intended recipient of the initial transmission. If the recipient does not respond within 15 days or did not receive the material, initiate a preliminary inquiry.

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.*

The PSO must approve transmission of TOP SECRET/SAP information aboard commercial aircraft.

- a. Prepare a courier authorization letter in accordance with Section 5-411.c of the NISPOM and brief in accordance with Appendix F. Brief couriers and then obtain the couriers' signatures acknowledging the briefing. Brief frequent couriers initially and annually thereafter. Debrief couriers on their return when problems are encountered or reported.
- b. Unless a single courier is approved by the PSO, a two-person courier team is required for Top Secret/SAP. A single-person courier can be used for Secret/SAP and below materials. Provisions shall be made for additional couriers and/or access to approved security containers for overnight storage when it appears continuous vigilance over the material cannot be sustained.

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 have been accomplished. For TOP SECRET documents a receipt on the secure facsimile may be required by the PSO.

WAIVED - ✓

UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

The following additional rules apply to secure facsimile transmission:

- a. Do not use facsimile terminals equipped with an automatic polling function.
- b. Establish voice contact with the recipient before sending Top Secret messages (sent via secure fax). Ensure that the Secure Telephone Unit (STU) III indicates Top Secret. Obtain a receipt at the time of transmission and include a date, copy number, subject, and signature of the recipient (communications operator). The communications operator will in turn obtain a written receipt on delivery to the intended office shown in the address element. The fax cover page (transmittal sheet) can be used for this purpose.

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.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

Use U.S. Postal Service certified mail for CONFIDENTIAL/SAR. "For Official Use Only" and unclassified HVSACO material may go by First Class mail. P.O. Boxes should be used only with prior approval of the PSO.

- a. Except for TS, USPS Express Mail can be used for overnight

transmission.

b. Use only currently approved U.S. Government contract commercial carrier.

c. These means of transmitting selected special access materials is in addition to, not a replacement for, other transmission means previously approved for such material. Secure facsimile remains the preferred method of transmission.

d. Use overnight delivery only when:

- Approved by the PSO.
- It is necessary to meet program requirements.
- It is essential to mission accomplishment.
- Time is of the essence, negating other approved methods of transmission.
- Government program management considers this method to be cost-effective.

e. Packages must meet the carrier's size and weight limitations or other similar restrictions.

f. Use the wrapping, addressing, and receipting procedures previously prescribed in paragraph 5-401 and approved contract security annexes. The commercial express carrier envelope is not considered the second envelope

for double-wrapping; hence, the carrier envelope becomes the third wrap. Check with the PSO to obtain the proper address and specific shipping instructions prior to use.

g. To ensure direct delivery to address provided by the PSO:

1. Do not execute the Waiver of Signature and Indemnity on U.S.P.S. Label.
2. Do not execute the release portion on commercial carrier forms.
3. Ensure an appropriate recipient s designated and available to receive material.
4. Do not disclose to the express service carrier that the package contains classified material.

h. When using an U.S. Government-approved contract carrier, ship packages only on Monday through Thursday to ensure that the carrier does not retain a classified package over a weekend.

i. Immediately report any problem, misdelivery, loss, or other security incident encountered with this transmission means to the PSO.

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.*

5-407. (Baseline). Do not remove program materials (classified or unclassified) from a SAPF without the PSO's/CPSO's approval. Within a facility or installation, transport program materials in envelopes contained within an outer container (briefcase, pouch, etc.). Place only the identity of the unclassified program or project office and the "national defense" label on the inner container. When transporting Top Secret materials, call ahead to the recipient's office, providing the name of the courier and estimated arrival time. On arrival, call the departure office to confirm the material's safe arrival.

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.

concepts, special management functions and techniques, and relationships with non-DoD activities remain classified, requiring special access authorization. The PSO controls disposition and access to historical material.

Do not release information concerning programs or technology to any non-program-accessed individual, firm, agency, or Government activity without the Security Director's or PSO's approval. Do not include information concerning SAPs in general or unclassified publications, technical review documents, or marketing literature. Submit all material proposed for release to the GPM or PSO 60 days before the proposed release date. After an approval is received for public release, additional case-by-case requests to release identical data are not required.

NOTE: Public release of information includes any form of, or anything related to, program information, items, or technology-classified or unclassified.

Submit any program information intended for discussion at symposia, seminars, conferences, or other form of non-program meeting to the GPM or PSO for review and approval 60 days before intended attendance and release.

Program history, system technological advances, operational

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.

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED -√

Post a notice indicating if equipment can or cannot be used for reproduction of classified material.

Reproduction of SAP material is to be restricted to authorized machines located within a SAPF.

Locate reproduction equipment (classified and unclassified) in program areas. Machines should be under routine surveillance by the personnel who are responsible for enforcing rules. Ideally, position reproduction equipment within document control workstations to assure immediate and positive accountability.

5-601. The PSO will approve reproduction of TS material in DoD.

FOR OFFICIAL USE ONLY

5-6-2

Section 7. Disposition and Retention

5-700. Disposition. 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.*

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

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.*

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

See Appendix G for guidance on retaining security documentation.

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.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

The destruction of accountable classified material must be conducted by at least two program-accessed individuals. See Chapter 8 for special destruction procedures involving computer media.

Classified Materials, Manufacturing Waste, and By Products. Where applicable, security provisions will be established to securely dispose of materials (e.g. Radar Absorbing Materials (RAM) and Radar Absorbing Structures (RAS)), waste, and manufacturing by products which provide a material signature of classified elements of a SAP. Procedures will be coordinated with the PSO.

5-703. The PSO must review and approve all destruction procedures. If materials are removed from a SAPF for destruction at a central activity, ensure that materials are destroyed the same day they are removed.

5-704. (Baseline). Destroy all classified waste as soon as possible, but do not allow materials to accumulate beyond 30 days. Apply this concept to all waste material containing classified information, such as preliminary drafts, carbon sheets, carbon ribbons, plates, stencils, and masters. Safeguard typewriter and computer equipment

ribbons used in transcribing classified material in the manner appropriate for the classification category involved. Mark this material PROTECT AS (enter appropriate classification). Consider all material, including unclassified, generated in program areas as classified waste and destroy accordingly. Contact the PSO for instructions and approval for disposal of waste products generated by laser and color output devices (e.g., laser printers, cartridges, film ribbons, and magnetic storage units).

5-707. (Baseline). Prepare certificates of destruction itemizing each accountable document (including computer media) or material destroyed and cite the appropriate document control or copy number. Destruction certificates must be completed and signed by both of the individuals completing the destruction immediately after destruction is completed. Show the date of destruction on document control logs.

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. *Memoranda of Agreement (MOA) are required prior to allowing SAPs with different CSAs to share a SAPF.*

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

All organizations must store SAP material in approved SAPFs. Update the accreditation checklist on completion of construction or when changes to physical security safeguards are planned. Before constructing a SAPF, prepare an accreditation checklist according to DCID 1/21, forward it to the PSO, and obtain the PSO's approval. Do not modify facilities (change physical security safeguards) without first obtaining the PSO's approval.

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 affect the physical safeguarding capability of the facility.*

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

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

When multicompartments within the same facility are present, ensure that sound-attenuation requirements, if appropriate, are met.

- 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.)*

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

- 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:

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

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 is 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.

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

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

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

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.

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

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

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

5-805. 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.

Provide verification of the previous accreditation and obtain the PSO's approval before introducing SAP material into an area.

- 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) may be required.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

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.

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

- a. **The following items do not pose a threat to a SAPF and can be taken into and out of a SAPF without approval:**

- **Hearing aids, heart pacemakers, and motorized wheelchairs.**
- **Amplified telephone handset and teletypewriters (when used by the hearing impaired).**
- **Audio and video equipment with no record capability.**
- **Compact disk players.**
- **Televisions and AM/FM radios.**
- **Receive-only (tone-only) beepers.**
- **Receive-only (voice) pagers.**

b. The following items may not be introduced into a SAPF:

- **Personally-owned computers and associated media.**
- **Personally-owned photographic, video and audio recording equipment.**
- **Two-way audio RF (e.g. two-way radios and cellular phones) transmitting devices that are government or company owned for program use can be authorized by the PSO (see NOTE below).**
- **Cameras and film, unless specifically approved by the PSO for a program mission requirement, (e.g., badge issuance or documenting test results).**
- **Other emanating and reproducing devices identified by the PSO.**

NOTE: Two-way audio RF transmitting devices can be authorized by the PSO when required for operational necessity.

c. See Chapter 8 for additional computer type items that are not permitted in SAPFs.

d. In exceptional circumstances, when necessary for a specific activity or threat, program manager or SO may apply more stringent requirements. Such requirements must be reported to the SAP Central Office.

e. Personally-owned equipment

brought into a SAPF is subject to inspection at any time. Any device removed from a SAPF also may be subjected to an inspection.

f. Allow emergency response forces such as guard forces and fire department personnel, as well as their two-way communications equipment, immediate access to SAPFs. Debrief these personnel when appropriate and execute a SAP Format 5, Inadvertent Disclosure Statement.

Chapter 6 Visits and Meetings

Section 1. Visits

6-100. General. *A visit certification request for all Program visits will be 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.

Continuously escort and closely control movement of non-program-accessed visitors who require access to a program area for any purpose. Use only program-accessed personnel as escorts.

- a. Establish and maintain adequate controls to ensure that program visitors are kept within the framework of the "need to know" requirement and that information discussed or furnished is within the visitor's level of access.
- b. Consider installing an internal warning system to warn accessed occupants of the presence of uncleared personnel. Employ other or additional methods (e.g., verbal warnings) to warn or remind personnel of the presence of uncleared personnel.

6-101. Visit Request Procedures. *All visit*

requests will be sent only via approved channels. In addition to the NISPOM, the following 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 information is correct.*

d. The PSO and personnel approved by the PSO may visit all program facilities, without furnishing advanced notification. Deny access and notify the CPSO or PSO whenever any visitor arrives at a Government or contractor facility unannounced.

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. Visit 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. Arrangement 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. *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 record. *This record will be maintained inside the SAPF, and retention may be required.*

WAIVED - ✓
UNACKNOWLEDGED - ✓
ACKNOWLEDGED - ✓

Maintain a visitor sign-in and sign-out record for all accessed program visitors. Show the visitor's name, SSN, organization or firm, date, time in and out, and sponsor on the log. When necessary to protect a SAP, maintain a separate record for uncleared visitors that shows the escort official instead of the sponsor.

Section 2. Meetings

6-200. Conduct meetings and conferences where program information is discussed only in approved SAPFs. PSOs may authorize additional locations.

6-201. Appoint a person to ensure that adequate security is provided.

6-202. Establish entry control and perimeter area surveillance when needed. When authorized, request a Technical Surveillance Countermeasures (TSCM) survey for unsecure conference rooms when SAP information is to be discussed.

NOTE: Use SAP Format 8 to request the TSCM.

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. *All 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.

When a subcontractor is identified who does not have a facility clearance, the PSO will initiate the necessary paperwork through program channels and coordinate

with DSS to initiate action to provide the subcontractor a facility clearance.

7-102. Security Agreements and Briefings.

In the pre-contract phase, the prime contractor will 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.
- l. 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.

shall be tailored to be consistent with the proposed support being sought. The DD Form 254 may be classified based on the information contained therein.

7-103. Transmitting Security Requirements. *Contract Security Classifications Specifications (DD254) prepared by the prime contractor will coordinate with the GPM/PSO and contracting officer prior to transmitting to the subcontractor. The DD254 prepared by the prime contractor will be forwarded to the GPM/PSO and contracting officer for coordination and signature.*

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

Prior to initiating contact with a prospective vendor or subcontractor, the CPSO will complete a SAP Format 13, Subcontractor/Supplier Data Sheet, for submission to the PSO. The CPSO will include the reason for considering a vendor and attach a proposed DD Form 254 to the SAP Format 13. The DD Form 254

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.

Requirements specified in this chapter apply to all AISs in SAP areas regardless of the classification level being processed on individual systems.

- 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.

Personally owned computers will not be introduced into SAP areas.

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 establishing and maintaining 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.

This notification of abnormal occurrences will be made within 72 hours. When a network is involved, the notification must be made within 12 hours.

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

2. Configuration Management. Participate in the configuration management process.

3. 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 Table 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.

6. With the approval of the PSO, the ISSR may delegate special approval authority to an alternate(s).

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:

Existing corporate configuration management programs may be used, provided control and documentation are adequate to meet the requirements of this chapter. Use SAP format 16 to aid in documentation and registration of word processing or personal computer data.

- (a) Hardware components (data retentive only).
- (b) Connectivity. (external and internal).
- (c) Firmware. Firmware will be tracked only when related to a demonstrated security deficiency or control feature.
- (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.

User statements will be accomplished and maintained in accordance with paragraph 8-700c.

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:

One Certification Report may be applicable to multiple AISs provided all variations of configuration and operation are reviewed and verified.

- (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; under 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.

An accreditation may apply to multiple stand-alone AISs, provided all variations of configuration and operation are reviewed and verified.

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

Interim approval will be granted for TS/SAR processing only when a critical mission requirement can be demonstrated.

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.

An MOA is recommended whenever an AIS is interfaced or networked between two or more providers (contractors).

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.

Such delegations of approval

authority are based on the PSO's assessment that an individual ISSR is qualified to make approval decisions on behalf of the PSO in the provider's facility.

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.

AIS security reviews will be scheduled as part of the general security review for the entire SAP.

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.

Compartmented and multi-level modes of operation are not normally approved for SAPs unless a unique

mission requirement justifies the additional risk inherent in such configurations.

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.

Audit records as specified by the PSO will be maintained for dedicated mode systems.

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, communications 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.

Automated audit trails will be used to the maximum extent possible. Where not available or where cost-prohibitive, the PSO may approve the use of manual logs.

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 all 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.

Time lockout must be activated after a maximum of 30 minutes of user inactivity and must automatically log the user out of the system. Software such as screen locks or “pause” functions must create audit entries to show initiation and termination.

(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.

NOTE: Certain categories of system-initiated events create this type of activity independent of any user actions. Such events need not be logged. Because such actions can be unique to specific systems, the PSO and ISSR will agree on items to be tracked and the AISSP will reflect the required audits.

(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 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.

NOTE: Compartmented security mode is not normally authorized for SAP activities. Exceptions may be made by the PSO.

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.

1. 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 audible 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 nonconcur circumvention 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-to-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.

Random password generation techniques will be used where available. When user-generated passwords are used, passwords must be constructed to resist “dictionary”-based attacks. The specific structure will be defined in the AISSP.

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 suspected 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.

Group log-on passwords will not be used as the primary method of authentication.

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.

Unencrypted modems are not normally authorized for use in a PSO SAPF. Exceptions may be approved by the PSO.

- e. **User Warning Notice.** The Customer may require log-on warning banners be installed. When technically feasible, the official DoD warning banner will be used on all AIS processing special access information.

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.

The ISSR must develop, implement, and monitor procedures that verify prior mode termination is properly performed in accordance with the PSO approved AISSP and that no other previously processed data remain active on the AIS.

- 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.

Logical disconnects may be approved by the PSO for TS/SAR when justified. Requests for use

must describe the equipment to be used and the procedures for use, and must describe the maximum possible extent of a contamination in the event of a failure. Logical disconnects for S/SAR and below may be employed, provided the procedures for use are clearly described in the AISSP.

- 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 (I/O) 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 electrically) 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 Table 3.

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:

Unclassified AIS must be approved by the PSO. Procedures for using unclassified AISs will be identical to those specified in the AISSP for classified processing unless they are specifically exempted by the PSO.

1. 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:

Unclassified portable AIS pose an extreme risk and will not be

introduced into an SAPF unless a specific mission requirement exists and prior approval is granted by the PSO.

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.

Personally owned portable AIS devices are prohibited in SAPFs. The ISSR will develop a plan for the management and control of personally owned calculators.

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. **Examples of audit logs and records will be attached to the AISSP as appendices for approval by the PSO.**
- 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 properly 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 weekly.

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.

Audit records will be maintained for 12 months. Printed copies need not be maintained when other storage options are available.

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 AISs 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 networks. 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 MOAs 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.

The interconnection of previously-accredited systems into an accredited network will require a reexamination of the AIS security features, and an update to the AISSP and submission to the PSO for approval.

- (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 Security Mode or higher. This monitoring may also include real-time 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.

Transaction records will be maintained for information electronically-transferred between different provider facilities or between a provider and the PSO when the transaction occurs between AISs that are not part of the same unified network (e.g., stand-alone computers with STU III data transfer capability). Logs and procedures for use will be described in the AISSP. Transfer records for C/SAP or unclassified information are not required.

FOR OFFICIAL USE ONLY

8-4-4

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.

The PSO will be notified of additions or changes to the software listed in the AISSP. Updated versions of the AISSP will reflect these changes. The ISSR will implement a procedure to ensure that all software introduced into the SAPF will be controlled and reviewed before use.

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 multi-level 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.

The ISSR will develop and implement specialized procedures for controlling magnetic media such as vendor software. The procedures will address storage, marking, classification, unauthorized copying, creation of working disks, etc., and be included in the AISSP.

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. Software 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 be removed from a SAPF for return to a vendor. When possible, software will be tested prior to its introduction into the secure facility.

Vendor software acquired before

implementation of a control program as described in paragraph 8-500b will not be released until a 100-percent review of the media is accomplished.

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.

Vendor-supplied maintenance software is a special category of software that requires additional protections. After it is introduced into a SAPF, this type of software will not be released. Handling procedures, such as use of classified working copies and write-protection features, will be developed by the ISSR and approved by PSO.

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 controlled 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.

The ISSR must develop and implement procedures for the control of data storage media that demonstrate a reasonable capability to protect the PSO's data from loss, alteration, or unauthorized disclosure. Given the ease and speed with which classified information can be copied to unclassified or unmarked media, these procedures must encompass all magnetic media in the SAPF. The procedures will be described in the AISSP.

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.

Identifying information will include data that can identify the individual responsible for the media. Removable media will be labeled on removal from the 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.

Flexible magnetic media will normally be destroyed instead of being downgraded or declassified. The PSO will evaluate requests on a case-by-case basis.

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 will 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 2.)

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

The sanitization, declassification, and release of media used to process program information may only be authorized on a case-by-case basis by the PSO and GPM. Various risk factors, such as the sensitivity and volume of the data, will be evaluated. If the PSO and GPM determine the information contained on the media is, or was, too sensitive to risk any possibility of exposure to unauthorized personnel, the media in question will be retained under SAP classification control or destroyed. Only customer-approved equipment and software may be used to overwrite and degauss magnetic media. These products will be tested to assure correct operation before each use, either by inspection or by built-in test devices. These products will be operated in accordance with the operating manual supplied by the manufacturer.

1. Overwriting Media. Overwriting is a software procedure that replaces the data previously stored on magnetic storage media with a predefined 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 II degaussers are used to degauss Type II magnetic media (i.e., media whose coercivity is no greater than 750 Oe). Currently there are no degaussers that can effectively degauss all Type III 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 NSA's *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 3D*.

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 3 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 2
Clearing and Sanitization Data Storage**

Type Media	Clear	Sanitize
(a) Magnetic Tape		
Type I	a or b	a, b, or destroy
Type II	a or b	b or destroy
Type III	a or b	Destroy
(b) Magnetic Disk Packs		
Type I		a, b, or c
Type II		b or c
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 3
Sanitizing AIS Components**

TYPE	PROCEDURE
Magnetic Bubble Memory	a, b, or c
Magnetic Core Memory	a, b, or d
Magnetic Plated Wire	d or 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 (FEPRM)	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

8-600. 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.

The AISSP will include procedures for the release and return of AIS components.

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 micro-coded 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.

Maintenance software for systems with fixed disks or other devices that make sanitizing unfeasible will be classified at the level of the system and brought into control.

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 3). 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 must 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 3. 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.

All nonvolatile memory components will require the ISSR to coordinate with the PSO in advance to determine the releasability.

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 security 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 IDs, 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 AIS 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.

The ISSR will maintain a record of topics presented and names of personnel receiving the training.

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.

SAPs that use Critical Secret/RD/FRD and Top Secret/RD/FRD material will protect those data in accordance with this chapter and any MOA or MOU established with the RD/FRD-cognizant security agency.

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.*

FOR OFFICIAL USE ONLY

9-1-4

Section 2. Secure Working Areas

9-200. Secure Working Areas.

- a. **General.** When not placed in approved storage, Critical SRD 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 door jambs shall provide the necessary barrier delay rating required 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 louvers, baffle plates, or astragals, when used, shall be reinforced and immovable from outside the area being protected.*

ings in uncontrolled adjacent buildings; or located 6 feet (1.83 m) from uncontrolled openings in the same barrier.

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 open-*

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.

- c. *In a steel filing cabinet, not meeting General Services Administration requirements, but approved for use prior to the date of this*

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.*

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-110 "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.

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).*

Chapter 10
International Security Requirements

Section 1. International Security

10-100. International Security.

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

International Security Considerations

- a. Normally, programs start foreign disclosure and security planning at the beginning of the acquisition process and systematically apply decisions throughout the life cycle. When a program is identified for international cooperation or foreign sale, consider and incorporate, as appropriate, all applicable National Disclosure Policy and technology transfer policy guidelines.**

- b. For policy guidance and the development of a Technology Assessment/Control Plan (TA/CP), Memorandum of Agreement, Security Manual, and SOP for all international programs (research/development, FMS, joint cooperation, and acquisition), contact the PSO.**

Chapter 11
Miscellaneous

Section 1. TEMPEST

11-100. 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.

NOTE: For DoD purposes, EMSEC means TEMPEST.

- a. Each department or agency has appointed Certified TEMPEST Technical Authorities (CTTAs) who must conduct and validate all TEMPEST countermeasure reviews by the National Policy.
- b. The program security officer, with guidance from a CTTA, shall determine if a review is required and direct the completion of a TEMPEST Requirements Questionnaire.
- c. If a review is required, a CTTA will determine if the equipment, system, or facility has a TEMPEST requirement, and if so, will recommend the most cost effective countermeasure which will contain compromising emanations within the inspectable space. The inspectable space is defined as the three dimensional space

surrounding equipment that

processes National Security Information (NSI) within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.

- d. Only those TEMPEST countermeasures recommended by CTTA and authorized by the program manager or contracting authority should be implemented. The processing of Special Category NSI or the submission of information for a TEMPEST countermeasure review does not imply a requirement to implement TEMPEST countermeasures. TEMPEST countermeasures which may be recommended by CTTA include, but are not limited to:
 - 1. The use of shielded enclosures or architectural shielding;
 - 2. The use of equipment which have TEMPEST profiles or TEMPEST zones which match the inspectable space, distance, or zone respectively; and
 - 3. The use of RED/BLACK installation guidance as provided by reference (c).

e. Telephone line filters, power filters, and non-conductive disconnects are not required for TEMPEST purposes unless recommended by a CTTA as part of a TEMPEST countermeasure requirement. Telephone line disconnects, not to be confused with telephone line filters, may be required for non-TEMPEST purposes.

Section 2. Government Technical Libraries

11-200. 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.*

Only authorized Government Contracting Officers may approve contractors to conduct SAP independent research and development (IR&D). A letter defining the authority to conduct IR&D, a DD Form 254, and an appropriate NISPOMSUP selector and classification guide will be provided to each contractor. Contractors who are conducting, or who desire to conduct SAP IR&D under this section, but who have not obtained proper authority, must contact the appropriate contracting authority.

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).

WAIVED - √
UNACKNOWLEDGED - √
ACKNOWLEDGED - √

The Program Offices for determining sanitization and releasability of SAP IR&D documents are identified in the contracts letter and DD Form 254.

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.*

These reviews normally will be conducted at the same time as reviews of other SAPs at that activity.

The Program Office/PSO will approve subcontracts before they are issued for IR&D efforts.

Section 4. Operations Security

11-400. 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.

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

Provide an OPSEC orientation to newly assigned personnel. Cover the activity OPSEC program, designated essential elements of friendly information (EEFI), OPSEC lessons learned, and the OPSEC role. Include OPSEC in annual refresher training. Include common OPSEC vulnerabilities, significance of unclassified data, tactical deception, new lessons learned, and other OPSEC subjects that are deemed appropriate.

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.

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

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.).

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

When conditions warrant, the PSO may require a TSCM survey of a SAPF for approval or reaccreditation of a previously used facility.

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 individually 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. **Decompartmentation.** *Prior to decompartmenting any classified SAP information or other material(s) developed within the Program, the CPSO will obtain the written approval of the GPM. Decompartmentation 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.

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

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.

WAIVED - √

UNACKNOWLEDGED - √

ACKNOWLEDGED - √

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.*

See 11-701 for overall requirements.

11-704. Treaty Guidance.

Treaty Guidance. DoD SAPs will be subject to an increasing number of various international arms control treaty verification or confidence and security building measures, many of which will impose a significant burden on program security concerns. SAPs will not be exempted from on-site inspections, overflights, or other intrusive activities involving multinational inspection teams. Therefore, SAPs must ensure that they are in compliance with treaty provisions, and they must participate in the preparation of Component Compliance and Implementation Plans so that the methodology of those plans adequately complements SAP program protection interests. SAP facility personnel should work with their SAP component treaty assistance team to ensure their equities will be protected during an inspection or other verification activity.

Each service entity must also ensure SAPs are included in that component's treaty inspection notification systems. Individual SAP facilities must establish an internal notification system to ensure that key personnel are advised of impending inspections.

a. Arms Control Treaty Implementation. DoD Directive

2060.1 provides that the implementation and compliance responsibilities for SAPs must be accomplished under the cognizance of the DoD SAP Oversight Committee in a manner consistent with the SAP Policy Directive, DoD Directive O-5205.7. The SAP Policy Directive provides that program access to DoD SAPs is controlled by the sponsoring DoD Component, unless the Secretary or Deputy Secretary of Defense has directed otherwise. Implementation of arms control treaties may require physical access to special access program facilities. Access to program information by international inspectors or U.S. personnel supporting inspection activities should not be necessary and may not be permitted without the specific approval of the affected component. Any inspection or verification issue directly related to SAPs must be decided within the SAP chain of command and administered by the appropriate Component-level SAP central office. Denial of access to the inspection team will only be considered if a SAP facility cannot be adequately prepared to protect program material, and access to that SAP space would compromise the program. In this case, a prepositioned access denial justification, approved by the Component-level SAP central office, is required.

b. Arms Control Treaty Inspection Background. SAPs, because of their enhanced security posture,

normally are handled separately from traditional security requirements. As noted above, DoD SAP facilities will not be exempted from arms control verification activities by foreign inspection teams. Thus, SAPs must be prepared to protect classified information and equities while inspections are being conducted at or near their facilities. Programs conducting sensitive work outdoors, even temporarily, also must be prepared for the possibility of "open skies" overflights or other verification activities to which they might be exposed.

c. General Guidance. Each Component-level SAP central office should develop an Inspection Readiness Plan (IRP) that provides general background information on treaty verification activities affecting SAPs and procedures for safeguarding SAP information while demonstrating treaty compliance. The IRP is a tool that should be used to help facilities prepare for an on-site inspection, overflight, or any other arms control verification activity. This general plan should provide adequate guidance for the majority of SAPs that do not have hardware concerns. Facilities that require additional program-specific preparation should develop an annex to the IRP specifying detailed procedures. If assistance is required, the SAP security manager should contact the Component-level SAP central office. Preparation for an on-site

inspection should be based on procedures for non-cleared visitors. The objective of preparation for an on-site inspection of any SAP facility is to blend SAP security infrastructure into the local facility's profile to the extent possible. Most importantly, all procedures should be established using low-cost, common-sense measures, consistent with program security requirements. The Component-level SAP central office is responsible for ensuring that plans are in place and have appropriate management concurrence or approval.

d. Inspection Preparation Plans.

The Chemical Weapons Convention (CWC) allows for on-site inspections by an international inspection team (IIT) on a recurring basis at declared facilities. In addition, intrusive challenge inspections can be conducted anytime, anywhere at an undeclared facility (government or industrial, worldwide). The CWC intentionally limits the time between notification and arrival of the IIT. Therefore, preparation time will be short. Plans must be in place in advance that detail how to protect classified information while an inspection is being conducted throughout the facility. The SAP security manager must be prepared to execute these plans immediately upon notification of an inspection. The SAP security manager should be familiar with the overall facility's compliance and implementation plans to

ensure that those efforts do not undermine established SAP arms control procedures and preparation activities. Plans prepared for CWC also could be used as a model for other types of on-site inspections or other verification activities. Plans should address, inter alia, the following:

1. Notification chains (who will receive notification, who else must be notified?).

2. Treaty points-of-contact and alternates (including 24-hour telephone numbers).

3. Up-to-date facility floor plans and facility layouts.

4. Specific steps and measures to be taken to protect security and proprietary interests.

e. Managed Access. "Managed access" is an OPSEC methodology used to restrict inspection team exposure to facility sensitivities while demonstrating compliance. Managed access procedures must be examined for each treaty or agreement, but generally encompass standard sanitization procedures: shrouding of displays, shapes, and equipment; de-energizing of computer systems; clean-desk policy; removal of project specific photographs; route and time control; proposing alternate means of verification suitable to your program/facility such as sampling on the perimeter of the facility; recommending changes to the inspection schedule; random selective

access; etc. Moving classified hardware to another storage location also may be an alternative for some programs. Component-level SAP central offices shall be prepared upon notification to address within the SAP chain of command any potential issues where managed access may be insufficient to protect program interests or demonstrate compliance with treaty requirements.

f. **On-Site Inspection Assistance.** In most cases, a treaty-knowledgeable representative from the OSD-level SAP central office or the cognizant Component-level SAP central office should be on-site within the first 24 hours after notification of an impending inspection. The SAP treaty representative will be a member of the on-site inspection team (i.e., Base Assistance Team or Tiger Team). When more than one SAP central office representative is present, early coordination among them will establish which one is accountable for each program. Each component is accountable for SAPs that it sponsors, unless relieved of that responsibility by the Secretary or Deputy Secretary of Defense. The responsible SAP component representative will conduct liaison between the SAP security manager and the U.S. Host Team to support the inspection. That individual will also provide treaty guidance and inspection preparation assistance for the facility, based on the preparation plan previously

developed by the facility or Program Office. The SAP security manager should meet with this individual as soon as possible after the arrival of the representative at the facility.

g. **Counterintelligence.** The SAP security manager may request the Component-level SAP central office to assist with obtaining vulnerability assessments, security counter-measures support, and other counter-intelligence or program protection support.

Appendix A Definitions

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

Access Evaluation. The process of reviewing the security qualifications of employees.

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.

Accountability. Assigning of a document control number (including copy #) which is used to establish individual responsibility for the document and permits traceability and disposition of the document.

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 accept 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.

Adjudication Authority. Entity which provides adjudication for eligibility or access.

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.

AIS Media Control System. A system of procedures, approved by the PSO, which provide controls over use, possession, and movement of magnetic media in SAPFs. The procedures must insure all magnetic media (classified and unclassified) are adequately protected to avert the unauthorized use, duplication, or removal of the media. The media must be secured in limited access containers or labeled with the identify of the individual responsible for maintaining the material.

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.

Control. A process which allows an organization to regulate material without providing full document accountability.

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

Contractor/Command 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).

EMSEC. For DoD purposes, EMSEC means TEMPEST.

Government Program Manager (GPM). The senior Government Program official

who has ultimate responsibility for all aspects of the Program.

Handle Via Special Access Control Channels Only (HVSACO). HVSACO is a protective marking, (similar to For Official Use Only), used within SAP control channels. It is used to identify CLASSIFIED or UNCLASSIFIED information which requires protection in Special Access channels. When HVSACO is used to help identify classified SAP information, the material will be protected in accordance with the security requirements of the individual SAP or the highest standard where more than one SAP is included.

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.

Letter of Compelling Need (LOCN). A letter, signed by the Security Officer and Program Manager, used to justify or offset the risk related to accessing an individual who does not fully meet access criteria. The LOCN describes the benefit to the specific SAP by describing the candidate's unique talent, particular expertise, or critically-needed skill.

Memorandum of Agreement (MOA). An agreement, the terms of which are delineated and attested to by the signatories thereto. MOA and 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 (OIS). An OIS is a special purpose AIS oriented to word processing, electronic mail, and other similar office functions. An OIS is normally comprised of one or more central processing units, control units, storage devices, user terminals, and interfaces to connect these components.

Operations Security (OPSEC). The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

Other Identifiers. i.e., SAR and SAP.

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.

SAP Central Office. Office within DoD or military department responsible for establishment and application of regulations, oversight, and security policy for Special Access Programs.

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

Security Director. Senior individual that is responsible for the overall security management of SAP within that activity.

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 Officer. When used alone, includes both Contractor Program Security Officers and activity security officers at government facilities.

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.

NOTE: the ISSR is responsible for magnetic media. The CPSO is responsible for overall document media.

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.

Temporary Help/Job Shopper. An individual employed by a cleared company whose services are retained by another cleared company or Government activity performing on SAP contracts and providing required services (e.g. computer, engineering, administrative support etc...) under a classified contractual agreement. This individual will have access to SAP material only at locations designated by the utilizing activity.

Trigraph. (See Digraph and/or 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.

Waived SAP. An Unacknowledged SAP to which access is extremely limited in accordance with the statutory authority of Section 119e of 10 U.S.C. Unacknowledged SAP protections also apply to Waived SAPs.

Working Paper(s). A draft classified document, portion of a classified document and material accumulated or created while preparing a finished document.

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

FOR OFFICIAL USE ONLY

A-9

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
LOGON	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 computer)	Personal Computer (i.e., desktop, laptop, notebook, or hand-held
PL	Public Law

PROM	Programmable Read-Only Memory
RAM	Radar Absorbing Materials
RAM	Random Access Memory
RAS	Radar Absorbing Structures
ROM	Read Only Memory
SAN	Separately Accredited Network
SAP	Special Access Program
SAPF	Special Access Program Facility
SCI	Sensitive Compartmented Information
SD	Security Director
STD	Standard
TA/CP	Technical Assessment/Control Plan
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	4.4 Hardware Transport and Release
1.1 Administration	4.5 Hardware Control and Audit Trails
1.2 Purpose and Scope	5.0 AIS SOFTWARE
2.0 SAPF DESCRIPTION	5.1 Authorized Software
2.1 Physical Environment	5.2 Software Procedures
2.2 Floor Layout	6.0 DATA STORAGE MEDIA
2.3 SAPF Access	6.1 Labeling and Storing Media
3.0 AIS DESCRIPTION	6.2 Media Sanitization and Destruction
3.1 General Information	6.3 Media Transport and Release
3.2 Configuration and Connectivity	6.4 Media Control
3.3 User Access and Operation	7.0 AIS SECURITY AWARENESS
3.4 Audit Trail	8.0 GLOSSARY OF TERMS
4.0 AIS HARDWARE	
4.1 Labeling Hardware	
4.2 Maintenance Procedures	
4.3 Hardware Sanitization and Destruction	

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 trail. State whether user access audit trails are manual or automatic.

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

Describe procedures for handling 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 *AIS 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 Management of Federal Information Resources
A-130 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-014 Guidelines for Formal Verification Systems [Purple Book]
- NCSC-TG-015 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-021 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-
91

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 1/16 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 1/19 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 1/22	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

**APPENDIX F
SPECIAL ACCESS PROGRAM FORMATS**

Section 1-General

1. Users obtain all blank SAP formats from the servicing PSO.
2. Users are responsible for all costs relating to the format's preparation program, to include the procurement and maintenance of necessary hardware and software.
3. This APP column reflects applicability:

A – Air Force only

4. Formats are available in DOS Windows FormFlow. Upon request, formats may be provided in DOS graphic form for import in Macintosh systems.

Section 2 – SAP FORMAT EXHIBIT

NUMBER	TITLE	DATE	APP
SAP Format 1	Program Access Request	1 Jul 93	
SAP Format 2	Special Access Program Indoctrination Agreement		
SAP Format 2a	Special Access Program Indoctrination Agreement (Polygraph Supplement)		
SAP Format 3	Request for Facility Clearance Action	1 Jan 91	A
SAP Format 4	SENIOR STAR Airlift Request	18 Jun 92	A
SAP Format 5	Inadvertent Disclosure Statement	1 Jan 91	
SAP Format 6	Notification of Foreign Travel	1 Jan 91	
SAP Format 7	Visit Authorization Request	2 Jan 91	
SAP Format 7L	Technical Visit Request	12 Jul 93	
SAP Format 8	TSCM Request	4 Jan 93	
SAP Format 9	Request for Files Check	2 Jan 91	A
SAP Format 10	Secure Communication Request	18 Jan 92	A
SAP Format 11	Subcontractor Status Report	1 Jan 91	
SAP Format 12	Waiver Request from Security Criteria	1 Jan 91	
SAP Format 13	Subcontractor/Supplier Data Sheet	1 Jan 91	
SAP Format 14	Reserved		
SAP Format 15	Facsimile Transmittal-Classified (Optional)	1 Jan 91	
SAP Format 16	Word Processor and Personal Computer Data Sheet	1 Jan 91	
SAP Format 17	Refresher Training Record	1 Dec 93	
SAP Format 18	Reserved		
SAP Format 19	Special Scope Security Review Report	4 Jan 93	
SAP Format 20	Foreign Relative or Associate Interview	1 Sep 94	
SAP Format 21	Computer System User Acknowledgment	31 Mar 95	
SAP Format 22	Reserved		
SAP Format 23a	SAP Annual Awards Program (Activity)	5 Oct 95	A
SAP Format 23i	SAP Annual Awards Program (Individual)	5 Oct 95	A
SAP Format 24	Agent of the Government (Appointment)	2 Jan 96	
SAP Format 25	Agent of the Government (Oath)	2 Jan 96	
SAP Format 26	Reserved		
SAP Format 27	Foreign Contact		
SAP Format 28	Courier Designations and Instructions		

APPENDIX G - SECURITY DOCUMENTATION RETENTION

IF RECORDS ARE OR PERTAIN TO	CONSISTING OF / WHICH ARE	MAINTAINED BY	DISPOSITION / DESTROY
Security Officer Appointments	Letters, Approvals, Forms	All	Destroy When Replaced or Superseded
Plans	Emergency Procedures, Security Operating Instructions, Tests, Manufacturing, SAP Formats 26, etc.	Contractor PMO PSO	Upon Termination of Program Forward to PSO One Year After Program Termination
Training Records	Security Education Attendance, Computer Listings, and SAP Formats 17	All	When Individual is Deceased
Exercise Reports	Of Emergency Plans and Guard Responses	All	Destroy After Two Consecutive Reviews
EMSEC Reports	Surveys	All	Destroy When Facility Becomes Unoccupied
Adverse Information Reports	Required by NISPOM/NISPOM Suppl or Other Gov't Directives	All	Destroy Five Years After Individual is Deceased
Contract Security Classification Inspections	DD Forms 254	Contractor PSO PMO	Destroy Five Years After Contract is Completed Destroy Five Years After Contract is Completed Retain Permanently
Visits	Visitor Requests, SAP Formats 7, 7I, 7U Visitor Logs	All	Destroy After One Year Destroy After Seven Years
Accreditations	Of Program Facilities which Include Facility Checklists and Open Storage Authorizations	Contractor PSO	Destroy When Facility Becomes Superseded or Unoccupied Destroy One Year After Decertification
Waivers	Security Criteria, SAP Formats 12	Contractor PSO/PMO	Destroy When Program is Terminated Destroy Five Years After Program is Terminated
Alarm Test Records	AF Forms 2530	All	Destroy After One Security Review Cycle

FOR OFFICIAL USE ONLY

Document Control Records	Receipts Mail Receipts/Logs Master Document Listings Destruction Certificates Top Secret Registers/Control Records	All	Destroy After Five Years Destroy After Two Years Destroy When Superseded or No Longer Needed IAW DoD 5200.1-R IAW DoD 5200.1-R
Access Approvals	Received From SPA	Contractor PSO/PMO	Attach to PAR Destroy Five Years After Program is Terminated
Access Lists	Information Copies Master Copy Prepared by Originator	PSO/PMO All	Destroy When New List is Received Destroy After Five Years
Audit Reports	Top Secret Inventories Top Secret Computer Audits	All	Destroy Two Years After Completed or After PSO Inspection, Whichever is Later Destroy After One Security Review Cycle
Briefing Statements (SAP Formats 2, 2A, 21)	Including Pre-Briefings, Indoctrinations and Debriefings	Contractor PSO/PMO	Forward to PSO Upon Debriefing Destroy Five Years After Program is Terminated, or IAW Agency Directives
Foreign Travel Reports	SAP Format 6	All	Destroy Five Years After Program is Terminated
Inadvertent Disclosure Statements	SAP Format 5	All	Destroy Five Years After Program is Terminated
Program Access Requests (PAR) - (SAP Formats 1, 1A, 9, 20)	Approved for Access Disapproved for Access	All Contractor PSO/PMO	Destroy After Five Years Destroy Upon Receipt of Disapproval Forward to Adjudicator Who Retains Permanently
Request to Transfer Documents to Another Program	Approved	PSO/PMO Contractor	Destroy After Five Years Destroy When Associated Documents Are Destroyed
Security Policy	Directive or Provide Interpretation	Contractor PSO/PMO	Destroy One Year After Program is Terminated Retain Permanently

FOR OFFICIAL USE ONLY

Security Review Reports (SAP Formats 19) on Checklists	Annual Self-Review	All	Destroy After One Year, But Maintain at Least Two Reports
	Reviews Conducted by PSO	Contractor PSO/PMO	Destroy After Three Years Destroy After Five Years
	Subcontractor Reviews	Contractor	Destroy After Five Years
Top Secret Access Records	AF Forms 144 or Equivalent	All	Destroy Two Years After Corresponding Document is Destroyed
Inspection Reports	After Duty Hour Inspections and Safe Check Records	All	Destroy at End of Each Month
	Entry/Exit Checks		Destroy After PSO Inspection
Subcontractor Documentation	Requests to Contact Including SAP Format 13	Contractor PSO/PMO	Destroy One Year After Program is Completed Destroy One Year After Program is Terminated
	Trip Reports	All	Destroy Two Years After Trip is Made
Security Classification Guides	Master	PSO/PMO	Retain Permanently
	Copies	Contractor	Destroy One Year After Program is Terminated
Technical Security Countermeasures Surveys	Including SAP Format 8	All	Destroy After Next Report is Received
Inquiries	Security Violations	All	Destroy After Two Years
Investigations	Compromises/Suspected Compromises/ Document Losses	All	Destroy Five Years After Program is Terminated
Recurring Reports	SAR Program Contract Security Report	All	Destroy After One Year
	Subcontractor Status Reports (SAP Format 11)	Contractor	Destroy One Year After Program is Terminated
		PSO/PMO	Destroy After Three Years
SATRAN Reports		All	Destroy When No Longer Needed
Program Management Directives		PMO	Retain Permanently
Courier Designations		All	Destroy After One Year

FOR OFFICIAL USE ONLY

Communication Requests	Secure Comm/FAX - (SAP Format 10)	Contractor PSO	Destroy One Year After Equipment is Installed Destroy Five Years After Program is Terminated
Circle (A, B) Investigations	Logs of Same	Contractor	Destroy One Year After Program is Terminated
Personnel Security Investigations	DDFM 1879/SF 86	All	Destroy When Individual is Deceased
Memorandums of Understanding (MOU)/Memorandums of Agreement (MOA)	By Government Agencies	Contractor PSO	Destroy When Facility is No Longer Used Destroy Five Years After Program is Terminated
Building Checks	Conducted by Guards	Contractor	Destroy After One Year
Reports of Espionage, Sabotage, or Subversion		All	Retain Permanently
Reports of Hostile Contacts		All	Retain Permanently
Shipment Tampering Reports		All	Destroy One Year After Program is Terminated
Media Information Attempts	Including Releases (Approved/Non-approved)	All	Destroy Five Years After Program is Terminated
Classification Changes		Contractor PSO/PMO	Destroy After Information is Included in Security Classification Guide Retain Permanently
Requests for Top Secret Reproduction		All	Incorporated into Document Control Records
Threats/Threat Assessments	Provided by Government Investigative Agencies	All	Destroy when Threat is Eliminated or After Five Years, Whichever is Sooner
Program Termination	Associated Documentation	Contractor PSO/PMO	Destroy Five Years After Program is Terminated Retain Permanently
Listing of Names, Codes and Convenience Numbers		All	Destroy Five Years After Program is Terminated

FOR OFFICIAL USE ONLY

Mark as Appropriate - _____ Special Access Required
 Mark as Appropriate - _____ UNCLASSIFIED
 Mark as Appropriate - _____ U-HVSACO

PROGRAM ACCESS REQUEST					
1. Program Name			2. Access Level	3. Billet Position <input type="checkbox"/> YES <input type="checkbox"/> NO Billet Number:	
4. Last Name, First Name, MI			5. Rank/Grade	6. SSN-	
7. Date of Birth (YYMMDD)	8. State/Country of Birth	9. <input type="checkbox"/> Military <input type="checkbox"/> Government Civilian <input type="checkbox"/> Contractor		10. Date Needed (YYMMDD)	
11. Position Description/Job Title			12. <input type="checkbox"/> Full Time <input type="checkbox"/> Temporary (Period of access) <input type="checkbox"/> Part Time		
13. Organization/Company Name		14. Assignment/Job Location (City and State)		15. Command/Facility ID Code	
16. Security Clearance	17. Granted By	18. Date Granted	19. Investigation Type	20. Conducted By	21. Date Completed
22. Security Investigation Status <input type="checkbox"/> In Progress <input type="checkbox"/> Not Started (See Remarks) <input type="checkbox"/> Current			23. Central Adjudication Review (When Required) Conducted By _____ <input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur		
24. Justification (_____) include the percentage of time to be spent supporting the program. CONTINUE ON SEPARATE SHEET IF NECESSARY Classification					
25. REQUESTOR (Functional Manager)					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
26. ACTIVITY SECURITY MANAGER (Government or Contractor)					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
27. GOVERNMENT/CONTRACTOR PROGRAM MANAGER					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
ADDITIONAL COORDINATION (As Required by the Specific Program)					
28. Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
29. Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
30. Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
31. PSO					
Typed Name/Title/Organization		Signature	32. DCII (OK or Referred to CAO on YYMMDD)	<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
33. FINAL APPROVAL AUTHORITY					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Approved <input type="checkbox"/> Non-Approved	Date
34. Remarks/Restrictions CONTINUE ON SEPARATE SHEET IF NECESSARY			35. Attachments: Not Required Attached		
			Standard Form 86 <input type="checkbox"/> <input type="checkbox"/>		
			Local Files Check (DCII) <input type="checkbox"/> <input type="checkbox"/>		
			Foreign Association Questionnaire <input type="checkbox"/> <input type="checkbox"/>		
			Other (LOC) <input type="checkbox"/> <input type="checkbox"/>		
			Derived From: Derived On:		

SAP Format 1, "Program Access Request", 1 July 93

PREVIOUS EDITIONS ARE OBSOLETE

*NOTICE: The Privacy Act 5, U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting you Social Security Account Number (SSAN) is Executive Order 9397. Your SSAN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, or 2) determine that your access to the information indicated has been terminated.

SPECIAL ACCESS PROGRAM INDOCTRINATION AGREEMENT

An Agreement Between _____ and the United States
(Name - Printed or Typed)(Last, First, Middle Initial)

1. I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or materials protected within Special Access Programs, hereinafter referred to in this Agreement as SAP information (SAPI). I have been advised that SAPI involves or derives from acquisition, intelligence, or operations and support activities, and is classified or is in the process of a classification determination under the standards of Executive Order 12958 or other Executive Order or statute. I understand and accept that by being granted access to SAPI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SAPI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SAPI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SAPI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SAPI or that I know to be SAPI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that authorized my access(es) (identified on the reverse) to SAPI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SAPI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SAPI, or related to or derived from SAPI, is considered by such Department or Agency to be SAPI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.

4. In consideration of being granted access to SAPI and of being assigned or retained in a position of special confidence and trust requiring access to SAPI, I hereby agree to submit for security review by the Department or Agency that authorized my access(es) (identified on the reverse) to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SAPI or description of activities that produce or relate to SAPI or that I have reason to believe are derived from SAPI, that I contemplate disclosing to any person not authorized to have access to SAPI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SAPI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SAPI. I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SAPI until I have received written authorization from the Department or Agency that authorized my SAP access(es) (identified on the reverse).

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SAPI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the SAP community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in the termination of my access to SAPI, removal from a position of special confidence and trust requiring such access, or termination of other relationships with any Department or Agency that provides me with access to SAPI. In addition, I have been advised that any unauthorized disclosure of SAPI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(a), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that provided me the access(es) (identified on the reverse) to SAPI, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SAPI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SAPI and does not set forth such other conditions and obligations not related to SAPI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(a) of Title 50, United States Code, and Executive Order 12958, as amended, so that I may read them at this time, if I so choose.

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the Military); Section 2302 (b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(a) of Title 50, United States Code. The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. This Agreement shall be interpreted under and in conformance with the law of the United States.

15. I make this Agreement without any mental reservation, purpose of evasion, and in absence of duress.

Signature

Date

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Special Access Program information.

WITNESS and ACCEPTANCE:

Signature

Date

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGMENT

(Special Access Programs by Initials Only)

SSN (See Notice Below)

Printed or Typed Name

Organization

BRIEF

Date _____

I hereby acknowledge that I was briefed on the above SAP(s):

Signature of Individual Briefed

DEBRIEF

Date _____

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the above SAP(s):

Signature of Individual Debriefed

I certify that the briefing presented by me on the above date was in accordance with relevant SAP procedures.

Signature of Briefing/Debriefing Officer

SSN (See Notice Below)

Printed or Typed Name

Organization (Name and Address)

NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information indicated has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

Format 2 "Special Access Program Indoctrination Agreement"

**SPECIAL ACCESS PROGRAM INDOCTRINATION AGREEMENT
(POLYGRAPH SUPPLEMENT)**

SECTION 1 - IDENTIFICATION DATA

Name (LAST, First, MI)	SSAN
Organization/Company	Job Position/Title/Grade
Clearance and Date of Clearance	Access Authority (Letter, Message, or Name Identification)

SECTION II - PREBRIEFING AGREEMENT

PART 1 - PREBRIEFING AGREEMENT

I understand that the briefing I am to receive, discloses information controlled in a special security system referred to as Special Access Program Information which is self-contained and administered directly by the sponsoring Department of Defense agency.

PART 2 - POLYGRAPH AGREEMENT

I further understand that by accepting access to this Special Access Program Information, I may be required to and I will voluntarily take a polygraph examination which will be limited to counterintelligence and/or counterespionage questions.

PART 3 - PREBRIEFING AND POLYGRAPH ACKNOWLEDGMENTS

I agree to the stipulations contained in the above agreements prior to receiving a program/project specific briefing.

Signature of Individual

Date

The execution of these Agreements was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Special Access Information.

WITNESSING OFFICIAL:

Signature

Date

SAP FORMAT 2a. "Special Access Program Indoctrination Agreement (Polygraph Supplement)

DO NOT Use Previous Editions

(CLASSIFY THIS FORMAT ONLY WHEN REQUIRED BY THE PROGRAM SECURITY DIRECTIVE)

WARNING: Do NOT Place Classified Information on this Form

Request for Facility Clearance Action

From: _____ Date: _____

To: _____ (PSO)

- Establish "covered" facility clearance
- TOP SECRET SECRET CONFIDENTIAL
- Change in level of facility clearance
From _____ To _____
- Confirm Carve-Out

Contractor Identity

Name of Facility _____

Address _____

CAGE _____

Specific Location of Carve-Out _____

Contract Number _____

Points of Contact

Contractor POC _____ Secure Phone _____

Government POC _____ Secure Phone _____

PSO Endorsement

Program Management Endorsement

CONFIDENTIAL (When Filled In)
Special Access Required - _____

Date/Time: _____ / _____ **Control #** _____ **Precedence** _____

From: _____ **Office Symbol** _____ **Phone #** _____

To: SAF/AQLE (703) 979-2407 (Mode 6)

Program: _____

Subject: SENIOR STAR Airlift Request (U)

Itinerary (fill in most important time block; remainder will be completed by AMC)

LOCATION	REQUESTED DATE	REQUESTED TIME (LOCAL)
DEP		
ARR		
LOCATION	REQUESTED DATE	REQUESTED TIME (LOCAL)
DEP		
ARR		

Passengers (If O-7 or civilian equivalent, include title)

RANK	NAME	RANK	NAME

Boxes/Cargo (Number, size and approximate weight. boxes must fit in a safe drawer for emergency storage.)

NUMBER	SIZE	WEIGHT

Points of Contact

LOCATION	NAME	PHONE NUMBER
SAF/AQL		(703) 697-9650/6174
AMC CP		(618) 256-2981/5970

Derived From: xxx
 Declassify On: xxx

Sent By: _____

INADVERTENT DISCLOSURE STATEMENT

1. Information from a class of Defense information, the source of which cannot be disclosed, has been either discussed with you or exposed to your view. This disclosure was unintentional; therefore it is necessary to acquaint you with the laws on the subject, and for you to execute this statement binding you to secrecy in connection with any information you may have gained from the disclosure.
2. The importance of safeguarding this information cannot be overemphasized. The time limit for safeguarding of such information NEVER expires. You are directed to avoid all references to the existence of this information or words which identify it.
3. Although you inadvertently gained information not intended for you, your signature below does NOT constitute an indoctrination of clearance or access to such information.

STATEMENT

I hereby affirm that I have read and fully understand the letter of instructions for maintaining the security of defense information. I certify that I shall never divulge any information which I may have learned from my having been exposed to this information, nor will I reveal to any person whomsoever, my knowledge of the existence of such information. I further certify that I shall never attempt to gain access to such information henceforth. I understand that transmission or revelation of this information in any manner to an unauthorized person is punishable under U.S. Code Title 18, Sections 793 and 794.

Signature

Organization/Firm and Location

Printed Name

Date

Witnessed this _____ day of _____, _____.

Signature of Witness

(When Filled In)

UNCLASSIFIED/HANDLE VIA SPECIAL ACCESS CHANNELS ONLY

Notification of Foreign Travel

To: PERSONNEL SECURITY MANAGER (Please do not list organization on this line)

1. BACKGROUND:

- a. Travel outside of the United States is a matter of security interest in view of the clearances you hold. Such travel includes points in Canada, the Caribbean, Mexico, and Europe, as well as more distant places.
- b. Knowledge of your whereabouts is needed primarily for personal protection and as a guide in locating you should an official search be required. Your itinerary should be adhered to as closely as possible.
- c. If major changes are made or if your estimated return date is extended by 24 hours or more, please advise Security accordingly to forestall any unnecessary concern as to your whereabouts. Contact Security upon your return for a debriefing. Any incidents of an intelligence nature which may have occurred must be reported.

2. Please complete the following information (paragraph 2a-d) and read paragraph 3a-j, Foreign Travel Briefing. Sign, date and return to Security at least thirty (30) days prior to your departure. When you return, arrange to complete paragraph 4, Foreign Travel Debriefing.

a. THIS TRAVEL IS OFFICIAL PERSONAL

b. _____
Name (Last, First, MI) Social Security Number

Home Address Home Telephone

Organization Work Telephone

c. PERSON WHO KNOWS YOUR PLANS AND WHEREABOUTS:

Name (Last, First, MI) Home Telephone

Home Address Work Telephone

d. DESTINATION ITINERARY: If more than one foreign country is to be visited, list countries in scheduled order of visit, together with all side trips and stop-overs.

Place	Date(s)	Carrier	Contacts

Expected date of return to the US _____

Traveler's Signature _____

Date _____

Security Concur _____

(When Filled In)

UNCLASSIFIED/HANDLE VIA SPECIAL ACCESS CHANNELS ONLY

3. As you prepare to travel outside of the United States, you may find yourself traveling to or through a country whose interests are inimical to those of the U.S. First and foremost, it is important that you be reminded of the continuing need to safeguard the classified information you carry around in your head and the broadening efforts of foreign intelligence services around the world. Second, this briefing is to impart a number of helpful tips so you can avoid situations which could cause you delay, embarrassment, or to be arrested while traveling.

- a. Don't mention, discuss or even imply involvement in special or classified projects or activities.
- b. Never take sensitive or classified material outside of the U.S. without written approval from the PSO.
- c. Avoid moral indiscretions or illegal activity which could lead to compromise or blackmail.
- d. Don't accept letters, photographs, material or information to be smuggled out of the country.
- e. Be careful of making statements which could be used for propaganda purposes. Don't sign petitions, regardless of how innocuous they may appear.
- f. Remember that all mail is subject to censorship. Be careful not to divulge personal or business matters which could be used for exploitation or propaganda purposes.
- g. Never attempt to photograph military personnel or installations or other restricted/controlled areas.
- h. Beware of overly friendly guides, interpreters, waitresses, hotel clerks, etc., whose intentions may go beyond being friendly.
- i. Carefully avoid any situation which, in your best judgment, would provide a foreign service with the means for exerting coercion or blackmail.
- j. Report to Security upon your return for debriefing. Incidents of an intelligence nature or foreign national contact must be reported.

Receipt and contents acknowledged:

Signature of Traveler

Date

Signature of Organization Travel Monitor

4. After you return, please arrange with your Organization Travel Monitor/security person to complete the debriefing below:

**Foreign Travel Debriefing
To be completed after you return**

- a. Did you deviate from the itinerary you provided prior to your departure? Yes No
- b. Did you have contact with anyone under circumstances you would consider as suspicious or unusual? Yes No
- c. If you answered "YES" to either of the above questions, explain on attached sheet.

Interview conducted by _____ Date _____

CONFIDENTIAL (When Filled In)
Special Access Required - _____

Date/Time: _____ **Control No.** _____ **Precedence** _____
From: _____ **Office Symbol.** _____ **Phone#** _____
To: _____
Info: _____

Subject: Visit Notification

1. (C/SAR) The following individual(s) will visit _____
on date(s) indicated for the purpose of _____
Point(s) of contact is/are _____

(U)	(U)	(U)	(C/SAR)	(U/HVSACO)
Name	SSAN	Clearance & Investigation	Program / Level of Access	Date(s) of Visit
		/	/	-
		/	/	-
		/	/	-
		/	/	-
		/	/	-
		/	/	-
		/	/	-
		/	/	-
		/	/	-

2. (U) Visit is approved by _____ Date: _____

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 3101 & EO 9397
PRINCIPAL PURPOSE: For granting visit approval to a **classified** program facility and to authorize access to program material.
ROUTINE USE: To record visit approval. Use of SSAN is necessary to make positive identification of the individual and records.

Disclosure is voluntary; failure to provide the information and SSAN could result in approval being denied.

Derived From:
Declassify On:

Sent By: _____

CLASSIFICATION (When Filled In) _____
Special Access Required - _____

Section I - FAX Transmittal Data			
Date/Time: _____ / _____	Control No. _____	Precedence _____	
From: _____	Office Symbol. _____	Phone# _____	
To: _____			
Info: _____			
Subject: Technical Visit Request (U)			

Section II - Briefing Data	
1. Subject/Title of Original Information	2. Master Library DCN
3. Briefer: (Name/Company) / _____	4. Sponsor: (Name/Agency) / _____
5. Requestor: (Name/Company) / _____	5. Phone Number: (Requestor/STU III)
7. Justification (Classification - _____)	

Section III - Individuals Receiving Briefing				
(U)	(U)	(U)	(C/SAR)	(U/HVSACO)
Name	SSAN	Clearance & Investigation	Program / Level of Access	Date(s) of Visit
		/		
		/		
		/		
		/		
		/		
		/		

Section IV - Coordination/Approval			
8. Requestor Security: (Signature)	(Date)	9. Sponsor Security: (Signature)	(Date)
10. Requestor Notified: (Name of Person & Means of Notification)			(Date)

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 3101 and EO 9397
 PRINCIPAL PURPOSE: For granting visit approval to a **classified** program facility and to authorize access to program material.
 ROUTINE USE: To record visit approval. Use of SSAN is necessary to make positive identification of the individual and records.

Disclosure is voluntary; failure to provide the information and SSAN could result in approval being denied.

11. Special Procedures:	Derived From: Declassify On:
-------------------------	---------------------------------

SAP Format 7L, "Technical Visit Request", 12 Jul 1993

Special Access Required - _____

CLASSIFICATION (WHEN FILLED IN) - _____

TSCM Request (U)	
(U) Facility _____ (Organization/Company Name)	_____ (Date of Request)
(U) Street _____ (Complete Address)	
(U) City _____ State _____ ZIP _____	
(S/SAR) Bldg Numbers _____ (Program Areas)	Total Number Requests _____ (Submit a Separate Request for Each Facility)
(S/SAR) Room Numbers _____ (Program Areas)	_____ sq. ft. (Total Sq. Ft.)
(S/SAR) Date All Construction Completed _____ (If Applicable)	
(S/SAR) Date All Equipment/Furnishing in Place _____ (Equipment Must Be Operational)	
(U) Highest Classification Level _____	(S/SAR) Desired Date _____
(S/SAR) Date of Last Survey _____ (If Known)	File No _____ (If Known)
(U) Gov't Security Manager _____ (SAF/AQ)	Work Phone _____
	Home Phone _____
(U) Facility POC _____ (Security Manager)	Work Phone _____
	Home Phone _____
(U) Alternate POC _____ (Alternate Security Manager)	Work Phone _____
	Home Phone _____
(S/SAR) Reason Survey Needed _____ _____ _____	
_____ (Signature of In-Place Security Manager)	_____ (Signature of Gov't Program Security Officer)
<p>(U) Note: At a minimum, include a sketch or building diagram. When available, submit blueprints. Include overall area/facility maps. Clearly outline program areas on submitted documents. Also provide information regarding physical characteristics such as construction, types and locations of equipment (computers, alarms, radio equipment), windows and any other factor potentially affecting security. Preferred method of receipt is on 8 1/2" x 11" paper. Use of this size may require copy reduction. If not feasible, forward attachments separately.</p> <p>DERIVED FROM: DOWNGRADE TO CONFIDENTIAL/SAR UPON COMPLETION OF TSCM ACTIVITY DECLASSIFY ON:</p>	

UNCLASSIFIED - Handle Via Special Access Channels Only

Date/Time: _____ / _____ Control No. _____ Precedence _____

From: _____ Phone# _____

Name of Servicing Government PSO: _____

To: **SAF/AQ Central Adjudications Facility**

Subject: Request for Files Check

Request a files check be conducted on the following personnel:

Name	(U)	(U)	(C/SAR)
SSAN		Level	A/D
		/	/
		/	/
		/	/
		/	/
		/	/
		/	/
		/	/
		/	/
		/	/

2. (U) Visit is approved by _____ Date: _____

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 8012; 44 U.S.C. 3101 and EO 9397
PRINCIPAL PURPOSE: For granting visit approval to a classified program facility and to authorize access to program material.
ROUTINE USE: To record visit approval. Use of SSAN is necessary to make positive identification of the individual and records.

Disclosure is voluntary; failure to provide the information and SSAN could result in approval being denied.

Derived From:
Declassify On:

Sent By: _____

SAP Format 9, "Request for Files Check", 2 Jan 1991

(Classification)

SECURE COMMUNICATIONS REQUEST

From: _____ Date: _____

To: _____

Thru: _____

SECTION I - GENERAL INFORMATION

1. Name of Program: _____

2. Company/Agency : _____

3. Building Number: _____ Room Number: _____

4. Street Address: _____

5. City/State/Zip Code: _____

6. Points of Contact: _____

7. Phone Numbers: _____

SECTION II - SERVICE REQUIRED

8. Service: _____

9. Key Level: _____

10. Required Operational Date: _____

11. Justification: _____

SECTION III - VALIDATION

12. Contractor Security Manager: _____ Date: _____
(Signature)

13. Government Security Manager: _____ Date: _____
(Signature)

14. Program Security Officer: _____ Date: _____
(Signature)

15. RFS Number: _____

16. Telephone Service Gov't office w/sterile lines Gov't office providing own support
 Contractor facility w/sterile lines Contractor facility w/non-sterile lines

17. Communications Special Projects Manager: Concur Non-Concur Date: _____

(Signature)

Derived From:
Declassify On:

SAP Format 10, "Secure Communications Request", 18 Jun 1992
(Preparation Instructions On Reverse)

DO NOT Use Previous Edition

(Classification) (Unclassified Until Filled In)

The following instructions provide a detailed description of the information required to complete this form. Each entry has been numbered to permit ease in completion.

TO: Route through the Government Program Manager and then to the Program Security Officer (PSO). Failure to follow this sequence results in rejection of this request.

1. Whenever possible, provide the specific program name, rather than a study or a project number.
- 2 thru 5. Be specific and provide accurate information. Make sure changes in this information between the time the request is submitted and the service provided are reported to the PSO to permit relay to the installers.
6. Two POCs are required. POCs should be the persons who have been previously assigned as the primary and alternate COMSEC managers for existing locations, or those persons who will be COMSEC managers for the new location.
7. When possible, provide existing STU III secure phone numbers.
8. Provide details (which includes the following) for each type of service:

STU III - Provide quantity of phones required, whether single or multi-line versions are needed (multi-line instruments are designed to operate on a 1A2 key system), and state what type of devices are required or planned to be used on the data port. Requests for facsimile service supported by a STU III may be combined with one STU III request.

FAXNET (Facsimile supported as a closed net using KG-84a Crypto) - Identify the net which you will be required to communicate with. If a new net is being established, a separate form must be prepared for each requirement. Identify the number of locations anticipated to be activated in the net over the next two years.

KG Support for Computer dial-ups, high-speed links, etc. - Provide a complete description of the intended installation, to include wiring diagrams showing signal connections to the KG on both the red and black side. The customer provides the installation support of all of the other components of the system, with the exception of the COMSEC. The customer also installs the appropriate cabling from the customer equipment to the point of installation for the COMSEC.

9. Enter SCI, Top Secret, or Secret. Bear in mind for Top Secret or SCI keys to be issued, personnel with the appropriate clearances must be available.

10. The following minimum lead times have been established as a guide which may vary depending upon the type of service requested and are obtained from the communications community from the time they receive the request from the PSO. (Allow extra time to process the request within your own channels):

Equipment or Keying Material Support Only - 90 days

Requests Requiring Leasing 9.6kb Data Service or Business Telephone Service to Support a Government Location - 90 days

Requests Requiring the Lease of Services Greater than 9.6kb to Support a Government Location - 120 days

11. Be specific. Government Program and Security Managers use this information to validate the request.
12. Applies only to contractor requests.
13. Channel all requests through the appropriate Program Manager prior to submission to the PSO.
- 14 thru 16. For PSO use only. Separate instructions have been provided.
16. Contractors provide the leased telephone services for their requirements. "Sterile" (foreign exchange) service is normally required. The PSO may permit a large contractor to use standard commercial service, but the PSO must sign a waiver assuming the risk. Contact the PSO for further information.

For Government locations, unless sterile lines are required, the customer arranges for telephone service support from the local base. If sterile lines are required, the PSO validates such need and requests the service on this form. DO NOT route telephone service through the base switchboard.

CONFIDENTIAL (When Filled In)
Special Access Required - _____

SUBCONTRACTOR STATUS REPORT (U)

1st Tier 2nd Tier 3rd Tier

- | | |
|--|--|
| 1. Company/Address _____

_____ | 2. Sterile Address _____

_____ |
| 3. Prime _____ | 4. Convenience Code _____ |
| 5. Facility Clearance _____ | 6. Facility Code _____ |
| 7. Telephone _____ | 8. Sterile Phone _____ |
| 9. Number of Personnel Briefed: Ceiling _____ Total _____
Level I _____ Level II _____ Level III _____ Level IV _____ | |
| 10. Product/Service _____ | |
| 11. Program/Project _____ | Classification _____ Level _____ |
| 12. CSM _____ | 13. PM _____ |
| 14. Prime Security Rep _____ | 15. Prime Procurement Rep _____ |
| 16. Secure Phone # _____ | 17. Secure Fax Yes _____ No _____ |
| 18. Storage Authority _____ | 19. Contract Value _____ |
| 20. DD Form 254 Date _____ | 21. Security Plan Date _____ |
| 22. Date of Last Insp _____ | 23. Rating _____ |
| 24. Classified Holdings (Update Yearly)
Confidential _____ Secret _____ Top Secret _____ | |
| 25. Status _____

_____ | |
| 26. Additional Remarks _____

_____ | |

CLASSIFICATION NOTICE: Classification based on relationships and products.

Derived From:
Derived On:

(Classification)

Special Access Required - _____

Waiver Request From Security Criteria (U)

Date _____

1. Request Number _____ 2. Expiration Date _____

3. From _____ Thru _____ To _____

4. Type Request (check one) Facility Equipment Procedural

Equivalent Other

5. REFERENCE Directive # _____ Paragraph # _____

6. Affected Area/Function _____

7. Brief Description of Specific Requirement _____

8. Brief Description of Deficiency _____

9. Proposed Corrective Action _____

10. Justification _____

11. Compensatory Measures _____

12. Estimated Cost of Correction _____

13. Estimated Correction Date _____

Special Access Required

Classification

(Classification)

Special Access Required - _____

14. Requester Coordination

Office	Name	Initials
_____	_____	_____
_____	_____	_____
_____	_____	_____

_____	_____	_____
Name of Program Manager	Signature	Date

_____	_____	_____
Name of Security Manager	Signature	Date

15. Reviewing Official Coordination & Recommendation

Approval _____ Disapproval _____

Comments _____

Name of Reviewing Official _____

Activity Represented _____

Signature _____

16. Approval Authority Coordination

Approved _____ Disapproved _____

Comments _____

Signature _____

17. Additional Information from Previous Page as Required (Indicate Item #)

Special Access Required

Classification

CLASSIFY AS APPROPRIATE

SUBCONTRACTOR/SUPPLIER DATA SHEET (U)

1. Prime Contractor _____ Subcontractor/supplier _____
Address _____

2. Initial Meeting
Date _____ Attended By _____
Location _____

3. Type of Procurement: Sole Source Yes No

4. Product _____ Classification _____

5. Subcontractor/Supplier Data
DoD Facility Clearance Level _____ Date Granted _____
DoD Storage Level _____ CAGE _____
Other Contracts with Prime _____
Approx Percentage of Firm's Business _____ Project Number/Name _____

6. Cover Story _____

7. Subcontractor/Supplier Contracts _____ Sterile Phone Numbers _____
Program Management _____
Technical _____
Contracts _____
Security _____

8. Sterile Address
Name _____
Address _____ City _____ State _____ Zip _____

9. Secure Communication Voice _____ Fax _____

10. Proposed Work Area/Location _____

11. Proposed Personnel Program Accesses
Level I _____ Level II _____ Level III _____ Level IV _____

12. Proposed Program Classified Storage
Storage NOT Approved _____ Storage Containers _____
Level Approved _____ Class VI _____

13. Remarks _____

CLASSIFICATION NOTICE: Classification based on compilation of special security procedures.

Derived From:
Derived On:

CLASSIFY AS APPROPRIATE

Date/Time: _____ / _____ Control # _____ Precedence _____
From: _____ Office Symbol _____ Phone # _____
To: _____
Info: _____
Subject: _____

Reference: _____

COVER ONLY: _____ COVER PLUS: _____
SENT BY: _____ Derived From: _____
Declassify On: _____

CLASSIFY AS APPROPRIATE

WORD PROCESSOR AND PERSONAL COMPUTER DATA SHEET

Initial Submission <input type="checkbox"/>	System Number: _____	Facility: _____
Configuration Change <input type="checkbox"/>	Date Submitted: _____	Room: _____
Addition <input type="checkbox"/> Deletion <input type="checkbox"/>	Date Approved: _____	User: _____
Recertification <input type="checkbox"/>	Date Implemented: _____	Custodian: _____

Level of Classified Processing: _____ Mode of Operations: _____
 Percentage Used for Classified: _____ Hours of Operation: _____

Equipment (I/O Devices)	Manufacturer	Model Name	Serial Number	Seal Number
Keyboard				
Mouse				
Monitor				
System Unit				
Disk Drive				
Printer				

Operating System: _____

Application Software

Storage Media	Internal Memory (RAM)
_____	_____
_____	_____

Communications Capabilities & Disconnects

Summary of System Use:

_____	_____
PSO Signature	Date

Refresher Training Record

For CY _____

This format provides for documentation of annual refresher training. This training may be accomplished throughout the year or at one session. The "COMPUTER SECURITY" listing is mandatory if the individual uses a computer.

Mandatory Topics Covered

- Foreign Intelligence Techniques
- Threat Reporting
- Effects of Unauthorized Disclosure
- Program Vulnerabilities/Threat & OPSEC
- Adverse Information Reporting
- Reporting Fraud, Waste & Abuse
- Derivative Classification & Marking
- Telephone Security/STU IIIs
- Security Inspection Common Problems

Date Completed

Programs/Projects

(Convenience Codes May Be Used)

Computer Security

- AIS Operating Procedures
- Audit Trails
- Logs, Forms & Receipts
- Media Protection
- Use of System
- Copyright Laws & Licensing Agreements

Videos/Films Shown

Other Topics Covered

- Visitor Procedures
- Document Control
- _____
- _____
- _____
- _____

Personal Status

(Optional)

I was provided an opportunity to review my DoD Personnel Security Questionnaire and report/change any previously unreported personal status changes.

Individual's Initials: _____

Printed Name

Organization/Firm

Signature

Location

Security Education Manager (SEM) or Instructor

Special Access Program Review Report										Date _____	
Section I - General Information											
1. Name of Activity						2. Address					
3. Management			Security Guide Date			4. Type of Activity			Cost		
PM			Major Program			<input type="checkbox"/> Government <input type="checkbox"/> Prime <input type="checkbox"/> Associate <input type="checkbox"/> Sub					
SM			PSO			6. Scope of Activity					
5. Review Dates						<input type="checkbox"/> Possession <input type="checkbox"/> COMSEC <input type="checkbox"/> Access Only <input type="checkbox"/> Graphic Arts <input type="checkbox"/> Dormant <input type="checkbox"/> Commercial Carrier					
Previous			From			To					
7. Number of Persons Accessed						8. Number of Documents					
LV1	LV2	LV3	LV4	Total		CONF	SECRET	TS	LV4	Total	
Section II - Review Data											
9. Type						<input type="checkbox"/> Complete <input type="checkbox"/> Re-Review <input type="checkbox"/> Partial <input type="checkbox"/> Close Out <input type="checkbox"/> Unannounced					
10. Overall Rating						<input type="checkbox"/> Superior <input type="checkbox"/> Satisfactory <input type="checkbox"/> Marginal <input type="checkbox"/> Unsatisfactory					
11. Deficiencies						<input type="checkbox"/> No Deficiencies <input type="checkbox"/> Finding		No.		<input type="checkbox"/> Deviations <input type="checkbox"/> COS	
12. Names of Reviewers										Time Expended	
13. Personnel Outbriefed											
Section III - Elements of Review											
Code	Functional Area			Rating	Code	Functional Area			Rating		
	Management				H	Physical					
B	Security				I	Access Control					
C	Personnel					Security					
					K	Transmission					
E	Marking				L	Security					
F	Reproduction					Contracting					
G	Destruction				N	Force					
Special Emphasis Item:											
Section IV - Report Processing											
14. Corrective Action Report						15. Respond To			16. Distribution		
<input type="checkbox"/> Required → <input type="checkbox"/> Not Required ↓ _____						_____ _____ _____			_____ _____		
										Derived From:	
										Declassify:	
SAP Format 19, "Special Access Program Review Report", 4 Jan 1993											

Section V - Synopsis

Code

Section VI - Deficiencies

Code

Section VI - Deficiencies (continued)

Code

Section VI - Deficiencies (continued)

--	--

17. Name of Review Team Chief	Signature of Review Team Chief	Date
-------------------------------	--------------------------------	------

18. Name of Reviewing Official	Signature of Reviewing Official	Date
--------------------------------	---------------------------------	------

CONFIDENTIAL (When Filled In)
Special Access Required - _____

Special Access Required - _____
CONFIDENTIAL (When Filled In)

Page _____ of _____

Foreign Relative or Associate Interview

Interviewee's Name: _____

Interviewee's SSAN: _____ Date of Interview: _____

Name of Relative or Associate: _____

Relationship: _____ Citizenship: _____

Current Address: _____

City/Country: _____

Has the relative or associate ever visited the U.S.? _____ Port of Entry: _____

When and for how long? _____

Frequency? _____

Most recent visit? _____

What is the relative's or associate's line of work? (If government employee, determine level: local, national, etc.)

Initial contact date/circumstances? _____

Frequency of interviewee's contact with relative or associate? _____

When/where did the last contact occur? (letter, phone call, in person, etc.) _____

Interviewee's reaction to any undue interest in his/her job? _____

Does or would the interviewee provide significant support? (If so, what type?) _____

Interviewee's bond with, affection for, or obligation to the relative or associate? _____

Would the relative's or associates welfare and safety be of significant concern (hostage situation)? _____

Interviewee's reaction to such a situation? _____

Remarks: _____

Security Representative's Signature and Date: _____

SAP Format 20, "Foreign Relative or Associate Interview", 1 Sep 1994

NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the dis-

Closure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that

Authority for soliciting your Social Security Account Number (SSAN) is Executive Order 9397. Your SSAN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, or 2) determine that you access to the information indicated has been terminated.

(Use additional sheets for Remarks, as needed)

Computer System User Acknowledgement Statement

I understand that as a computer system user, it is my responsibility to comply with all security measures necessary to prevent unauthorized disclosure, modification, or destruction of information. I have read the computer system standard operating procedures for the system(s) to which I have access and agree to:

1. Protect and safeguard information in accordance with the System Operating Procedures.
2. Sign all logs, forms and receipts as required.
3. Escort personnel not on the access list for the environment in such manner as to prevent their access to data which they are not entitled to view.
4. Protect all media used on the system by properly classifying, labeling, controlling transmitting and destroying it in accordance with security requirements.
5. Protect all data viewed on the screens and/or hardcopies at the highest classification level of the data processed unless determined otherwise by the data owner.
6. Notify the System Security Custodian of all security violations, unauthorized use, and when I no longer have a need to access the system (i.e., transfer, termination, leave of absence, or for any period of extended non-use).
7. Use of the system is for the purpose of performing assigned organizational duties, never personal business and I will not introduce, process, calculate, or compute data on these systems except as authorized according to these procedures.
8. Comply with all software copyright laws and licensing agreements.

Initial Certification

Printed Name of User

Signature of User

Printed Name of Custodian

Signature of Custodian

Organization/Firm

Date

Annual Recertification

Signature of User

Date

Signature of User

Date

Signature of User

Date

Signature of User

Date

Signature of User

Date

Signature of User

Date

Signature of User

Date

Signature of User

Date

Nomination for SAP Security Education Award - Activity

Name/Address of Organization/Activity:

Description of Security Education Program:

Statement of Accomplishments:

Effectiveness of Accomplishments:

Supporting Evidence of Effectiveness:

Nomination for SAP Security Education Award - Individual

Name/Address of Organization/Activity:

Job Description:

Statement of Accomplishments:

Effectiveness of Accomplishments:

Supporting Evidence of Effectiveness:

Letter of Appointment

To:

Company:

Subject to your acceptance and execution of the Oath of Confidentiality attached hereto, you are hereby appointed an Agent of the United States Government for the _____ Program. This appointment is for the limited purpose of reviewing Personnel security Questionnaires (PSQs), Security Questionnaires (SQs), and Program Access Request packages (PARs) for accuracy, completeness, and obvious disqualifying factors.

For the limited purposes of this agency you are obligated to treat personnel information as data protected by the Privacy Act (5 U.S. Code 552a) for all employees of your parent company whose questionnaires you review. Disclosure of personal information to any person not authorized to receive it may subject you to sanctions, including criminal penalties, provided by the Privacy Act, and to appropriate administrative and civil remedies.

Should you decline to accept, or refuse to execute the Oath of Confidentiality attached hereto, you should consider this tender of appointment to be canceled.

Program Security Officer

Acceptance of Appointment and Oath of Confidentiality

I, _____, the undersigned, do hereby accept appointment as an Agent of the United States Government for the _____ Program for the limited purpose of reviewing Personnel Security Questionnaires (PSQs), Security Questionnaires (SQs) and Program Access Request packages (PARs) for accuracy, completeness, and obvious disqualifying factors revealed in the PSQs, SQs or PARs.

I acknowledge that in accepting this appointment as an Agent of the Government, I agree that I will not disclose to any person, not lawfully entitled to receive it within the scope of this employment or agency with the U.S. Government, personal information revealed on the PSQs, SQs or PARs I review. I also acknowledge, accept and agree that I will not use or reveal personal information to anyone except for the purposes stated herein.

I further acknowledge that by virtue of this appointment, I am bound by the provisions of the Privacy Act (5 U.S. Code 552a), including its criminal penalties for wrongful disclosure of information contained in protected records. I have been informed that PSQs, SQs and PARs are records protected by the Privacy Act.

Signature and Date

Appointing Official

Signature and Date

Typed Name and Title

FOREIGN CONTACT FORM

To:

From:

Name	Employee Number	Social Security Number
Telephone Number		

Instructions:

- Please answer the following questions listed below to the best of your ability.
 - For further information or questions, contact Program Security.
-

1. **Full name of Non-U.S. citizen contact: (include maiden name or aliases if appropriate. If possible, provide name in both English and Native language characters.)**

2. **Date of Birth (or approximate age if DOB is unknown), place of birth (city, country):**

3. **Citizenship:**

4. **Current address:**

5. **Occupation/Employer:**

6. **Known since/how did you meet:**

7. **Last contact date/plans for future contact:**

8. **Description of type of relationship:**

NOTE: If responding "YES" on questions below, please provide details in the remarks section at the bottom of this form.

- | | | | |
|-----|-----|----|--|
| 9. | YES | NO | Are you aware of any known political/military/intelligence activities of the contact or their relatives? |
| 10. | YES | NO | Is this contact witting of your Government involvement? (If yes, please note how and why) |
| 11. | YES | NO | Do you have any relatives or friends from the same country as the contact? |
| 12. | YES | NO | Did the individual ask what type of work you do? What was your response? |
| 13. | YES | NO | Did the contact express an interest in any topics or technologies? |
| 14. | YES | NO | Did you discuss your involvement in U.S. Government related activities? |
| 15. | YES | NO | Did the contact offer to arrange any special treatment for you? |
| 16. | YES | NO | Did the contact offer to pay for anything (i.e., meals, gifts)? |
| 17. | YES | NO | Have you received any gifts from this person? |
| 18. | YES | NO | Did you exchange business cards, telephone numbers or addresses? (Please attach a copy to this form) |
-

COMMENTS:

PRIVACY ACT STATEMENT

Notice: The above information is protected by provisions of the Privacy Act, 5 U.S.C. 522a. You are hereby advised that authority for soliciting your Social Security Account Number (SSAN) is Executive Order 9397. Your SSAN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above. Although disclosure is not mandatory, your failure to do so may impede certification or determinations.

DESIGNATION AND COURIER INSTRUCTIONS

- A. **Maintain constant custody of the material from receipt until delivery. Never allow the material out of your sight or physical contact.**
- B. **Place all material in a locked briefcase of normal appearance or a strong, locked carry-on bag. Based on the volume of material, use additional couriers as necessary (a minimum of two couriers is required for Top Secret; one for secret and below).**
- C. **Do not schedule on overnight stop. Remain in the airport terminal if a connecting flight is part of your itinerary.**
- D. **Do not consume alcoholic beverages.**
- E. **Pre-plan travel routes. Include alternate routes. In unfamiliar areas, mark and use maps.**
- F. **Transiting airport security checkpoints:**
 - 1. **Before departure, obtain a courier authorization letter. Do not show this letter to airport security unless specifically asked. Also display military or company ID cards when asked.**
 - 2. **When two couriers are used, one courier passes through the checkpoint and waits for the second courier to transfer the package through the x-ray machine. The second courier passes through the checkpoint after material has been received by the first courier.**
 - 3. **Only open your briefcase if airport security asks you to do so.**
 - 4. **If airport security asks you to open the document package, produce your courier letter and identification card. Inform security personnel that you are couriating classified data and that the package cannot be opened. If security personnel do not accept this explanation, contact the Airport Security Manager and explain the situation.**
 - 5. **If airport security, Airport Security Managers, airline officials, or anyone insists on opening the document package, refuse and cancel your trip.**
- G. **Emergency situations:**
 - 1. **In case of any emergency en route emergency or if paragraph F5 applies, immediately contact your Security Officer. After receiving such notification, Activity and Contractor Security Officers must immediately contact the Program Security Officer.**
 - 2. **In the event of a skyjacking, do not reveal your courier assignment. Use common sense. Do not attempt to hide the material or dispose of it. Leave it in your briefcase. If anyone insists on opening your briefcase, do not argue or physically attempt to stop them. Notify Airport Security Managers on your release as soon as possible.**
 - 3. **If a bomb threat occurs while you are on board an aircraft, present your courier letter and identification card to Customs, FAA, or Federal agents. Explain your situation and permit x-ray or electronic scanning. If any of these officials insist on opening the sealed document package, ask that they do so in a segregated area, away from other individuals or passengers. Remain with them when the package is opened. After the search is completed, obtain the names, agency, and telephone numbers of the searching individuals. Immediately supply this information to your Security Manager. NOTE: Security officials will defensively debrief these individuals as necessary. Do not conduct the debriefings yourself.**
 - 4. **If you are forced to abandon a trip because of failure to make connections, sickness, etc.,**

keep the material in constant personal contact. If a motel is required, rent only one room for the two-person courier team (if male-female team, rent adjoining rooms). Have meals delivered to the room. Contact the Security Manager for instructions and possible locations where the material may be taken and deposited.

5. If there is a vehicle mishap en route, e.g. a breakdown or accident, contact the Security Manager at both your departure and destination points. Explain the general nature and importance of your business travel to law enforcement officials. Display your courier letter and identification card. If these officials insist on opening the document package or seizing it, do not physically resist. Obtain names, badge numbers, and telephone numbers, and ask to talk to superior officers. Explain the situation to the superiors and ask them if they will allow you to put them in contact with the Program Security Officer. If conditions warrant, one of the couriers should remain with the vehicle, while the other travels the shortest distance possible to obtain assistance.

- H. If you arrive at your destination after working hours, make prior arrangements to secure the material in an approved SAP facility. If you are delayed or unable to reach your contact at the destination point, notify your Security Manager. If you are unable to contact the Security Manager at either the delivery or departure point, proceed to the facility or activity and attempt to obtain telephone numbers of persons you positively know are program-accessed. Ask them to assist you in contacting security personnel. Do not leave your package with non-accessed personnel or within non-program areas. As a last resort, keep the material within your control.
- I. Be cautious while in telephone booths, public restrooms, cafeterias, and similar areas to ensure that your briefcase is not switched or stolen. Stay out of these areas as much as possible. While on board the aircraft, place your briefcase under the seat in front of you; do not place it in the overhead storage compartment.
- J. Always require and obtain a receipt for the material at the point of departure and point of origin.

ENDORSEMENT

I have read the instructions above and will fully comply with these instructions. I understand the seriousness of this mission and am aware of the extreme detrimental effects on this mission and am aware of the extreme detrimental effects on the national security that would result should the material I am couriating be compromised. I further understand that should my negligence result in a compromise or loss, disciplinary may be taken. I am aware that transmission or revelation (by loss or any method) of this information to unauthorized persons could subject me to prosecution under the Espionage Law (U.S.) Code, Title 18, Sections 793, 794, and 798) or other applicable statutes and, if convicted, could result in up to a 10-year sentence in prison or a \$10,000 fine, or both.

Name of courier (1) (Type or Print)	Signature of Courier (1)	Date
-------------------------------------	--------------------------	------

Name of courier (2) (Type or Print)	Signature of Courier (2)	Date
-------------------------------------	--------------------------	------

Name of Security Officer	Signature of Security Officer	Date
--------------------------	-------------------------------	------