



JOINT AIR FORCE - ARMY - NAVY

JAFAN 6/0

Manual

**Special Access Program
Security Manual - Revision 1**

29 May, 2008

FOREWORD


This manual standardizes security guidance for all Air Force, Army and Navy (hereafter referred to as service components) Special Access Programs (SAPs). This manual is applicable to all service component SAPs.

In cases of doubt over the requirements of this manual, users should consult the Government Program Security Officer (PSO) prior to taking any action or expending program-related funds. In cases of extreme emergency requiring immediate attention, action taken should protect the Government's interest and the security of the program from compromise.

In situations where conditions or unforeseen factors render full compliance to these standards unreasonable, the PSO may apply commensurate levels of protection. Applying commensurate protective measures to a particular SAP means that equivalent protections are being used rather than following the exact wording of this manual. Commensurate levels of protection will not be designed with the intent to reduce or lessen the security protection of the area of consideration. Within 90 days of implementing commensurate protective measures, the Government PSO will notify the service component Special Access Program Central Office (SAPCO) for validation and final approval.

On occasion, it may be necessary to waive the requirements in this manual. Requests for waivers will be provided to the appropriate service component SAPCO for approval. Adherence to the standards set forth in this manual will ensure compliance with national-level policy and allow for reciprocity between service component SAPs.

At a minimum, this manual will be implemented within six months of the date of publication. All contractual documents will be amended to reflect use of this manual. Any cost impacts will be forwarded to the appropriate contracting officer and forwarded to the cognizant service component SAPCO for resolution.



JOHN B. HENNESSEY
Director, Security, CI, and Special
Programs Oversight
USAF



MICHAEL KOBBE
Director, Technology Management
Office (TMO)
USA



JOHN E. PIC
Director, Special Programs
Office (CNO (N89))
USN

TABLE OF CONTENTS

	<u>Page</u>
CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS	
Section 1. Introduction	1
Section 2. General Requirements	3
Section 3. Reporting Requirements	11
CHAPTER 2. SECURITY CLEARANCES	
Section 1. Facility Clearances	15
Section 2. Personnel Clearances and Access	15
Section 3. Foreign Ownership, Control, or Influence (FOCI) & National Interest Determinations (NIDs)	20
CHAPTER 3. SECURITY TRAINING AND BRIEFINGS	28
CHAPTER 4. CLASSIFICATION AND MARKING	
Section 1. Classification	32
Section 2. Marking Requirements	32
CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION	
Section 1. General Safeguarding Requirements	34
Section 2. Control and Accountability	34
Section 3. Storage and Storage Equipment	36
Section 4. Transmission	36
Section 5. Disclosure	41
Section 6. Reproduction	42
Section 7. Disposition and Retention	42
Section 8. Construction Requirements	43
Section 9. Control of Portable Electronic Devices (PEDs)	44
CHAPTER 6. VISITS AND MEETINGS	
Section 1. Visits	45
Section 2. Meetings	46
CHAPTER 7. SUBCONTRACTING	48
CHAPTER 8. INFORMATION ASSURANCE	49

CHAPTER 9. INTERNATIONAL SECURITY REQUIREMENTS	50
Section 1. General and Background Information	50
Section 2. Disclosure of U.S. Information to Foreign Interests	50
Section 3. Foreign Government Information (FGI)	53
Section 4. International Transfers	55
Section 5. International Visits and Control of Foreign Nationals	60
Section 6. Contractor Operations Abroad	64
Section 7. NATO Information Security Requirements	65
CHAPTER 10. MISCELLANEOUS	
Section 1. TEMPEST	71
Section 2. Government Technical Libraries	72
Section 3. Independent Research and Development	72
Section 4. Operations Security	72
Section 5. Counterintelligence (CI) Support	73
Section 6. Decompartmentation, Disposition, and Technology	
Transfer Procedures	73
Section 7. Close-Out Actions	74
Section 8. Patents	74
Section 9. Telephone Security	74
Section 10. Treaty Guidance	75
APPENDICES	
A. Handle Via Special Access Channels Only (HVSACO) Procedures	77
B. Standard Operating Procedures (SOP) - Topical Outline	79
C. Security Documentation Retention	85
D. Operations Security (OPSEC) Plan - Topical Outline	89
E. Inspection Readiness Planning	93
F. Security Inspection Checklist	95
G. SAP Formats	109
H. SAP NID Request Package (Sample)	134
I. Inspection Data Call Letter (Sample)	143
TABLES	
1. Training Requirements	28

Chapter 1

General Provisions and Requirements

Section 1. Introduction

1-100. Purpose. This manual prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of SAP information and to control authorized disclosure of classified information.

1-101. Authority. This manual is promulgated pursuant to authorities and responsibilities assigned to the Directors, Special Access Program Central Office (SAPCO) for the protection of SAPs under their cognizance. These authorities and responsibilities may be found in Title 10 United States Code (U.S.C). 119(e); National Security Act of 1947, as amended; in Executive Order (EO) 12958, as amended; in the Code of Federal Regulations, 32CFR2103 (per Information Security Oversight Office Directive No. 1); and in other applicable laws and orders. Component-level SAPCO have been established to execute, manage, administer, oversee, and maintain records on the SAPs they exert cognizant authority over. These offices exercise the authorities and responsibilities as outlined in DoD Directive 5205.7 and DoD Instruction 5205.11.

1-102. Scope.

- a. This manual applies to all service component SAPs and participants within these SAPs. These procedures are also applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.
- b. This manual applies to and shall be used by service components and their contractors to safeguard classified information released during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, performance, and termination. This manual also applies to classified information not released under a contract, license, certificate or grant, and to foreign government information furnished to contractors that requires protection in the interest of national security. The manual implements applicable Federal Statutes, Executive orders, National Directives, international treaties, and certain government-to-government agreements.
- c. If a contractor determines that implementation of any provision of this manual is more costly than provisions imposed under previous U.S. Government policies, standards or requirements, the contractor shall notify the cognizant security authority (CSA) through the PSO (also see para 1-104 below). The notification shall indicate the prior policy, standard or requirement and explain how this manual's requirement is more costly to implement. Contractors will implement the provisions of this manual on initial contract award or modification or subsequent modification to an existing contract normally incorporated via a Contract Security Classification Specification (DD Form 254).

d. In the interest of clarity, consistency and procedural guidance; all contractual requirements outlined in this manual and as directed by the government will be made official only when forwarded through contracting channels.

1-103. Agency Agreements. The service component SAPCOs may enter into agreements with each other that establish the terms of responsibilities for administration and operation of SAPs of mutual interest. See paragraphs 1-208 and 209 of this manual.

1-104. Security Cognizance. The term "Cognizant Security Authority" (CSA) denotes the service component SAPCO. SAPCOs may delegate any aspect of security administration regarding classified activities and contracts under their purview to another CSA. Any further delegations from the SAPCO will be in writing and maintained in the appropriate SAPCO.

1-105. Manual Interpretations. Interpretations of this manual will be resolved at the PSO-level. Any unresolved interpretations will be forwarded by the PSO to the appropriate service component SAPCO.

1-106. Waivers. For the purposes of this manual, a waiver is any action to increase or decrease the security requirements of any of the Joint Air Force Army Navy (JAFAN) Manuals.

a. On occasion, it may be necessary to grant a waiver to the requirements of this manual. Every effort will be made to avoid waivers to established SAP policies and procedures unless they are in the best interest of the Government. Waivers¹ can only be approved by the appropriate service component SAPCO.

b. In those cases where waivers are required, a request will be submitted to the service component SAPCO or designee via the PSO's chain of command. Submit the completed SAP Format 12 to the PSO, who will process the waiver to the cognizant service component SAPCO. Security Officers at all levels shall maintain a file of approved waivers. Attach maps, floor plans, photos, or drawings to waiver requests when necessary. Subcontractors submit SAP Format 12 through their prime contractor, who will sign as the "Reviewing Official". The requester ensures adequate compensatory measures are documented on the request and if approved, executed.

1-107. Commensurate Levels of Protection. In situations where conditions or unforeseen factors render full compliance to these standards unreasonable, the cognizant PSO may apply commensurate levels of protection. Applying commensurate protective measures to a particular SAP means that equivalent protections are being used rather than following the exact wording of this manual. Commensurate levels of protection will not be designed with the intent to reduce or lessen the security protection of the area of consideration and/or requirements of this manual. Within 90 days of implementing commensurate protective measures, the PSO will notify the service component SAPCO of the commensurate level of protection and request validation and final approval.

¹ Service SAPCOs will forward all requests for waivers which exceed the requirements outlined in this manual to the DoD SAPCO for approval.

1-108. Special Access Program Categories and Types

- a. Categories. There are three categories of SAPs: (1) Acquisition; (2) Intelligence; and (3) Operations and Support.
- b. Types. There are two types of service component SAPs, Acknowledged and Unacknowledged.

(1) An Acknowledged SAP is a program which may be openly recognized or known; however, specifics are classified within that SAP. An Acknowledged SAP is acknowledged to exist and whose purpose is identified (e.g., the B-2 or the F- 117 aircraft program) while the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is generally unclassified.

(2) An Unacknowledged SAP's existence is protected as special access and the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is often unacknowledged, classified, or not directly linked to the program.

Note: An unacknowledged SAP for which the Secretary of Defense has waived applicable reporting requirements under Title 10 U.S.C. 119(e) is identified as a "Waived-SAP" and, therefore, has more restrictive Congressional reporting.

Section 2. General Requirements

1-200. Responsibilities.

- a. Service Component and Contractor SAP Security Officer titles:

Government:

(1) Program Security Officer (PSO): The PSO is responsible for the program security management and execution of all security policies and requirements for a specific SAP program, sub-compartment or project. The PSO exercises these authorities on behalf of the SAPCO or service component designee. The PSOs will be appointed, in writing, by the SAPCO or designee.

(2) Government SAP Security Officer (GSSO): The individual appointed at a government program facility to provide security administration and management based on guidance provided by the PSO. GSSOs will be appointed in writing and assigned to specific facilities/projects/subcompartments. Copies of appointment letters will be provided to the PSO.

Contractor:

(1) Contractor Program Security Officer (CPSO): The individual appointed at a contractor program facility to provide security administration and management based on guidance provided by the PSO.

(2) CPSOs will be appointed in writing and assigned to specific facilities/projects/subcompartments. Copies of appointment letters will be provided to the PSO.

b. Each activity associated with a SAP will assign one or more SAP Security Officers to each SAP. SAP Security Officers are technical specialists and serve as the primary SAP security focal points at each government and contractor facility. They are appointed to perform the duties indicated below and responsible for implementing program SAP security policies within each facility. All SAP Security Officers will have the position, responsibility, and authority commensurate with the degree of SAP security support required for each organization.

c. GSSO/CPSOs will:

(1) Possess a personnel clearance at least equal to the highest level of classified information for which they require access.

(2) Possess access to all SAPs assigned to the facility(s) for which he/she is responsible.

(3) Provide facility security administration and management.

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

(5) Ensure adherence to the provisions of this manual.

(6) Oversee an information management system for each SAP used to facilitate the control of requisite information within each SAP.

(7) Conduct an annual accountable classified material inventory.

(8) Maintain a Special Access Program Facility (SAPF) IAW JAFAN 6/9.

(9) Ensure Information Systems (IS) are IAW JAFAN 6/3.

(10) Establish and oversee a visitor control program.

(11) Establish reproduction and destruction capability of SAP information.

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

(13) Ensure the conduct of program indoctrination and annual refresher, briefings and debriefings of personnel.

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

(15) When required, ensure contractual specific SAP security requirements such as TEMPEST and Operations Security (OPSEC) are accomplished.

1-201. Standard Operating Procedures (SOP). The GSSO/CPSO will prepare comprehensive SOPs to implement the security policies and requirements unique to their facilities. SOPs will address and reflect methods of implementing the security aspects of the Program. Forward proposed SOPs and SOP changes to the PSO for approval. The GSSO/CPSO will utilize the topics, as applicable, provided in Appendix "B". SOPs should address local implementation of applicable security directives.

a. Contractors are not required to prepare an SOP for Pre-Solicitation Activity, a Program Research and Development Announcement, Request for Information, or Request for Proposal 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 Security Classification Guide (SCG) suffice as the SOP. If a formal contract is not executed, one of the following three actions (or combination of the three actions) will be taken:

(1) The material will be returned to the Government.

(2) The material will be inventoried, documented, and certified as destroyed and documentation will be provided to the PSO. In the case of TOP SECRET, a copy of the destruction certificate will be provided to the Government.

(3) Documentation can be retained by the contractor, provided a contractual relationship exists and if approved by the PSO/Program Contracting Officer (PCO). A DD Form 254 will be prepared and provided to the contractor outlining the retention, storage, reuse and continued access procedures. If information is retained, written security procedures are required.

b. Contractors are not required to prepare written SOPs when all work is performed at a government facility. Subcontractors are not required to prepare written SOPs when all work by is performed at a prime contractor facility. Storage normally is not authorized at the subcontractor location. Keep program access records and other program documentation at the prime contractor facility.

1-202. Badging. When all individuals within a SAPF cannot be personally identified, a badging system may be required by the PSO. The best form of entry control is personal introduction and identification. Use this procedure to the maximum extent possible. 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 badge system is considered necessary it will be documented in the facility SOP and address topics such as badge accountability, storage, inventory, disposition, destruction, format and use. If card readers are used

in conjunction with badges and a means exists to lockout lost, unused, and/or relinquished badges, the PSO may negate the requirements stated above for badge inventory, accountability and destruction.

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

1-204. Two-Person Integrity (TPI). TPI is an enhanced security option that mandates the minimum of two indoctrinated persons at all times in a SAPF. This security protection can only be authorized by the CSA.

1-205. Perceived Excessive Security Requirements. All personnel are encouraged to identify excessive security measures that they believe have no value or are cost prohibitive. These excessive requirements should be reported through the PSO to the service component SAPCO.

1-206. Security Compliance Inspections. The Security Compliance Inspection Process represents a unified and streamlined approach to the SAP inspection process. All service component SAP Program Security Officers (PSOs), Government SAP Security Officers (GSSOs) and Contractor Program Security Officers (CPSOs) are required to follow the Security Compliance Inspection Process outlined below unless explicitly modified by the Service SAPCO. PSOs should work with their respective Contracting Officers to add it as a compliance, contract deliverable (via a revised DD Form 254). This oversight methodology provides an opportunity for a reduction in the number of inspections a contractor is subjected to within a defined inspection cycle (with demonstrated performance) and therefore, with good stewardship, result in cost savings to both the Government and Contractors alike. The frequency² type and scope of Security Inspections (e.g., Government inspections, evaluations, and security surveys) are determined by the service component SAPCO.

a. Two-Phase Process. The Security Compliance Process is a two phase process which gives PSO's a structured and consistent approach in conducting inspections. The process begins with the scoping and validation of the Self Inspection Checklist, followed by review and validation of the Core Compliance Items (CCI). The Security Compliance Process has two distinct types of inspections. The first type is the Core Compliance Inspection, which is the initial inspection by the Government. The second type is a Full Scope Inspection, which is a more in-depth inspection designed for those facilities which have either received a previous rating of Marginal or Unsatisfactory; or there are significant systemic security issues which occurred during the inspection cycle.

(1) Phase One - Self-Inspections. Depending on the location (Government/Industry) of the SAP, annual self-inspections are conducted by the GSSO/CPSO (as appropriate) and will address issues reflected in the "Security Inspections Checklist" found in Appendix "F", this manual. Self-inspection reports will be submitted to the PSO within 30 days following completion of the inspection. The PSO will be notified immediately if the self-inspection discloses the loss, compromise or suspected compromise of classified material. Self-inspection reports will be retained for two years following the formal government CSA inspection. All outstanding items must be completed prior to the destruction of the self-inspection.

² Security inspections will not be conducted more frequently than every 12 months. However, if security risks warrant additional security oversight each service SAPCO reserves the right to conduct inspections more frequently.

(2) Phase Two-Government Compliance Inspections. The Compliance Inspection focuses on the Self-Inspection Checklist and the Core Compliance Items identified below:

- (a) Top Secret SAP Data/Materials Accountability
- (b) Security Education and Training
- (c) Personnel Security
- (d) Security Management and Oversight
- (e) Computer Security (Information Assurance)

(3) Special Emphasis Items (SEIs). In addition to the Core Compliance Items identified above, PSO's will be required to validate SEIs which are will be determined annually by the Service Component SAPCOs.

b. Conducting the Inspections:

(1) Step 1-Scheduling the Inspection. PSO or Team Chief (Joint Inspections) shall schedule inspections for the calendar year no later than 31 January. Upon schedule confirmation with the facility, PSO's will send a data call letter which outlines the pre-inspection requirements. PSO's should receive information listed in the Inspection Data Call Letter which is sent to the activity prior to being inspected (see Appendix "I" for a sample letter). The Inspection Data Call Letter and Inspection Checklist will be forwarded at least thirty days prior to the scheduled inspection date. The PSO should review the checklist and familiarize themselves with the inspected activity, affected SAPs and other pertinent information. This will prepare the PSO in validating the checklist prior to arriving on-site. At this point the PSO determines what resources he/she may need in order to conduct the inspection (i.e., team composition, inclusion of participants from other agencies having a vested interest, etc).

(2) Step 2-Conducting the In-brief. PSO's will conduct the in-brief with the CPSO/GSSO, Site Program Manager, and Security Management. The in-brief will outline the inspection schedule, team composition, SEIs and general ground rules for conduct of the inspection (to include roles of the CPSO/GSSO).

(3) Step 3-Validating the Self-Inspection Checklist. After the in-brief has been completed the PSO will review and validate the Self-Inspection Checklist with the CPSO.

(a) The PSO validates the checklist discussing each functional area with the CPSO. This is an opportunity for the CPSO to provide an overview of their security operations and processes. The PSO will, in turn, validate the findings reflected in the self-inspection checklist. Once the PSO has conducted the validation of the checklist, he/she will determine the rating of the program/facility – see below for definitions of each rating.

(b) If the rating is below Satisfactory, the PSO will document and explain the rationale behind the assigned rating with the CPSO/GSSO, Site Program Manager, and Security Management. The PSO will then terminate this phase of the inspection and schedule a return visit within 90 days to conduct a Full Scope Inspection.

Note: A Full Scope Inspection is a complete inspection of all functional areas identified on the SAP Format 19. Full scope inspections consist of validating all items within the Self-Inspection Checklist.

(4) Step 4-Validating the Core Compliance Items and Special Emphasis Items (SEIs). Once the validation of the Self-Inspection Checklist has been completed, and has been determined to be Satisfactory, the PSO will inspect the Core Compliance Items and Special Emphasis Items.

(a) Upon completion of the Core Compliance Items and Special Emphasis Items the PSO will determine the rating. If the rating is Satisfactory the PSO will then prepare the out brief for the CPSO/GSSO, Security Management, and Site Program Manager. During the out brief, the PSO will identify the overall rating for the program inspected and provide to the facility a copy of completed SAP Format 19 within 10 working days following completion of the inspection. At this time the PSO will decide whether the facility will be inspected on a 12, 18 or 24 month cycle.

(b) If the rating is less than Satisfactory during the inspection of the Core Compliance Items and Special Emphasis Items, the PSO will explain the rationale behind the rating with the CPSO/GSSO, Site Program Manager, and Security Management. The PSO will return within 90 days and conduct a Full Scope Inspection.

Note: For any facility which received a less than Satisfactory rating during any portion of an inspection, that facility will be inspected in a 12 month cycle. Should that facility during the course of the next inspection be Satisfactory in all areas, at all times during the inspection, the facility may then be placed in a 12, 18 or 24 month cycle.

c. SAPCO Notifications. The cognizant SAPCO will immediately be notified whenever a facility receives a rating of less than Satisfactory.

d. Prime Contractor Representative. A security representative from the prime contractor should be present and participate during inspections of subcontractors. Contractor personnel will not serve as Inspection Team Chiefs, assign ratings, conduct in/out briefings, or be responsible for completing the security inspection report.

e. Joint Government Team Compliance Inspections. Inspections will be coordinated between the service components and conducted jointly to the greatest extent possible. Joint Team Compliance Inspections will be fully coordinated between participating components/agencies/activities by the assigned Team Chiefs. Each component/agency/activity is responsible for production/release of their findings/reports, etc per the cognizant SAPCOs direction.

f. Inspection Ratings. The following is an overview of the Inspection Ratings³ to be used:

(1) Superior: A Superior rating is reserved for contractors who have consistently and fully implemented the requirements of the JAFAN series in an effective fashion resulting in a superior security posture, compared with other contractors of similar size and complexity. The facility must have documented procedures that heighten the security awareness of the contractor employees and that foster a spirit of cooperation within the security community. This rating requires a sustained high level of management support for the security program and the absence of any serious security issues. For more complex facilities, minimal administrative findings are allowable.

(2) Commendable: A Commendable rating is assigned to contractors who have fully implemented the requirements of the JAFAN series in an effective fashion resulting in a commendable security posture, compared with other contractors of similar size and complexity. This rating denotes a security program with strong management support, the absence of any serious security issues and minimal administrative findings.

(3) Satisfactory: Satisfactory is the most common rating and denotes that a facility's security program is in general conformity with the basic requirements of the JAFAN series. This rating may be assigned even though there were findings in one or more of the security program elements. Depending on the circumstances, a Satisfactory rating can be assigned even if there were isolated serious findings during the security review.

(4) Marginal: A Marginal rating indicates a substandard security program. This rating signifies a serious finding in one or more security program areas that could contribute to the eventual compromise of classified information if left uncorrected. The facility's size, extent of classified activity, and inherent nature of the problem are considered before assigning this rating. A compliance security review is required within a specified period to assess the actions taken to correct the findings that led to the Marginal rating.

(5) Unsatisfactory: Unsatisfactory is the most serious security rating. An Unsatisfactory rating is assigned when circumstances and conditions indicate that the facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified material in its possession or to which it has access. This rating is appropriate when the security review indicates that the contractor's security program can no longer preclude the disclosure of classified information to unauthorized persons. When an Unsatisfactory rating is assigned, the applicable government contracting activities are notified of the rating and the circumstances on which that rating was based. In addition, a compliance security review must be conducted after a specified interval to assess the corrective actions taken before the contractor's security rating can return to the Satisfactory level.

³ Ratings are based on those published in DSS's Industrial Security Newsletter (ISL) 2006-02 (22 August, 2006).
JAFAN 6-0, Revision 1

1-207. Fraud, Waste, Abuse and Corruption (FWAC). Government and industry fraud, waste, abuse and corruption reporting will be accomplished through channels designated by the service component SAPCO. Do not use other advertised FWAC hotlines when SAP information may be revealed. Therefore, normal FWAC reporting channels (e.g., non-SAP, DoD advertised FWA hotline) must not be used for SAPs.

- a. When requested, confidentiality may be granted. Individuals must be assured that they can report FWAC 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. This information will be prominently displayed throughout each SAPF.
- 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.

1-208. Memorandums of Agreement (MOAs). MOAs are required when SAP resources (i.e. manpower, money, and/or hardware) are committed between programs, DoD components and/or non-DoD activities. MOAs will be approved by the respective service component SAPCO.

1-209. Memorandums of Understanding (MOUs). MOUs are agreements between programs that do not obligate SAP resources.⁴ MOUs will be executed when it is necessary to exchange SAP technology between Services. MOUs maybe approved by the respective Government Program Managers (GPMs) or as specified by the respective Service SAPCO.

1-210. Co-utilization Agreements (CUAs). If multiple SAPs are located within a SAPF, a CUA will be executed between PSOs prior to occupancy. This CUA will define areas of authorities and responsibilities. The first SAP in an area, unless otherwise agreed upon, shall be considered to be the host activity and therefore responsible for the physical security accreditation unless authority or responsibility is otherwise delegated in the CUA. The CUA shall be executed prior to the introduction of the second SAP into the SAPF.

- a. Agencies desiring to co-utilize a SAPF may accept the current accreditation of the cognizant agency. Prospective tenant activities will be informed of all waivers to the requirements of this manual prior to co-utilization. Any security enhancements required by an agency or department requesting co-utilization should be funded by that organization and must be approved by the appropriate service component SAPCO prior to implementation.

⁴ The provisions of a MOU or MOA shall provide for sufficient access by Component Headquarters oversight personnel. These personnel ensure effective oversight exclusively of their Services participation and compliance with the terms of the MOU/MOA in accordance with DoD Directive 5205.7. Determination and approval of need-to-know will be made by the requesting Service SAPCO.

- b. Co-utilization of Sensitive Compartmented Information within a SAPF, or Special Access Program within a Sensitive Compartmented Information Facility (SCIF), will require authorization from the PSO and the servicing Special Security Officer (SSO).

Section 3. Reporting Requirements

1-300. General. The PSO will be made aware of any reports which affect the baseline facility clearance or any incident of a personnel security clearance nature. The PSO will forward all reportable information to the appropriate officials (i.e. Special Access Program Central Adjudication Facility (SAPCAF), CI commands/agencies, etc).

- a. Adverse Information. All briefed personnel 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 Format 2 (Special Access Program Indoctrination Agreement (SAPIA)). A report will be submitted to the PSO on an employee who refuses to sign a SAPIA. If a SAPIA 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. 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.
- e. Foreign Travel. All travel outside the continental United States, Hawaii, Alaska and the U.S. possessions (i.e., Puerto Rico) will be reported to the GSSO/CPSO thirty days in advance. Travel by Program-briefed individuals into or through countries listed on the PSO-provided National Security Threat List, will not be undertaken without prior notification to the PSO. 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 is required upon completion of travel. Provide foreign travel briefings and debriefings in accordance with this paragraph and SAP Format 6 or Sensitive Compartmented Information (SCI) comparable form. A record of all foreign travel will be retained in official personnel Program files. Travel records will be retained for the life of the Program and will be reviewed by the PSO during routine visits.

CPSOs/GSSOs Responsibilities:

- (1) Review all proposed foreign travel itineraries of Program accessed personnel.

- (2) Notify the PSO before program accessed personnel travel to any country, with special emphasis on travel to countries identified on the National Security Threat List.
- (3) Ensure that program accessed personnel traveling outside the continental U.S., Hawaii, Alaska, and the U.S. possessions (i.e. Puerto Rico) except same-day travel to border areas (i.e. Canada or Mexico) are given a foreign travel briefing.
- (4) Within 30 days of completing foreign travel, debrief the traveler and complete section 4 of SAP Format 6 or on the appropriate SCI-equivalent form.
- (5) In coordination with the PSO, follow-up on security or CI-related issues developed as a result of foreign travel.

Same Day Travel:

- a. CONUS-Assigned Personnel: Same-day travel to Canada or Mexico does not require thirty days advance notice, however it will be reported to the GSSO/CPSO. Upon return, a debriefing must be conducted within 30 days.
- b. OCONUS-Assigned Personnel: Same-day travel to border countries does not require thirty days advance notice, but it will be reported to the GSSO/CPSO. Upon return, a debriefing must be conducted within 30 days.
- f. Arms Control Treaty Visits. The GPM and PSO will be notified in advance of any Arms Control Treaty Visits. Such reports permit the GPM and PSO to assess potential impact on the SAP activity and effectively provide guidance and assistance.
- g. Litigation. Litigation or public proceedings which may involve a SAP will be reported. These include legal proceedings and/or administrative actions in which the prime contractor, subcontractors, or Government organizations and their program briefed individuals are a named party. The PSO will be made aware of 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. Violations and Infractions. All security violations will be reported within 24 hours of discovery to the CPSO/GSSO/PSO, as appropriate. Violations involving contractor personnel will be reported by the PSO using the appropriate Defense Security Service (DSS) SAP channels. The PSO, through the chain of command, must promptly advise the service component SAPCO in all instances where national security concerns would impact on collateral security programs or clearances of program-accessed individuals. The PSO shall notify and report security violations to the GPM with copy to the appropriate service component SAPCO. The security official of the affected facility will determine the scope of the corrective action taken in response to this section and report it to the PSO.

a. Security Violations and Infractions:

(1) Security Violation. Any incident that involves the loss, compromise or suspected compromise of classified information. Additionally, (1) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958 or its implementing directives; or (3) any knowing, willful, or negligent action to create or continue a SAP contrary to the requirements of E.O. 12958.

(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 or unclassified HVSACO 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 exposure, and (2) may be requested to complete an Inadvertent Disclosure Form (see SAP Format 5). Inadvertent disclosures will be investigated to determine exposure and compromise.

(1) If during emergency response situations, guard personnel or local emergency authorities (e.g., police, medical, fire, etc.) are inadvertently exposed to program material, they will be interviewed to determine the extent of the exposure. If circumstances warrant, a preliminary inquiry will be conducted. Discuss these actions with the PSO who will make the determination if an inquiry is required.

(2) Refusal to sign an inadvertent disclosure oath will be reported by the GSSO/CPSO to the PSO by the next duty day.

1-302. Social Contact Reporting (other than foreign). Report social contact when:

a. The individual is questioned regarding the specifics of his or her job, organization, mission, etc.

b. Questioning is persistent regarding social obligations, family situations, etc.

c. A request by anyone for illegal or unauthorized access to classified or controlled information.

1-303. Reporting Foreign Contacts. Foreign contacts meeting the following criteria must be reported to the CPSOs/GSSOs within the next business day. The GSSO/CPSO shall provide the information to the PSO. Report any of the following:

- a. Contact with personnel from foreign diplomatic establishments.
- b. Recurring contact with a non-US citizen when financial ties are established or involved.
- c. 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.

Chapter 2 Security Clearances

Section 1. Facility Clearances

2-100. General. DoD Contractors will possess a Defense Security Service (DSS) Facility Security Clearance (validated by the PSO) and be accredited by the PSO IAW JAFAN 6/9 standards prior to receiving, generating, using, and/or storing SAP classified information. Government facilities must be accredited by the PSO IAW JAFAN 6/9 standards prior to receiving, generating, using, and/or storing SAP classified information. The GSSO/CPSO shall notify the PSO of any activity that affects the Facility Security Clearance and/or accreditation.

2-101. Co-utilization of SAPF. If multiple SAPs are located within a SAPF, a CUA will be executed between PSOs following the guidance outlined in paragraph 1-210 of this manual.

Section 2. Personnel Clearances and Access

2-200. General. Personnel security requirements are established in accordance with Executive Order 12968 and JAFAN 6/4. JAFAN 6/4 outlines the procedures for determining access eligibility of personnel to 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 along with a valid need-to-know.

2-201. Supplementary Measures and Polygraph. All personnel having access to DoD SAPs are subject to a random Counterintelligence-scope polygraph examination. However, using a polygraph examination as an access determination requirement shall be a condition specifically approved by the Deputy Secretary of Defense in conjunction with the establishment of the SAP and consistently applied to all candidates according to DoD Directive 5210.48. CI-scope polygraph examinations shall not be used as the only basis for granting access to DoD SAPs.

(Note: See Appendix "G". SAP Format 2a has been rescinded; the polygraph agreement is now incorporated into the SAP Format 2 (JAFAN Edition)(Special Access Program Indoctrination Agreement (SAPIA)).

2-202. Suspension and Revocation. When time is of the essence, service component adjudication authorities and PSOs are empowered to verbally suspend a person's access. Unless unusual conditions prevail, written confirmation of the verbal direction will be provided to the command/contractor no later than the next working day. Suspension of access by a PSO or the SAPCAF for security related reasons must be fully documented and reported to adjudication authorities.

a. Terminology. The following definitions are provided to assist with understanding and implementing the Suspension and Revocation process:

- (1) Suspension of access. An action taken regarding a currently accessed individual as a result of certain personnel security conditions or questionable

circumstances. This action is temporary but access cannot be reinstated until a full review of details and a formal SAPCAF readjudication of the individual's access eligibility is completed.

(2) Revocation of access. An action taken when an individual with current access is formally determined to be ineligible for access after receipt and review of new or additional disqualifying information. Due process and appeal notification procedures are required if the individual is formally determined to be ineligible for access as a result of this action.

b. SAP Suspension and Revocation Process

(1) PSO: The PSO is responsible for taking the following immediate actions when new adverse or questionable information is developed regarding an individual with current access:

(a) Coordinate with the appropriate service component SAPCO or designee and make an initial determination regarding possible access suspension.

(b) If suspension is required, ensure suspension notification information is entered in all appropriate service component SAP personnel access databases.

(c) Notify the GPM and GSSO/CPSO.

(d) Obtain or prepare a detailed report of facts and circumstances.

(e) Provide the information to the service component SAPCAF.

(f) Request an inquiry or investigation to obtain additional details.

(g) Based upon the final report of inquiry or investigation initiate readjudication. Request the SAPCAF review the reports to determine access eligibility.

(h) Provide written notification to the GPM, GSSO/CPSO, and the service component servicing SAPCAF of the readjudication decision if continued access is approved. Ensure access reinstatement information is entered into the service component SAP personnel access databases.

(2) SAPCAF. The service component servicing SAPCAF is responsible for assisting with or completing the following:

(a) Provide general access eligibility guidance and assistance to the PSO.

(b) Provide required initial and final adverse action reports to the service component CAF or to DSS as appropriate.

- (c) Monitor the progress and conclusion of all suspension actions.
- (d) Assist with third tier adjudication requirements as appropriate.
- (e) Assist PSO with due process notifications.
- (f) Assist with notification of access ineligibility to other agencies as appropriate.

2-203. Appeal Process. The requirements of each service component SAPCO appeal process will apply.

2-204. Transfer of Eligibility (TOE). TOE is a process by which an individual's eligibility for access to SAPs may be transferred from one DoD Component or contractor and accepted by another DoD Component or contractor. TOE will be negotiated between the losing and gaining cognizant PSO/PM. Utilize SAP Format 32 (Transfer of Eligibility Request Form) to facilitate the TOE process. Individuals with SAP access may exercise TOE under the following guidelines:

- (a) The individual's Personnel Security Clearance must be currently active and the individual's Personnel Security Investigation (SSBI, Phased Periodic Reinvestigation (PPR), ANACI or NACLC) is current or a PR has been submitted prior to the expiration of the last investigation.
- (b) The individual must have been previously SAP accessed without a Waiver.

2-205. Program Access Roster. GSSOs/CPSOs will maintain current separate program access roster/data base for each program resident within that SAPF when warranted. PSOs may authorize the use of a consolidated program access roster, as warranted. Access rosters will be properly protected and maintained in accordance with the program Security Classification Guide (SCG). The access roster should be continually reviewed and reconciled for any discrepancies. The data base or listing will contain the name of the individual, position, billet number (if applicable), level of access, social security number, and security clearance information. Security personnel will not count against any billet structure.

2-206. Personnel Security Files. Records must be maintained within a personnel security file for each individual accessed to SAP information. These files, which can be paper or electronic, will be maintained by the responsible security officer and will consist of:

- a. Current eQIP Printout or SF 86/SF-86c. (Note: Each individual will review their eQIP printout or SF86/SF86c or equivalent on an annual basis and update it as necessary.)
- b. Consultant Agreement (as necessary).
- c. SAP Format 1 (JAFAN Edition).

- d. SAP Format 2 (JAFAN Edition). (Special Access Program Indoctrination Agreement (SAPIA) *(Note: (see Appendix "G") (SAP Format 2a has been rescinded; the polygraph agreement is now incorporated into the SAP Format 2 (JAFAN Edition))*).
- e. Appointment/Designation/Delegation Letters (for example: CPSO, Top Secret Control Officer (TSCO), Security Manager, Tier Review Official, Classified Courier, etc).
- f. Security Education and Training Awareness Records. (SAP Format 17)
- g. Records of Foreign Travel/Contacts.
- h. SAP Format 5 (Inadvertent Disclosure Form).
- i. Letters of Compelling Need (LOCNs)/Waiver Letters.
- j. Reports of Security Infractions and Violations.
- k. Other Local Files or Records (if legally available).

2-207. Contractor Consultants / Purchase Labor

a. A contractor consultant/purchase labor is an individual whose services are retained 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.

(1) 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 Access Approval Authority (AAA) and PSO. The transfer of a consultant's security clearance will be requested by the sponsoring activity requiring the services. A copy of the Consultant Security Agreement which identifies the consultant's security responsibility should be attached to the transfer request. The consultant will perform classified work at an approved SAPF in accordance with the sponsoring company's DD Form 254. In addition, before the consultant can be considered to perform his or her specialized service, the company sponsoring the consultant must submit to the PSO, a copy of the Professional Service Agreement (PSA) 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 the prospective Consultant Security Agreement, can be adjudicated for access to the program. A Consultant Security Agreement can be obtained from the PSO.

(2) Upon access approval, the consultant will be given a thorough and in-depth security and technical briefing outlining the policies and procedures on how the SAPF operates in a Special Access environment in addition to the specific requirements in regards to the Consultant Security Agreement.

(3) 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. Temporary Help. A Temporary Help Supplier, purchased/leased labor (hereafter referred to as "Purchased Labor") may be necessary, as are Consultants, on a case-by-case basis to provide required services to a command/contractor performing on SAP contracts. In such cases, the "Purchased Labor" must have the appropriate Personnel Security Clearance on file (via their employer) with the sponsoring organization (command/contractor performing on SAP contracts) and be approved for program access by the GPM/PSO.

(1) The sponsoring organization, before the "Purchased Labor" can be considered to perform his/her specialized service on SAPs, must submit to the PSO a copy of the Unclassified Contractual Agreement/Purchase Order and Statement of Work (SOW) detailing specific tasks the "Purchase Labor" will be performing for the sponsoring organization.

(2) The GSSO/CPSO is required to submit the SAP Format 1 (JAFAN 6/4 Edition), including the SOW and a signed copy of the Contractual Agreement/Purchase Order, to the PSO for program access eligibility determination.

2-208. Congressional Access Requirements. Guidance on Congressional access to DoD SAPs is contained in DoD Instruction 5205.11. Should a Member of Congress require SAP access, the DoD SAPCO is to be provided prior notification by DoD Components, through the appropriate service component SAPCO, of any members of the congressional staff or Congress that may be provided access. All communications and information flow between the authorized Congressional Members and staff shall be coordinated through the DoD SAPCO. Legislative employees nominated for access first shall have been the subjects of a favorably-adjudicated background investigation conducted by a DoD-approved investigative agency as appropriate to the personnel security requirements of the particular SAP. The following are those who may be granted access:

a. Members of Congress assigned to the Defense committees (**see Note 1 below*) may be accessed to all DoD SAPs, except waived SAPs. Access to Waived SAPs is restricted to the Chair and the Ranking Minority Member.

**Note 1: Defense Committees includes the House Appropriations Committee (HAC), Senate Appropriations Committee (SAC), House Armed Services Committee (HASC) and Senate Armed Services Committee (SASC). This also applies to the Intelligence committees for Intelligence SAPs. These committees are the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI).*

b. Members of Congress not assigned to the Defense committees (or to the Intelligence committees for Intelligence SAPs) may be granted access to non-waived DoD SAPs with the concurrence of the Department of Defense after consultation with the Chair and the Ranking Minority Member of the defense committees.

c. Access to acknowledged / unacknowledged SAPs by professional staff members (**see Note 2 below) of the Defense and Intelligence committees may be granted with the concurrence of the Department of Defense after consultation with the Chair and the Ranking Minority Member of the Defense committees.

***Note 2: Professional Staff Members must have a favorable DoD adjudication of a Single-Scope Background Investigation (SSBI).*

d. The personal staff of a Member of Congress shall not be granted access to DoD SAPs (note the difference of designation between "professional" staff members vs. "personal" staff members - see para 2-209c above).

Section 3. Foreign Ownership, Control, or Influence (FOCI) & National Interest Determinations (NIDs)

2-300. Policy. Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the policy of the U.S. Government to allow foreign investment consistent with the national security interests of the United States. The following FOCI policy for U.S. companies subject to an FCL is intended to facilitate foreign investment by ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to critical technology, classified information, and special classes of classified information.

a. A U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

b. Whenever a company has been determined to be under FOCI, the primary consideration shall be the safeguarding of classified information. The CSA is responsible for taking whatever interim action is necessary to safeguard classified information, in coordination with other affected agencies as appropriate.

c. A U.S. company determined to be under FOCI is ineligible for an FCL unless and until security measures have been put in place to negate or mitigate FOCI. When a contractor determined to be under FOCI is negotiating an acceptable FOCI mitigation/negation measure, an existing FCL shall continue so long as there is no indication that classified information is at risk of compromise. An existing FCL shall be invalidated if the contractor is unable or unwilling to negotiate an acceptable FOCI mitigation/negation measure. An existing FCL shall be revoked if security measures cannot be taken to remove the possibility of unauthorized access or adverse affect on classified contracts.

d. If the company does not have possession of classified material, and does not have a current or impending requirement for access to classified information, the FCL shall be administratively terminated.

e. Changed conditions, such as a change in ownership, indebtedness, or the foreign intelligence threat, may justify certain adjustments to the security terms under which a company is operating or, alternatively, that a different FOCI negation method be employed. If a changed condition is of sufficient significance, it might also result in a determination that a company is no longer considered to be under FOCI or, conversely, that a company is no longer eligible for an FCL.

f. The Federal Government reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information is effectively precluded and that performance of classified contracts is not adversely affected.

g. Nothing contained in this section shall affect the authority of the Head of an Agency to limit, deny or revoke access to classified information under its statutory, regulatory or contract jurisdiction.

2-301. Factors. The following factors relating to the company, the foreign interest, and the government of the foreign interest, as appropriate, shall be considered in the aggregate to determine whether an applicant company is under FOCI, its eligibility for an FCL, and the protective measures required:

- a. Record of economic and government espionage against U.S. targets.
- b. Record of enforcement and/or engagement in unauthorized technology transfer.
- c. The type and sensitivity of the information that shall be accessed.
- d. The source, nature and extent of FOCI, including whether foreign interests hold a majority or substantial minority position in the company, taking into consideration the immediate, intermediate, and ultimate parent companies. A minority position is deemed substantial if it consists of greater than 5 percent of the ownership interests or greater than 10 percent of the voting interest.
- e. Record of compliance with pertinent U.S. laws, regulations and contracts.
- f. The nature of any bilateral and multilateral security and information exchange agreements that may pertain.
- g. Ownership or control, in whole or in part, by a foreign government.

2-302. Procedures. A company is required to complete a Certificate Pertaining to Foreign Interests when applying for an FCL or when significant changes occur to information previously submitted. In the case of a corporate family, the form shall be a consolidated response rather than separate submissions from individual members of the corporate family.

a. If there are any affirmative answers on the Certificate Pertaining to Foreign Interests, or other information is received which indicates that the applicant company may be under FOCI, the CSA shall review the case to determine the relative significance of the information in regard to:

- (1) Whether the applicant is under FOCI,
- (2) The extent and manner to which the FOCI may result in unauthorized access to classified information or adversely impact classified contract performance; and
- (3) The type of actions, if any, that would be necessary to negate the effects of FOCI to a level deemed acceptable to the Federal Government. Disputed matters may be appealed and the applicant shall be advised of the government's appeal channels by the CSA.

b. When a contractor with an FCL enters into negotiations for the proposed merger, acquisition, or takeover by a foreign interest, the contractor shall submit notification to the CSA of the commencement of such negotiations. The submission shall include the type of transaction under negotiation (stock purchase, asset purchase, etc.), the identity of the potential foreign interest investor, and a plan to negate the FOCI by a method outlined in 2-303. The company shall submit copies of loan, purchase and shareholder agreements, annual reports, bylaws, articles of incorporation, partnership agreements, and reports filed with other Federal agencies to the CSA.

c. When factors not related to ownership are present, positive measures shall assure that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on classified contracts. Examples of such measures include modification or termination of loan agreements, contracts and other understandings with foreign interests; diversification or reduction of foreign-source income; demonstration of financial viability independent of foreign interests; elimination or resolution of problem debt; assignment of specific oversight duties and responsibilities to board members; formulation of special executive-level security committees to consider and oversee matters that affect the performance of classified contracts; physical or organizational separation of the contractor component performing on classified contracts; the appointment of a technology control officer; adoption of special Board Resolutions; and other actions that negate or mitigate foreign influence.

2-303. FOCI Action Plans. The following are the methods that can be applied to negate or mitigate the risk of foreign ownership or control.

a. **Board Resolution.** When a foreign interest does not own voting interests sufficient to elect, or otherwise is not entitled to representation on the company's governing board, a resolution(s) by the governing board shall normally be adequate. The governing board shall identify the foreign shareholder and describe the type and number of foreign-owned shares; acknowledge the company's obligation to comply with all industrial security program and export control requirements; and certify that the foreign owner does not require, shall not have, and can be effectively precluded from unauthorized access to all classified and export-controlled information entrusted to or held by the company. The governing board shall provide for annual certifications to the CSA acknowledging the continued effectiveness of the resolution. The company

shall distribute to members of its governing board and to its key management personnel copies of such resolutions, and report in the company's corporate records the completion of such distribution.

b. Voting Trust Agreement and Proxy Agreement. The Voting Trust Agreement and the Proxy Agreement are arrangements whereby the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government. Under a Voting Trust Agreement, the foreign owner transfers legal title in the company to the Trustees. Under a Proxy Agreement, the foreign owner's voting rights are conveyed to the Proxy Holders. Neither arrangement imposes any restrictions on the company's eligibility to have access to classified information or to compete for classified contracts.

(1) Establishment of a Voting Trust or Proxy Agreement involves the selection of Trustees or Proxy Holders, all of whom must become members of the company's governing board. Both arrangements must provide for the exercise of all prerogatives of ownership by the Trustees or Proxy Holders with complete freedom to act independently from the foreign owners, except as provided in the Voting Trust or Proxy Agreement. The arrangements may, however, limit the authority of the Trustees or Proxy Holders by requiring that approval be obtained from the foreign owner(s) with respect to matters such as:

- (a) The sale or disposal of the company's assets or a substantial part thereof;
- (b) Pledges, mortgages, or other encumbrances on the company's assets, capital stock or ownership interests;
- (c) Mergers, consolidations, or reorganizations;
- (d) Dissolution; and
- (e) Filing of a bankruptcy petition.

However, the Trustees or Proxy Holders may consult with the foreign owner, or vice versa, where otherwise consistent with U.S. laws, regulations and the terms of the Voting Trust or Proxy Agreement.

(2) The Trustees or Proxy Holders assume full responsibility for the foreign owner's voting interests and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign owner shall be insulated from the company, thereby solely retaining the status of a beneficiary. The company must be organized, structured, and financed so as to be capable of operating as a viable business entity independent from the foreign owner.

c. Special Security Agreement (SSA) and Security Control Agreement (SCA). The SSA and SCA are arrangements that, based upon an assessment of the FOCI factors, impose various industrial security and export control measures within an institutionalized set of company practices and procedures. They require active involvement in security matters of senior management and certain Board members (outside directors), who must be cleared U.S. citizens; provide for the establishment of a Government Security Committee (GSC) to oversee classified and export control matters; and preserve the foreign owner's right to be represented on the Board (inside

directors) with a direct voice in the business management of the company while denying unauthorized access to classified information.

(1) When a company is not effectively owned or controlled by a foreign interest and the foreign interest is nevertheless entitled to representation on the company's governing board, the company may be cleared under an SCA. There are no access limitations under an SCA.

(2) A company that is effectively owned or controlled by a foreign interest may be cleared under an SSA arrangement. Access to proscribed information by a company cleared under an SSA may require that the Government Contracting Activity (GCA) complete a National Interest Determination (NID) to determine that release of proscribed information to the company shall not harm the national security interests of the United States. The CSA shall advise the GCA on the need for a NID.

(a) The NID can be program, project or contract specific. A separate NID is not required for each contract under a program or project. The NID decision shall be coordinated with the GCA's Program Executive Office level and approved by the appropriate service SAPCO. If the proscribed information is under the classification or control jurisdiction of another agency, the GCA shall advise the agency; e.g., National Security Agency for COMSEC, Director of National Intelligence (DNI) for Sensitive Compartmented Information (SCI), Department of Energy (DOE) for Restricted Data (RD). These agencies may determine that release to the contractor of an entire category of information under their control may not harm the national security. Use the standard NIDs request package at Appendix "H" and submit to the cognizant SAPCO for approval.

(b) The GCA shall forward the completed NID to the CSA. The CSA shall not delay implementation of a FOCI action plan pending completion of a GCA's NID process as long as there is no indication that a NID shall be denied.

2-304. Citizenship of Persons Requiring PCLs. Under all methods of FOCI mitigation or negation, management positions requiring PCLs in conjunction with the FCL must be filled by U.S. citizens residing in the United States.

2-305. Qualifications of Trustees, Proxy Holders, and Outside Directors. Individuals who serve as Trustees, Proxy Holders, or Outside Directors must be:

a. Resident U.S. citizens who can exercise management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively insulated from the company;

b. Except as approved by the CSA in advance and in writing, completely disinterested individuals with no prior involvement with the company, the entities with which it is affiliated, or the foreign owner; and

- c. Issued a PCL at the level of the facility's FCL.

2-306. GSC. Under a Voting Trust, Proxy Agreement, SSA and SCA, the contractor is required to establish a permanent committee of its Board of Directors, known as the GSC.

- a. Unless otherwise approved by the CSA, the GSC consists of Voting Trustees, Proxy Holders or Outside Directors, as applicable, and those officers/directors who hold PCLs.

- b. The members of the GSC are required to ensure that the contractor maintains policies and procedures to safeguard classified and export controlled information entrusted to it, and that violations of those policies and procedures are promptly investigated and reported to the appropriate authority when it has been determined that a violation has occurred.

- c. The GSC shall also take the necessary steps to ensure that the contractor complies with U.S. export control laws and regulations and does not take action deemed adverse to performance on classified contracts. This shall include the appointment of a Technology Control Officer (TCO) and the establishment of Technology Control Plan (TCP).

- d. The contractor's FSO shall be the principal advisor to the GSC and attend GSC meetings. The Chairman of the GSC must concur with the appointment and replacement of FSOs selected by management. The FSO and TCO functions shall be carried out under the authority of the GSC.

2-307. TCP. A TCP approved by DSS shall be developed and implemented by those companies cleared under a Voting Trust Agreement, Proxy Agreement, SSA and SCA and when otherwise deemed appropriate by the CSA. The TCP shall prescribe all security measures determined necessary to reasonably foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which they are not authorized. The TCP shall also prescribe measures designed to assure that access by non-U.S. citizens is strictly limited to only that specific information for which appropriate Federal Government disclosure authorization has been obtained; e.g., an approved export license or technical assistance agreement. Unique badging, escort, segregated work area, security indoctrination schemes, and other measures shall be included, as appropriate.

2-308. Annual Review and Certification

- a. Annual Review. The CSA shall meet at least annually with the GSCs of contractors operating under a Voting Trust, Proxy Agreement, SSA, or SCA to review the purpose and effectiveness of the clearance arrangement and to establish common understanding of the operating requirements and their implementation. These reviews shall also include an examination of the following:

- (1) Acts of compliance or noncompliance with the approved security arrangement, standard rules, and applicable laws and regulations;

(2) Problems or impediments associated with the practical application or utility of the security arrangement; and

(3) Whether security controls, practices, or procedures warrant adjustment.

b. Annual Certification. For contractors operating under a Voting Trust Agreement, Proxy Agreement, SSA or SCA, the Chairman of the GSC shall submit to the CSA one year from the effective date of the agreement and annually thereafter an implementation and compliance report. Such reports shall include the following:

(1) A detailed description of the manner in which the contractor is carrying out its obligations under the agreement;

(2) Changes to security procedures, implemented or proposed, and the reasons for those changes;

(3) A detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of steps that were taken to prevent such acts from recurring;

(4) Any changes, or impending changes, of key management personnel or key board members, including the reasons therefore;

(5) Any changes or impending changes in the organizational structure or ownership, including any acquisitions, mergers or divestitures; and

(6) Any other issues that could have a bearing on the effectiveness of the applicable agreement.

2-309. Limited FCL. The United States has entered into Industrial Security Agreements with certain foreign governments. Some of these agreements establish arrangements whereby a foreign-owned U.S. company may be considered eligible for an FCL without any additional FOCI negotiation or mitigation instrument. Access limitations are inherent with the granting of Limited FCLs and are imposed upon all of the company's employees regardless of citizenship.

a. A Limited FCL may be granted upon satisfaction of the following criteria:

(1) There is an Industrial Security Agreement with the foreign government of the country from which the foreign ownership is derived.

(2) Release of classified information is in conformity with the U.S. National Disclosure Policy. Key management personnel may be citizens of the country of ownership for whom the United States has obtained security assurances at the appropriate level.

b. In extraordinary circumstances, a Limited FCL may also be granted even if the above criteria cannot be satisfied if there is a compelling need to do so consistent with U.S. national security interests. In any such case, the GCA shall provide a compelling need statement to the CSA to justify the FCL and verify that access to classified information is essential for contract performance. The CSA shall acknowledge the existence of a Limited FCL only to that GCA.

2-310. Foreign Mergers, Acquisitions and Takeovers, and the Committee on Foreign Investment in the United States (CFIUS)

- a. The CFIUS, an interagency committee chaired by the Treasury Department, conducts reviews of proposed mergers, acquisition or takeovers of U.S. persons by foreign interests under section 721 (Exon-Florio amendment) of the Defense Production Act (reference (n)). CFIUS review is a voluntary process and affords an opportunity to foreign persons and U.S. persons entering into a covered transaction to submit the transaction for review by CFIUS to assess the impact of the transaction on U.S. national security.
- b. The CFIUS review and the CSA industrial security FOCI review are carried out in two parallel but separate processes with different time constraints and considerations.
- c. If a transaction under CFIUS review would require FOCI negation or mitigation measures if consummated, the CSA shall promptly advise the parties to the transaction and request that they submit to the CSA a plan to negate or mitigate FOCI. If it appears that an agreement cannot be reached on material terms of a FOCI action plan, or if the U.S. party to the proposed transaction fails to comply with the FOCI reporting requirements of this Manual, the CSA may recommend a full investigation of the transaction by CFIUS to determine the effects on national security.
- d. If the CSA becomes aware of a proposed transaction that should be reviewed by CFIUS, and the parties thereto do not file a joint voluntary notice with CFIUS to initiate review within a reasonable time, the CSA shall initiate action to have CFIUS notified.

Chapter 3 Security Training and Briefings

3-100. General. Every SAP will have a Security Education, Training and Awareness (SETA) program approved by the PSO. GSSOs/CPSOs will ensure that the SETA program meets specific and unique requirements of individual SAPs. The security education program applies to all program-accessed individuals. The use of general, non-program specific and/or company-wide security briefings may be used to form the basis for or supplement the SETA requirement. However, the requirement for providing the unique (program specific) parameters of the program are required for each SAP. Table 1 below outlines training frequency and documentation requirements. Training topics are listed in SAP Format 17.

Type	Frequency	Documentation	Remarks
Indoctrination	One time	SAP Format 2 (<i>see Appendix "G"</i>) (<i>SAP Format 2a has been rescinded; the polygraph agreement is now incorporated into the SAP Format 2 (JAFAN Edition-Oct 07)</i>)	Gear toward specific job being performed
Refresher	Annual	SAP Format 17/ Electronic Data Base	Mandatory subjects
Foreign Travel	Event-driven	Notification of Foreign Travel – see para 3-105	Mandatory subjects
Termination	One time	SAP Format 2	Mandatory subjects

Table 1. Training/Briefing Requirements

3-101. Initial/Refresher Training. Every individual accessed to a SAP will be given an initial indoctrination. Indoctrinations will be conducted by the PSO/GSSO/CPSO or designee. Additionally, each accessed individual will receive refresher training annually. As a minimum the topics covered in SAP Format 17 and the facility Standard Operating Procedures will be discussed. The briefing will clearly identify program specific information which is to be protected and the reasons why. Each individual will review their eQIP/SF86 printout on an annual basis and update it as necessary (annual refresher training sessions are a good opportunity to accomplish this). If the eQIP printout/SF86 is out of date, it may be updated with pen and ink changes made by the candidate. The candidate must also re-sign and re-date the updated eQIP printout/SF86. As an alternative, SF 86c can be utilized to certify/revalidate recent changes to the candidate's eQIP or SF 86.

3-102. Debriefing Acknowledgments. The SAPIA will be executed at the time of the debriefing and forwarded to PSO within two business days. Persons briefed to SAPs will be debriefed by the PSO/GSSO/CPSO or designee and the personnel security access database will be updated to reflect this action. The debriefing will include as a minimum a reminder of each individual's responsibilities according to the SAPIA which states that the individual has no program or program-related material in his/her possession, and that he/she understands his/her responsibilities regarding the disclosure of classified program information.

- a. Design a formal debriefing program that appropriately addresses the following:
 - (1) How to obtain a release before publishing.
 - (2) What can and cannot be discussed or placed in resumes and applications for security clearances.
 - (3) Turning in all holdings.
 - (4) Applicability of, and penalties for, engaging in espionage.
 - (5) Where to report suspected Foreign Intelligence Service (FIS) contacts or any attempt by unauthorized persons to solicit program data. The priority (top to bottom) for reporting this information is as follows:
 - (a) PSO,
 - (b) GSSO/CPSO or member of GSSO's/CPSO's organization,
 - (c) Servicing SAP CI support office,
 - (d) Nearest Federal Bureau of Investigation (FBI) office.
 - (6) Ensure that appropriate espionage laws and codes are available (as an optional handout) and provide the same on request.
- b. Debriefings will be conducted in a SAPF or other secure area when possible, as authorized by the PSO.
- c. Procedures for debriefing will be arranged to allow each individual the opportunity to ask questions and receive substantive answers from the person providing the debrief.
- d. 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 as agreed to in the SAPIA.
 - (2) Remind the individual that the SAPIA is a legal contract between the individual and the U.S. Government.
 - (3) Advise that all classified information to include program information is 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 SAPIA 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 nondisclosure 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 GSSO/CPSO. The individual will be provided a telephone number for the GSSO/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 has signed the Debriefing Acknowledgment portion of the SAPIA, he/she is never released from the original SAPIA unless specifically notified in writing.

e. 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.

f. When access and/or clearance is suspended or an individual is debriefed for cause, the GSSO/CPSO will notify all agency PSOs holding interest in that person's clearance/accesses. The GSSO/CPSO may not be aware of all programs an individual is accessed to the PSO will notify their service component SAPCAF who will notify their service counterparts who are known to have activity at a particular location.

g. The person conducting the debriefing will advise persons who refuse to sign a debriefing acknowledgment portion of the SAPIA 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 CAF and/or DSS. 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.

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

3-103. Administrative Debriefings. Efforts to have all program-briefed personnel sign a Debriefing Acknowledgment portion of the SAPIA may prove difficult. If attempts to locate an individual either by telephone or mail are not successful, and the whereabouts of the individual cannot be determined in 30 days; administratively debrief the individual by completing a debriefing form, annotating the form with "INDIVIDUAL NOT AVAILABLE - ADMINISTRATIVELY DEBRIEFED". The appropriate database should be updated to reflect the individual was debriefed. The GSSO/CPSO will check to ensure that no program material is charged out to, or in the possession of these persons. The personnel security access database will be updated to reflect this action.

3-104. Foreign Travel Defensive Briefing and Debriefing. Briefings and debriefings are required for all accessed personnel prior to and following return of travel using SAP Format 6, Notification of Foreign Travel, or its SCI community equivalent form (either are acceptable). SCI foreign travel related forms (i.e., foreign travel questionnaires and contact reporting) are available in Appendix “G” and DoD 5105.21-M-1 (Appendix ”I”, Attachments 8 and 9— Foreign Travel Questionnaire/Foreign Contacts). Likewise, the SAP Format 27, Foreign Contact Form, or its SCI community equivalent may be used. For example, in order to satisfy both SAP and SCI reporting requirements, an individual with both SAP and SCI accesses need only complete the SCI community equivalent foreign travel forms and submit them to the cognizant PSO and SSO simultaneously. When completing these briefings, include both general and country-specific information and threat advisories, when appropriate. Topics for Foreign Travel Defensive Briefings and Debriefings will include:

- a. Foreign intelligence techniques, terrorist activities, civil situations, or other hazards to personal safety for the region being visited.
- b. Reporting foreign travel and foreign contacts of significance.
- c. Completion and processing procedures for specified reporting forms.
- d. PSOs and CI-elements may ask for additional information as required.

Chapter 4 Classification and Markings

Section 1. Classification

4-100. General. All SAP indoctrinated individuals share responsibility for accuracy, currency, and necessity of classification applied to documents and material.

4-101. Program Classification. Each SAP will have a Security Classification Guide to identify Critical Program Information (CPI). Challenges to SAP classified information and/or material classifications shall be forwarded through the PSO to the appropriate Original Classification Authority (OCA). All such challenges shall remain in program channels.

4-102. Nicknames and Code Words. Special access programs and subcompartments will be identified by a two word unclassified nickname and/or a single codeword. Nicknames and codewords must be selected and registered based on procedures specified in Chairman Joint Chief of Staff Manual (CJCSM) 3105.29B, "Codeword, Nickname, and Exercise Term (NICKA) System", to prevent inadvertent duplication.

4-103. Contract Security Classification Specification (DD Form 254) Requirements

- a. DD Forms 254 will be prepared for each contractor performing work on SAPs. This form will be used to transmit the SCG and/or other documents containing security guidance.
- b. Do not attach lengthy attachments to DD Forms 254 that merely repeat information, policy, and/or procedures contained in any other security directive.
- c. The PSO will review and coordinate the DD Form 254 with the Government Contracting Officer (GCO). The GCO will approve the 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 review before release to subcontractors.
- d. The PSO provides guidance on preparation of DD Forms 254 related to classification, release to the DSS, carve-out status, etc.

Section 2. Marking Requirements

4-200. General. Classified material developed under a SAP will be marked and controlled in accordance with this manual, NISPOM (baseline marking requirements), the program SCG, and other program guidance.

4-201. TOP SECRET Engineering Notebooks. TOP SECRET engineering notebooks will be permanently bound documents. Notebook pages will not be removed. These notebooks will adhere to the following guidelines:

- a. Each notebook will be entered into the TOP SECRET accountability system;

- b. The outer covers and each page will be marked with the highest classification and program identification(s) contained in the notebook;
- c. Classification Authority/Declassification Instructions will be marked according to the program SCG;
- d. Each page will be numbered consecutively, front and back, i.e. 1 of 50, 2 of 50, etc. Data incorporated/attached will not be removed;
- e. Portion markings are not required;
- f. A Table of Contents is not required;
- g. Engineering notebooks created prior to this issuance of this manual may be retained for historical reference without adherence to the aforementioned requirements.

4-202. Cover Sheets. Cover sheets are required except when stored in security containers. Cover sheets when used as a Record of Disclosure will remain affixed to TOP SECRET documents at all times.

Chapter 5

Safeguarding Classified Information

Section 1. General Safeguarding Requirements

5-100. General. SAP classified and unclassified HVSACO material must be appropriately stored in approved SAPFs. Any deviations must have prior approval of the service component SAPCO or designee. Deviations as a result of emergency or unforeseen conditions may be approved by the PSO with notification to the SAPCO within 24 hours of the deviation.

5-101. Use of STE/STU-III Encryption. SAP Government and Industry personnel are encouraged to use the "SECURE" mode on STE/STU-III telephones for all business discussions and are required to use encryption when talking about specific program matters. Crypto Ignition Keys (CIK) may remain in STU-III telephones and Krypton Crypto Cards (KCC)/Fortezza Cryptocards may remain in STE telephones located within SAP accredited facilities at all times when the following conditions are met:

- a. All resident personnel in the facility are cleared to the same level or higher as programmed on all STE/STU-III telephones within the facility;
- b. All unescorted visitors in the facility are cleared to the same level or higher as programmed on all STE/STU-III telephones within the facility, and
- c. All escorted visitors are closely monitored and if allowed to use a STE/STU-III telephone will be strictly monitored.

Note: CIKs/KCCs are controlled cryptographic items and accountability must be maintained at all times. The individual user/custodian will retain accountability responsibility for the CIK/KCC. Misuse or loss of a CIK/KCC is immediately reported to the COMSEC custodian as well as the PSO/GSSO/CPSO.

Section 2. Control and Accountability

5-200. General. An information management system will be developed and maintained which enables control of SAP classified information. This system must reflect external receipt and dispatch records for all SAP material. The system must reflect the date of receipt or dispatch, the classification, and the unclassified description of the material.

5-201. Accountability/Accountability System. The following types of classified information require accountability:

- a. All TOP SECRET SAP information. This material will be entered into a PSO approved document control accountability system whenever it is received, generated or dispatched either internally or externally to other SAPFs. This accountability system will be required to produce a Master Document Listing that reflects all transactions within 30 days of generation, receipt or dispatch. If an automated system is used, a backup duplicate record (manual or automated) will be maintained. Maintain an

access disclosure sheet (see Appendix "G") for each Top Secret Document. Record the identity of the persons given access to the information and the date of the disclosure on the cover sheet. Record the name only once regardless of the number of times subsequent access occurs.

- b. All COMSEC material will be accounted for in accordance with published COMSEC guidelines.
- c. Media Control System. Media control is addressed in Chapter 8 of this manual and JAFAN 6/3.
- d. At the direction of the service component SAPCO, full accountability may be required for SECRET/SAP material.
- e. SAP TOP SECRET Control Officials (TSCOs) shall be designated in writing by the Program Manager. The SAP TSCO will be responsible to the for the receipt, dispatch, transmission, and maintenance of access and accountability records for TOP SECRET SAP information.
- f. Each item of TOP SECRET SAP material will be:
 - (1) numbered in series and identified with an individual copy number and total copy count (i.e., Copy 6 of 13 Copies);
 - (2) copies generated from an original copy will be marked as follows: "Copies generated from Copy 6 (original) will be marked Copy 6A, Copy 6B, etc)";
 - (3) annotated with an individual Document Control Number on each page of the document;
 - (4) numbered consecutively and include a total page count (i.e., Page 6 of 13 Pages).

5-202. Annual Inventory. Annually a 100 percent inventory of accountable SAP classified will be conducted by the TSCO or alternate and a disinterested party. Inventories will be conducted by sighting all copies of accountable material held within the facility. The results of the inventory will be maintained in the SAPF and made available during security inspections. Discrepancies will be immediately reported to the PSO and investigated.

5-203. TOP SECRET/SAP Working Papers Accountability and Marking

- a. TOP SECRET/SAP working papers shall be properly classified, program marked and protected in an approved SAPF. Attach a cover sheet marked with the date of origin, originator's name and annotation "WORKING PAPER" on the cover sheet. Also add the "Destroy Not Later Than Date" to the document.
- b. TOP SECRET/SAP working papers shall either be entered into the accountability system or destroyed after 30 calendar days from the date of origin.
- c. Prior to transmission outside of the SAPF a TOP SECRET/SAP working paper will be appropriately marked and brought into formal accountability.

5-204. SECRET/SAP Working Papers. If the service component SAPCO established an accountability requirement for program SECRET/SAP material, then the instructions in this manual shall apply to all SECRET/SAP working papers and Engineering Notebooks.

5-205. Collateral Classified Material. Such 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 another SAP or collateral program. The process for introduction of collateral material will be approved by the PSO.

Section 3. Storage and Storage Equipment

5-300. General. Refer to JAFAN 6/9 for physical security requirements of SAPFs. Nothing in this manual shall be construed to contradict or inhibit compliance with the law or building codes. Cognizant security officials shall work to meet appropriate security needs according to the intent of this manual and at an acceptable cost.

5-301. General Services Administration (GSA) Storage Equipment. GSA establishes and publishes uniform standards, specifications, and supply schedules for security containers, vault door and frame units, and key-operated and combination padlocks suitable for the storage and protection of classified information. Manufacturers, and prices of storage equipment approved by the GSA, are listed in the Federal Supply Schedule. Copies of specifications and schedules may be obtained from any regional office of the GSA.

Section 4. Transmission

5-400. General. SAP classified material will only be transmitted outside the SAPF using one of the methods identified within this section. Establish a focal point to oversee transmission of program material. Use the following order of precedence:

- a. Cryptographic communications systems (Secure Facsimile/IS).
- b. Courier (PSO approval required for commercial courier).
- c. Defense Courier Service (DCS) for TOP SECRET SAP only.
- d. United States Postal Service (USPS) for SECRET SAP and below

5-401. Preparation. All classified SAP material will be prepared, reproduced, and packaged by program-briefed personnel in SAPFs.

- a. Receipts are required for the transmission of all classified (SECRET/TOP SECRET) material.
 - (1) Classify receipts only when compilation of subject material requires classification.

(2) Show an unclassified address on the "TO" and "FROM" blocks.

b. When a receipt or acknowledgment of a shipment of material is not returned within 30 days:

(1) Initiate tracer action.

(2) Reproduce a copy of the receipt held in suspense control files; mark it "TRACER ACTION-ORIGINAL RECEIPT NOT RECEIVED-PLEASE RESPOND WITHIN 7 DAYS".

(3) Send the tracer receipt to the intended recipient of the initial transmission.

(4) If the recipient does not respond within 15 days or did not receive the material, immediately initiate a preliminary inquiry.

c. SAP information requires double-wrapping using opaque material which precludes observation of contents. Materials used for packaging shall be of such strength and durability to ensure the necessary protection while the material is in transit. Include name of the person or activity for whom the material is intended. Retain an inventory of the material until verification is received that the information was delivered to an authorized recipient. Prepare packages for distribution as described below:

(1) Inner Wrapper

(a) Place address of receiving SAPF in the center of package; place address of sending SAPF in upper left corner.

1. Stamp or print in large letters above the pouch address of the receiving SAPF: "TO BE OPENED ONLY BY (appropriate SAP security official, i.e. PSO, GSSO, CPSO or combination thereof)."

2. Stamp or print in large letters on each side, the appropriate security classification, appropriate Di/Trigraph(s) and handling caveat. SAP code words will not be used on any wrapper.

3. Besides the classification markings, inner containers will be marked with the following:

<p style="text-align: center;">TO BE OPENED ONLY BY: (Insert the name of the individual to whom the material is sent.) (A receipt may be required.)</p>
--

4. Also 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. IF FOUND, PLEASE DO NOT OPEN. CALL THE FOLLOWING NUMBERS: *(area code) (number)* (PSO/GSSO/CPSO work number) DURING WORKING HOURS OR *(area code) (number)* (PSO/GSSO/CPSO) AFTER WORKING HOURS.

Note: See Appendix "A" for additional guidance regarding control, dissemination, and transmission of HVSACO.

(2) Outer Wrapper

- (a) Place the address of receiving SAPF in the center of the package; place address of sending SAPF in the upper left corner.
- (b) Secure outer containers by a means which will identify surreptitious access.
- (c) When the use of DCS is authorized/approved, packages will be prepared in accordance with published DCS guidelines.
- d. SAP material will be transported from one SAPF to another in an unobtrusive and secure manner. For local travel, SAP material may be hand-carried using a locked container as the outer wrapper. Local travel is defined as within a 50 mile radius of the originating facility. Attach a tag or label with the following the individual's name, organization and telephone number.

5-402. Couriers. The PSO/GSSO/CPSO will provide detailed courier instructions to program briefed couriers when hand-carrying SAP material.

- a. TOP SECRET/SAP: Two-person courier teams are required for all TOP SECRET/SAP data unless a single-person courier is approved in advance by the cognizant PSO.
- b. SECRET/SAP or below: A single-person courier may be used for SECRET/SAP and below materials.

Note: Provisions shall be made for additional couriers and/or overnight storage (regardless of classification) when it appears continuous vigilance over the material cannot be sustained by a single individual.

- c. Courier Authorization letters (i.e., SAP Format 28) or card. As a minimum, the PSO/GSSO/CPSO from the departure location will provide each authorized courier with a copy of the Courier Authorization letter outlining the courier procedures.

- (1) At a minimum, the Courier Authorization and pre-departure instructions should address the: a) method of transportation, b) travel itinerary (intermittent/unscheduled stops, remain-overnight scenarios, etc), c) specific courier

responsibilities (primary/alternate roles-as necessary), and d) completion of receipts (as necessary) and full identification of the classified data being transferred and e) a discussion of emergency/contingency plans (include after-hours POCs, primary/alternate contact data, telephone numbers, etc). Each courier will acknowledge receipt/understanding of this briefing in writing.

(2) Experienced program-briefed individuals who frequently or routinely perform duties as classified couriers may be issued Courier Authorization cards by the PSO/GSSO/CPSO in lieu of individual letters for each trip (this does not negate the necessity for a complete understanding of courier responsibilities listed above, but does alleviate the requirement to acknowledge receipt/understanding of the briefing in writing). Courier cards should be revalidated/reissued annually.

d. The Transportation Security Administration (TSA) publishes airport screening guidelines for handling classified material. PSOs will ensure couriers are aware of the limitations and restrictions surrounding screening procedures which include:

(1) Classified materials must not be opened or read by screeners.

(2) Screeners should be discreet when they learn that a passenger is carrying classified material.

(3) Screeners should not bring public attention to the passenger.

(4) Screeners will not know that a passenger is carrying classified materials unless it becomes necessary to inspect the bag containing the material.

(5) If screeners request to inspect the bag containing classified material, carriers of government classified material will notify the screener that they would like to have the bag inspected in private. The screener should notify the screening supervisor of the need for a private screening.

(6) Couriers having their bag inspected in private will present a copy of the Courier Authorization letter/card authorizing him or her to carry classified material.

(7) Under no circumstances will screeners open or request the passenger to open the double-sealed envelopes containing the classified material. If necessary, couriers may authorize the screeners to remove the sealed envelopes containing the classified material from the outer container such as a briefcase or pouch.

e. Problems encountered enroute will be immediately reported to the PSO. The PSO may authorize exceptions to the above requirements when operational considerations or emergency situations dictate.

Note: Screeners may gently pat down the outside of the envelopes. However, under no circumstances shall the screeners open or request the passenger to open the envelopes containing the classified material. The most significant change to DoD SAP Courier actions is the need to request a "Private Screening" if/when TSA airport screening personnel request to view the material being hand carried. Upon private screening, SAP couriers are to present valid courier authorization/identification to TSA authorities and, if needed, assist them in contacting the SAP official authorizing the carrying of classified material aboard commercial aircraft. If the screening supervisor satisfactorily concludes that no prohibited items are present, the classified materials shall be cleared for transport. However, if the screening supervisor cannot make that determination, he or she shall inform the passenger that the materials cannot be transported; the courier contacts the originating PSO and returns to the originating activity.

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 will approve the system in writing. TOP SECRET documents require a separate receipt on the secure facsimile at the time of transmission. The provisions of this section do not apply to the electronic transmission of information within an information system network. Guidance on information system networks is contained in JAFAN 6/3. The following additional rules apply to secure facsimile transmission:

- a. Do not use facsimile terminals equipped with the automatic polling function enabled unless authorized by the PSO.
- b. When approved by the PSO, SAP documents classified SECRET/SAP and below may be receipted for via an automated generated message that confirms undisturbed transmission and receipt. This provision does not apply, however, to TOP SECRET or TOP SECRET/SAP documents transmitted over a secure facsimile terminal. Receipting for TOP SECRET or TOP SECRET/SAP documents passed over a secure facsimile terminal must adhere to standard receipt procedures for TOP SECRET material. The recipient must acknowledge receipt of the TOP SECRET material and return his/her signature to the sender on a receipt at the time of transmission.

5-404. U.S. Postal Mailing. When approved by the PSO, a U.S. Postal mailing channel may be established to ensure mail is received only by appropriately cleared and accessed personnel. Use USPS registered mail or USPS Express Mail for SECRET/SAP material. Use U.S. Postal Service certified mail for CONFIDENTIAL/SAP. "For Official Use Only" and unclassified HVSACO material may be sent by First Class mail. When associations present an OPSEC concern, sterile P.O. Boxes may be established with approval of the PSO.

- a. Except for TOP SECRET, a U.S. Government approved contract carrier (i.e. United States Postal Service (USPS) Express Mail) can be used for overnight transmission on a case-by-case basis with approval of the PSO. Packages may only be shipped on Monday through Thursday to ensure that the carrier does not retain the classified package over a weekend.
- b. These methods of transmitting selected special access materials are in addition to, not a replacement for, other transmission means previously approved

for such material. Use of secure electronic means is the preferred method of transmission.

- c. Use overnight delivery only when:
 - (1) Approved by the PSO.
 - (2) It is necessary to meet program requirements.
 - (3) It is essential to mission accomplishment.
 - (4) Time is of the essence, negating other approved methods of transmission.
- d. To ensure direct delivery to address provided by the PSO:
 - (1) Do not execute the Waiver of Signature and Indemnity on USPS Label.
 - (2) Do not execute the release portion on commercial carrier forms.
 - (3) Ensure an appropriate recipient is designated and available to receive material.
 - (4) Do not disclose to the express service carrier that the package contains classified material.
- e. Immediately report any problem, misdelivery, loss, or other security incident encountered with this transmission means to the PSO.
- f. Before any movement of classified SAP assets develop a transportation plan and obtain the PSO's approval at least 30 days in advance of the proposed movement. 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 Program Security requirements.

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.C., Titles 10 and 42. Any attempt by unauthorized personnel to obtain program information and sensitive data will be reported immediately to the GPM through the PSO. Do not release information concerning programs or technology to any non-program-accessed individual, firm, agency, or Government activity without

SAPCO approval. Do not include classified or sensitive information concerning SAPs in general or unclassified publications, technical review documents, or marketing literature. Submit all material proposed for release to the GPM through the PSO 60 days before the proposed release date. After an approval is granted additional case-by-case requests to release identical data are not required. Releases will be tracked by the SAP program office.

Note: Public release of information is defined as the release of any program information, or program related material, regardless of its classification. Submit any program information intended for discussion at symposia, seminars, conferences, or other form of non-program meeting to the GPM and PSO for review and approval 60 days before intended attendance and release. Program history, system technological advances, operational concepts, special management functions and techniques, and relationships with non-DoD activities remain classified, requiring special access authorization. The CSA controls disposition and access to historical material.

Section 6. Reproduction

5-600. General. Program material will only be reproduced on equipment approved by the PSO. The GSSOs/CPSOs will be required to prepare written reproduction procedures. Post a notice indicating if equipment can or cannot be used for reproduction of classified material. Equipment may be used outside a SAPF (i.e.; within a Temporary Secure Work Area), provided written procedures are approved by the PSO (including procedures for clearing of equipment, accessing of operators, clearing of media, handling malfunctions, etc.). Position reproduction equipment to assure immediate and positive monitoring.

Note: Advancement in technology has warranted a more in-depth review and closer scrutiny of reproduction equipment to preclude unauthorized disclosures through overlooked or undefined capabilities, i.e. remote diagnostics, dial-up connectivity, networking capabilities and data retention within removable and non-removable magnetic media. Refer to JAFAN 6/3 for further guidance.

Section 7. Disposition and Retention

5-700. Disposition. GSSOs/CPSOs may be required to inventory, dispose of, request retention, or return for disposition all classified SAP-related material (including IS media) at contract completion and/or close-out. Request for proposals, solicitations, or bids and proposals 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 will be submitted to the PSO and Program Contracting Officer for concurrence. Upon contract close-out, requests for retention of classified information will be submitted to the Contracting Officer through the PSO for review and approval.

5-701. Retention of SAP Material. Contractors are required to submit a request to the Contracting Officer through the PSO for authority to retain classified material beyond the end of the contract performance period. The contractor will not retain any program information unless specifically authorized in writing by the Contracting Officer. A final DD Form 254 will be issued for the storage and retention of program material. Storage and control requirements will be approved by the PSO.

5-702. Destruction. Appropriately indoctrinated personnel shall ensure the destruction of classified SAP data. Accountable SAP material will be destroyed using two program-briefed employees. Non-accountable SAP material may be destroyed by a single program-briefed employee. See JAFAN 6/3 for destruction procedures for Information System Media and associated material and hardware.

5-703. Destruction Procedures and Equipment. 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. Destruction Time Requirements. Destroy all classified waste as soon as possible, but do not allow materials to accumulate beyond 30 days unless approved by the PSO. Consider all material, including unclassified, generated in program areas as classified waste and destroy accordingly.

5-705. Methods of Destruction. Classified material may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing (for example, hammer mills, choppers, and disintegration equipment). Pulpers, pulverizers, or shredders may be used only for the destruction of paper products. High Wet Strength paper, paper mylar, durable-medium paper substitute, or similar water repellent type papers are not sufficiently destroyed by pulping or shredding; other methods such as disintegration or burning shall be used to destroy these types of papers. Residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed. Only NSA approved crosscut shredders will be used to destroy program information. Classified material in microform; that is, microfilm, microfiche, or similar high data density material may be destroyed by burning or chemical decomposition or other methods as approved by the PSO.

- a. Public destruction facilities may be used only with the approval of and under conditions prescribed by the PSO.
- b. COMSEC material will be destroyed in accordance with National Security Agency requirements.

5-706. Destruction Certificates. Prepare certificates of destruction itemizing each accountable document or material destroyed, to include citing the appropriate document control and copy number. Destruction certificates must be completed and signed by both of the individuals completing the destruction immediately after destruction is completed.

Section 8. Construction Requirements

5-800. General. See JAFAN 6/9 for all SAPF physical security and construction requirements.

Section 9. Control of Portable Electronic Devices (PEDs)

5-900. Control of Electronic Equipment within Special Access Program Facilities

(SAPFs). Electronic equipment poses an inherent vulnerability and must be controlled. Portable Electronic Devices (PEDs) are portable electronic devices assigned to and used as work-related support tools. "PED" is a generic term used to describe a wide-range of readily available, small electronic items, including cellular telephones, two-way pagers, palm sized quasi-computing devices such as Palm Pilots®, Blackberries®, Handspring® devices or similar personnel data assistants (PDAs), data diaries, palmtop, laptop, and other portable computing devices, two-way radios, devices with audio/video/data recording and playback features, watches and other devices with communications or synchronization software/hardware.

a. The introduction of these tools pose an unacceptable risk to classified information and the SAPF. PEDs with the exception of the following, are prohibited within a SAPF:

- (1) Electronic calculators, spell checkers, language translators, etc.
- (2) Receive-only pagers.
- (3) Audio and video playback devices.
- (4) Receive only Radios.
- (5) Infrared (IR) devices that convey no intelligence data (text, audio, video, etc.), such as an IR mouse and/or remote controls.

b. Medical, life and safety portable devices. To accommodate those personnel who bring personal electronic equipment to their work location, designated areas may be identified at the entry point to all program areas for the storage of these devices. Where PED storage areas/containers are allowed by the PSO to be within the SAPF, the PEDs will be turned off and power source removed. These designated PED storage areas/containers will be confined to designated "Non-Discussion" areas.

c. Mission essential government/contractor owned laptops introduced into the SAPF facility will be approved by the PSO and conform to the requirements outlined in JAFAN 6/3.

d. Waivers to this policy shall be in writing and approved by the SAPCO or designee. Requests for waivers shall be:

- (1) approved on a case-by-case basis based on mission requirements;
- (2) coordinated with appropriate DAAs for each affected IS within the SAPF;
- (3) valid for a limited, specific duration;
- (4) identify mitigations, if any; and
- (5) identify risks (after mitigation) to classified information.

Chapter 6

Visits and Meetings

Section 1. Visits

6-100. General. A written/electronic visit notification (see para 6-101 below) will be coordinated in advance and acknowledged/approved prior to visiting a SAPF. All visit requests will be transmitted via PSO-approved channels, and can be:

- a. Hard copy. Use SAP Format 7, Visit Notification (Authorization) Request, or other PSO-approved equivalent form for this purpose.
- b. Electronic transfer/database. Secure electronic transmission or data transfer system approved by the PSO.

6-101. Visit Request Procedures.

a. Advance planning. SAP indoctrinated personnel must make every effort to provide ample advance notification to their supporting security office. They will work closely with the GSSO/CPSO/PSO in coordinating the requisite SAP accesses/badging and courier requirements (if any).

(1) Routine Visit Requests. The GPM or his/her designated representative will approve all visits between program activities. The PSO or designee will certify the accesses to the facility.

(a) Visits between a prime contractor and the prime's subcontractors (and/or approved associates) may be approved by the Contractor Program Manager (CPM).

(b) The CPSO will certify the SAP accesses to the facility.

(2) Emergency Visit Requests. Unforeseen operational or emergency situations may arise which warrant the PSO's passing a verbal visit certification telephonically. Each instance of a verbal authorization will be followed-up with written certification/confirmation within 24 hours.

(3) Courier/Hand carrying Activity. Advance arrangements will be coordinated between the visitor, the visitor's cognizant security officer and the destination facility's security officer regarding the hand carrying of program material.

b. Duration. Twelve-month visit requests are not authorized unless approved in writing by the PSO.

c. Cognizant PSO Exemption. In the execution of their program security oversight roles, the PSO and supporting security staff members (as determined by the PSO) may visit all program facilities under their cognizance without furnishing advanced notification.

- d. Validation/Identification of Visitors. The positive identification of each visitor will be made using an official State or Federal-issued identification card/credential with a photograph.
- e. Unannounced/Non-Validated Arrivals. Deny access and notify the GSSO/CPSO or PSO whenever any visitor arrives at a Government or contractor facility unannounced or without the requisite SAP accesses.
- f. Escorting of Visitors. Continuously escort and closely control movement of non-program accessed visitors requiring access to a SAPF. Use only resident program-accessed personnel as escorts. Consider installing an internal warning system (such as rotating light beacons, etc) to warn accessed occupants of the presence of uncleared personnel. Employ other or additional methods (e.g., verbal announcements) to warn or remind personnel of the presence of uncleared personnel.
- g. 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 PSO/GSSO/CPSO or his/her designated representative will immediately notify all recipients of the cancellation or termination of the visit request.

6-102. Non-Program-Briefed Visitor Record. All non-program briefed personnel (e.g., maintenance workers, repair technicians, etc) are required to complete the visitor's record and be escorted by a resident program-briefed individual. Sanitization procedures will be implemented in advance to ensure SAP information is not discussed/exposed whenever a non-briefed visitor is in the area. Show the visitor's name, last four digits of the individual's SSN, organization or firm, date, time in and out, and sponsor on the log.

6-103. Program Briefed Visitor Record. A separate program visitor's record will be established for program briefed visitors. This record will be maintained inside the SAPF. Maintain a visitor sign-in and sign-out record for all accessed program visitors. Show the visitor's name, last four digits of the individual's SSN, organization or firm, date, time in and out, and sponsor on the log.

6-104. Guidelines for Congressional Visits. The service component SAPCO will provide the necessary guidance when a proposed Congressional visit to a SAPF is proposed. In the event of the unannounced arrival of a Congressional delegation, the command/ contractor shall contact the PSO for guidance. The PSO shall contact the service component SAPCO for instructions. All communications and information flow between the authorized Congressional Members or their staff shall be coordinated through the SAPCO.

Section 2. Meetings

6-200. General. Conduct meetings and conferences only in approved SAPFs. PSOs may authorize additional locations, i.e. Temporary Secure Working Area (TSWA).

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

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

Note: Use SAP Format 8 to request the TSCM.

Chapter 7

Subcontracting

7-100. General. This section addresses the responsibilities and authorities of prime contractors concerning the release of classified SAP information to subcontractors. The prime contractor will determine the scope of the bid and procurement effort prior to entering into a formal relationship with the prospective subcontractor. The prime contractor will obtain approval from the PSO prior to any release of classified information. When conducting business with non-program briefed subcontractors, prime contractors will ensure program information is not inadvertently released. Any relationship with a prospective subcontractor requires prior approval by the PSO. The PSO will ensure that the association with the government activity or any program capability is not disclosed.

7-101. Determining Clearance Status of Subcontractors

- a. Facility. When a subcontractor does not have the requisite facility clearance, the prime CPSO will initiate the necessary FCL paperwork and submit to the PSO. The PSO will coordinate with DSS to initiate action to provide the subcontractor a facility clearance.
- b. Personnel. All subcontractor personnel will have the appropriate security clearance and meet the investigative and access eligibility criteria prior to being briefed into a SAP. In the event a subcontractor does not have the appropriate security clearances, the prime contractor will request that the cognizant PSO assist with the appropriate security clearance action.

7-102. Security Agreements and Briefings. In the pre-contract phase, the prime contractor will 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. The CPSO will complete a SAP Format 13, Subcontractor/Supplier Data Sheet, for submission to the PSO. Discussions with prospective subcontractors may occur provided they are limited to general interest topics without association to the government agency and scope of effort. The CPSO will include the reason for considering a subcontractor and attach a proposed DD Form 254 to the SAP Format 13. The DD Form 254 shall be tailored to be consistent with the proposed support being sought. The DD Form 254 may be classified based on its content.

7-103. Transmitting Security Requirements. DD Form 254s are prepared by prime contractor CPSOs and forwarded to the PSO for approval before signature by the prime contractor and release to subcontractors. PSOs will coordinate these DD Form 254s with the GPM and Government Contracting Officer (GCO).

Chapter 8

Information Assurance (IA)

8-100. Information Assurance Guidance. JAFAN 6/3, “Protecting Special Access Program Information within Information Systems“, is applicable to all government and contractor personnel participating in SAPs. Questions concerning the requirements of JAFAN 6/3 will be referred to the PSO. In cases of emergency requiring immediate attention, the action taken should protect the Government's interest and the security of the program from compromise.

Note: A non-technical supplement, "JAFAN 6/3 Implementation Guide", was developed to assist with the implementation of JAFAN 6/3. This supplement is made available through the PSO.

8-101. IS Media Control System. A system of procedures, approved by the PSO, which provides controls over use, possession, and movement of media in SAPFs. These procedures must insure all media (classified and unclassified) is adequately protected to avert the unauthorized use, duplication or removal of the media. Unclassified media must be secured in limited access containers or labeled with the identity of the individual responsible for maintaining the material.

8-102. Data Storage Media. The Information Assurance Manager (IAM)/Information Assurance Officer (IAO) must develop and implement procedures for the control of data storage media that demonstrate a reasonable capability to protect SAP 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 media in the SAPF. The procedures will be described in the ISSP.

8-103. TOP SECRET Electronic Files. These files do not need to be receipted when transmitted between system users within the same unified network provided the information/data remains resident within the information system. All TOP SECRET output will be brought into the accountability system at the facility where the document is printed in accordance with this manual.

Chapter 9

International Security Requirements

Section 1. General and Background Information

9-100. General. This Chapter provides policy and procedures governing the control of classified information in international programs.

9-101. Applicable Federal Laws. The transfer of articles and services and related technical data to a foreign person, within or outside the U.S., or the movement of such material or information to any destination outside the legal jurisdiction of the U.S. constitutes an export. Depending on the nature of the articles or data, most exports are governed by the Arms Export Control Act (AECA) (reference (u)), the Export Administration Act (EAA) (reference (v)), and reference (c).

9-102. Bilateral Security Agreements. Bilateral security agreements are negotiated with various foreign governments. Confidentiality requested by some foreign governments prevents a listing of the countries that have executed these agreements.

a. The General Security Agreement, negotiated through diplomatic channels, requires that each government provide to the classified information provided by the other substantially the same degree of protection as the releasing government. The Agreement contains provisions concerning limits on the use of each government's information, including restrictions on third party transfers and proprietary rights. It does not commit governments to share classified information, nor does it constitute authority to release classified material to that government. It satisfies, in part, the eligibility requirements of reference (u) concerning the agreement of the recipient foreign government to protect U.S. classified defense articles and technical data. (The General Security Agreement also is known as a General Security of Information Agreement and General Security of Military Information Agreement. The title and scope are different, depending on the year the particular agreement was signed.)

b. Industrial security agreements have been negotiated with certain foreign governments that identify the procedures to be used when foreign government information is provided to industry. The Office of the Under Secretary of Defense (Policy) negotiates Industrial Security Agreements as an Annex to the General Security Agreement and the Director, DSS, has been delegated authority to implement the provisions of the Industrial Security Agreements. The Director of Security, NRC, negotiates and implements these agreements for the NRC.

Section 2. Disclosure of U.S. Information to Foreign Interests

9-200. Authorization for Disclosure. Disclosure guidance will be provided by the GCA. Disclosure authorization may be in the form of an export license, a technical assistance agreement, a manufacturing license agreement, a letter of authorization from the U.S. Government licensing authority, or an exemption to the export authorization requirements. Disclosure guidance provided for a previous contract or program shall not be used unless the contractor is so instructed in writing by the GCA or the licensing authority. Classified information normally will be authorized for disclosure and export as listed below:

- a. Government-to-Government International Agreements. Classified information shall not be disclosed until agreements are signed by the participating governments and disclosure guidance and security arrangements are established. The export of technical data pursuant to such agreements may be exempt from licensing requirements of the International Traffic in Arms Regulation (ITAR) (reference (w)).
- b. Symposia, Seminars, Exhibitions, and Conferences. Appropriately cleared foreign nationals may participate in classified gatherings if authorized by the Head of the U.S. Government Agency that authorizes the conduct of the conference.
- c. Foreign Visits. Disclosure of classified information shall be limited to that specific information authorized in connection with an approved visit request or export authorization.
- d. Temporary Exports. Classified articles (including articles that require the use of classified information for operation) exported for demonstration purposes shall remain under U.S. control. The request for export authorization shall include a description of the arrangements that have been made in-country for U.S. control of the demonstrations and secure storage under U.S. Government control.

9-201. Direct Commercial Arrangements. The disclosure of classified information may be authorized pursuant to a direct commercial sale only if the proposed disclosure supports a U.S. or foreign government procurement requirement, a government contract, or an international agreement. A direct commercial arrangement includes sales, loans, leases, or grants of classified items, including sales under a government agency sales financing program. If a proposed disclosure is in support of a foreign government requirement, the contractor should consult with U.S. in-country officials (normally the U.S. Security Assistance/Armaments Cooperation Office or Commercial Counselor). An export authorization is required before a contractor makes a proposal to a foreign interest that involves the eventual disclosure of U.S. classified information. The contractor should obtain the concurrence of the GCA before submitting an export authorization request.

9-202. Contract Security Provisions.

- a. When a U.S. contractor is authorized to award a subcontract or enter into a Manufacturing License Agreement, Technical Assistance Agreement, or other direct commercial arrangement with a foreign contractor that will involve classified information, security provisions will be incorporated in the subcontract document or agreement and security classification guidance via a Contract Security Classification Specification will be provided. A copy of the signed contract with the provisions and the classification guidance shall be provided to the CSA. If the export authorization specifies that additional security arrangements are necessary for performance on the contract, contractor developed arrangements shall be incorporated in appropriate provisions in the contract or in a separate security document.
- b. The contractor shall prepare and maintain a written record that identifies the originator or source of classified information that will be used in providing defense

articles or services to foreign customers. The contractor shall maintain this listing with the contractor's record copy of the pertinent export authorization.

c. Security provisions, substantially as shown below, shall be included in all contracts and subcontracts involving classified information that are awarded to foreign contractors.

(1) All classified information and material furnished or generated under this contract shall be protected as follows:

(a) The recipient will not release the information or material to a third-country government, person, or firm without the prior approval of the releasing government.

(b) The recipient will afford the information and material a degree of protection equivalent to that afforded it by the releasing government; and

(c) The recipient will not use the information and material for other than the purpose for which it was furnished without the prior written consent of the releasing government.

(2) Classified information and material furnished or generated under this contract shall be transferred through government channels or other channels specified in writing by the Governments of the United States and (insert applicable country) and only to persons who have an appropriate security clearance and an official need for access to the information in order to perform on the contract.

(3) Classified information and material furnished under this contract will be remarked by the recipient with its government's equivalent security classification markings.

(4) Classified information and material generated under this contract must be assigned a security classification as specified by the contract security classification specifications provided with this contract.

(5) All cases in which it is known or there is reason to believe that classified information or material furnished or generated under this contract has been lost or disclosed to unauthorized persons shall be reported promptly and fully by the contractor to its government's security authorities.

(6) Classified information and material furnished or generated pursuant to this contract shall not be further provided to another potential contractor or subcontractor unless:

(a) A potential contractor or subcontractor which is located in the United States or (insert applicable country) has been approved for access to classified information and material by U.S. or (insert applicable country) security authorities; or,

(b) If located in a third country, prior written consent is obtained from the United States Government.

(7) Upon completion of the contract, all classified material furnished or generated pursuant to the contract will be returned to the U.S. contractor or be destroyed.

(8) The recipient contractor shall insert terms that substantially conform to the language of these provisions, including this one, in all subcontracts under this contract that involve access to classified information furnished or generated under this contract.

Section 3. Foreign Government Information (FGI)

9-300. General. The contractor shall notify the CSA when awarded contracts by a foreign interest that will involve access to classified information. The CSA shall administer oversight and ensure implementation of the security requirements of the contract on behalf of the foreign government, including the establishment of channels for the transfer of classified material.

9-301. Contract Security Requirements. The foreign entity that awards a classified contract is responsible for providing appropriate security classification guidance and any security requirements clauses. The failure of a foreign entity to provide classification guidance shall be reported to the CSA.

9-302. Marking Foreign Government Classified Material.

a. Foreign government classified information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the government entity that furnished the information. The equivalent U.S. classification and the country of origin shall be marked on the front and back in English.

9-303. Foreign Government RESTRICTED Information and “In Confidence” Information.

a. Some foreign governments have a fourth level of classification that does not correspond to an equivalent U.S. classification that is identified as RESTRICTED Information. In many cases, bilateral security agreements require RESTRICTED information to be protected as U.S. CONFIDENTIAL information.

b. Some foreign governments may have a category of unclassified information that is protected by law. This latter category is normally provided to other governments on the condition that the information is treated “In Confidence.” The foreign government or international organization must state that the information is provided in confidence and that it must be protected from release. A provision of Title 10 of the U.S. Code (reference (x)) protects information provided “In Confidence” by foreign governments or international organizations to the Department of Defense which is not classified but meets special requirements stated in section 130c reference (x). This provision also applies to RESTRICTED information which is not required by a bilateral agreement to be protected as classified information. The contractor shall not disclose information

protected by this statutory provision to anyone except personnel who require access to the information in connection with the contract.

c. It is the responsibility of the foreign entity that awards the contract to incorporate requirements for the protection and marking of RESTRICTED or "In Confidence" information in the contract. The contractor shall advise the CSA if requirements were not provided by the foreign entity.

9-304. Marking U.S. Documents Containing FGI

a. U.S. documents containing foreign government information shall be marked on the front, "THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION." In addition, the portions shall be marked to identify both the country and classification level, e.g., (UK-C); (GE-C). The "Derived From" line shall identify U.S. as well as foreign classification sources.

b. If the identity of the foreign government must be concealed, the front of the document shall be marked "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION;" paragraphs shall be marked FGI, together with the classification level, e.g., (FGI-C); and the "Derived From" line shall indicate FGI in addition to any U.S. source. The identity of the foreign government shall be maintained with the record copy of the document.

c. A U.S. document, marked as described herein, shall not be downgraded below the highest level of foreign government information contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations concerning downgrading or declassification shall be submitted to the GCA or foreign government contracting authority, as applicable.

9-305. Marking Documents Prepared For Foreign Governments. Documents prepared for foreign governments that contain U.S. and foreign government information shall be marked as prescribed by the foreign government. In addition, they shall be marked on the front, "THIS DOCUMENT CONTAINS UNITED STATES CLASSIFIED INFORMATION." Portions shall be marked to identify the U.S. classified information.

9-306. Storage and Control. Foreign government material shall be stored and access shall be controlled generally in the same manner as U.S. classified material of an equivalent classification. Foreign government material shall be stored in a manner that will avoid commingling with other material which may be accomplished by establishing separate files in a storage container.

9-307. Disclosure and Use Limitations. Foreign government information is provided by the foreign government to the United States. It shall not be disclosed to nationals of a third country, or to any other third party, or be used for other than the purpose for which it was provided without the prior written consent of the originating foreign government. Requests for other uses or further disclosure shall be submitted to the GCA for U.S. contracts, and through the CSA for direct commercial contracts. Approval of the request by the foreign government does not eliminate the requirement for the contractor to obtain an export authorization.

9-308. Transfer. Foreign government information shall be transferred within the U.S. and its territories using the same channels as specified by this manual for U.S. classified information of an equivalent classification, except that non-cleared express overnight carriers shall not be used.

9-309. Reproduction. The reproduction of foreign government TOP SECRET information requires the written approval of the originating government.

9-310. Disposition. Foreign government information shall be destroyed on completion of the contract unless the contract specifically authorizes retention or return of the information to the GCA or foreign government that provided the information. TOP SECRET destruction must be witnessed and a destruction certificate executed and retained for 2 years.

9-311. Reporting of Improper Receipt of Foreign Government Material. The contractor shall report to the CSA the receipt of classified material from foreign interests that is not received through government channels.

9-312. Subcontracting

a. A U.S. contractor may award a subcontract that involves access to FGI to another U.S. contractor, except as described in subparagraph b, on verifying with the CSA that the prospective subcontractor has the appropriate FCL and storage capability. The contractor awarding a subcontract shall provide appropriate security classification guidance and incorporate the pertinent security provisions in the subcontract.

b. Subcontracts involving FGI shall not be awarded to a contractor in a third country or to a U.S. company with a limited FCL based on third-country ownership, control, or influence without the express written consent of the originating foreign government. The CSA will coordinate with the appropriate foreign government authorities.

Section 4. International Transfers

9-400. General. This section contains the procedures for international transfers of classified material. The requirements in this section do not apply to the transmission of classified material to U.S. Government activities outside the United States.

9-401. International Transfers of Classified Material

a. All international transfers of classified material shall take place through channels approved by both governments. Control of classified material must be maintained until the material is officially transferred to the intended recipient government through its designated government representative (DGR).

b. To ensure government control, written transmission instructions shall be prepared for all international transfers of classified material. Preparation of the instructions shall be the responsibility of the contractor for direct commercial arrangements, and the GCA for government arrangements.

c. The CSA shall be contacted at the earliest possible stage in deliberations that will lead to the international transfer of classified material. The CSA shall advise the contractor on the transfer arrangements, identify the recipient government's DGR, appoint a U.S. DGR, and ensure that the transportation plan prepared by the contractor or foreign government is adequate.

d. Requests for export authorizations that will involve the transfer of classified material shall be accompanied by a Department of State Form DSP-83, Non-Transfer and Use Certificate. The form shall be signed by an official of the responsible foreign government who has the authority to certify that the transfer is for government purposes and that the classified material will be protected in compliance with a government-approved security agreement.

9-402. Transfers of Freight

a. Transportation Plan (TP). A requirement to prepare a TP shall be included in each arrangement that involves the international transfer of classified material as freight. The TP shall describe arrangements for the secure shipment of the material from the point of origin to the ultimate destination. The U.S. and recipient government DGRs shall be identified in the TP as well as any requirement for an escort. The TP shall provide for security arrangements in the event the transfer cannot be made promptly. When there are to be repetitive shipments, a Notice of Classified Consignment will be used.

b. Government Agency Arrangements. Classified material to be furnished to a foreign government under such transactions normally will be shipped via government agency-arranged transportation and be transferred to the foreign government's DGR within the recipient government's territory. The government agency that executes the arrangement is responsible, in coordination with the recipient foreign government, for preparing a TP. When the point of origin is a U.S. contractor facility, the GCA shall provide the contractor a copy of the TP and the applicable Letter of Offer and Acceptance (LOA). If a freight forwarder is to be used in processing the shipment, the freight forwarder shall be provided a copy of the TP by the GCA.

c. Commercial Arrangements. The contractor shall prepare a TP in coordination with the receiving government. This requirement applies whether the material is to be moved by land, sea, or air, and applies to U.S. and foreign classified contracts. After the CSA approves the TP, it shall be forwarded to the recipient foreign government security authorities for final coordination and approval.

d. International Carriers. The international transfer of classified material shall be made using only ships, aircraft, or other carriers that:

- (1) are owned or chartered by the U.S Government or under U.S. registry,
 - (2) are owned or chartered by or under the registry of the recipient government,
- or;

(3) are carriers other than those described that are expressly authorized to perform this function in writing by the Designated Security Authority of the GCA and the security authorities of the foreign government involved. This authority shall not be delegated and this exception may be authorized only when a carrier described in (1) or (2) above is not available and/or an urgent operational requirement dictates use of the exception.

9-403. Return of Material for Repair, Modification, or Maintenance. A foreign government or contractor may return classified material to a U.S. contractor for repair, modification, or maintenance. The approved methods of return shall be specified in either the GCA sales arrangement, the security requirements section of a direct commercial sales arrangement, or, in the case of material transferred as freight, in the original TP. The contractor, on receipt of notification that classified material is to be received, shall notify the applicable CSA.

9-404. Use of Freight Forwarders.

a. A commercial freight forwarder may be used to arrange for the international transfer of classified material as freight. The freight forwarder must be under contract to a government agency, U.S. contractor, or the recipient foreign government. The contract shall describe the specific functions to be performed by the freight forwarder. The responsibility for security and control of the classified material that is processed by freight forwarders remains with the U.S. Government until the freight is transferred to a DGR of the recipient government.

b. Only freight forwarders that have a valid FCL and storage capability at the appropriate level are eligible to take custody or possession of classified material for delivery as freight to foreign recipients. Freight forwarders that only process unclassified paperwork and make arrangements for the delivery of classified material to foreign recipients do not require an FCL.

9-405. Handcarrying Classified Material. To meet contractual requirements, the CSA may authorize contractor employees to handcarry classified material outside the United States. SECRET is the highest level of classified material to be carried and it shall be of such size and weight that the courier can retain it in his or her possession at all times. The CSA shall ensure that the contractor has made necessary arrangements with U.S. airport security and customs officials and that security authorities of the receiving government approve the plan. If the transfer is under a contract or a bilateral or multinational government program, the request shall be approved in writing by the GCA. The CSA shall be notified by the contractor of a requirement under this section at least 5 work days in advance of the transfer. In addition:

a. The courier shall be a full-time, appropriately cleared employee of the dispatching contractor.

b. The courier shall be provided with a Courier Certificate that shall be consecutively numbered and be valid for one journey only. The journey may include more than one stop if approved by the CSA and secure Government storage has been arranged at each stop. The Courier Certificate shall be returned to the dispatching security officer immediately on completion of the journey.

- c. Before commencement of each journey, the courier shall read and initial the Notes to the Courier attached to the Courier Certificate and sign the Courier Declaration. The Declaration shall be maintained by the FSO until completion of the next security inspection by the CSA.
- d. The material shall be inventoried, and shall be wrapped and sealed in the presence of the U.S. DGR. The address of the receiving security office and the return address of the dispatching company security office shall be shown on the inner envelope or wrapping. The address of the receiving government's DGR shall be shown on the outer envelope or wrapping along with the return address of the dispatching office.
- e. The dispatching company security office shall prepare three copies of a receipt based on the inventory and list the classified material involved. One copy of the receipt shall be retained by the dispatching company security office. The other two copies shall be packed with the classified material. The security office shall obtain a receipt for the sealed package from the courier.
- f. The dispatching company security office shall provide the receiving security office with 24 work hours advance notification of the anticipated date and time of the courier's arrival and the identity of the courier. The receiving security office shall notify the dispatching company security office if the courier does not arrive within 8 hours of the expected time of arrival. The dispatching security office shall notify its DGR of any delay, unless officially notified otherwise of a change in the courier's itinerary.
- g. The receiving DGR shall verify the contents of the consignment and shall sign the receipts enclosed in the consignment. One copy shall be returned to the courier. On return, the courier shall provide the executed receipt to the dispatching security office.
- h. Throughout the journey, the consignment shall remain under the direct personal control of the courier. It shall not be left unattended at any time during the journey, in the transport being used, in hotel rooms, in cloakrooms, or other such location, and it may not be deposited in hotel safes, luggage lockers, or in luggage offices. In addition, envelopes and packages containing the classified material shall not be opened en route, unless required by customs or other government officials.
- i. When inspection by government officials is unavoidable, the courier shall request that the officials provide written verification that they have opened the package. The courier shall notify the FSO as soon as possible. The FSO shall notify the U.S. DGR. If the inspecting officials are not of the same country as the dispatching security office, the designated security authority in the country whose officials inspected the consignment shall be notified by the CSA. Under no circumstances shall the classified consignment be handed over to customs or other officials for their custody.

j. When carrying classified material, the courier shall not travel by surface routes through third countries, except as authorized by the CSA. The courier shall travel only on carriers as described in the NISPOM and travel direct routes between the U.S. and the destination.

9-406. Classified Material Receipts. There shall be a continuous chain of receipts to record international transfers of all classified material from the contractor through the U.S. DGR and the recipient DGR to the ultimate foreign recipient. The contractor shall retain an active suspense record until return of applicable receipts for the material. A copy of the external receipt that records the passing of custody of the package containing the classified material shall be retained by the contractor and each intermediate consignee in a suspense file until the receipt that is enclosed in the package is signed and returned. Follow-up action shall be initiated through the CSA if the signed receipt is not returned within 45 days.

9-407. Contractor Preparations for International Transfers Pursuant to Commercial and User Agency Sales. The contractor shall be responsible for the following preparations to facilitate international transfers:

- a. Ensure that each party to be involved in the transfer is identified in the applicable contract or agreement, and in the license application or letter request.
- b. Notify the appropriate U.S. DGR when the material is ready.
- c. Provide documentation or written certification by an empowered official (as defined in the ITAR) to the U.S. DGR to verify that the classified shipment is within the limitations of the pertinent export authorization or an authorized exemption to the export authorization requirements, or is within the limitations of the pertinent GCA contract.
- d. Have the classified shipment ready for visual review and verification by the DGR. As a minimum this will include:
 - (1) Preparing the packaging materials, address labels, and receipts for review.
 - (2) Marking the contents with the appropriate U.S. classification or the equivalent foreign government classification, downgrading, and declassification markings, as applicable.
 - (3) Ensuring that shipping documents (including, as appropriate, the Shipper's Export Declaration) include the name and contact information for the CSA that validates the license or letter authorization, and the FSO or designee for the particular transfer.
 - (4) Sending advance notification of the shipment to the CSA, the recipient, and to the freight forwarder, if applicable. The notification will require that the recipient confirm receipt of the shipment or provide notice to the contractor if the shipment is not received in accordance with the prescribed shipping schedule.

9-408. Transfers of Technical Data Pursuant to an ITAR Exemption

- a. The contractor shall provide to the DGR valid documentation (i.e., license, Letter of Offer and Acceptance, or agreement) to verify the export authorization for classified technical data to be transferred under an exemption to reference (w). The documentation shall include a copy of the Form DSP-83 associated with the original export authorization.
- b. Classified technical data to be exported pursuant to reference (w) exemptions 125.4(b)(1), 125.4(c), 125.5, 126.4(a), or 126.4(c) shall be supported by a written authorization signed by an Authorized Exemption Official or Exemption Certifying Official who has been appointed by the responsible Principal Disclosure Authority of the GCA. A copy of the authorization shall be provided by the contractor through the CSA to the Office of Defense Trade Controls.
- c. Exports shall not be permitted under a Manufacturing License or Technical Assistance Agreement for which the authorization has expired.

Section 5. International Visits and Control of Foreign Nationals

9-500. General. This section describes the procedures that the United States and foreign governments have established to control international visits to their organizations and cleared contractor facilities.

9-501. International Visits

- a. The contractor shall establish procedures to monitor international visits by their employees and visits or assignments to their facilities of foreign nationals to ensure that the disclosure of, and access to, export-controlled articles and related information are limited to those that are approved by an export authorization.
- b. Visit authorizations shall not be used to employ or otherwise acquire the services of foreign nationals that require access to export-controlled information. An export authorization is required for such situations.

9-502. Types and Purpose of International Visits. Visit requests are necessary to make administrative arrangements and disclosure decisions, and obtain security assurances. There are three types of international visits:

- a. One-time Visits. A visit for a single, short-term occasion (normally less than 30 days) for a specified purpose.
- b. Recurring Visits. Intermittent, recurring visits over a specified period of time, normally up to 1 year in duration, in support of a Government-approved arrangement, such as an agreement, contract, or license. By agreement of the governments, the term of the authorization may be for the duration of the arrangement, subject to annual review, and validation.

c. Extended Visits. A single visit for an extended period of time, normally up to 1 year, in support of an agreement, contract, or license.

9-503. Emergency Visits. Some foreign governments will accept a visit request submitted within 7 calendar days of the proposed visit for an "emergency visit." To qualify as an emergency visit, the visit must relate to a specific Government-approved contract, international agreement or announced request for proposal, and failure to make the visit could be reasonably expected to seriously jeopardize performance on the contract or program, or result in the loss of a contract opportunity. Emergency visits are approved only as a single, one-time visit. The requester should coordinate the emergency visit in advance with the person to be visited and ensure that the complete name, position, address, and telephone number of the person and a knowledgeable foreign government point of contact are provided in the visit request, along with the identification of the contract, agreement, or program and the justification for submission of the emergency visit request.

9-504. Requests for Recurring Visits. Recurring visit authorizations should be requested at the beginning of each program. After approval of the request, individual visits may be arranged directly with the security office of the location to be visited subject to 3 working days advance notice.

9-505. Amendments. Visit requests that have been approved or are being processed may be amended only to change, add, or delete names and change dates. Amendments requesting earlier dates than originally specified shall not be accepted. Emergency visit authorizations shall not be amended.

9-506. Visits Abroad by U.S. Contractors. Many foreign governments require the submission of a visit request for all visits to a government facility or a cleared contractor facility, even though classified information may not be involved. They also require that the requests be received a specified number of days in advance of the visit. These lead times for North Atlantic Treaty Organization (NATO) countries are in the NISPOM. An export authorization must be obtained if export controlled technical data is to be disclosed or, if information to be divulged is related to a classified U.S. Government program, unless the disclosure of the information is covered by an ITAR exemption. Visit request procedures are outlined as follows:

a. Request Format. The visit request format is contained in the NISPOM. The visit request shall be forwarded to the security official designated by the CSA. The host for the visit should coordinate the visit in advance with appropriate government authorities who are required to approve the visit. It is the visitor's responsibility to ensure that such coordination has occurred.

b. Government Agency Programs. When contractor employees are to visit foreign government facilities or foreign contractors on U.S. Government orders in support of a government contract or agreement, a visit request shall be submitted by the contractor.

9-507. Visits by Foreign Nationals to U.S. Contractor Facilities. Requests for visits by foreign nationals to U.S. contractor facilities that will involve the disclosure of (a) classified information, (b) unclassified information related to a U.S. Government classified program, or (c) plant visits covered by Section 125.5 of reference (w) shall be processed through the sponsoring foreign government (normally the visitor's embassy) to the U.S. Government agency for approval. As described below, the U.S. government agency may approve or deny the request or decline to render a decision.

(Note: Requests for visits by foreign nationals that involve only commercial programs and related unclassified information may be submitted directly to the contractor. It is the contractor's responsibility to ensure that an export authorization is obtained, if applicable.)

- a. Government-Approved Visits. U.S. Government-approved visits constitute an exemption to the export licensing provisions of the ITAR. U.S. Government approved visits shall not be used to avoid the export licensing requirements for commercial initiatives. When the cognizant U.S. Government agency approves a visit, the notification of approval shall contain instructions on the level and scope of classified and unclassified information authorized for disclosure, as well as any limitations. Final acceptance of the visit shall be subject to the concurrence of the contractor who shall notify the U.S. Government agency when a visit is not desired.
- b. Visit Request Denials. If the U.S. Government agency does not approve the disclosure of the information related to the proposed visit, it will deny the visit request. The requesting government and the contractor to be visited shall be advised of the reason for the denial. The contractor may accept the visitor(s). However, only information that is in the public domain may be disclosed.
- c. Non-Sponsorship. The U.S. Government agency will decline to render a decision on a visit request that is not in support of a U.S. Government program. A declination notice indicating that the visit is not government-approved (i.e., the visit is non-sponsored) shall be furnished to the requesting foreign government with an information copy to the U.S. contractor to be visited. A declination notice does not preclude the visit, provided the contractor has, or obtains, an export authorization for the information involved and, if classified information is involved, has been notified that the requesting foreign government has provided the required security assurance of the proposed visitor to the U.S. Government agency in the original visit request. It shall be the responsibility of the contractor to consult applicable export regulations to determine licensing requirements regarding the disclosure of export controlled information during such visits by foreign nationals.
- d. Access by Foreign Visitors to Classified Information. The contractor shall establish procedures to ensure that foreign visitors are not afforded access to classified information and other export-controlled technical data except as authorized by an export license, approved visit request, or other exemption to the licensing requirements. The contractor shall not inform the foreign visitor of the scope of access authorized or of the limitations imposed by the government. Foreign visitors shall not be given custody of classified material except when they are acting as official couriers of their government and the CSA authorizes the transfer.

e. Visitor Records. The contractor shall maintain a record of foreign visitors when the visit involves access to classified information. These records shall be maintained for 1 year.

f. Visits to Subsidiaries. A visit request authorization for a visit to any element of a corporate family may be used for visits to other divisions or subsidiaries within the same corporate family provided disclosures are for the same purpose and the information to be disclosed does not exceed the parameters of the approved visit request.

9-508. Control of Access by On-Site Foreign Nationals

a. Extended visits and assignments of foreign nationals to contractor facilities shall be authorized only when it is essential that the foreign national be at the facility pursuant to a contract or government agreement (e.g., joint venture, liaison representative to a joint or multinational program, or direct commercial sale).

b. If the foreign national will require access to export-controlled information related to, or derived from, a U.S. Government classified contract, the contractor shall obtain the written consent of the GCA before making a commitment to accept the proposed visit or assignment. A copy of the written consent shall be included with the request for export authorization, when such authorization is required.

c. The applicable CSA shall be notified in advance of all extended visits and assignments of foreign nationals to cleared contractor facilities. The notification shall include a copy of the approved visit authorization or the U.S. Government export authorization, and the TCP if applicable.

d. Classified U.S. and foreign government material in a U.S. contractor facility is to remain under U.S. contractor custody and control and is subject to inspection by the FSO and the CSA. This does not preclude a foreign visitor from being furnished a security container for the temporary storage of classified material, consistent with the purpose of the visit or assignment, provided the CSA approves and responsibility for the container and its contents remains with the U.S. contractor. Exceptions to this policy may be approved on a case-by-case basis by the CSA for the storage of foreign government classified information furnished to the visitor by the visitor's government through government channels. Exceptions shall be approved in advance in writing by the CSA and agreed to by the visitor's government. The agreed procedures shall be included in the contractor's TCP, shall require the foreign nationals to provide receipts for the material, and shall include an arrangement for the CSA to ensure compliance, including provisions for the CSA to inspect and inventory the material.

9-509. TCP. A TCP is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities unless the CSA determines that procedures already in place at the contractor's facility are adequate. The TCP shall contain procedures to control access for all export-controlled information. A sample of a TCP may be obtained from the CSA.

9-510. Security and Export Control Violations Involving Foreign Nationals. Any violation of administrative security procedures or export control regulations that would subject classified information to possible compromise by foreign visitors or foreign national employees shall be reported to the CSA.

Section 6. Contractor Operations Abroad

9-600. General. This section sets forth requirements governing contractor operations abroad, including PCLs for U.S. contractor employees assigned outside the United States and their access to classified information.

9-601. Access by Contractor Employees Assigned Outside the United States.

- a. Contractor employees assigned outside the United States, its possessions or territories may have access to classified information in connection with performance on a specified United States, NATO, or foreign government classified contract.
- b. The assignment of an employee who is a foreign national, including intending citizens, outside the United States on programs that will involve access to classified information is prohibited and negates the basis on which an LAA may have been provided to such employee.
- c. A consultant shall not be assigned outside the United States with responsibilities requiring access to classified information.

9-602. Storage, Custody, and Control of Classified Information Abroad by Employees of a U.S. Contractor.

- a. The storage, custody, and control of classified information required by a U.S. contractor employee abroad is the responsibility of the U.S. Government. Therefore, the storage of classified information by contractor employees at any location abroad that is not under U.S. Government control is prohibited. The storage may be at a U.S. military facility, a U.S. Embassy or Consulate, or other location occupied by a U.S. Government organization.
- b. A contractor employee may be furnished a security container to temporarily store classified material at a U.S. Government agency overseas location. The decision to permit a contractor to temporarily store classified information must be approved in writing by the senior security official for the U.S. Government host organization.
- c. A contractor employee may be permitted to temporarily remove classified information from an overseas U.S. Government-controlled facility when necessary for the performance of a GCA contract or pursuant to an approved export authorization. The responsible U.S. Government security official at the U.S. Government facility shall verify that the contractor has an export authorization or other written U.S. Government approval to have the material, verify the need for the material to be removed from the facility, and brief the employee on handling procedures. In such cases, the contractor employee shall sign a receipt for the classified material. Arrangements shall also be made with the U.S. Government custodian for the return

and storage of the classified material during non-duty hours. Violations of this policy shall be reported to the applicable CSA by the security office at the U.S. Government facility.

d. A contractor employee shall not store classified information at overseas divisions or subsidiaries of U.S. companies incorporated or located in a foreign country.

(Note: The divisions or subsidiaries may possess classified information that has been transferred to the applicable foreign government through government-to-government channels pursuant to an approved export authorization or other written U.S. Government authorization. Access to this classified information at such locations by a U.S. contractor employee assigned abroad by the parent facility on a visit authorization in support of a foreign government contract or subcontract, is governed by the laws and regulations of the country in which the division or subsidiary is registered or incorporated. The division or subsidiary that has obtained the information from the foreign government shall provide the access.)

e. U.S. contractor employees assigned to foreign government or foreign contractor facilities under a direct commercial sales arrangement will be subject to the host-nation's industrial security policies.

9-603. Transmission of Classified Material to Employees Abroad. The transmission of classified material to a cleared contractor employee located outside the United States shall be through U.S. Government channels. If the material is to be used for other than U.S. Government purposes, an export authorization is required and a copy of the authorization, validated by the DGR, shall accompany the material. The material shall be addressed to a U.S. military organization or other U.S. Government organization (e.g., an embassy). The U.S. government organization abroad shall be responsible for custody and control of the material.

9-604. Security Briefings. An employee being assigned outside the United States shall be briefed on the security requirements of his or her assignment, including the handling, disclosure, and storage of classified information overseas.

Section 7. NATO Information Security Requirements

9-700. General. This section provides the security requirements needed to comply with the procedures established by the U.S. Security Authority for NATO (USSAN) for safeguarding NATO information provided to U.S. industry.

9-701. Classification Levels. NATO has the following levels of security classification: COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). Another marking, ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom Atomic information that has been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

9-702. NATO RESTRICTED. NATO RESTRICTED does not correspond to an equivalent U.S. classification. NATO RESTRICTED does not require a PCL for access. An FCL is not required if the only information to which the company will have access is NATO RESTRICTED. IS handling only NATO RESTRICTED information do not require certification or accreditation. NATO RESTRICTED information may be included in U.S. unclassified documents. The U.S. document must be marked, "THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION." NATO RESTRICTED material may be stored in locked filing cabinets, bookcases, desks, or other similar locked containers that will deter unauthorized access.

9-703. NATO Contracts. NATO contracts involving NATO-unique systems, programs, or operations are awarded by a NATO Production and Logistics Organization (NPLO), a designated NATO Management Agency, the NATO Research Staff, or a NATO Command. In the case of NATO infrastructure projects (e.g., airfields, communications), the NATO contract is awarded by a contracting agency or prime contractor of the NATO nation responsible for the infrastructure project.

9-704. NATO Facility Security Clearance Certificate. A NATO Facility Security Clearance Certificate (FSCC) is required for a contractor to negotiate or perform on a NATO classified contract A U.S. facility qualifies for a NATO FSCC if it has an equivalent U.S. FCL and its personnel have been briefed on NATO procedures. The CSA shall provide the NATO FSCC to the requesting activity. A NATO FSCC is not required for GCA contracts involving access to NATO classified information.

9-705. PCL Requirements. Access to NATO classified information requires a final PCL at the equivalent level.

9-706. NATO Briefings. Before having access to NATO classified information, employees shall be given a NATO security briefing that covers the requirements of this section and the consequences of negligent handling of NATO classified information. The FSO shall be initially briefed by a representative of the CSA. Annual refresher briefings shall also be conducted. When access to NATO classified information is no longer required, the employee shall be debriefed. The employee shall sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information. Certificates shall be maintained for 2 years for NATO SECRET and CONFIDENTIAL, and 3 years for COSMIC TOP SECRET and all ATOMAL information. The contractor shall maintain a record of all NATO briefings and debriefings in the CSA-designated database.

9-707. Access to NATO Classified Information by Foreign Nationals. Foreign nationals of non-NATO nations may have access to NATO classified information only with the consent of the NATO Office of Security and the contracting activity. Requests shall be submitted to the Central U.S. Registry (CUSR). Access to NATO classified information may be permitted for citizens of NATO member nations, provided a NATO security clearance certificate is provided by their government and they have been briefed.

9-708. Subcontracting for NATO Contracts. The contractor shall obtain prior written approval from the NATO contracting activity and a NATO FSCC must be issued prior to awarding the subcontract. The request for approval will be forwarded through the CSA.

9-709. Preparing and Marking NATO Documents. All classified documents created by a U.S. contractor shall be portion-marked. Any portion extracted from a NATO document that is not portion marked, must be assigned the classification that is assigned to the NATO document.

a. All U.S.-originated NATO classified documents shall bear an assigned reference number and date on the first page. The reference numbers shall be assigned as follows:

(1) The first element shall be the abbreviation for the name of the contractor facility.

(2) The second element shall be the abbreviation for the overall classification followed by a hyphen and the 4-digit sequence number for the document within that classification that has been generated for the applicable calendar year.

(3) The third element shall be the year; e.g., MM/NS-0013/93.

b. COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall bear the reference number on each page and a copy number on the cover or first page. Copies of NATO documents shall be serially numbered. Pages shall be numbered. The first page or index or table of contents shall include a list, including page numbers, of all Annexes and Appendices. The total number of pages shall be stated on the first page. All Annexes or Appendices will include the date of the original document and the purpose of the new text (addition or substitution) on the first page.

c. One of the following markings shall be applied to NATO documents that contain ATOMAL information:

(1) "This document contains U.S. ATOMIC Information (RESTRICTED DATA or FORMERLY RESTRICTED DATA) made available pursuant to the NATO Agreement for Cooperation Regarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly."

(2) "This document contains UK ATOMIC Information. This information is released to NATO including its military and civilian agencies and member states on condition that it will not be released by the recipient organization to any other organization or government or national of another country or member of any other organization without prior permission from H.M. Government in the United Kingdom."

d. Working papers shall be retained only until a final product is produced.

9-710. Classification Guidance. Classification guidance shall be in the form of a NATO security aspects letter and a security requirements checklist for NATO contracts, or a Contract Security Classification Specification. If adequate classification guidance is not received, the contractor shall contact the CSA for assistance. NATO classified documents and NATO information in other documents shall not be declassified or downgraded without the prior written consent of the originating activity. Recommendations concerning the declassification or downgrading of NATO classified information shall be forwarded to the CUSR.

9-711. Further Distribution. The contractor shall not release or disclose NATO classified information to a third party or outside the contractor's facility for any purpose without the prior written approval of the contracting agency.

9-712. Storage of NATO Documents. NATO classified documents shall be stored as prescribed for U.S. documents of an equivalent classification level, except as follows:

- a. NATO classified documents shall not be commingled with other documents.
- b. Combinations for containers used to store NATO classified information shall be changed annually. The combination also shall be changed when an individual with access to the container departs or no longer requires access to the container, and if the combination is suspected of being compromised.
- c. When the combination is recorded it shall be marked with the highest classification level of documents stored in the container as well as to indicate the level and type of NATO documents in the container. The combination record must be logged and controlled in the same manner as NATO classified documents.

9-713. International Transmission. NATO has a registry system for the receipt and distribution of NATO documents within each NATO member nation. The central distribution point for the U.S. is the CUSR located in the Pentagon. The CUSR establishes subregistries at U.S. Government organizations for further distribution and control of NATO documents. Subregistries may establish control points at contractor facilities. COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents shall be transferred through the registry system. NATO CONFIDENTIAL documents provided as part of NATO infrastructure contracts shall be transmitted via government channels.

9-714. Handcarrying. NATO SECRET and NATO CONFIDENTIAL documents may be handcarried across international borders if authorized by the GCA. The courier shall be issued a NATO Courier Certificate by the CSA. When handcarrying is authorized, the documents shall be delivered to a U.S. organization at NATO, which shall transfer them to the intended NATO recipient.

9-715. Reproduction. Reproductions of COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL information shall be performed by the responsible Registry. The reproduction of NATO SECRET, and CONFIDENTIAL documents may be authorized to meet contractual requirements unless reproduction is prohibited by the contracting entity. Copies of COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall be serially numbered and controlled and accounted for in the same manner as the original.

9-716. Disposition. Generally, all NATO classified documents shall be returned to the contracting activity that provided them on completion of the contract. Documents provided in connection with an invitation to bid also shall be returned immediately if the bid is not accepted or submitted. NATO classified documents may also be destroyed when permitted. COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents shall be destroyed by the Registry that provided the documents. Destruction certificates are required for all NATO classified documents except NATO CONFIDENTIAL. The destruction of COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents must be witnessed.

9-717. Accountability Records. Logs, receipts, and destruction certificates are required for NATO classified information, as described below. Records for NATO documents shall be maintained separately from records of non-NATO documents. COSMIC TOP SECRET and all ATOMAL documents shall be recorded on logs maintained separately from other NATO logs and shall be assigned unique serial control numbers. Additionally, disclosure records bearing the name and signature of each person who has access are required for all COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL, and all other ATOMAL or NATO classified documents to which special access limitations have been applied.

- a. Minimum identifying data on logs, receipts, and destruction certificates shall include the NATO reference number, short title, date of the document, classification, and serial copy numbers. Logs shall reflect the short title, unclassified subject, and distribution of the documents.
- b. Receipts are required for all NATO classified documents except NATO CONFIDENTIAL.
- c. Inventories shall be conducted annually of all COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents.
- d. Records shall be retained for 10 years for COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents and 5 years for NATO SECRET, NATO SECRET ATOMAL, NATO CONFIDENTIAL, and NATO CONFIDENTIAL ATOMAL documents.

9-718. Security Violations and Loss, Compromise, or Possible Compromise. The contractor shall immediately report the loss, compromise, or suspected loss or compromise, as well as any other security violations involving NATO classified information to the CSA.

9-719. Extracting from NATO Documents. Permission to extract from a COSMIC TOP SECRET or ATOMAL document shall be obtained from the CUSR.

- a. If extracts of NATO information are included in a U.S. document prepared for a non-NATO contract, the document shall be marked with U.S. classification markings. The caveat, "THIS DOCUMENT CONTAINS NATO (level of classification) INFORMATION" also shall be marked on the front cover or first page of the document. Additionally, each paragraph or portion containing the NATO information shall be marked with the appropriate NATO classification, abbreviated in parentheses (e.g., NS) preceding the portion or paragraph. The "Declassify on" line of the document shall show "Source marked OADR" and the date of origin of the most recent source document unless the original NATO document shows a specific date for declassification.
- b. The declassification or downgrading of NATO information in a U.S. document requires the approval of the originating NATO activity. Requests shall be submitted to the CUSR for NATO contracts, through the GCA for U.S. contracts, and through the CSA for non-NATO contracts awarded by a NATO member nation.

9-720. Release of U.S. Information to NATO.

a. Release of U.S. classified or export-controlled information to NATO requires an export authorization or other written disclosure authorization. When a document containing U.S. classified information is being prepared for NATO, the appropriate NATO classification markings shall be applied to the document. Documents containing U.S. classified information and U.S. classified documents that are authorized for release to NATO shall be marked on the cover or first page "THIS DOCUMENT CONTAINS U.S. CLASSIFIED INFORMATION. THE INFORMATION IN THIS DOCUMENT HAS BEEN AUTHORIZED FOR RELEASE TO (cite the NATO organization) BY (cite the applicable license or other written authority)." The CSA shall provide transmission instructions to the contractor. The material shall be addressed to a U.S. organization at NATO, which shall then place the material into NATO security channels. The material shall be accompanied by a letter to the U.S. organization that provides transfer instructions and assurances that the material has been authorized for release to NATO. The inner wrapper shall be addressed to the intended NATO recipient. Material to be sent to NATO via mail shall be routed through the U.S. Postal Service and U.S. military postal channels to the U.S. organization that will make the transfer.

b. A record shall be maintained that identifies the originator and source of classified information that are used in the preparation of documents for release to NATO. The record shall be provided with any request for release authorization.

9-721. Visits. NATO visits are visits by personnel representing a NATO entity and relating to NATO contracts and programs. NATO visits shall be handled in accordance with the NISPOM . A NATO Certificate of Security Clearance will be included with the visit request.

a. NPLO and NATO Industrial Advisory Group (NIAG) Recurring Visits. NATO has established special procedures for recurring visits involving contractors, government departments and agencies, and NATO commands and agencies that are participating in a NPLO or NIAG contract or program. The NATO Management Office or Agency responsible for the NPLO program will prepare a list of the Government and contractor facilities participating in the program. For NIAG programs, the list will be prepared by the responsible NATO staff element. The list will be forwarded to the appropriate clearance agency of the participating nations, which will forward it to the participating contractor.

b. Visitor Record. The contractor shall maintain a record of NATO visits including those by U.S. personnel assigned to NATO. The records shall be maintained for 3 years.

Chapter 10 Miscellaneous

Section 1. TEMPEST

10-100. TEMPEST Requirements. When compliance with TEMPEST standards is required, 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: Within DoD, TEMPEST is known as EMSEC.

- a. Each department or agency has an appointed Certified TEMPEST Technical Authorities (CTTAs) who must conduct and validate all TEMPEST countermeasure reviews by the National Policy.
- b. If a review is required, the service component 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.
- c. Only those TEMPEST countermeasures recommended by CTTA and authorized by the government 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 NSTISSAM TEMPEST 2/95A.
- d. 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

10-200. Warning. SAP information will not be sent to the Defense Technical Information Center or the U.S. Department of Energy Office of Scientific and Technical Information.

Section 3. Independent Research and Development

10-300. 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 GPM and executed by the Government Contracting Officer. Procedures and requirements necessary for safeguarding SAP classified information will be outlined in the DD Form 254 signed by the PSO. A letter defining the authority to conduct IR&D, a DD Form 254, and appropriate classification guidance will be provided to each contractor. Subcontracting of IR&D efforts will follow the same process as outlined in paragraph 4-103 of this manual.

10-301. Retention of SAP Classified Documents Generated Under IR&D Efforts. If determined by the GPM and PSO to be in the best interests of the government, the contractor may be allowed to retain the classified material generated in connection with the IR&D effort.

10-302. Review of Classified IR&D Efforts. IR&D operations and documentation that contain SAP classified information will be subject to review in the same manner as other SAP classified information in the possession of the contractor.

Section 4. Operations Security

10-400. General. Operations Security (OPSEC) requires all SAPs to identify, define, and develop countermeasures to vulnerabilities. OPSEC can be achieved through the use of an OPSEC Plan (see Appendix “D”) or through inclusion of OPSEC principles codified in one or more of the following:

- a. Component-Level OPSEC Directives, Instructions, and Regulations
- b. Program Security Classification Guide
- c. Standard Operating Procedures (SOPs)
- d. Validated Threat Assessment
- e. Security, Education, Training & Awareness
- f. DD Form 254

Section 5. Counterintelligence (CI) Support

10-500. Counterintelligence (CI) Support. Analysis of foreign intelligence threats and risks to program information, material, personnel, and activities will be undertaken by the appropriate Government CI agency. As necessary, resulting information that may have a bearing on the security of a SAP will be provided by the Government CI agency to the affected SAP PM and PSO. 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.

Section 6. Decompartmentation, Disposition, and Technology Transfer Procedures

10-600. General. Personnel currently or previously briefed to a SAP are obligated to provide to the GPM and PSO a copy of any proposed intended release of information which could potentially contain SAP information, for review prior to public release. Information considered for release such as models, software, and technology may impact other SAPs and will require additional coordination prior to release. The information and materials proposed for release will remain within program security channels until authorized for release.

10-601. 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.

- a. **Decompartmentation.** Prior to decompartmenting any classified SAP information or other material(s) developed within the program, the PSO/GSSO/CPSO will obtain the written approval of the SAPCO. Decompartmentation initiatives at a program activity will include justification and rationale for decompartmentation. 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 benefit to the U.S. Government and program information is not compromised. Technology transfer as used in this section refers to transfer of information/material between U.S. Government Agencies. Transfer of technology between Government agencies will be codified in an MOA/MOU as outlined in paragraphs 1-208 and 1-209 of this manual. For transfer of technology information/material/classified military information to a foreign government or international organization, see Chapter 9.

- (1) **Contractor Responsibilities.** PSOs/GSSOs/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 HVSACO information have been sanitized 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 sanitization will accompany the information or material(s) forwarded to the GPM and Original Classification Authority (OCA) for review and approval.

(2) Government Responsibilities. The PSO and GPM will make every attempt to review and approve technology transfer 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. Close-Out Actions

10-700. Close-Out Actions - At the initiation of a contract close-out, termination or completion of the contract effort, the PSO/GSSO/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 PSO may require the contractor to submit a termination plan to the Government. The master classified material accountability record (log or register) will be transferred to the PSO at program close-out.

Section 8. Patents

10-800. 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.

Section 9. Telephone Security

10-900. 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 JAFAN 6/9 and Telephone Security Group (TSG) standards.

Section 10. Treaty Guidance

10-1000. Treaty Guidance.

- a. Background. DoD Directive 2060.1 provides that the Arms Control implementation and compliance responsibilities for SAPs must be accomplished under the cognizance of the DoD SAP Oversight Committee (SAPOC) in a manner consistent with the SAP Policy DoD Directive 5205.7, and DoD Instruction 5205.11. DoD SAPs must be prepared to demonstrate compliance with treaties and agreements to which the United States Government (USG) is a signatory. DoD SAPs shall be protected against unnecessary or inadvertent exposure during USG participation in authorized verification activities, confidence-building measures, and overflights. The PSO/GSSO/ CPSO should be familiar with various arms control verification activities in order to exercise security oversight for SAPs.
- b. Inspection Readiness Plans. Each service component sponsoring or acting as the executive agent for a SAP is responsible for providing arms control implementation guidance and direction to all SAPs under its cognizance. If required, inspection readiness plans should be site-specific and should include detailed managed access provisions. Risk assessment is a crucial part of the development of such plans, and should form the basis for plan content, level of detail, etc. Sample plan outline at Appendix "F" aids in the preparation of risk assessment and inspection readiness plans.
- c. On-Site Inspection Assistance. Each component is accountable for assisting the SAPs that it sponsors, unless relieved of that responsibility by the Secretary or Deputy Secretary of Defense. In most cases, a treaty knowledgeable representative from the OSD and/or from a service component SAPCO office will be on-site to support DoD SAP facilities within the first 24 hours of USG notification of an impending inspection. In the event of an inspection that questions U.S. compliance with international agreements, such as a Chemical Weapons Convention Challenge Inspection, a member of the Special Security Countermeasures Policy Office, Office of the Deputy Under Secretary of Defense for Policy Support, will serve as a consensus member of the USG Host Team. This individual is the acknowledged DoD Security Policy representative responsible for negotiating inspection activities. The responsible SAP service component representative will conduct liaison between the PSO/GSSO/CPSO and the U.S. Host Team representative mentioned above.
- d. SAP Treaty Vulnerability. As part of a continuing OPSEC program, potential treaty vulnerabilities must be addressed as part of all SAP vulnerability assessments. Impacts must be considered prior to accreditation of a SAP facility. The PSO should contact the service component SAPCO office for guidance on obtaining the treaty portion of these assessments.
- e. Arms Control Compliance Reviews. Each component will monitor SAP activities for compliance with arms control agreements and, as necessary, conduct or direct reviews to determine if there are issues that should be brought before a Senior Review Group (SRG) to ensure compliance.

f. The Defense Treaty Inspection Readiness Program (DTIRP). DTIRP is a security preparedness and outreach program providing security education and awareness training regarding arms control implementation operational activities. DTIRP provides advice, assistance, and information to DoD military and DoD contractor facilities. SAPs should not contact DTIRP directly, but should request assistance from their service component SAPCO office.

APPENDIX A

HANDLE VIA SPECIAL ACCESS CHANNELS ONLY (HVSACO)

1. **General.** The purposes of Handle Via Special Access Channels Only (HVSACO) are:
 - a. To preclude the disclosure of Critical Program Information and general program-related information outside established acknowledged and unacknowledged Special Access Program (SAP) channels.
 - b. To minimize Operations Security (OPSEC) indicators.
 - c. To facilitate communication of information within SAPs.

2. **Use of HVSACO.** Dissemination of information warranting HVSACO protection will be limited to persons briefed into a SAP and retained within SAP approved channels. Formal indoctrination or execution of briefing/debriefing forms specifically for HVSACO is not required. The term SAP channels denotes secure, approved SAP communications systems, Special Access Program Facilities (SAPFs), or PSO-approved SAP storage areas. HVSACO is not a classification level, but rather a protection or handling system. Examples of HVSACO uses may include:
 - a. For general non-program specific, unclassified communications between and within SAPs. More specifically, on information related to SAP security procedures, test plans, transportation plans, manufacturing plans, and notional concepts related to research, development, testing, and evaluation of SAPs.
 - b. When a paragraph or document contains information that is unique to a SAP and its distribution.
 - c. When necessary to protect relationships.
 - d. To protect information that does not warrant classification under E.O. 12958.
 - e. When using a SAP nickname for an unacknowledged SAP.

3. **Release.** Upon request for public release, the originator of the material must review the material involved to determine whether to retain it within program channels:
 - a. If public release is appropriate, remove the HVSACO marking from the document, or
 - b. Inform the requestor of the decision not to release the information, citing an appropriate authority.

4. **Training.** Training on HVSACO should be included in annual security awareness refresher sessions.

5. **Marking.** Procedures for the use of HVSACO should be included in program Security Classification Guides.

6. **Storage.** Materials warranting HVSACO protection may be stored openly or placed in desks, lock-bar containers, or similar storage containers within an approved SAPF. PSOs may grant an exception to allow the taking of unclassified HVSACO materials to alternate temporary storage areas, provided the material is under an appropriately authorized individual's direct control, or under "key lock protection" which is controlled by that individual.

7. **Transmission.**

a. At a minimum, use U.S. First Class mail for shipment of unclassified materials requiring HVSACO protection.

b. Use the secure mode when discussing HVSACO protected material on the telephone (STE/STU-III).

c. Use only approved, secure facsimile equipment when transmitting HVSACO protected material.

d. Do not transmit HVSACO protected material via unclassified email.

8. **Reproduction.** Reproduce unclassified HVSACO protected information only on equipment approved by the PSO.

9. **Accountability.** HVSACO protection does not require accountability. Document accountability is based on classification level or unique program requirements. Document control numbers, entry into document control systems, or internal or external receipts are not required for unclassified HVSACO protected material.

10. **Destruction.** Destroy HVSACO protected information according to the procedures approved for classified material. Destruction certificates are not required for non-accountable HVSACO protected materials.

11. **Improper Handling or Misuse.** Based on GSSO/CPSO assessment of the OPSEC risk, notify the PSO within 24 hours of any possible improper handling or misuse of HVSACO protected information and its impact. An inquiry should be conducted by the GSSO/CPSO to determine if a compromise occurred as a result of practices dangerous to security. The PSO and GPM will ensure that prompt corrective action is taken on any practices dangerous to security. When classified information is involved, follow the procedures in paragraph 1-301.

12. **Removal of HVSACO Markings.** Contact the originating office for permission to remove HVSACO markings

APPENDIX B
SOP TOPICAL OUTLINE (*Sample Only*)

STANDARD OPERATING PROCEDURES
(SOP)

(ACTIVITY NAME AND ADDRESS)

APPROVED:

(PSO)

(YYMMDD)

SOP TABLE OF CONTENTS - *SAMPLE*

CHAPTER 1 - GENERAL PROVISIONS AND REQUIREMENTS

Section 1. Introduction

1-100	Purpose	X
1-101	Scope	X
1-102	SAP Program Area	X
1-103	Waivers	XX
1-104	Facility background and operating concept	XX
	a. Temporary Secure Working Area (TSWA)	XX
	b. Shared/Alternating/Co-utilization of Facilities	XX

Section 2. General Requirements

1-200	Responsibilities	XX
	a. SAP Central Office (SAPCO)	XX
	b. Program Security Officer (PSO)	XX
	c. Government SAP Security Officer (GSSO)	XX
	d. Contractor Program Security Officer (CPSO)	XX
	e. Program Management (GPM/CPM).....	XX
	f. Individual Program Personnel	XX
1-201	Badge Systems	XX
	a. Badge Control	XX
	b. Badge Issue and Identification	XX
	c. Escort Procedures & Visitor Badges	XX
1-202	Communications Security	XX
	a. Secure Communications	XX
	b. STE/STU-III Operations	XX
	c. Secure Telephone Lines/Closets	XX
1-203	Security Inspections	XX
	a. Government	XX
	b. Self-Inspections	XX

Section 3. Reporting Requirements

1-300	General	XX
1-301	Security Violations and Improper Handling of Classified Information	XX
	a. Security Violations and Infractions	XX
	b. Inadvertent Disclosures	XX
	c. Preliminary Inquiries/Investigations	XX
	d. Fraud, Waste, Abuse and Corruption (FWAC)	XX

CHAPTER 2 - SECURITY CLEARANCES

Section 1. Facility Clearances

2-100	General	XX
2-101	Defense Security Services	XX

Section 2. Personnel Clearances and Access

2-200	General	XX
2-201	SAP Access Procedures	XX
2-202	Program Access Requests and Tier Review Process	XX
2-203	Suspension and revocation	XX

CHAPTER 3 - SECURITY TRAINING AND EDUCATION

Section 1. Security Training and Briefings

3-100	General	XX
3-101	Security Training	XX
3-102	Refresher Training	XX
3-103	Computer-based training (CBT)	XX
3-104	Debriefing and/or access termination	XX
3-105	Personnel Security Reporting Requirements	XX
3-106	Foreign Travel/Contacts	XX
3-107	Specialized or event-driven training	XX

CHAPTER 4 - CLASSIFICATION AND MARKINGS

Section 1. Classification

4-100	Classification management	XX
4-101	Security Classification Guidance	XX
4-102	Nicknames, Code Words, and other Program Identifiers	XX
4-103	DD Form 254 requirements	XX
4-104	Changes, challenges, and reviews	XX
4-105	Subcontractor classification guidance	XX
4-106	Use of Cover Sheets	XX

Section 2. Marking Requirements

4-200	General	XX
4-201	Program Specific	XX
4-202	File Exemption Series	XX

CHAPTER 5 - SAFEGUARDING CLASSIFIED INFORMATION

Section 1. General Safeguarding Requirements

5-100	General	XX
5-101	Clean desk policy	XX
5-102	Facility access controls	XX
5-103	Building access	XX
5-104	Program SAPFs	XX
5-105	Shared/alternating use area access	XX
5-106	Common use area access	XX
5-107	Unescorted access	XX
5-108	After-Hours access	XX
5-109	Facility opening/securing procedures	XX
5-110	Alarm System Procedures	XX

Section 2. Control and Accountability

5-200	General	XX
5-201	Program material tracking system	XX
	a. SAP Accountability	XX
	b. SAP Transmission	XX
	c. SAP Reproduction	XX
5-202	Collateral material	XX
5-203	Annual inventories	XX
5-204	Working Papers and Engineer Notebooks	XX

Section 3. Storage and Storage Equipment

5-300	Storage policy	XX
5-301	Control of locks and combinations	XX
5-302	Security container records of use	XX

Section 4. Transmission

5-400	General	XX
5-401	Preparation	XX
5-402	Couriers	XX
5-403	Secure facsimile and/or electronic transmission	XX

5-404	U.S. Postal Services (USPS)	XX
	a. Post Office box usage	XX
	b. Receipt procedures (as required)	XX

Section 5. Disclosure

5-501	a. Need-to-Know	XX
-------	-----------------------	----

Section 6. Reproduction

Section 7. Disposition and Retention

5-700	Termination of security agreement	XX
5-701	Retention of classified material	XX
5-702	Document reduction	XX
5-703	Bids and proposals	XX
5-704	Methods of destruction	XX
5-705	Destruction procedures	XX

Section 8. Construction and other Security Requirements

5-800	General	XX
5-801	Physical security	XX
5-802	SAPFs identification	XX
5-803	Prohibited items (Control of PEDs, etc)	XX
5-804	Magnetic media	XX
5-805	Access control and alarm system	XX
5-806	Security checks and inspections	XX
5-807	Alarm responses	XX
	a. Normal Duty Hours	XX
	b. After Hours	XX
	c. Alarm Malfunctions/Alarm System Shutdown	XX
	d. Semi-Annual Alarm Response Checks	XX

CHAPTER 6 - VISITS AND MEETINGS

Section 1. Visits

6-100	General	XX
6-101	Visit request procedures	XX
6-102	Identification and control of visitors	XX
6-103	Non-program-briefed visitors	XX
6-104	Visitor records	XX

Section 2. Meetings

6-200	General	XX
6-201	Host responsibilities	XX

CHAPTER 7 - SUBCONTRACTING

Section 1. Prime Contracting Responsibilities

7-100	General	XX
7-101	Determining clearance status of prospective subcontractors	XX
7-102	Security agreements and briefings	XX

CHAPTER 8 - AUTOMATED INFORMATION SYSTEMS (AIS)

8-100	General	XX
8-101	Data Transfer Procedures (High to Low, etc)	XX

CHAPTER 9 - MISCELLANEOUS

Section 1. Emissions Security (EMSEC)

Section 2. Operations Security (OPSEC)

Section 3. Emergencies

9-300	General	XX
9-301	Protection of classified during emergencies	XX
9-302	Access by emergency response personnel	XX
9-303	Emergency after-hours access	XX

FIGURES

1	Nomination Form	XX
2	Visitor Register	XX
3	Security Container Record	XX
4	Facility End-of-Day Security Checklist	XX
5	Temporary Relocation of Classified Material Log	XX
6.	Certificate of Destruction	XX
7.	Media Control Log	XX

ANNEXES

1	Special Access Program and Facility Security Debriefings	XX
2	Foreign Travel, Contact and Defensive Briefings	XX
3	Automated Information Systems Standard Operating Procedures (AIS SOP) ...	XX

APPENDIX C SECURITY DOCUMENT RETENTION

(This guidance is for the retention requirements for SAP-related documents and records; paper or electronic.)

IF RECORDS ARE OR PERTAIN TO	CONSISTING OF / WHICH ARE	MAINTAINED BY	DISPOSITION / DESTROY
Access Approvals	Received from Program Office	Contractor ----- PSO/PM -----	Forward to PSO upon debriefing Destroy Five years after program is terminated or IAW agency directives
Access Lists	Information copies ----- Master copy prepared by originator -----	PSO/PM ----- All -----	Destroy when new list received Destroy after Five years
Accreditations	Of Program Facilities which include Facility Checklists and Open Storage Authorizations	Contractor ----- PSO -----	Destroy when facility becomes unoccupied or the Fixed Facility Checklist is superseded Destroy One year after decertification
Adverse Information Reports	Required by NISPOM or other Gov Directives	All -----	Destroy Five years after individual is debriefed
Alarm Test Records	JAFAN 6/9, Annex B	All -----	Destroy after PSO inspection
Audit Reports	TS inventories ----- Computer audits -----	All ----- ----- -----	Destroy Two years after completed or after PSO inspection whichever is later Destroy after One security inspection cycle
Building/Facility Security Patrol Checklists	Conducted by Guards	All	Destroy after PSO inspection
Classification Change Requests	Prepared by originator	Contractor ----- PSO/PM -----	Destroy after change is incorporated into SCG retain permanently
Communication Requests	Secure Voice/Facsimile	Contractor ----- PSO -----	Destroy One year after equipment is installed Destroy Five years after communication is no longer needed
Contract Security Classification Specifications	DD Form 254	Contractor ----- PSO -----	Destroy Five Years after contract is completed Destroy Five Years after contract is completed
Courier Designations	(SAP Format 28)	All	Destroy after One year

IF RECORDS ARE OR PERTAIN TO	CONSISTING OF / WHICH ARE	MAINTAINED BY	DISPOSITION / DESTROY
Document Control Records	Receipts -----	All-----	Destroy after Five years
	Mail Receipts/Logs -----	-----	Destroy after Two years
	Master Document Lists --	-----	Destroy when superseded or no longer needed
	Destruction Certificates --	-----	Destroy after Five years
	TS Registers/Control Records -----	-----	Destroy Five years after register closed
EMSEC Reports	Surveys	All -----	Destroy when facility becomes unoccupied
Exercise Reports	Of Emergency Plans and Guard Responses	All -----	Destroy After Two consecutive inspections
Foreign Travel Reports	(SAP Format 6)	All -----	Forward to PSO upon debriefing (file in Personnel folder) Destroy Five years after program is terminated or IAW agency directives
Inadvertent Disclosure Statements	(SAP Format 5)	All -----	Destroy Five years after program is terminated
Indoctrination Agreements (SAP Formats 2 and 2a if applicable)	Including pre-briefings, indoctrinations and debriefings	Contractor ----- PSO/PM -----	Forward to PSO upon debriefing Destroy Five years after program is terminated or IAW agency directives
Information gathered by or released to Media outlets	Include approved and denied releases	All	Destroy Five years after program is terminated
Inquiries	Security Violations	All	Destroy after Five years following program termination
Inspection Reports (SF-series forms related to Physical Security-Facility-, Safe Checks, etc)	After Duty Hour inspections and Safe Check records -----	All -----	Destroy after PSO/GSSO/CPSO review
	Entry/Exit Checks -----	-----	Destroy after PSO/GSSO/CPSO review
Investigations	Compromises/Suspected Compromises/Document Losses	All	Destroy Five years after program is terminated
Listings of Names, Codes and/or Convenience Numbers	Prepared by originator	All	Destroy Five years after program is terminated

IF RECORDS ARE OR PERTAIN TO	CONSISTING OF / WHICH ARE	MAINTAINED BY	DISPOSITION / DESTROY
Memorandums of Agreement (MOA) and Memorandum of Understanding (MOU)	Prepared by originator		Destroy Five years after program is terminated
Personnel Security Investigations	Standard Form (SF) 86 or eQIP printout including SF 86c	All	Destroy when individual is debriefed
Plans	Emergency Procedures, Security Operating Instructions, Tests, Manufacturing, etc.	Contractor ----- PM ----- PSO -----	Upon termination of program Forward to PSO One Year after program termination
Program Access Requests (PAR) - (SAP Format 1)	Approved for access ----- Disapproved for access ---	All ----- Contractor -----	Destroy Five years after program is terminated Destroy upon receipt of disapproval
Program Management Directives	Prepared by originator	PM	Retain permanently
Program Termination	All Associated Documentation	Contractor ----- PSO/PM -----	Destroy Five years after program is terminated retain permanently
Recurring Reports	SAP Program Contract Security Report	All ----- Contractor ----- PSO/PM -----	Destroy after one year Destroy One year after program is terminated Destroy after Three years
Requests for TS Reproduction	Prepared by originator	All	Incorporated into Document Control and Accountability Records
Request to Transfer Documents to another Program	Approved	PSO/PM----- Contractor -----	Destroy after Five years Destroy when associated documents are destroyed
Reports of Espionage, Sabotage, or Subversion	Prepared by originator	All	Retain permanently
Reports of FIS Contact	Prepared by originator	All	Retain permanently
Reports of Shipment Tampering	Prepared by originator	All	Destroy One year after program is terminated
Reports of Threats and Threat Assessments	Prepared by originator	All	Destroy when threat is eliminated or after Five years, whichever is sooner
Satellite Transmission (SATRAN) Reports	Prepared by originator	All	Destroy when no longer needed
Security Classification Guides (SCG)	Master ----- Copies -----	PSO/PM ----- Contractor -----	Retain permanently Destroy Five years after program is terminated

IF RECORDS ARE OR PERTAIN TO	CONSISTING OF / WHICH ARE	MAINTAINED BY	DISPOSITION / DESTROY
Security Inspection Reports (SAP Format 19) or Checklists	Annual Self-Inspection ---	All -----	Destroy after Two years
	Inspections conducted by PSO -----	Contractor ----- PSO/PM -----	Destroy after Three years Destroy after Five years
	Subcontractor Inspections	Contractor -----	Destroy after Five years
Security Officer Appointments	Letters, Approvals, Forms	All -----	Destroy when replaced or superseded
Security Policy	Directive or provide interpretation	Contractor ----- PSO/PM -----	Destroy One year after program is terminated Retain permanently
Subcontractor Documentation	Requests to Contact -----	Contractor ----- PSO/PM -----	Destroy One year after Program is completed Destroy one year after program is terminated
	Trip Reports -----	All -----	Destroy Two years after trip
Technical Security Countermeasures Surveys (TSCM)	Including SAP Format 8	All	Destroy after next report is received
Training Records	Security Education Attendance, Computer listings, & SAP Format 17	All -----	When individual is debriefed
TS Access Records	Prepared by originator	All -----	Destroy Two years after corresponding document is destroyed
Visits	Visitor Requests ----- (SAP Formats 7 and 7L)	All -----	Destroy after One year
	Visitor Logs -----	-----	Destroy after Five years
Waivers	Security Criteria (SAP Format 12)	Contractor -----	Destroy when program is terminated
		PSO/PM -----	Destroy Five years after program is terminated

APPENDIX D
OPSEC PLAN – TOPICAL OUTLINE (*Sample Only*)

TABLE OF CONTENTS

Cover	X
Foreword	X
Table of Contents	X
Section I. Introduction	X
Section II. The OPSEC Process	XX
Section III. Program Scope, Policy, and Responsibilities	XX
A. Program Overview	XX
B. Threat Analysis	XX
C. Program Specifics	XX
D. Guidance for Contractors	XX
E. Critical Information	XX
F. Requirements	XX
Section IV. Intelligence Collection Threat	XX
A. Intelligence Collection Activities and Disciplines	XX
1. Defining Intelligence	XX
2. Planning and Direction	XX
3. Collection	XX
4. Processing	XX
5. Production	XX
6. Dissemination	XX
7. Intelligence Collection Disciplines	XX
8. Human Intelligence (HUMINT)	XX
9. Signals Intelligence (SIGINT)	XX
10. Measurement and Signature Intelligence (MASINT)	XX
11. Imagery Intelligence (IMINT)	XX

12. Open Source Intelligence (OSINT)	XX
13. Computer Intrusion for Collection Operations	XX
14. All Source Intelligence	XX
B. Adversary Foreign Intelligence Operations	XX
1. Russian Intelligence Collection Capabilities	XX
2. Russian Intelligence Organizations	XX
a. Russian Foreign Intelligence Service (SVR)	XX
b. Main Intelligence Directorate of the General Staff (GRU) .	XX
c. Federal Agency for Government Communications and	
Information (FAPSI)	XX
3. Russian Intelligence Operations	XX
a. HUMINT	XX
b. SIGINT	XX
c. IMINT	XX
d. MASINT	XX
4. Russian Intelligence Collection Trends	XX
5. Chinese Intelligence Collection Capabilities	XX
6. Chinese Intelligence Collection Organizations	XX
a. Ministry of State Security (MSS)	XX
b. Military Intelligence Department (MID)	XX
c. Technical Department	XX
d. New China News Agency (NCNA)	XX
7. Chinese Intelligence Operations	XX
a. HUMINT	XX
b. SIGINT	XX
c. IMINT	XX
8. Chinese Intelligence Collection Trends	XX
9. Cuban Intelligence Collection Capabilities	XX
10. North Korean Intelligence Collection Operations	XX
11. Romanian Intelligence Collection Operations	XX
C. Terrorist Intelligence Operations	XX
1. Terrorist Group Categories	XX
2. Terrorist Tactics	XX
3. Terrorist Objectives	XX
4. Terrorist Threats to the United States	XX
5. Terrorist Sponsors	XX
a. Libya	XX
b. Syria	XX
c. Iran	XX

d. Sudan	XX
e. Iraq	XX
f. Cuba	XX
g. North Korea	XX
6. Islamic Fundamentalist Groups	XX
a. Islamic Resistance Movement (HAMAS)	XX
b. Party of God (Hizballah)	XX
c. Palestine Islamic Jihad (PIJ)	XX
d. Abu Nidal Organization (ANO)	XX
e. Islamic Group (Al-Gama'a al-Islamiyya)	XX
7. Terrorism Trends	XX
D. Economic Intelligence Collection Directed against the US	XX
1. Targeted Information and Technologies	XX
2. Collection Methods	XX
3. Classic Agent Recruitment	XX
4. Volunteers	XX
5. Surveillance and Surreptitious Entry	XX
6. Specialized Technical Operations	XX
7. Tasking of Foreign Employees of U.S. Firms	XX
8. Elicitation during International Conferences and Trade Fairs	XX
9. Foreign Government use of Private Sector Organizations, Front Companies, and Joint Ventures	XX
10. Tasking of Liaison Officers at Government-to-Government Projects	XX
11. National Economic Intelligence Collection Efforts	XX
a. Japan	XX
b. France	XX
c. South Korea	XX
d. Germany	XX
e. Israel	XX
12. Industrial Espionage	XX
13. Economic Impact	XX
E. Open Source Collection	XX
1. Benefits of Open Source Information Collection	XX
2. The Changing Nature of Open Source Information	XX
3. Traditional Open Source Assets	XX
4. Electronic Databases	XX
5. Commercial Imagery	XX
6. Implications for OPSEC Managers	XX

F.	The Changing Threat and OPSEC Programs	XX
	1. Changing Nature of the Intelligence Collection Threat	XX
	a. Information has Value	XX
	b. Information is more Readily Available	XX
	c. Availability of Collection Assets	XX
	d. Worldwide Media Access	XX
	e. Interconnected Communications Systems	XX
	2. Assessing the Intelligence Collection Threat	XX
	3. Obtaining threat Assessment Information and OPSEC	
	Planning Assistance	XX
	a. Federal Bureau of Investigation (FBI)	XX
	b. Defense Intelligence Agency (DIA)	XX
	c. Defense Security Service (DSS)	XX
	d. Department of Energy (DOE) Counterintelligence Division	XX
	e. Department of State (DOS) Bureau of Diplomatic Security	XX
	f. National Counterintelligence Center (NACIC)	XX

APPENDIX E

INSPECTION READINESS PLANNING

1. Background. Current and emerging international treaties and agreements to which the United States is, or will be, a signatory, impact a variety of DoD installations, facilities, sites and activities. This may include facilities that house DoD Special Access Programs (SAPs). Although the likelihood that a SAP Facility (SAPF) may be inspected will vary from site to site, all facilities should plan for inspection readiness. In order to determine the impact of international agreements at or in the vicinity of SAP sites and information, it is necessary to understand individual treaty provisions as they relate to the degree of intrusiveness allowed for an on-site inspection. Also, in order to effectively protect DoD equities, a risk assessment should be carried out to identify the sensitivities involved - exactly what information or processes need to be protected from the threat posed by the mere presence of foreign inspectors, as well as uncleared U.S. Government personnel. A close look should be taken at what security countermeasures should be adopted, and what procedures should be developed for implementing these countermeasures on a timely basis prior to inspection.

2. The Process. Preparing for an inspection incorporates many aspects of the ongoing Operations Security (OPSEC) process. Traditionally the OPSEC process denies adversaries information about capabilities or activities by identifying, controlling, and protecting generally unclassified evidence or information on the planning and execution of sensitive operations or activities. OPSEC considers the changing nature of threats, vulnerabilities and operational and activity phases of a plan, operation, program, activity or project to identify vulnerabilities and determine appropriate countermeasures. Aspects of this approach are applicable to preparing for an inspection as well.

a. The protection of critical information is the objective of inspection planning. In this case, "critical information" is that which, if obtained by a foreign inspector, could result in the compromise of national security, undesired technology transfer, or loss of proprietary information. Each site where a SAP is located should determine precisely what critical information it has on hand and whether there are any obvious indicators that could lead to compromise of the SAP information. Size, shape, substance, and program operation are just a few of the factors that should be taken into account when trying to determine what is on site that could disclose valuable information.

b. It is necessary for SAPFs located on declared inspection sites to understand specific treaty provisions, rights and obligations. All other SAPFs (i.e., not located on declared treaty sites) must realize they can still be inspected during an on-site challenge-type inspection. Treaty provisions provide for verification activities that could include data declarations or exchanges, imaging overflights, on-site inspection (with its own range of activities), consultations, or confidence- and security building measures. Knowing these provisions in advance will provide the ability to construct and put in place the proper security countermeasures.

c. Each treaty affords inspectors certain rights and obligations during the inspection process, and it is crucial to be aware of these rights and how they can impact on SAPF security. Such rights may include access to buildings, structures, records, and personnel interviews; visual observation; measuring and weighing; sampling and analysis; and

photography. Treaties also obligate inspectors to conduct their activities with minimal intrusion or operational impact, and to consider proposals to alter certain aspects of the inspection when requested by the facility or organization hosting the inspection team. Program managers and program security managers should be provided implementation guidance and direction from their service component SAPCO to become aware of rights such as these, and learn what measures legally can be adopted to counteract the inspection team requests, when providing alternate means to demonstrate compliance.

d. Once site-specific critical information has been determined, and the treaties have been examined to determine their potential impact in the event of an inspection, the final phase of readiness planning should be to identify appropriate countermeasures and methods of implementation. It is especially important to do this BEFORE notification of an inspection is received, in order to allow enough time for the measures to be put in place. Countermeasures should be selected based on factors such as feasibility, ease of implementation, proposed effectiveness, and overall cost. They might include basic procedural changes, deception, perception management, physical security measures, and intelligence countermeasures--anything that will reduce the inspection teams' collection capabilities, and what is necessary to protect vital SAP information and U.S. national security interests.

APPENDIX F SECURITY INSPECTION CHECKLIST

This Security Inspection Checklist should be used as discussed in Chapter 1, paragraph 1-206, when conducting self reviews. Each checklist should be marked with the appropriate security classification markings and declassification instructions. **Core Compliance Items (CCI) are identified in *blue italic font*.** (Note: In addition to the references provided, local Activity or individual Agency/Component Service policy, procedures, and regulations may also apply).

Code / No.	Question	References	Yes	No	N/A
A. SECURITY MANAGEMENT					
A-1	Has the contractor implemented the provisions of the JAFAN 6-0 on initial contract award or modification or subsequent modification? (Note: Implementation must be within 6 months of publication of the JAFAN 6-0 via a Contract Security Classification Specification (DD Form 254))	6/0: 1-102c & Foreword			
A-2	Are requests for waivers to established SAP policies and procedures only submitted when they are in the best interest of the Government?	6/0: 1-106a			
A-3	In those cases where waivers are required, has the waiver request been submitted to the service component SAPCO or designee via the PSO's chain of command?	6/0: 1-106b			
A-4	Within 90 days of electing to implement commensurate protective measures, has the PSO notified the service component SAPCO of the commensurate level of protection and requested validation/final approval?	6/0: 1-107			
A-5	Are PSOs appointed, in writing, by the SAPCO or designee?	6/0: 1-200a(1)			
A-6	Are GSSOs appointed, in writing, and assigned to specific facilities/projects/ subcompartments? Are copies of appointment letters provided to the PSO?	6/0: 1-200a(2)			
A-7	Are CPSOs appointed, in writing, and assigned to specific facilities/projects/ subcompartments? Are copies of appointment letters provided to the PSO?	6/0: 1-200a(2)			
<i>A-8</i>	<i>Does the SAP Security Officer have the position, responsibility, and authority commensurate with the degree of SAP security support required?</i>	<i>6/0: 1-200b</i>			
A-9	Has the GSSO/CPSO prepared comprehensive SOPs to implement the security policies & requirements unique to their facilities?	6/0: 1-201			
A-10	Are proposed SOPs and SOP changes forwarded to the PSO for approval?	6/0: 1-201			

Code / No.	Question	References	Yes	No	N/A
A-11	<i>Has an annual self-inspection been conducted by GSSO/CPSO (as appropriate) and did it address issues reflected in the "Security Inspections Checklist" found in JAFAN 6-0, Appendix F?</i>	6/0: 1-206d			
A-12	Are self-inspection reports submitted to the PSO within 30 days following completion of the inspection?	6/0: 1-206d			
A-13	Is the PSO notified immediately if the inspection discloses the loss, compromise or suspected compromise of classified material?	6/0: 1-206d			
A-14	Are self-inspection reports retained for two years following the formal government CSA inspection?	6/0: 1-206d			
A-15	Are all outstanding items (<i>i.e., those with on-going corrective actions</i>) completed prior to the destruction of the self-inspection?	6/0: 1-206d			
A-16	Are instances of Government and Industry fraud, waste, abuse and corruption reported through channels designated by the service component SAPCO?	6/0: 1-207			
A-17	Is the name and telephone number for the current FWAC manager or monitor prominently displayed throughout each SAPF?	6/0: 1-207b			
A-18	If multiple SAPs are located within a SAPF, has a CUA been executed between PSOs prior to occupancy?	6/0: 1-210			
A-19	Where there is co-utilization of SCI within a SAPF, or SAP within a SCIF, has authorization from the PSO & the servicing SSO been obtained?	6/0: 1-210b			
A-20	Are the GPM and PSO notified in advance of any Arms Control Treaty Visits?	6/0: 1-300f			
A-21	Is the PSO made aware of any litigation actions that may pertain to the SAP, to include the physical environments, facilities or personnel or as otherwise directed by the GPM?	6/0: 1-300g			
A-22	<i>Are all security violations reported within 24 hours of discovery to the CPSO/GSSO/PSO, as appropriate?</i>	6/0: 1-301			
A-23	Are violations involving contractor personnel reported by the PSO using the appropriate Defense Security Service (DSS) SAP channels?	6/0: 1-301			
A-24	Has the PSO promptly advised the service component SAPCO in all instances where national security concerns would impact on collateral security programs or clearances of program-accessed individuals?	6/0: 1-301			

Code / No.	Question	References	Yes	No	N/A
A-25	Has the security official of the affected facility determined the scope of the corrective action taken in response to a security infraction/violation and reported it to the PSO?	6/0: 1-301			
A-26	Are security infractions documented and made available for review by the PSO during visits?	6/0: 1-301a(2)			
B. SECURITY PLANNING					
B-1	When a badge system is considered necessary has it been documented in the facility SOP & address topics such as badge accountability, storage, inventory, disposition, destruction, format & use?	6/0: 1-202			
B-2	Is a badge system in place to permit total personal identification & access level determinations (unless the program area is small enough (normally less than 25 people))?	6/0: 1-202			
B-3	When all individuals within a SAPF cannot be personally identified, has a badging system been implemented by the PSO?	6/0: 1-202			
B-4	Are TEMPEST Requirement Questionnaires (TRQ) submitted when processing data on an information system?	6/0: 10-100b			
B-5	Has the PSO, with guidance from a CTTA, determined if countermeasures are required based upon the completed TRQ?	6/0: 10-100b			
B-6	Are OPSEC plans/surveys accomplished to identify, define, and develop countermeasures to vulnerabilities?	6/0: 10-400			
C. PERSONNEL SECURITY					
C-1	Does the GSSO/CPSO possess a personnel security clearance at least equal to the highest level of classified information for which they require access? Possess access to all SAPs assigned to the facility(s) for which he/she is responsible?	6/0: 1-200c(1) & (2)			
C-2	<i>Do personnel possess access to all SAPs assigned to the facility(s) for which he/she is responsible?</i>	6/0: 1-200c(4)			
C-3	<i>Are all briefed personnel reporting to the PSO any information which may adversely reflect on the Program-briefed employee's ability to properly safeguard classified Program information?</i>	6/0: 1-300a			
C-4	Is all travel outside the continental United States, Hawaii, Alaska and the U.S. possessions (i.e., Puerto Rico) reported to the GSSO/CPSO thirty days in advance?	6/0: 1-300e & 1-303			
C-5	Has the CPSO/GSSO notified the PSO before program accessed personnel travel to any country, with special emphasis on travel to countries identified on the National Security Threat List?	6/0: 1-300c			

Code / No.	Question	References	Yes	No	N/A
C-6	Is a written report of all changes in the personal status of SAP indoctrinated personnel provided to the PSO?	6/0: 1-300c			
C-7	Have personnel determined to have had unauthorized or inadvertent access to classified SAP information: (1) been interviewed to determine the extent of the exposure, and; (2) been requested to complete an Inadvertent Disclosure Form (see SAP Format 5)?	6/0: 1-301b			
C-8	Has the PSO been made aware of any reports which affect the baseline facility clearance or any incident of a personnel security clearance nature?	6/0: 1-300 & 2-100			
C-9	Has the PSO forwarded all reportable information to the appropriate officials (i.e. Special Access Program Central Adjudication Facility (SAPCAF), CI commands/agencies, etc)?	6/0: 1-300			
<i>C-10</i>	<i>Do SAP-accessed personnel have a valid need-to-know and certification that he/she will materially and directly contribute to the Program?</i>	<i>6/4: 1.2c</i>			
C-11	Is SAP Format 2 "Special Access Information Agreements" signed prior to briefing an individual approved for access?	6/0: 1-300b			
C-12	Does the access data base or listing will contain the name of the individual, position, billet number (if applicable), level of access, social security number, and security clearance information?	6/0: 2-205			
<i>C-13</i>	<i>Has every individual accessed to a SAP been given an initial indoctrination? Are these indoctrinations conducted by the PSO/GSSO/CPSO or designee?</i>	<i>6/0: 3-101</i>			
C-14	Has a formal debriefing program been developed?	6/0: 3-102a			
C-15	Do formal debriefings include: (1) how to obtain a release before publishing, (2) what can & cannot be discussed or placed in resumes & applications for security clearances, (3) turning in all holdings, (4) applicability of & penalties for engaging in espionage, (5) where to report suspected Foreign Intelligence Service (FIS) contacts or any attempt by unauthorized persons to solicit program data and, (6) appropriate espionage laws and codes.	6/0: 3-102a(1) through (6)			
C-16	Has a SAPIA been executed at the time of the debriefing and forwarded to PSO within two business days?	6/0: 3-102			

Code / No.	Question	References	Yes	No	N/A
C-17	If attempts to locate an individual either by telephone or mail are not successful, and the whereabouts of the individual cannot be determined in 30 days; is the individual administratively debriefed (i.e., completion of a debriefing form, annotating the form with "INDIVIDUAL NOT AVAILABLE- ADMINISTRATIVELY DEBRIEFED")? Is the appropriate database updated to reflect this?	6/0: 3-103			
C-18	Are Foreign Travel briefings and debriefings conducted for all accessed personnel prior to and following return of travel using SAP Format 6, Notification of Foreign Travel, or its SCI community equivalent form (either are acceptable)?	6/0: 3-104			
C-19	Do individuals processed for program access meet the prerequisite personnel clearance and/or investigative requirements?	6/4: 1.2c & 3.2			
C-20	Does the candidate nomination package contain a completed PAR, a copy of the nominee's PSQ (SF 86/86c or eQIP printout - current within one year) and results of the Local Records Check (if legally available)?	6/4: 3.3b			
C-21	When the candidate's nomination package is ready to be forwarded to the Government PSO, has the CPSO completed the PAR, to include their signature, date of signature, concurrence and a check to ensure all pertinent attachments are identified and included, as appropriate?	6/4: 3.3d			
C-22	Do Letters of Compelling Need (LOCN) accompany those access approval requests which require a waiver? Do LOCNs describe the candidate's unique skills or knowledge and the benefit to the program?	6/4: 4.3.d(4)			
C-23	<i>Are those candidate nomination packages that cannot be mitigated at the 2nd Tier level forwarded to the SAPCAF for action?</i>	6/4: 7.1			
C-24	When an access eligibility determination is unfavorable, has the SAPCAF issued a Letter of Intent (LOI)?	6/4: 7.4			
C-25	Has the CPSO or GSSO provided the LOI to the candidate?	6/4: 7.4			
C-26	When a candidate is unsuccessful in his/her appeal, has the SAPCAF forwarded the candidate a Letter of Denial (LOD) or Letter of Revocation (LOR)?	6/4: 7.5			

Code / No.	Question	References	Yes	No	N/A
D. ACCOUNTABILITY					
D-1	Are TOP SECRET engineering notebooks permanently bound documents and each page numbered consecutively, front and back?	6/0: 4-201a & d			
D-2	Are the outer covers and each page of TOP SECRET engineering notebooks marked with the highest classification and program identification(s) contained in the notebook?	6/0: 4-201b			
D-3	Has a Top Secret Control Official (TSCO) been designated in writing?	6/0: 5-201e			
<i>D-4</i>	<i>Has an annual 100 percent inventory of accountable SAP classified been conducted by the TSCO or alternate and a disinterested party?</i>	<i>6/0: 5-202</i>			
D-5	Are these inventories conducted by sighting all copies of accountable material held within the facility?	6/0: 5-202			
<i>D- 6</i>	<i>Has all TOP SECRET SAP information been entered into a PSO approved document control accountability system whenever it is received, generated or dispatched either internally or externally to other SAPFs?</i>	<i>6/0: 5-201a</i>			
D- 7	Is each item of TOP SECRET SAP material numbered in series and identified with an individual copy number and total copy count?	6/0: 5-201f			
D- 8	Do all TOP SECRET working papers have a cover sheet marked with the date of origin, originator's name and the annotation "WORKING PAPER"?	6/0: 5-203			
D- 9	Are all TOP SECRET SAP working papers EITHER entered into the accountability system OR destroyed after 30 calendar days from the date of origin?	6/0: 5-203b			
E. CLASSIFICATION AND MARKING					
<i>E-1</i>	<i>Does each SAP have a Security Classification Guide to identify Critical Program Information (CPI)?</i>	<i>6/0: 4-101</i>			
E-2	Are challenges to SAP classified information and/or material classifications forwarded through the PSO to the appropriate Original Classification Authority (OCA)?	6/0: 4-101			
E-3	Has a DD Form 254, Contract Security Classification Specification Requirements, been prepared for each contractor performing work on SAPs?	6/0: 4-103			
E-4	Is all SAP material marked and controlled in accordance with JAFAN 6-0, NISPOM (baseline marking requirements), the program SCG, and other program guidance?	6/0: 4-200			

Code / No.	Question	References	Yes	No	N/A
E-5	<i>Do cover sheets when used as a Record of Disclosure will remain affixed to TOP SECRET documents at all times? Does the Record of Disclosure include the identity of all persons given access to the information and the date of the disclosure?</i>	6/0: 4-202 & 5-201a			
E-6	Is Unclassified HVSACO information safeguarded IAW Appendix "A"?	6/0: Appendix "A"			
F. REPRODUCTION					
F-1	Is program material only reproduced on equipment approved by the PSO?	6/0: 5-600			
F-2	Have the GSSOs/CPSOs prepared written reproduction procedures?	6/0: 5-600			
F-4	Is reproduction equipment positioned to assure immediate and positive monitoring?	6/0: 5-600			
F-5	Has a notice indicating if equipment can or cannot be used for reproduction of classified material been posted?	6/0: 5-600			
F-6	Are procedures approved in writing by the PSO (including clearing of equipment, accessing of operators, clearing of media, handling malfunctions, etc.) when reproduction equipment is used outside a SAPF (i.e. TSWA)?	6/0: 5-600			
G. DESTRUCTION					
G-1	Upon contract close-out, are requests for retention of classified information submitted to the Contracting Officer through the PSO for review and approval?	6/0: 5-700			
G-2	Has the contractor submitted a request to the Contracting Officer through the PSO for authority to retain classified material beyond the end of the contract performance period?	6/0: 5-701			
G-3	Is all classified waste destroyed as soon as possible (not allowing materials to accumulate beyond 30 days unless approved by the PSO)?	6/0: 5-704			
G-4	Is classified waste residue inspected during each destruction to ensure that classified information cannot be reconstructed?	6/0: 5-705			
G-5	Has the PSO reviewed and approved all destruction procedures?	6/0: 5-703			
G-6	Are destruction certificates completed and signed by both of the individuals completing the destruction immediately after destruction is completed?	6/0: 5-706			

H. PHYSICAL SECURITY					
H-1	Has the SAPF been formally accredited in writing by a government PSO or designee prior to conducting any SAP activities?	6/9: 1.1.4			
H-2	Has an accreditation checklist (e.g., JAFAN 6/9, Annex A, SAPF Fixed Facility Checklist) been completed and approved by the PSO?	6/9: 2.2.1			
H-3	Are PEDs, with the exception of the following, prohibited within a SAPF: (1) Electronic calculators, spell checkers, language translators, etc. (2) Receive-only pagers. (3) Audio and video playback devices. (4) Receive only Radios. (5) Infrared (IR) devices that convey no intelligence data (text, audio, video, etc.), such as an IR mouse and/or remote controls. (6) Medical, life and safety portable devices.	6/0: 5-900			
H-4	Are entry/exit inspections conducted to deter the unauthorized removal of classified material, and deter the introduction of prohibited items or contraband?	6/9: 2.7			
H-5	Has the PSO instituted procedures for control of electronic devices and other items introduced into or removed from the SAPF?	6/9: 2.8.1			
H-6	When conditions warrant, has a TSCM evaluation been requested (at the discretion of the PSO)?	6/9: 2.3.3			
H-7	Are combinations changed immediately whenever: <ul style="list-style-type: none"> • a combination lock is first installed or used? • a combination has been subjected, or believed to have been subjected to compromise? • whenever a individual knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock? • at other times when considered necessary by the PSO? 	6/9: 2.6.1			
H-8	Has co-location/co-utilization of Sensitive Compartmented Information within a SAPF been authorized via PSO?	6/9: 2.4.2			

Code / No.	Question	References	Yes	No	N/A
I. ACCESS CONTROL					
I-1	Is a written/electronic visit notification coordinated in advance & acknowledged/ approved prior to visiting a SAPF (via hardcopy/electronic transfer/database)?	6/0: 6-100			
I-2	Has the GPM or his/her designated representative approved all visits between program activities? Has the PSO or designee certified the accesses to the facility?	6/0: 6-101a(1)			
I-3	Are twelve-month visit certifications not authorized unless approved in writing by the PSO?	6/0: 6-101b			
I-4	Are all visit requests transmitted via PSO-approved channels (via hardcopy/electronic transfer/database)?	6/0: 6-100			
I-5	Has the PSO/GSSO/CPSO or his/her designated representative immediately notified all recipients of the cancellation or termination of visit requests?	6/0: 6-101g			
I-6	Is positive identification of each visitor made using an official State or Federal-issued identification card/credential with a photograph?	6/0: 6-101d			
I-7	Are non-program accessed visitors continuously escorted and their movements closely controlled while in a SAPF?	6/0: 6-101f			
I-8	Are advance arrangements coordinated between the visitor, the visitor's cognizant security officer and the destination facility's security officer regarding the hand carrying of program material?	6/0: 6-101(3)			
I-9	Has use of internal warning systems been considered or employed along with other additional methods (e.g., verbal announcements) to warn or remind personnel of the presence of uncleared personnel?	6/0: 6-101f			
I-10	Are all non-program briefed personnel (e.g., maintenance workers, repair technicians, etc) required to complete the visitor's record and be escorted by a resident program-briefed individual?	6/0: 6-102			
I-11	Has a separate program visitor's record been established for program briefed visitors? Does it show the visitor's name, last four digits of the individual's SSN, organization or firm, date, time in and out, and sponsor on the log?	6/0: 6-103			
I-12	Are program meetings and conferences conducted only in approved SAPFs? (<i>Note: PSOs may authorize additional locations, i.e. Temporary Secure Working Area (TSWA)</i>)	6/0: 6-200			

Code / No.	Question	References	Yes	No	N/A
J. COMPUTER SECURITY					
J-1	<p>Does a formal IA Program exist with all required Documentation available, current and complete?</p> <ul style="list-style-type: none"> a. Certification and Accreditation b. Delegations of Authority c. MOUs & CUAs d. SSP/SSAA and other procedural documents e. Guest systems documentation f. Audit documents 	<p>J-1: 6/3: 2.B.6.c(1) J-1: 6/3: 9.F.2 a: 6/3: 2.B.4.c; 9.D.4 b: 6/3:2.B.2.b(3) b: 6/3:9.D.3.b(1) c: 6/3: 9.D.2.b(2) d: 6/3:2.B.7.c(3) d: 6/3:9.C.3 e: 6/3: 8.B.6 f: 6/3: 4.B.1.b(2) f: 6/3: 4.B.2.a(4)(c)</p>			
J-2	<p>Does a Configuration Management program appropriate for the PL exist?</p> <ul style="list-style-type: none"> a. Is it a formally documented process? b. Does it address all aspects of hardware & software management. c. Does it address maintenance and disposition of equipment 	<p>J-2: 6/3: 5.B.1.a(2) a: 6/3: 2.B.7.c(7) b: 6/3: 5.B.1.a(2)(b) c: 6/3: 8.B.5.e c: 6/3: 8.B.8.c(7)</p>			
J-3	<p>Does a formal IA Training Program exist that addresses all users:</p> <ul style="list-style-type: none"> a. IAM/ISSM/ISSR duties b. SysAdmin and privileged users c. Regular Users d. Special Requirements (DTO etc) 	<p>J-3: 6/3: 8.B.1.a a: 6/3: 2.B.5.c(9) a: 6/3: 8.B.1.b b: 6/3: 8.B.1.c(1) c: 6/3: 8.B.1.c(2) d: 6/3: 8.B.1.b(4)</p>			
J-4	<p>Does a media management plan exist that addresses the following:</p> <ul style="list-style-type: none"> a. Does it address ALL media in the facility b. Are formal procedures for data extraction/data transfer approved and in use c. Does the plan address media movement & day to day management d. Are sanitization/disposition procedures in place for ALL media types in use e. Are appropriate markings and labeling procedures in use 	<p>J-4: 6/0: 8-101 a: 6/0: 8-102 b: 6/3: 8.B.3 c: 6/0: 8-102 d: 6/3: 8.B.5 e: 6/3: 8.B.2.a</p>			

Code / No.	Question	References	Yes	No	N/A
K. TRANSMISSION					
K-1	If transmission by a commercial courier is anticipated, has the PSO approved its use?	6/0: 5-400b			
K-2	Is all classified SAP material prepared, reproduced, and packaged by program-briefed personnel in SAPFs?	6/0: 5-401			
K-3	Are receipts for the transmission of all classified (SECRET/TOP SECRET) material used/maintained?	6/0: 5-401a			
K-4	Is tracer action initiated when a receipt or acknowledgment of a shipment of material is not returned within 30 days?	6/0: 5-401b(1)			
K-5	Are Two-Person courier teams used for all handcarry of TOP SECRET/SAP data unless a single-person courier is approved in advance by the cognizant PSO?	6/0: 5-402a			
K-6	Are problems encountered by couriers while enroute will be immediately reported to the PSO?	6/0: 5-402e			
K-7	<p>Are Courier Authorization letters (i.e., SAP Format 28) or card (<i>see below</i>) issued by the PSO/GSSO/CPSO from the departure location outlining the courier procedures?</p> <p>(1) Does the Courier Authorization and pre-departure instructions address the: a) method of transportation, b) travel itinerary (intermittent/unscheduled stops, remain-overnight scenarios, etc), c) specific courier responsibilities (primary/alternate roles-as necessary), and d) completion of receipts (as necessary) and full identification of the classified data being transferred and e) a discussion of emergency/contingency plans (include after-hours POCs, primary/alternate contact data, telephone numbers, etc)</p> <p>(2) Has each courier will acknowledge receipt/understanding of this briefing in writing.</p> <p>(3) In the case of experienced program-briefed individuals who frequently or routinely perform duties as classified couriers, are they issued Courier Authorization cards by the PSO/GSSO/CPSO in lieu of individual letters for each trip?</p> <p>(4) Are courier cards revalidated/reissued annually?</p>	6/0: 5-402c(1) & (2)			

Code / No.	Question	References	Yes	No	N/A
K-8	<i>Is Top Secret material transmitted only by authorized means (e.g., 2-person courier, secure electronic means)?</i>	6/0: 5-402a & 5-403			
K-9	Is SAP information double-wrapped using opaque material which precludes observation of contents?	6/0: 5-401c			
K-10	When secure facsimile and/or electronic transmission is permitted, has the PSO approved the system in writing?	6/0: 5-403			
K-11	When a U.S. Postal mailing channel is approved by the PSO, is mail received only by appropriately cleared and accessed personnel?	6/0: 5-404			
K-12	Are problems, misdeliveries, losses, or other security incidents encountered with transmission of SAP information immediately reported to the the PSO?	6/0: 5-404e			
K-13	Before any movement of classified SAP assets are transportation plans developed and approved by the PSO at least 30 days in advance of the proposed movement?	6/0: 5-404f			
K-14	Are two program briefed personnel destroying accountable classified program material?	6/0: 5-702			
K-15	Are receipts maintained IAW Appendix "C" (five year period)?	6/0: Appendix "C"			
L. SECURITY EDUCATION					
L-1	<i>Have all individuals received initial and refresher training per Table 1, JAFAN 6-0, and topics covered as listed on SAP Format 17?</i>	6/0: 3-100 & Appendix "G"-SAP Format 17			
L-2	Have GSSOs/CPSOs ensured that the Security Education & Training program meets specific and unique requirements of individual SAPs?	6/0: 3-100			
L-3	Has each individual reviewed their eQIP/SF86 printout on an annual basis and updated it as necessary? <i>(Note: annual refresher training sessions are a good opportunity to accomplish this)</i>	6/0: 3-101			
M. CONTRACTING					
M-1	When a subcontractor does not have the requisite facility clearance, has the prime CPSO initiated the necessary FCL paperwork and submitted it to the PSO? Has the PSO coordinated with DSS to initiate action to provide the subcontractor a facility clearance?	6/0: 7-101			

Code / No.	Question	References	Yes	No	N/A
M-2	In the pre-contract phase, has the prime contractor advised the prospective subcontractor (prior to any release of SAP information) of the procurement's enhanced special security requirements? Have arrangements for subcontractor program access been pre-coordinated with the PSO?	6/0: 7-102			
M-4	Has the CPSO completed a SAP Format 13, Subcontractor/Supplier Data Sheet, and submitted it to the PSO?	6/0: 7-102			
M-5	Has the CPSO included the reason for considering a subcontractor and attached a proposed DD Form 254 to the SAP Format 13? <i>(Note: The DD Form 254 shall be tailored to be consistent with the proposed support being sought.)</i>	6/0: 7-102			
M-6	Are DD Form 254s prepared by prime contractor CPSOs and forwarded to the PSO for approval (before signature by the prime contractor and release to subcontractors)? Have PSOs coordinated these DD Form 254s with the GPM and Government Contracting Officer (GCO)?	6/0: 7-103			
N. GUARD FORCE					
N-1	Within the U.S. at at <u>CLOSED</u> storage SAPF, is a response force capable of responding to an alarm within <u>15</u> minutes after annunciation and a reserve response force available to assist the responding force?	6/9: 3.1.1.1			
N-2	Within the U.S. at at <u>OPEN</u> storage SAPF, is a response force capable of responding to an alarm within <u>5</u> minutes after annunciation and a reserve response force available to assist the responding force?	6/9: 3.1.2.1			
N-3	Are response force personnel appropriately trained and equipped according to SOPs to accomplish initial or follow-up response to situations that may threaten the SAPF's security?	6/9: Annex B, para 5.2.2			
N-4	Is the IDE maintained by US citizens? <i>(Note: Non-US citizens shall not provide these services without prior written approval by the PSO)</i>	6/9: Annex B, para 5.3.1			
N-5	Is the alarm monitoring station continuously supervised and operated by US citizens who are trained alarm monitors, cleared to the SECRET level?	6/9: Annex B, para 5.1.1			

O. SPECIAL EMPHASIS ITEMS

**APPENDIX G
SPECIAL ACCESS PROGRAM FORMATS**

<u>NUMBER</u>	<u>TITLE</u>	<u>DATE</u>
SAP Format 1, (JAFAN EDITION)	Program Access Request (PAR) <i>(*supercedes all previous editions; insert in JAFAN 6-4 as a page change)</i>	May 08
SAP Format 2 (JAFAN EDITION)	Special Access Program Indoctrination Agreement (SAPIA) <i>(Note: SAP Format 2a, Special Access Program Indoctrination Agreement (Jan 9)(Polygraph Supplement), has been rescinded effective the date of this publication. Polygraph agreement language has not changed and has been incorporated into the SAPIA Agreement as Items 16 & 17)</i>	Dec 07
SAP Format 5	Inadvertent Disclosure Statement	Jan 98
SAP Format 6	Notification of Foreign Travel <i>(Note: SCI Comparable Form may be used- DoD 5105.21-M-1, Appendix I, Atchs 8 & 9 – Foreign Travel/Foreign Contact Questionnaires are included)</i>	Jan 98
SAP Format 7	Visit Notification (Authorization) Request	Jan 98
SAP Format 8	TSCM Request	Jan 98
SAP Format 12	Waiver Request from Security Criteria	Jan 98
SAP Format 13	Subcontractor/Supplier Data Sheet	Jan 98
SAP Format 17	Refresher Training Record	May 08
SAP Format 19	Special Access Program Inspection	May 08
SAP Format 20	Foreign Relative or Associate Interview	Jan 98
SAP Format 21	Computer System User Acknowledgment	Jan 98
SAP Format 27	Foreign Contact	Jan 98
SAP Format 28	Courier Designations and Instructions	Jan 98
SAP Format 32	SAP Transfer of Eligibility Request Form	Jun 07

Note: Previous editions of SAP Formats NOT listed above have been deemed obsolete and have been discontinued.

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

PROGRAM ACCESS REQUEST					
1. Program Name		2. Access Level		3. Date Requested	
4. Last Name, First Name, Middle Initial		5. Rank/Grade	6. U.S. Citizen <input type="checkbox"/> Yes <input type="checkbox"/> No	7. SSAN	
8. Date of Birth (YYMMDD)	9. City/State/Country of Birth		10. <input type="checkbox"/> Military <input type="checkbox"/> Government Civilian <input type="checkbox"/> Contractor		11. Date Needed By
12. Position Description/Job Title			13. <input type="checkbox"/> Full Time <input type="checkbox"/> Temporary (Period of access) <input type="checkbox"/> Part Time (From: _____ To: _____)		
14. Organization/Company Name		15. Assignment/Job Location (City & State)		16. Command/Facility/Office Symbol/Agency Identifier (if any)	
17. Security Clearance	18. Granted By	19. Date Granted	20. Investigation Type	21. Conducted By	22. Date Completed
23. Security Investigation Status (results of Joint Personnel Adjudication System (JPAS) check) <input type="checkbox"/> In Progress (Date Initiated/Submitted: _____ (YYMMDD) (include additional information in the "Remarks" section below as needed) <input type="checkbox"/> Current <input type="checkbox"/> Out-of-Scope Approval _____ (YYMMDD) _____ (Signature of Waiver Authority)			24. Defense Central Investigations Index (DCII) & Joint Personnel Adjudication System Checks (conducted by Government) Conducted By: _____ Date Checked: _____ (YYMMDD) <input type="checkbox"/> Acceptable DCII check results <input type="checkbox"/> Acceptable JPAS check results <input type="checkbox"/> Referred to next Tier Review Official level		
25. Justification (_____) (include detailed justification as to how this candidate will support and contribute to the program) (CONTINUE ON SEPARATE SHEET IF NECESSARY) CLASSIFICATION					
26. Billet Number (if any): _____					
27. Requestor (Government/Contractor)					
Typed Name/Title/Organization		Signature		Telephone Number	Date
28. Additional Coordination (As Necessary)					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
29. Government SAP Security Officer/Contractor Program Security Officer (GSSO/CPPO)					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
30. Government/Contractor Program Manager (GPM/CPM)					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
Tier Review (Refer to JAFAN 6/4, Tier Review Process Manual) (Government/Contractor)					
31. FIRST TIER REVIEW OFFICIAL (TRO) (Typed Name/Title/Organization)		Signature		<input type="checkbox"/> First Tier Eligible <input type="checkbox"/> First Tier Ineligible	Date
32. SECOND TIER REVIEW OFFICIAL (TRO) (Typed Name/Title/Organization)		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
33. THIRD TIER REVIEW OFFICIAL (TRO) (Typed Name/Title/Organization)		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
34. Government Program Security Officer (PSO) (Government Only)					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Concur <input type="checkbox"/> Non-Concur	Date
35. SAP Central Office (SAPCO) (Government Only) (If SAPCO Waiver Required)					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Waiver - Approved <input type="checkbox"/> Waiver - Disapproved	Date
36. Access Approval Authority (AAA) (Government Only)					
Typed Name/Title/Organization		Signature		<input type="checkbox"/> Access Approved <input type="checkbox"/> Access Disapproved	Date
37. Remarks/Restrictions (CONTINUE ON SEPARATE SHEET IF NECESSARY)				Derived From: Reason: Declassify On: Authority: File Series Exemption dtd 30 March 2005	

SAP Format 1-JAFAN Edition "Program Access Request," May 2008 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 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 your access to the information indicated has been terminated.

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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.

16. 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.

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

18. SIGNATURE		b. DATE (YYYYMMDD)
19. WITNESS AND ACCEPTANCE. The execution of this Agreement was witnessed by me who accepted it on behalf of the United States Government as a prior condition of access to Special Access Program Information.	a. SIGNATURE	b. DATE (YYYYMMDD)

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):	
_____ <i>Signature of Individual Briefed</i>	

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):	
_____ <i>Signature of Individual Debriefed</i>	

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

Signature of Briefing Officer

Signature of Debriefing Officer

Printed or Typed Name

Printed or Typed Name

SSN (See Notice Below)

SSN (See Notice Below)

Organization (Name and Address)

Organization (Name and Address)

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. §7311 and applicable DoD Directives / Executive Orders

PRINCIPAL PURPOSE(S): To obtain accountability information for managing employee access to special access program (SAP) information and to document individual SAP access briefings and debriefings.

ROUTINE USE(S): None

DISCLOSURE: Disclosure of the information is voluntary for the individual being briefed or debriefed and the official performing the briefing or debriefing. However, failure of the aforementioned individuals to provide the requested information may delay the briefing or debriefing. In addition, failure of the individual being briefed to provide the requested information may result in his or her being declared ineligible for access to SAP information.

SAP Format 2, JAFAN Edition "Special Access Program Indoctrination Agreement," December 2007 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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 _____

SAP Format 6, "Notification of Foreign Travel," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

TSCM Request (U)

(U) FACILITY _____ (Date of Request) _____
(Organization/Company Name)

(U) STREET _____
(Complete Address)

(U) CITY _____ STATE _____ ZIP _____

(S/SAR) BLDG NUMBERS _____ TOTAL NUMBER REQ _____
(Program Areas) (Submit a Separate Request for Each Facility)

(S/SAR) ROOM NUMBERS _____
(Program Areas) (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 _____ FILE NO _____
(If Known) (If Known)

(U) GOVT SECURITY MANAGER _____ WORK PHONE _____
HOME PHONE _____

(U) FACILITY POC _____ WORK PHONE _____
(Security Manager) HOME PHONE _____

(U) ALTERNATE POC _____ WORK PHONE _____
(Alternate Security Manager) HOME PHONE _____

(S/SAR) REASON SURVEY NEEDED _____

(Signature of In-Place Security Manager) (Signature of Govt Program Security Officer)

(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.

DERIVED FROM:
DECLASSIFY ON:

SAP Format 8, "TSCM Request," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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 _____

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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 #)

SAP Format 12, "Waiver Request From Security Criteria," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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 _____

SAP Format 13, "Subcontractor/Supplier Data Sheet," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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.

Mandatory Topics Covered	Date Completed	Programs/Projects
<input type="checkbox"/> Protection of classified relationships	_____	_____
<input type="checkbox"/> Operations Security (OPSEC) / Program Threats	_____	_____
<input type="checkbox"/> Use of Nicknames and Code Words	_____	_____
<input type="checkbox"/> COMSEC Procedures	_____	_____
<input type="checkbox"/> Special Test-Range security procedures	_____	_____
<input type="checkbox"/> Writing unclassified resumes, appraisals & reviews	_____	_____
<input type="checkbox"/> Tier Review process	_____	_____
<input type="checkbox"/> Courier / Other Secure Transmission modes/procedures	_____	_____
<input type="checkbox"/> Types & Categories of SAPs	_____	_____
<input type="checkbox"/> Trends from Govt Inspections / Other Self-Reviews	_____	_____
<input type="checkbox"/> Visit Certifications / Visit Procedures	_____	_____
<input type="checkbox"/> Document Control & Receipt / Dispatch	_____	_____
<input type="checkbox"/> Foreign Intelligence Service (FIS) Techniques	_____	_____
<input type="checkbox"/> STU-III / STE Telephone Usage / Procedures	_____	_____
<input type="checkbox"/> Terrorism & Potential Impact on SAPs	_____	_____
<input type="checkbox"/> Original & Derivative Classification	_____	_____
<input type="checkbox"/> Adverse Information Reporting Requirements	_____	_____
<input type="checkbox"/> SAP Fraud, Waste & Abuse Reporting	_____	_____

Computer Security

<input type="checkbox"/> JAFAN 6/3 (IA Operating Procedures)	_____	_____
<input type="checkbox"/> Data Transfers (High to Low transfers)	_____	_____
<input type="checkbox"/> Password Protection	_____	_____
<input type="checkbox"/> Media Protection / Media Control / Copy Procedures	_____	_____

Other Topics Covered

- _____
- _____
- _____
- _____

Personal Status

I have reviewed my SF 86 / EPSQ (DoD Personnel Security Questionnaire) and have updated and reported any previously unreported status changes.

Individual's Initials: _____

Full Name (Printed) _____

Organization/Firm _____

Signature (Trainee) _____

Location _____

Signature (Trainer) PSO / GSSO / CPSO _____

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

SPECIAL ACCESS PROGRAM INSPECTION REPORT Date:

SECTION I - GENERAL INFORMATION

1. NAME OF ACTIVITY:			2. ADDRESS: (Physical Street address)		
3. MANAGEMENT : PM: Major Program:			4. TYPE OF ACTIVITY: <input type="checkbox"/> Government <input type="checkbox"/> Prime Contractor <input type="checkbox"/> Subcontractor		
CPSO/GSSO:			PSO:		
5. INSPECTION DATES:			6. SCOPE OF ACTIVITY:		
Last Insp: (To-From)		Current Insp: (To-From)	<input type="checkbox"/> Active <input type="checkbox"/> Inactive		<input type="checkbox"/> Close Out
7. NUMBER OF PERSONS ACCESSED:			8. NUMBER OF DOCUMENTS:		
SECRET	TOP SECRET	TOTAL	TOP SECRET:	SECRET:	CONFIDENTIAL:
			Total:		

SECTION II - INSPECTION SUMMARY

9. TYPE: <input type="checkbox"/> Full-Scope <input type="checkbox"/> Re-inspection <input type="checkbox"/> Core Compliance <input type="checkbox"/> Close Out <input type="checkbox"/> Unannounced					
10. OVERALL RATING: <input type="checkbox"/> Superior <input type="checkbox"/> Commendable <input type="checkbox"/> Satisfactory <input type="checkbox"/> Marginal <input type="checkbox"/> Unsatisfactory					
11. DEFICIENCIES: <input type="checkbox"/> No Deficiencies Findings Deviations Corrected-On-The-Spot					
12. INSPECTOR NAMES/AGENCIES: SEE ATTACHED REPORT Time Expended: <input type="checkbox"/> Days <input type="checkbox"/> Hours					
13. PERSONNEL OUTBRIEFED: SEE ATTACHED REPORT					

SECTION III - FUNCTIONAL AREAS INSPECTED

CODE	FUNCTIONAL AREA	RATING	CODE	FUNCTIONAL AREA	RATING
A	Security Management	<input type="checkbox"/>	H	Physical Security	<input type="checkbox"/>
B	Security Planning	<input type="checkbox"/>	I	Access Control	<input type="checkbox"/>
C	Personnel Security	<input type="checkbox"/>	J	Computer Security	<input type="checkbox"/>
D	Accountability	<input type="checkbox"/>	K	Transmission	<input type="checkbox"/>
E	Marking	<input type="checkbox"/>	L	Security Education	<input type="checkbox"/>
F	Reproduction	<input type="checkbox"/>	M	Contracting	<input type="checkbox"/>
G	Destruction	<input type="checkbox"/>	N	Guard Force	<input type="checkbox"/>
O	Special Emphasis Item(s):				

SECTION IV - REPORT PROCESSING

14. CORRECTIVE ACTION REPORT: <input type="checkbox"/> Required → <input type="checkbox"/> Not Required ↓	15. RESPOND TO: _____ _____	16. DISTRIBUTION:
		Derived From: Reason: E.O. 12958, Section 1.4(a) and (c) Declassify On: Authority: File Series Exemption (dated 30 March 2005)

17. ATTACHMENT(S): 1. SAP Inspection Report ___ 2. Other: ___ (see description)

SAP Format 19, "Special Access Program Inspection Report," May 2008 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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," Jan 1998 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 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 your access to the information indicated has been terminated.

(Use additional sheets for Remarks, as needed)

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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

SAP Format 21, "Computer System User Acknowledgement Statement," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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:

SAP Format 27, "Foreign Contact Form," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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:

*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.

SAP Format 27, "Foreign Contact Form," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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 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 rough 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.

SAP Format 28, "Courier Designations and Instructions," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

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 couriering 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 (Type or Print)

Signature of Security Officer

Date

SAP Format 28, "Courier Designations and Instructions," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

DoD 5105.21-M-1, Appendix I, Attachment 8 – Foreign Travel Questionnaire

AP1.A8. APPENDIX 1, ATTACHMENT 8

SAMPLE FORMAT FOR FOREIGN TRAVEL QUESTIONNAIRE

Name: _____ SSN: _____

Date of birth (mm/dd/yy): _____ Organization/government: _____

Traveler's job title/duties (Brief narrative description of traveler's duties and responsibilities):

Passport type/number: _____ Visa number/country: _____

Date/location of departure and re-entry into U.S. (e.g., 16 FEB 92, Kennedy Airport, New York, NY, or Border Crossing, San Diego, CA):

Purpose for travel (Specify):

Recreation, to visit family members/friends (List names of those visited).

Business (Identify Government entities, companies, organizations, or universities visited).

Country/countries visited (include cities/towns) and date(s)

(NOTE: Please attach additional sheets if detailed narratives are required.)

1. Were any problems encountered at the time of arrival or departure from the foreign country?
 YES NO

2. Did you have any unusual experiences while traveling to include harassment, suspected surveillance, detention, unusual customs inspection, searches of hotel room or trash, listening devices found, telephone monitoring, etc.?
 YES NO

3. Any travel restrictions imposed by the country during the visit? Where any abrupt changes made in the itinerary?
 YES NO

DoD 5105.21-M-1, Appendix I, Attachment 8 – Foreign Travel Questionnaire

DoD 5105.21-M-1, Appendix I, Attachment 8 – Foreign Travel Questionnaire (continued)

- 4. Were any probing inquiries made relative to traveler's job, duties, studies, and/or company or organization? (If yes, complete Foreign Contact Questionnaire.)
 YES NO

- 5. Any blatant indication of possible approach/efforts to compromise by foreign intelligence service?
 YES NO

- 6. Did traveler meet a foreign national who requested future contact? (If yes, complete Foreign Contact Questionnaire.)
 YES NO

- 7. Has the traveler been debriefed by any other agency or official?
 YES NO
(If yes, please list.) _____

- 8. Was the traveler a victim of a criminal act? Was the traveler detained or arrested? Did the traveler witness any acts that may be considered terrorist like? Was the traveler approached by anyone offering to exchange currency?
 YES NO

- 9. Did the traveler lose/misplace any official materials or personal luggage? Did the traveler take any personal pictures of foreign government, military installations, or equipments? Were you hospitalized during the trip? Did the traveler check in and out with the local embassy or consulate?
 YES NO

- 10. What is the traveler's opinion of the briefing received prior to travel? Any suggestions for improvement?

Signature of Traveler

Date

DoD 5105.21-M-1, Appendix I, Attachment 8 – Foreign Travel Questionnaire (continued)

DoD 5105.21-M-1, Appendix I, Attachment 9 – Foreign Contact Questionnaire

AP1.A9. APPENDIX 1, ATTACHMENT 9

SAMPLE FORMAT FOR FOREIGN CONTACT QUESTIONNAIRE

Name: _____ SSN: _____

Position/Title: _____ Work telephone number: _____

(Classify completed questionnaire according to content.)

1. Foreign contact information.

a. Name: _____

a. Contact's citizenship: _____

b. Date of occurrence: _____

c. Contact's profession/affiliation: _____

d. Place of occurrence: _____

2. How was the contact initiated? _____

3. Was the person of the same ethnic/nationality as you?
___YES ___NO

4. Was the person of the same sex?
___YES ___NO

5. Do you any relatives or friends in this person's country?
___YES ___NO

6. Did the individual volunteer personal information on him/herself?
___YES ___NO

7. Did the individual seem to control the direction of the conversation?
___YES ___NO

8. Did the individual ask you where you work?
___YES ___NO

DoD 5105.21-M-1, Appendix I, Attachment 9 – Foreign Contact Questionnaire

DoD 5105.21-M-1, Appendix I, Attachment 9 – Foreign Contact Questionnaire (continued)

9. Did the individual ask what type of work you do?

YES NO

10. Did you discuss involvement in government related activities?

YES NO

11. Did the person ask about your political affiliations?

YES NO

12. Did the contact offer to arrange any special treatment?

YES NO

13. Did the contact offer to pay for anything (i.e., lunch, dinner, gifts)?

YES NO

14. Did you, or have you received any gifts from this person?

YES NO

15. Did you exchange business cards, telephone numbers, or addresses?

(If yes, please provide a copy)

YES NO

16. Did the individual express interest in any further contact?

YES NO

17. To the best of your knowledge, describe the physical characteristics of the person you had contact with (e.g., approximate age, height, weight, color of hair and eyes, complexion, marks, scars, etc).

18. Identify those topics or technologies which the contact expressed an interest in which you believe are classified, sensitive, or proprietary.

Employee Signature

Date

DoD 5105.21-M-1, Appendix I, Attachment 9 – Foreign Contact Questionnaire (continued)

TRANSFER OF ELIGIBILITY (TOE) REQUEST FORM

PART 1-Subject Information (To be completed by Gaining or Losing PSO/GSSO/Security Manager/Organization)

Full Name (Last, First, Middle) _____
 Social Security Number (SSN): _____
 Rank/Grade/Position/Title: _____
 Date & Place of Birth: _____
 Security Clearance/Date: _____
 Investigation Type/Date: _____
 Losing Organization: _____
 Projected Departure Date: _____
 Gaining Organization: _____
 Projected Reporting Date: _____
 1st Tier Date/Eligibility: _____ (Completed by Losing Org)
 2nd Tier Date/Eligibility (If Applicable): _____
 3rd Tier Date/Eligibility/CAO Review Date (If Applicable): _____

JPAS/DCII Check (Completed within 1 year-per JAFAN 6/4): Favorable _____ Unfavorable _____

SF 86/SF 86c/eQIP Printout: (Validated with the last year; any updates/changes are reflected on SF 86c)
 _____ Current _____ Updates/Changes Reflected on SF 86c (Completed by Losing Org)

SAP Access: _____ YES _____ NO _____ LEVEL (TS / S - (Circle One))
 SCI Access: _____ YES _____ NO _____

_____	_____	_____
Gaining Organization	PSO/GSSO/Security Manager Name/Signature/Tel #	Date

PART 2-Losing Organization PSO/GSSO/Security Manager Concurrence

_____	_____	_____
Losing Organization	PSO/GSSO/Security Manager Name/Signature/Tel #	Date

PART 3-Validation of TOE (to be completed by losing organization PSO/GSSO/Security Manager)

Personnel security folder transferred: _____ (Date) Hardcopy _____ Electronic _____

PART 4-Validation of TOE (to be completed by gaining organization PSO/GSSO/Security Manager)

Personnel security folder received: _____ (Date) Hardcopy _____ Electronic _____

Appropriate data on subject entered into appropriate databases with organizational information on
 _____ (Date) by _____ (Name, Title, Organization, Tel #).

Notes:

- 1) TOEs can only occur if the subject's investigation is current or a PR has been submitted. If not current or submitted, a waiver by the SAPCO must be obtained.
- 2) Actual access cannot be transferred, a TOE foregoes the tier review process when subject arrives at the new organization and will be briefed into SAPs

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

MEMORANDUM FOR ASSISTANT SECRETARY OF THE XXXXXXXXXXXXX (THROUGH XXXX/XXXX)

FROM: FULL NAME / IDENTIFICATION OF REQUESTING GOVERNMENT CONTRACTING AUTHORITY (GCA)

SUBJECT: Request for Consideration of National Interest Determination (NID) (FOUO)

References: "National Industrial Security Program Operating Manual" (NISPOM) (DoD 5220.22-M, para 2-309) and Executive Order 12829, "National Industrial Security Program" (NISP)

1. Pursuant to the above references, request favorable consideration of the _____ in granting a National Interest Determination (NID) to FULL NAME / IDENTIFICATION AND ADDRESS OF COMPANY (complete identification to include all subcontractors, subsidiaries, partnerships, and full description of relationships/individual product lines, etc will be detailed in Tab "A" as outlined below).

2. The following justification and supporting data is provided for your review and consideration:

a. We request favorable consideration be given SPECIFIC PROGRAM/PROJECT NAME/LEVEL OF DETAIL (detail specific "proscribed information" to include specific levels, etc). In the enclosed attachments our request will detail compelling evidence that release of such information to our company advances the national security interests of the United States. The attachments are as follows:

(1) Tab "A": Staff Summary Sheet – HQ XXXX Coordination with Cognizant PM. Cognizant CO, Cognizant PEO, XXXXXXXXXXX. XXXXXXXXXXX, XXXXXXXXXXX, SAF/GC; Approval XXXX - XXXX.

(2) Tab "B": Identification of the proposed awardee along with a synopsis of its foreign ownership (include solicitation and other reference numbers to identify the action).

(3) Tab "C": General description of the procurement and performance requirements.

(4) Tab "D": Identification of national security interests involved and the ways in which award of the contract helps advance those interests.

(5) Tab "E": A description of any alternate means available to satisfy the requirement, and the reasons alternative means are not acceptable.

(6) Tab "F": Government's Counterintelligence Assessment / Foreign Ownership Issues.

(7) Tab "G": Proposed NID Approval / Disapproval Letter (XXXXX)

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

Processing Note: All requests for NIDs shall be initiated by the GCA. A company may assist in the preparation of an NID, but the GCA is not obligated to pursue the matter further unless it believes further consideration to be warranted. The GCA shall, if it is supportive of the NID, forward the case through appropriate agency channels to the ultimate approval authority within that agency. If the proscribed information is under the classification or control jurisdiction of another agency, the approval of the cognizant agency is required; e.g., NSA for COMSEC, DCI for SCI, DOE for RD and FRD, the Military Departments for their TOP SECRET information, and other Executive Branch Departments and Agencies for classified information under their cognizance. It is the responsibility of the cognizant approval authority to ensure that pertinent security, counterintelligence, and acquisition interests are thoroughly examined. Agency-specific case processing details and the senior official(s) responsible for rendering final approval of NID's shall be contained in the implementing regulations of the U.S. agency whose contract is involved.

3. The designated point of contact for all matters related to this specific NID request may be directed to the undersigned. You may contact me via unclassified email at: ira.sample@emailaddress.com or telephone (xxx-xxx-xxxx).

IRA M. SAMPLE
Government Cognizant Authority (GCA)

7 Atchs

1. Tab A (Staff Summary Sheet – HQ XXXX Coordination with Cognizant PM. Cognizant CO, Cognizant PEO, XXXXXXXXXXX. XXXXXXXXXXX, XXXXXXXXXXX, XXXXX GC; Approval XXXXX - XXXXX)
2. Tab B (Full company identification & foreign ownership synopsis)
3. Tab C (Procurement and performance requirements)
4. Tab D (Rationale for advancement of National Security interests)
5. Tab E (Alternative means of satisfying requirements)
6. Tab F (Counterintelligence Assessment / Foreign Ownership Issues)
7. Tab G (Proposed NID Approval / Disapproval Letter, XXXXX)

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

Tab A

*(Staff Summary Sheet – HQ XXXX Coordination with
Cognizant PM. Cognizant CO, Cognizant PEO,
XXXXXXXXXX. XXXXXXXXXXXX, XXXXXXXXXXXX, XXXX GC;
Approval XXXXX - XXXXX)*

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

Tab B

(Full company identification & foreign ownership synopsis)

1. Full Company Identification:

- a. Company Name: _____
- b. FSC/Cage Code: _____
- c. Facility Clearance: _____
- d. Physical Location (Street Address):

- e. Is Corporate Headquarters same as Item "d" above: Yes ___ No ___
(1) If "No" - specify / list Corporate Headquarters information (Items "a" - "d" above).

- f. Facility Clearance: _____
- g. Product Line (relevant to this request; detail by location/activity and by subsidiary/subcontractor relationship, etc):

- h. Foreign Ownership Synopsis & Corporate Relationships: (detail all foreign ownership, partnerships, subsidiaries, affiliations - in addition to narrative; provide a linear organizational chart depicting all corporate entities/relationships, etc)



- i. Detail all previously granted and current Special Security Agreements, Security Control Agreements, Voting Trust Agreements and Proxy Agreements and/or other relevant National Interest Determinations:

(Note: All question/answer spaces above are not representative of allowable narrative - continue on additional sheets of paper to sufficiently detail)

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

Tab C ***(Procurement and performance requirements)***

(Note: Include sufficiently detailed narrative to support this NID request. Keep in mind, NISPOM, para 2-309 stipulates that each proposed NID request will be prepared and sponsored by the GCA whose contract or program, is involved. NIDs are initiated by the GCA, not the Program Security Officer (PSO). The PSO will be included in the coordination process (see Tab "A" - Staff Summary Sheet). Further, the subject company may assist in the preparation of an NID, but the GCA is not obligated to pursue the matter further unless it believes further consideration to be warranted. The GCA shall, if it is supportive of the NID, forward the case through appropriate agency channels to the ultimate approval authority within that agency. If the proscribed information is under the classification or control jurisdiction of another agency, the approval of the cognizant agency is required; e.g., NSA for COMSEC, DCI for SCI, DOE for RD and FRD, the Military Departments for their TOP SECRET information, and other Executive Branch Departments and Agencies for classified information under their cognizance.)

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

Tab D

(Rationale for advancement of National Security interests)

(Note: Include sufficiently detailed narrative to support this NID request. Keep in mind, NISPOM, para 2-309 stipulates that each proposed NID request will be prepared and sponsored by the GCA whose contract or program, is involved. NIDs are initiated by the GCA, not the Program Security Officer (PSO). The PSO will be included in the coordination process (see Tab "A" - Staff Summary Sheet). Further, the subject company may assist in the preparation of an NID, but the GCA is not obligated to pursue the matter further unless it believes further consideration to be warranted. The GCA shall, if it is supportive of the NID, forward the case through appropriate agency channels to the ultimate approval authority within that agency. If the proscribed information is under the classification or control jurisdiction of another agency, the approval of the cognizant agency is required; e.g., NSA for COMSEC, DCI for SCI, DOE for RD and FRD, the Military Departments for their TOP SECRET information, and other Executive Branch Departments and Agencies for classified information under their cognizance.)

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

Tab E ***(Alternative means of satisfying requirements)***

(Note: Include sufficiently detailed narrative to support this NID request. Keep in mind, NISPOM, para 2-309 stipulates that each proposed NID request will be prepared and sponsored by the GCA whose contract or program, is involved. NIDs are initiated by the GCA, not the Program Security Officer (PSO). The PSO will be included in the coordination process (see Tab "A" - Staff Summary Sheet). Further, the subject company may assist in the preparation of an NID, but the GCA is not obligated to pursue the matter further unless it believes further consideration to be warranted. The GCA shall, if it is supportive of the NID, forward the case through appropriate agency channels to the ultimate approval authority within that agency. If the proscribed information is under the classification or control jurisdiction of another agency, the approval of the cognizant agency is required; e.g., NSA for COMSEC, DCI for SCI, DOE for RD and FRD, the Military Departments for their TOP SECRET information, and other Executive Branch Departments and Agencies for classified information under their cognizance.)

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

Tab F

(Counterintelligence Assessment / Foreign Ownership Issues)

(Note: To be completed by cognizant Counterintelligence service activity and forwarded to the Government Contracting Activity for inclusion in the NID Request package)

Appendix H – SAP National Interest Determination Request (SAMPLE)

*** Classification – According to Content ***

Tab G

(Proposed NID Approval / Disapproval Letter (XXXXXX))

APPENDIX I – INSPECTION DATA CALL LETTER
(SAMPLE ONLY)



Assistant Secretary
(Acquisition)

(Classification)

DEPARTMENT OF THE XXXXXXXXXXXX
WASHINGTON DC

(DATE)

MEMORANDUM FOR (SAP CONTRACTOR / LOCATION)
(ATTN: Mr / Ms _____)

FROM: (PSO - Team Chief)

SUBJECT: Special Access Program Security Compliance Inspection (U/HVSACO)

1. (_____) On behalf of the (Service Component SAP Central Office – SAPCO) a Special Access Program Security Compliance Inspection is scheduled for your location during (inclusive dates). The scope of this inspection includes all program areas and support facilities, all program briefed personnel, and all documentation/materials generated or received under the security cognizance of the SAPCO. The inbriefing is tentatively scheduled for 0900 on (Date). The out-briefing is tentatively scheduled for 1500 on (Date).

2. (_____) The SAP Inspection Team will require a dedicated secure work area with secure telephone, a dedicated security container/drawer, a computer with the Microsoft Office suite and printer, as well as a means to project briefing slides in the area where the Team inbriefing/outbriefing will occur. Please ensure the following are on hand/made available to the SAP Inspection Team upon arrival:

1) (U) All applicable standard operating procedures, program security guides, waivers, self-inspections or reviews, last security review report & follow-up correspondence, and facility/computer accreditations. Also include all DD Form 254s and other pertinent documentation is available for review immediately following the Team inbrief.

2) (U) Arrange for Unescorted Access facility/area badges and an exemption from entry/exit inspections for each member of the SAP Inspection Team. A listing of individual SAP Inspection Team members (positions/clearances/accesses) will be forwarded under separate cover.

(Classification)

(Classification)

3. (_____) Reminder: The SAP Security Compliance Inspection process calls for a two phase inspection:

- (U) Phase One is the on-site validation of your last self-inspection/review (key to the successful completion of this inspection). **Note: Electronic copies of all current self-inspections/reviews must be submitted to this office NLT ____ days prior to the arrival of the inspection team.**
- (U) Phase Two will focus on the Core Compliance functional areas – as listed on the SAP Format 19 (includes but not limited to Security Management, Personnel Security, Security Education, Computer Security, Top Secret Accountability and the current Special Emphasis Items, IS data extraction, Contract Close-Out and DD Forms 254).

4. (_____) In preparation for this visit, please provide the following information at the time of the Team inbriefing:

- a. (_____) A listing (e.g., formatted in EXCEL spreadsheet) of all your SAPs, projects, research and development efforts, (IRAD, CRAD etc.) under the SAPCO's cognizant security authority (CSA), with the current status of each (e.g., Active, Closed-Out with document retention, etc), and the assigned CPSO/GSSO/PSO for each;
- b. (_____) A listing of all SAP contractors, and/or subcontractors/subordinate activities holding SAP information/material;
- c. (_____) A list identifying your program facilities, sorted by building and room numbers, with the following data for each: *(classify as appropriate)*
 - 1) the number of personnel accessed;
 - 2) the number of accountable items;
 - 3) the number of classified computers;
 - 4) the number of unclassified computers;
 - 5) the number of IS networks (i.e., LANS, WANS, Internet and organizational non-SAR connected computers, etc.); including a schematic of LANS and WANS
 - 6) the identity of sub-contractors possessing SAP information.

5. (_____) I can be contacted at (xxx) xxx-xxxx (STE) or via the following Unclassified email address: xxxxxxxxxxxx@xxxxxxxxxx.xxx. We look forward to seeing you and please contact me directly if you have any questions regarding this inspection.

XXXXXXXXXXXXXXXXXX
PSO or Team Chief *(as applicable)*

cc: SAPCO

(Classification)