JOINT AIR FORCE - ARMY – NAVY

JAFAN 6/0

Manual

Special Access Program Security Manual

20 December, 2007

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 incorporates the policies, requirements, and processes reflected in the National Industrial Policy Operating Manual NISPOM) Supplement and the Department of Defense (DoD) Overprint to the NISPOM Supplement. 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 that this manual will be used in lieu of the NISPOM Supplement and DoD Overprint. 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

CHAPTER 10. MISCELLANEOUS

APPENDICES

TABLES

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. Waivers 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.

1-108. 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 Inspections

a. General. The frequency, type and scope of Security Inspections (e.g., Government inspections, evaluations, and security surveys) are determined by the service component SAPCO.

b. Joint Efforts. Inspections will be coordinated between the service components and conducted jointly to the greatest extent possible.

c. 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.

d. Self-inspections. Depending on the location of the SAP (Government/Industry) annual self-inspection are conducted by GSSO/CPSO as appropriate and will address issues reflected in the "Security Inspections Checklist" found in Appendix F. 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 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.

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.[1] 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

[1] 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.

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.

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 App "G". SAP Format 2a has been rescinded; 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 App "G") (SAP Format 2a has been rescinded; polygraph agreement is now incorporated into the SAP Format 2 (JAFAN Edition-Oct 07)*

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. Foreign Ownership, Control, or Influence (FOCI)

a. 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 a Facility (Security) Clearance (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:

(1) 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 affect adversely the performance of classified contracts.

(2) A U.S. company determined to be under FOCI is ineligible for an FCL, or an existing FCL shall be suspended or revoked unless security measures are taken as necessary to remove the possibility of unauthorized access or the adverse affect on classified contracts.

(3) 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.

(4) 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.

(5) 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. For purposes of this Section, the term "agency" has the meaning provided in 5 U.S.C. 552(f), to include the term "DoD Component."

b. All special access programs will follow established FOCI procedures outlined in Chapter 2, Section 3 of the NISPOM.

2-301. National Interest Determinations (NIDs)

a. A NID is a determination that advances the national security interests of the U.S. Approvals of NIDs are based upon compelling evidence that release of SAP information to a company effectively owned or controlled by a foreign person/entity and cleared under a Special Security Agreement (SSA)) is in the best interest of the U.S. Government. To be initially considered for access to SAP information the following must occur:

(1) The foreign owned or controlled company must have a Special Security Agreement with the Federal Government; and

(2) A favorable NID must be approved by the service component SAPCOs. This NID must be prepared by the requiring activity in coordination with the contracting officer and shall include (see Appendix H for sample):

(a) Identification of the proposed awardee, with a synopsis of its foreign ownership (include solicitation and other reference numbers to identify the action);

(b) General description of the acquisition and performance requirements;

(c) Identification of the national security interests involved and the ways in which award of the contract helps advance those interests;

(d) A description of any alternate means available to satisfy the requirement, e.g., use of substitute products or technology or alternate approaches to accomplish the program objectives.

b. 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 Government Contracting Activity’s (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.

2-302. Annual Review and Certification

a. Annual Review. The SAPCO or designee shall meet at least annually with the Government Security Committees (GSCs) of contractors operating under a Voting Trust, Proxy Agreement, Special Security Agreement (SSA), or Security Control Agreement (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 SAPCO 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.

2-303. Technology Control Plan (TCP). Each SAP program will have a unique TCP developed and implemented by those companies cleared under a Voting Trust Agreement, Proxy Agreement, SSA and SCA which has been approved by the SAPCO. 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.

2-304. Compliance. Failure on the part of the company to ensure compliance with the terms of any approved security arrangement may constitute grounds for revocation of the company's FCL.

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.

Table 1. Training/Briefing Requirements

Type	Frequency	Documentation	Remarks
Indoctrination	One time	SAP Format 2 *(see App "G") (SAP Format 2a has been rescinded; polygraph agreement is now incorporated into the SAP Format 2 (JAFAN Edition-Oct 07)*	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

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 (SAP Formats 703, 703a, 704 and 705) will be applied to SAP documents when the documents are created or distributed. Cover sheets when used as a Record of Disclosure will remain affixed to TOP SECRET documents at all times. Cover sheets are not required on classified documents while stored in security containers.

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. TOP SECRET Control Officials (TSCOs) shall be designated in writing by the activity. The TSCO will be responsible to the PSO/GSSO/CPSO 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:

TO BE OPENED ONLY BY: (Insert the name of the individual to whom the material is sent.) (A receipt may be required.)

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 shedders 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

9-100. General. The National Disclosure Policy (NDP) governs all foreign disclosures of classified military information. All SAPs shall comply with the National Disclosure Policy. SAPs will include foreign disclosure and security planning at the beginning of the Prospective SAP process or at the earliest date that possible foreign disclosure is identified in an ongoing SAP. Security planning for foreign disclosure is an ongoing process that requires reviews at each milestone in the SAP lifecycle. When a SAP is identified for international cooperation or foreign disclosure, all foreign disclosure and policy guidance will be in accordance with the NDP-1, DoDD 5230.11, enclosure 7 to DoDD 5530.3, and the International Program Security Handbook, et al.

a. The GPM/PSO will coordinate policy guidance for the development of a Technology Assessment/Control Plan (TA/CP), Memorandum of Agreement, and security documentation for all international programs (research/development, Foreign Military Sales (FMS), joint cooperation, and acquisition), with the Foreign Disclosure Office and the service component SAPCO, as appropriate.

b. This Chapter provides policy and procedures governing the control of classified information in international programs. It also provides procedures for those aspects of the International Trafficking in Arms Regulation (ITAR) that require compliance with this manual (the terms used in this Chapter may differ from those in the ITAR). This Section contains information concerning the Federal laws and regulations, the National Disclosure Policy, and the international agreements that govern the disclosure of classified and other sensitive information to foreign interests.

9-101. Policy. The private use of classified information is not permitted except in furtherance of a lawful and authorized Government purpose. Government Agencies have appointed individuals to the positions of Principal and Designated Disclosure Authorities to oversee foreign disclosure decisions. These officials authorize the release of their agency's classified information that is involved in the export of articles and services. They determine that the release is essential to the accomplishment of the specified Government purpose; the information is releasable to the foreign government involved; and the information can and will be adequately protected by the recipient foreign government.

9-102. 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, the Export Administration Act, and the Atomic Energy Act.

a. The Arms Export Control Act (AECA) (22 U.S.C. 2751). This Act governs the export of defense articles and services, and related technical data that have been determined to constitute "arms, munitions, and implements of war," and have been so designated by incorporation in the U.S. Munitions List. The AECA is implemented by the Department of State (Office of Defense Trade Controls) in the ITAR (22 CFR 120 et seq.). Exports of classified defense articles and data on the U.S. Munitions List are

also subject to the provisions of the National Disclosure Policy. The AECA requires agreement by foreign governments to protect U.S. defense articles and technical data provided to them.

b. The Export Administration Act (EAA) (50 U.S.C. app. 2401 Note). This Act governs the export of articles and technical data that are principally commercial in nature and deemed not appropriate for inclusion on the U.S. Munitions List. The EAA is implemented by the Department of Commerce (Bureau of Export Administration) in the Export Administration Regulation (15 CFR 368 et seq.). This Regulation establishes a list of commodities and related technical data known as the Commerce Control List. Some of these controlled commodities are referred to as "dual-use." That is, they have an actual or potential military as well as civilian, commercial application. Therefore, export of certain dual-use commodities requires DoD concurrence. Exports under the EAA do not include classified information. (NOTE: The EAA expired in 1990, but was revived in 1993 (Public Law (P.L.) 103-10); however, the administrative controls have been in continuous effect under E.O. 12730 and E.O. 12868).

c. The Atomic Energy Act (AEA) of 1954, as amended (42 U.S.C. 2011). This Act provides a program of international cooperation to promote common defense and security, and makes available to cooperating nations the benefits of peaceful applications of atomic energy, as expanding technology and considerations of the common defense and security permit. RD and Formerly Restricted Data (FRD) may be shared with another nation only under the terms of an agreement for cooperation.

d. The Defense Authorization Act of 1984 (10 U.S.C. 130). This Act authorizes the Secretary of Defense to withhold from public disclosure unclassified technical data that has military or space application, is owned or controlled by the DoD, and is subject to license under the AECA or EAA. Canada has a similar law. A qualified contractor in the United States and Canada that is registered at the Joint Certification Office, Defense Logistics Agency, may have access to this technical data in support of a U.S. or Canadian Government requirement. A foreign contractor may have access to the U.S. technical data upon issuance of an export license or other written U.S. Government authorization, and their agreement to comply with requirements specified in the export authorization. The information that is subject to these additional controls is identified by an export control warning and distribution statements that describe who may have access and the reasons for control.

9-103. National Disclosure Policy (NDP). Decisions on the disclosure of classified military information to foreign interests, including classified information related to defense articles and services controlled by the ITAR, are governed by the NDP. U.S. Government policy is to avoid creating false impressions of its readiness to make available classified military information to foreign interests. The policy prescribes that commitments shall not be expressed or implied and

there may be no disclosure of any information until a decision is made concerning the disclosure of any classified information. Decisions on the disclosure of classified military information are contingent on a decision by a principal or designated disclosure authority that the following criteria are met:

a. The disclosure supports U.S. foreign policy.

b. The release of classified military information will not have a negative impact on U.S. military security.

c. The foreign recipient has the capability and intent to protect the classified information.

d. There is a clearly defined benefit to the U.S. Government that outweighs the risks involved.

e. The release is limited to that classified information necessary to satisfy the U.S. Government objectives in authorizing the disclosure.

9-104. 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 the AECA concerning the agreement of the recipient foreign government to protect U.S. classified defense articles and technical data.

NOTE: 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, Defense Security Service has been delegated authority to implement the provisions of the Industrial Security Agreements. The Director of Security, Nuclear Regulatory Commission (NRC), negotiates and implements these agreements for the NRC.

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. TEMPEST Requirement Questionnaires (TRQ) are required to be submitted when processing data on an information system. The PSO, with guidance from a CTTA, shall determine if countermeasures are required based upon the completed TRQ.

c. 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.

d. 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.

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

Section 2. Government Technical Libraries

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*

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 ---------- Mail Receipts/Logs ------- Master Document Lists -- Destruction Certificates -- TS Registers/Control Records ----------	All---------- ---------- ---------- ---------- ----------	Destroy after Five years Destroy after Two years Destroy when superseded or no longer needed Destroy after Five years 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	After Duty Hour inspections and Safe Check records ---------- Entry/Exit Checks ---------	All ---------- ----------	Destroy after PSO inspection Destroy after PSO inspection
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
Memorandums of Agreement (MOA) and Memorandum of Understanding (MOU)	Prepared by originator		Destroy Five years after program is terminated

IF RECORDS ARE OR PERTAIN TO	CONSISTING OF / WHICH ARE	MAINTAINED BY	DISPOSITION / DESTROY
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 --- Inspections conducted by PSO ---------- Subcontractor Inspections	All ---------- Contractor -------- PSO/PM -------- Contractor --------	Destroy after Two years Destroy after Three years Destroy after Five years 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 ------- Trip Reports ----------	Contractor -------- PSO/PM -------- All ----------	Destroy One year after Program is completed Destroy one year after program is terminated 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) Visitor Logs ----------	All ---------- ----------	 Destroy after One year Destroy after Five years
Waivers	Security Criteria (SAP Format 12)	Contractor -------- PSO/PM --------	Destroy when program is terminated Destroy Five years after program is terminated

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

TABLE OF CONTENTS

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 with an asterisk (*) and *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	Are the JAFAN documents reflected in the contractual documents (i.e. DD Form 254)?	6/0: Foreword			
A-2	Are waiver requests fully justified, including adequate compensatory measures and are detailed procedures written? Are all waivers submitted in writing through and coordinated by the PSO and approved by the appropriate level of security management?	6/0: 1-106b			
A-3	*Is the security officer knowledgeable of SAP procedures and requirements?*	*6/0: 1-200b*			
A-4	Has a SAP Contractor Program Security Officer (CPSO) or Government SAP Security Officer (GSSO) been designated in writing? (with copy forwarded to the PSO)	6/0: 1-200b			
A-5	Does the CPSO have the position, responsibility, knowledge and authority commensurate with the degree of security support required of that organization?	6/0: 1-200b			
A-6	Has the PSO been notified, in writing, of the initial nomination of the CPSO/GSSO and any subsequent changes and has the PSO approved the appointment?	6/0: 1-200b NISPOM Sup: 1-200			
A-7	Have Standard Operating Procedures (SOP) been developed to implement/supplement the security policies and requirements for each program?	6/0: 1-201			
A-8	Are changes to the SOP made and submitted to the PSO as they occur?	6/0: 1-201			
A-9	Has the SOP and any changes been approved by the PSO?	6/0: 1-201			
A-10	*Are in-depth self-reviews conducted, documented, with adequate, prompt corrective actions initiated when deficiencies noted?*	*6/0: 1-206* *6/3: 9.B.4.f*			
A-11	Has a comprehensive annual self-review program been established? -- Are deficiencies annotate and corrected, and has a corrective action plan been implemented?	6/0: 1-206d			

Code / No.	Question	References	Yes	No	N/A
A-12	Have deficiencies identified during Cognizant Security Agency (CSA) Inspections and Contractor Self-Inspections been corrected?	6/0: 1-206d			
A-13	Does the CPSO/GSSO submit reports to the PSO when required?	6/0: 1-206d; 6/0: 1-300			
A-14	Has the Fraud, Waste, Abuse and Corruption reporting program been implemented? Is the SAP Hotline number posted throughout the SAPF?	6/0: 1-207			
A-15	*Are security violations and infractions involving classified information reported to the PSO within 24 hours via program channels?*	*6/0: 1-300.a* *6/0: 1-301*			
A-16	*Are security incidents reported?*	*6/0: 1-301* *6/3: 2.B.6.c(10)* *6/3: 8.B.7*			
A-17	*Are corrective actions taken sufficient to prevent recurrence?*	*6/0: 1-301* *6/3: 2.B.6.c(11)*			
A-18	Are security infractions documented and made available for review by the PSO during visits?	6/0: 1-301.a.2			
A-19	If a follow-on contract has been issued, has a request for the retention of materials been submitted to the contracting officer through the PSO for materials that are required to support the follow-on?	6/0: 5-700			
A-20	When retention of SAP classified documents is required, is permission requested of the contracting officer?	6/0: 5-701			
A-21	Have all Critical Compliance Items (CCI) been reviewed? Are they in compliance? Should this be a core compliance item?	6/0: Appendix F Checklist			
B. SECURITY PLANNING					
B-1	Has the badging system been approved as part of the SOP and have detailed procedures been included (e.g. documenting the badge approach, addressing badge accountability, storage, inventory, disposition, destruction, format, use, etc.?	6/0: 1-202			
B-2	If considered necessary, has the badging system been implemented when over 25 people have been accessed to the SAPF?	6/0: 1-202			
B-3	Has an ID badge system been established and approved by the PSO when personal identification checks are unreasonable?	6/0: 1-202			
B-4	Have Co-utilization Agreements (CUAs) been established between different CSAs prior to sharing a SAPF?	6/0: 1-208 6/0: 1-209			
B-5	Are EMSEC standards adhered to when required?	6/0: 10-100			

Code / No.	Question	References	Yes	No	N/A
B-6	Are OPSEC plans/surveys accomplished to define and provide countermeasures to vulnerabilities when contractual provisions require?	6/0: 10-400			
C. PERSONNEL SECURITY					
C-1	Does the CPSO/GSSO possess a security clearance and program access at least equal to the highest level of program classified information involved?	6/0: 1-200.c.1 6/0: 1-200.c.2			
C-2	*Do all program briefed personnel possess the appropriate personnel security investigations?*	*6/0: 1-200.c.4* *6/4: 1.2.c*			
C-3	*Are program personnel aware of their responsibility to report adverse information?*	*6/0: 1-300a*			
C-4	Is the activity reporting to the PSO adverse information, foreign travel, etc., that may affect the person's ability to protect program information?	6/0: 1-300a			
C-5	Are changes in employee status reported to the PSO?	6/0: 1-300c			
C-6	Is foreign travel and foreign contact reported to the CPSO/GSSO/PSO and are all reports maintained in the individuals' personnel files IAW Appendix C?	6/0: 1-300c			
C-7	Are personnel that have had unauthorized or inadvertent access to classified SAP information given an Inadvertent Disclosure Oath for their signature?	6/0: 1-301.b			
C-8	Is all information that affects baseline facility clearance, and incidents of a personnel security clearance nature, forwarded to the CSA (e.g., DSS for contractors)?	6/0: 2-100			
C-9	*Do accessed persons possess a need to know and materially contribute to the program?*	*6/0: 2-200* *6/0: 2-207* *6/4: 1.2.c*			
C-10	Is SAP Format 2 "Special Access Information Agreements" signed prior to briefing an individual approved for access?	6/0: 2-201			
C-11	Does the access roster contain the name of the individual, position, billet number (if applicable), level of access, SSAN, and security clearance information?	6/0: 2-205			
C-12	*Are program personnel properly indoctrinated?*	*6/0: 3-100*			
C-13	Does every individual accessed receive an initial indoctrination?	6/0: 3-101			
C-14	Has a formal debriefing program been developed?	6/0: 3-102			
C-15	Does the debriefing include all required information?	6/0: 3-103a-h			

Code / No.	Question	References	Yes	No	N/A
C-16	Do these individuals sign a debriefing acknowledgment?	6/0: 3-103d			
C-17	Are administrative debriefings used when attempts to locate an individual with program access, by phone or mail, are not successful?	6/0: 3-104			
C-18	Are foreign travel briefings provided before travel?	6/0: 3-105			
C-19	Do personnel attending international conferences and symposia receive a defensive briefing?	6/0: 3-105			
C-20	Do individuals processed for program access meet the prerequisite personnel clearance and/or investigative requirements, as verified by review of the JPAS, DCII, etc?	6/4: 1.2.c			
C-21	Does the PAR package that is sent to the government contain the signed PAR and a copy of the nominee's PSQ, SF 86/86c, or eQIP (if required) printout current within one year?	6/4: 1.3.b			
C-22	Are Program Access Requests (PARs), SAP Format 1, for personnel nominated for program access properly coordinated?	6/4: 3.3.d 6/4: 5.1 Fig 1			
C-23	Does the CPSO/GSSO review the PAR for accuracy, local records check (for disqualifying information) and ensure all required signatures are present before sending the PAR for approval?	6/4: 3.3.d			
C-24	Are Letters Of Compelling Need (LOCN) submitted when required?	6/4: 4.3.d(4)			
C-25	Is program access granted only after receipt of Government approval?	6/4: 5.1 (fig 1) 6/4: 6.1 (fig 1)			
C-26	*Are personnel security packages sent to the CAO for adjudication for those personnel who do not meet 1st or 2nd Tier guidelines and are awaiting initial SAP access?*	*6/4: 7.1*			
C-27	Is access to the SAPF controlled by a cleared employee or by supplanting an access control device or system?	6/9: Annex D			
D. ACCOUNTABILITY					
D-1	When bound engineer's notebooks are used, are the pages pre-numbered and controlled as one document?	6/0: 2-201a 6:0: 2-201c			
D-2	Is the engineer notebook's outer cover and first page marked with the highest classification level contained in the notebook?	6/0: 2-201b			
D-3	Are code words NOT printed on coversheets?	6/0: 4-202			
D-4	Has a Top Secret Control Official (TSCO) been designated to receive, transmit and maintain access and accountability records for TS material?	6/0: 4-204			
D-5	Is an annual inventory of accountable classified material conducted?	6/0: 4-204 6/4: 5-202			

Code / No.	Question	References	Yes	No	N/A
D-6	Is the transmission of Top Secret information covered by a continuous receipt system both within and outside the facility?	6/0: 4-204b			
D-7	Is each accountable document or material assigned a document control number and a copy number?	6/0: 4-204c			
D-8	*Are document accountability records, which show individual responsibility, maintained for Top Secret information?*	*6/0: 5-200c*			
D-9	*Is Top Secret material that has been reproduced subject to the same protection as the original document?*	*6/0: 5-201*			
D-10	Is Top Secret information accounted for?	6/0: 5-201 6/0: 5-202			
D-11	*Are inventories of Top Secret material conducted at least annually and upon change of custodians?*	*6/0: 5-202*			
D-12	Are the results of that annual inventory and any discrepancies reported, in writing, to the PSO?	6/0: 5-202			
D-13	Are classified working papers dated when created, marked with the overall classification, marked with the annotation "WORKING PAPER," and destroyed when no longer needed?	6/0: 5-204a			
D-14	Is Top Secret information entered into formal accountability when either, a) generated, b) received, c) dispatched or, d) within 30 days for working papers?	6/0: 5-204b 6/0: 5-200			
E. MARKING					
E-1	*Are program personnel knowledgeable and apply the correct classifications to classified material?*	*6/0: 4-100*			
E-2	Are all challenges to SAP classified information and/or material forwarded through the CPSO/GSSO to the PSO for clarification?	6/0: 4-101			
E-3	Has current classification guidance been issued and is it being adhered to?	6/0: 4-101 6/0: 4-103.a			
E-4	Is all classified material marked IAW Program SCG?	6/0: 4-200			
E-5	*Are disclosure (access) records maintained and attached to Top Secret documents that identify persons given access to the information and the date of disclosure?*	*6/0: 4-202*			
E-6	Are coversheets applied to SAP documents when documents are created or distributed?	6/0: 4-202			
E-7	Is Unclassified/HVSACO information handled IAW Appendix A?	6/0: 5-200b			

F. REPRODUCTION					
F-1	Has the PSO or CPSO approved the reproduction equipment (copiers, printers, facsimile machines with copy capability, etc.) that reproduce program material?	6/0: 5-600			
F-2	Has the CPM/CPSO prepared written reproduction procedures when the equipment?	6/0: 5-600			
F-3	Is permission to reproduce obtained from the PSO before reproduction of Top Secret information?	6/0: 5-600			
F-4	Is reproduction equipment 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	Is all classified waste destroyed within 30 days, including computer disks?	6/0: 5-704			
G-2	Does destruction of program material preclude recognition or reconstruction of the classified information or material?	6/0: 5-705			
G-3	Has the PSO approved destruction procedures?	6/0: 5-705			
G-4	Are destruction records being accomplished for accountable classified program material, including computer media, immediately upon destruction?	6/0: 5-706			
G-5	Are destruction certificates properly annotated and signed by both of the individuals completing the destruction immediately after destruction is completed?	6/0: 5-706			
H. PHYSICAL SECURITY					
H-1	Is classified material stored in approved security containers, an approved vault, or has approval been granted for open storage by the PSO in a closed area?	6/0: 5-302			
H-2	Is Secret and Confidential material stored in the same manner as TS or in a safe, steel file cabinet or safe-type steel file container ?	6/0: 5-302			
H-3	If a steel file cabinet is used, does it have four sides, top and bottom permanently attached by welding, rivets or peened bolts, and secured by a rigid metal lock bar and an approved lock?	6/0: 5-302			

H-4	Has the CPSO established a SAPF and received the PSO's accreditation before commencing work or storing SAP material?	6/0: 5-800 6/9: 1.1.4			
H-5	Has an accreditation checklist (e.g., DCID 6/9, Annex A, Fixed Facility Checklist -- JAFAN 6/9, Annex A, SAPF Fixed Facility Checklist) been completed and approved by the PSO?	6/0: 5-800			
H-6	Has the area been accredited by the PSO?	6/0: 5-800 6/9: 1.1.4			
H-7	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-8	Are prohibited items such as cameras and recording devices not allowed to enter SAPFs?	6/0: 5-900 6/9: 2.8.1			
H-9	When the condition warrants, has a TSCM been requested for the approval or reaccreditations of facilities?	6/9: 2.3.3			
H-10	Are combinations safeguarded in accordance with the highest classification of the material authorized for storage in the container?	6/9: 2.6			
H-11	Are combinations changed when a) initially used, b) termination/access revocation of an employee having knowledge of the combination or, c) the compromise or suspected compromise of the combination (unattended safes included) has occurred?	6/9: 2.6.1			
H-12	Is a random sampling system of inspections being conducted on all persons who enter and exit a program facility?	6/9: 2.7			
H-13	Are SAPF areas constructed with true floor to true ceiling drywall construction and STC requirements?	6/9: Annex A			
H-14	Are construction standards IAW DCID/JAFAN 6/9? If we have this do we need the above question?	6/9: Annex A			
H-15	Is the SAPF protected by an intrusion detection system IAW JAFAN 6/9?	6/9: Annex B			

I. ACCESS CONTROL					
I-1	Is a visit certification received prior to all program visits?	6/0: 6-100			
I-2	Does the GPM or PSO or their designated representative approve all visits between program activities (Exception: Prime visiting Subs)?	6/0: 6-100			
I-3	Are twelve-month visit certifications not authorized unless approved in writing by the PSO?	6/0: 6-100			
I-4	Are visit requests only sent via approved channels?	6/0: 6-101			
I-5	Does the GSSO/CPSO or their designated representative immediately notify all recipients of a cancellation or termination of a visit request?	6/0: 6-102			
I-6	Is an official photograph identification used for identifying visitors?	6/0: 6-103			
I-7	Are persons without program access escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot be effectively prevented?	6/0: 6-103b			
I-8	Does the host CPSO contact the visitor's CPSO by secure means to inform him/her of the visitor's plan to hand-carry classified information?	6/0: 6-103b			
I-9	Is a warning device employed when announcing uncleared personnel in the program area?	6/0: 6-103b			
I-10	Do non-program briefed visitors sign in on a visitor's record?	6/0: 6-105			
I-11	Do program briefed visitors sign in on a separate visitor's record?	6/0: 6-106			
I-12	Are all classified discussion held within approved areas?	6/0: 6-200			
COMPUTER SECURITY					
J-1	Do data storage media markings include a means of identifying a responsible individual?	6/0: 8-101 6/3: 4.B.1.b(2)(a) [Audit1] PL 1-5			
J-2	*Are approved policies/procedures in place for data transfers?* *- Is a mission critical justification required for each transfer?*	*6/3: Preface* *6/3: 8.B.3.a*			
J-3	Was the requirement to perform each download/data extraction validated as being mission essential?	6/3: Preface			
J-4	Has an IS Security Policy been published or captured in the SSP that accurately addresses the classified processing environment to ensure compliance with JAFAN 6/3?	6/3: 1.F.6 6/3: 4.B.1.b(1) [Doc1] PL 1-5			
J-5	Have there been any IS security incidents since the last review?	6/3: 2.B.2.b(6) 6/3: 2.B.6.c(10)			

J-6	Has an IAM/IAO been formally appointed to manage IS security and: -- has a copy of the appointment letter been forwarded to the DAA/PSO? -- is a copy maintained on file with the IAM?	6/3: 2.B.6 6/3: 2.B.7 6/3: 9.F.2.d			
J-7	Are all persons who are responsible for and access computers aware of proper operational and security-related procedures?	6/3: 2.B.6-.9			
J-8	Are IAO/IAMs properly trained and have the appropriate skills to perform their job?	6/3: 2.B.6.b(2) 6/3: 2.B.7.b(2)			
J-9	Is the IAM/IAO fully aware of his/her responsibilities?	6/3: 2.b.6.c 6/3: 2.B.7.c			
J-10	Has an IS Security Program been established?	6/3: 2.B.6.c(1)			
J-11	Is the DAA/PSO notified of any anomalies and/or is there a formal process in place to notify the DAA/PSO in the event of any anomaly?	6/3: 2.B.6.c(10) 6/3: 8.B.7			
J-12	Has the IAM/IAO attended training appropriate for the operating environment (Information Security)?	6/3: 2.B.6.c(5) 6/3: 8.B.1			
J-13	Do the technical and non-technical functionality outlined in the SSPs accurately depict the target system and its environment?	6/3: 2.B.7.c(5) 6/3: 4.B.1.c(1) [Doc1] PL 1-5			
J-14	*Is configuration management applied to all security relevant elements of the IS? (hardware, software, changes, documentation, etc.)*	*6/3: 2.B.7.c(7)*			
J-15	Are the privileged users aware of their responsibilities?	6/3: 2.B.8.c			
J-16	Is all media (classified and unclassified) maintained in a secure area, labeled, and controlled?	6/3: 2.B.9.b(4) 6/3: 8.B.2.a(1)(b) 6/3: 8.B.4			
J-17	Has the IAO developed procedures for controlling, reviewing, and approving files, media, and software brought into the SAPF, either manually or electronically, and included these procedures in the SSP?	6/3: 2.B.9.b(4) 6/3: 8.B.4			
J-18	Do ALL users have the required security clearance/accesses, authorizations and NTK for the IS based upon the Protection Level?	6/3: 3.C.2			
J-19	Are changes in employee status that affect access to Information Systems reported to the IAO/IAM?	6/3: 3.C.2			
J-20	Are there systems processing SAPI in another location? (i.e. in a SCIF/outside of the SAPF)	6/3: 4.B.1.a(1) [Access1] PL 1-5			
J-21	Does the IS require internal/technical user authentication? (i.e. password)	6/3: 4.B.1.a(2) [I&A1] PL 1 6/3: 4.B.1.b(3) [I&A2] A/R PL 1; PL 2-5			
J-22	Does the IS require external/procedural authentication (i.e. manual log)?	6/3: 4.B.1.a(2) [I&A1] PL 1			

J-23	Are there recovery procedures to ensure that the system recovery is accomplished in a trusted and secure manner?	6/3: 4.B.1.a(4) [Recovery] PL 1-5			
J-24	*Are backups accomplished on a regular basis in accordance with the approved SSP?* *- Are recovery procedures also in place?*	*6/3: 4.B.1.a(4) [Recovery] PL1-5* *6/3: 5.B.1.a(1)* *6/3: 6.B.1.a(2) [Backup1]*			
J-25	Are screen locks employed on the system?	6/3: 4.B.1.a(5) [ScrnLck] PL 1-5			
J-26	Are screen locks set to activate after 15 minutes of idle time?	6/3: 4.B.1.a(5)a [ScrnLck] PL 1-5			
J-27	Do users engage screen lock when away from their workstation?	6/3: 4.B.1.a(5)a [ScrnLck] PL 1-5			
J-28	Is the DoD Warning present on all devices?	6/3: 4.B.1.a(6) [SessCtrl1] PL 1-5			
J-29	Is the IS used for unattended processing? If so, has approval of open storage for media been granted?	6/3: 4.B.1.a(7) [Storage] PL 1-5			
J-30	Is information distributed electronically via approved means? (i.e. closed area, PDS, NSA-approved encryption)	6/3: 4.B.1.a(8) [Trans1] PL 1-5			
J-31	Are User IDs properly controlled and immediately disabled whenever a User no longer has a need-to-know?	6/3: 4.B.1.b(1)(d) [AcctMan] A/R PL 1; PL 2-5			
J-32	Are disabled accounts deleted from the system as soon as practical? (i.e. disabled for 6 months, then deleted from the system)	6/3: 4.B.1.b(1)(e) [AcctMan] A/R PL 1; PL 2-5			
J-33	Are audit trails appropriate for the approved mode of operation?	6/3: 4.B.1.b(2) [Audit1] A/R PL 1; PL 2-5 6/3: 4.B.2.a(5) [Audit2] PL 2-5			
J-34	Are security significant events being recorded? (i.e. logon, logoff, etc.)	6/3: 4.B.1.b(2) [Audit1] A/R PL 1; PL 2-5 6/3: 8.B.7.d(2)			
J-35	*Are audit reviews in compliance with audit policy stated in SSP?*	*6/3: 4.B.1.b(2) [Audit1] PL 1-5*			
J-36	Does the audit mechanism provide granularity to the individual user level?	6/3:4.B.1.b(2)(a) [Audit1] A/R PL 1; PL 2-5 6/3: 4.B.1.b(3) [I&A2] A/R PL 2; PL 3-5			
J-37	Does the IS provide adequate protection of audit trail logs?	6/3: 4.B.1.b(2)(b) [Audit1] A/R PL 1; PL 2-5			

J-38	Are Audit Trail Records and Logs as well as other audit-related events being reviewed for anomalies and annotated by the IAO on at least a weekly basis, or as specified in the SSP?	6/3: 4.B.1.b(2)(c) [Audit1] A/R PL 1; PL 2-5			
J-39	Are automated audit trails used whenever available?	6/3:4.B.1.b(2)(d) [Audit1] A/R PL1; PL 2-5			
J-40	Are all relevant data captured with respect to logons & logoffs, unsuccessful attempts to access objects, changes to authenticators, disabling User ID, terminal or access port, and account lockout?	6/3: 4.B.1.b(2)(d) [Audit1] A/R PL 1; PL 2-5			
J-41	When the authenticator in use is a password, are all aspects of password use addressed? (i.e. length, composition, method of generation, aging, history, protection)	6/3: 4.B.1.b(3) [I&A2] A/R PL 1; PL 2-5			
J-42	Are system logon passwords properly defined, managed, and controlled (i.e. defaults changed)?	6/3: 4.B.1.b(3) [I&A2] A/R PL 1; PL 2-5			
J-43	Are Group logon passwords used as a primary means of authentication?	6/3: 4.B.1.b(3) [I&A2] A/R PL 1; PL 2-5			
J-44	Are review records maintained for at least 12 months or one inspection cycle, whichever is longer?	6/3: 4.B.1.b.2.c [Audit1] A/R PL 1; PL 2-5			
J-45	Are procedures and system configurations periodically reviewed to ensure currency and compliance?	6/3: 4.B.1.c(2) [SysAssur1] PL 1-5 6/3: 4.B.2.b(6) [Test2] PL 2-5 6/3: 5.B.1.a(2) [CM1] I-B,M,H 6/3: 5.B.2.b(1) [Validate] I-M,H			
J-46	Has a viable procedure, intended to ensure that all software introduced into the SAPF will be controlled and reviewed before use, been instituted and documented in the SSP?	6/3: 4.B.1.c(2)(a) [SysAssur1] PL 1-5 6/3: 5.B.1.a(4) [MalCode] I-B,M,H			
J-47	Are unauthorized persons denied physical access to the IS?	6/3: 4.B.2.a(1) [Access1] PL 1-5			
J-48	Has the ability to use bootable devices been locked down?	6/3: 4.B.2.a(1)(b) [Access1] PL 1-5			
J-49	Are users and processes granted the most restricted set of privileges or accesses needed for the performance of authorized tasks?	6/3: 4.B.2.a(10) [LeastPrv] PL 2-5			

J-50	Are procedures or mechanisms employed to ensure that the user or the system marks all data transmitted or stored by the system? - If all data is NOT marked on a PL2 system, is it handled at the highest level of the system and printed output marked appropriately?	6/3: 4.B.2.a(11) [Marking] PL 2-3			
J-51	Does the system ensure that resources contain no residual data before allocation?	6:3: 4.B.2.a(14) [ResrcCtrl] PL 2-5			
J-52	Does the system close a logon session after a specified period of user inactivity?	6/3: 4.B.2.a(17)(b) [SessCtrl2] PL2-5			
J-53	Does the IS control successive logon attempts by locking the account?	6/3: 4.B.2.a(17)(c) [SessCtrl2] PL 2-5			
J-54	Does the system audit users logged into more than one workstation?	6/3: 4.B.2.a(17)(c) [SessCtrl2] PL 2-5			
J-55	Does the SSP contain procedures for moving classified media between approved facilities?	6/3: 4.B.2.a(19) [Trans1] PL1-5			
J-56	Does the IS provide Discretionary Access Controls?	6/3: 4.B.2.a(2) [Access2] PL 2-5			
J-57	Are the contents of the audit trails protected from unauthorized access, modification, or deletion?	6/3: 4.B.2.a(4)(b)			
J-58	Does the system have a Privileged User's Guide? If so, does it adequately address system configuration, use of the system's security features and system vulnerabilities? (This requirement is usually met for PL 1-2 if the SSP contains like guidance.)	6/3: 4.B.2.b(2) [Doc2] PL 2-5			
J-59	Does the system have a General User's Guide? If so, does it adequately address system operation within the environment? (General User's Guide is not normally required for PL 2.)	6/3: 4.B.2.b(3) [Doc3] A/R PL 2; PL 3-5			
J-60	If required, was an IS Technical Evaluation Test Plan completed?	6/3: 4.B.2.b(3)(a) [Doc3] PL 3; A/R PL 2			
J-61	Has the IAM provided the DAA written verification that the system operates in accordance with the SSP?	6/3: 4.B.2.b(6) [Test2] PL 2-5			
J-62	Is classified and unclassified media physically segregated?	6/3: 4.B.4.a(27) [TranSep] PL 4-5 6/3: 8.B.4			
J-63	Is security-relevant software tested to verify the security features function as specified?	6/3: 4.B.a.c(2) [SysAssur1] PL 1-5			
J-64	Has a CM program been established for the IS?	6/3: 5.B.1.a(2)			
J-65	Is all newly acquired software or data files acquired from authorized sources and scanned for viruses with an updated antivirus software application before being loaded, copied, or installed on systems in the SAPF?	6/3: 5.B.1.a(4) [MalCode] I-B,M,H			

J-66	Have the privileged users attended appropriate training to accomplish their responsibilities?	6/3: 8.B.1.			
J-67	Have individuals responsible for performing this process received training in the process, tools, and risks involved?	6/3: 8.B.1.a			
J-68	Is the release of systems, components, and media performed in accordance with approved procedures?	6/3: 8.B.1.b(3)			
J-69	Is a System User Training and Awareness program in place?	6/3: 8.B.1.c(2)			
J-70	Are all systems, classified and unclassified, clearly marked and physically separated?	6/3: 8.B.2			
J-71	Are write-protection methods tested and verified?	6/3: 8.B.2.a(1)			
J-72	In areas where both classified and unclassified information are processed and stored, are UNCLASSIFIED media labels used to identify media that contain only unclassified information?	6/3: 8.B.2.a(1)(b)			
J-73	Are there procedures for marking hardware?	6/3: 8.B.2.b			
J-74	Are there procedures for marking output?	6/3: 8.B.2.c			
J-75	Is the first page of printed output a banner page that includes a warning?	6/3: 8.B.2.c(1) 6/3: 8.B.2.c(3)			
J-76	Are records maintained of all risk managed downloads/data extractions, to include descriptions of files/data removed?	6/3: 8.B.3			
J-77	Are there approved Risk Managed Download Procedures in place for copying Unclassified or lower classified information from a classified IS and is it being followed? - Material content is properly reviewed and certified? - The download/extraction process uses the appropriate tools? - Human review of the newly created media is performed? - Media is removed and properly marked/controlled?	6/3: 8.B.3.a			
J-78	Have any risk managed downloads/data extractions been performed in the SAPF since the last review?	6/3: 8.B.3.a			
J-79	Are transaction receipts (i.e., equipment sanitization, media/equipment release records) being maintained?	6/3: 8.B.4 6/3: 8.B.5.e(2)			
J-80	Has a viable procedure addressing specialized procedures for controlling unclassified vendor software (i.e., COTS) media, been instituted?	6/3: 8.B.4 6/3: 8.B.2.a(1)(b)			

J-81	Are there approved written procedures for clearing/reutilization and sanitization and destruction of data storage media and memory components? (overwriting, degaussing, sanitizing and destroying media; i.e. sanitize prior to release, etc.)	6/3: 8.B.5 6/3: 8.B.8.c(3)			
J-82	Are all hardcopy and magnetic media produced on the system protected at the level of the system until properly reviewed?	6/3: 8.B.5			
J-83	Has all test equipment used in the secure area been evaluated by the IAO for the existence of nonvolatile memory and has approval been received from the customer to utilize equipment that permanently retains information?	6/3: 8.B.5.d 6/3: 8.B.8.c(5) 6/3: 8.B.8.c(6)			
J-84	If ALL maintenance is not performed inside the SAPF, are electronic components and boards containing memory properly evaluated, controlled, and sanitized (based on the type of memory involved) prior to release from the secure area IAW customer approved procedures?	6/3: 8.B.5.e			
J-85	How many information systems (IS) are housed within the SAPF processing SAP information?	6/3: 8.B.6			
J-86	Have IS security requirements been applied to ALL IS in the SAP areas regardless of the processing level of the system?	6/3: 8.B.6			
J-87	Are special procedures for the co-location of classified and unclassified computers (or systems processing different levels/compartments) documented by the IAO in the SSP and approved by the DAA/PSO?	6/3: 8.B.6			
J-88	Are Unclassified or Lower Classified IS located within the SAPF, i.e., along with classified-use IS?	6/3: 8.B.6			
J-89	*Are there guest systems in the facility?* *- Is there proof of accreditation?* *- Is a guest system POC identified in the event of a data spill, etc?*	*6/3: 8.B.6* *6/3: 9.B.4*			
J-90	Are IS approved for processing unclassified information physically separated from any classified IS?	6/3: 8.B.6.b(2)			
J-91	Have any personally owned or any leased IS been introduced into the SAPF? (Additional PED questions are found at the end of the IS portion of the checklist.)	6/3: 8.B.6.c			
J-92	Are any modems (ex. STU-III, etc.) present within the SAPF?	6/3: 8.B.6.c(3)			
J-93	Are personally owned IS used to process classified information?	6/3: 8.B.6.c(4)			

J-94	Are portable systems specifically approved by the customer and have specific procedures been implemented for conducting security reviews of the devices and contained data?	6/3: 8.B.6.c(4)			
J-95	Has a formal notification process been established to notify the DAA/PSO within the specific time periods of abnormal occurrences?	6/3: 8.B.7			
J-96	Have procedures for cleared and uncleared maintenance support been established and approved?	6/3: 8.B.8			
J-97	Is unclassified vendor supplied maintenance/diagnostic software controlled as classified or protected at the level of the system it is used on?	6/3: 8.B.8.b(4)			
J-98	Are audit records maintained for system maintenance, software changes, upgrade/downgrade actions, sanitization/declassification and use of seals?	6/3: 8.B.8.c(1)			
J-99	Is a Maintenance/Repair Log being maintained?	6/3: 8.B.8.c(1)			
J-100	Is all test equipment introduced, controlled, and documented as outlined	6/3: 8.B.8.c(5)			
J-101	Are remote diagnostic links present and approved?	6/3: 8.B.8.d(3)			
J-102	Have deficiencies (to include noted discrepancies) from past Security Inspection(s) been corrected?	6/3: 9.B.4.f 6/3: 9.D.4.b			
J-103	Has the IAO been authorized "Special Approval Authority? (Verify that the IAO has NOT further delegated this authorization without PSO/DAA approval.)	6/3: 9.D.3.a(1) PL 1-2			
J-104	Are any of the IS interconnected to other IS? If so, has an ISA been established?	6/3: 9.D.3.c 6/3: 9.D.3.c(4)			
J-105	*Do all IS within the facility have Approval to Operate?* *- If not, has an SSP been submitted and the DAA provided Interim Approval to Operate?*	*6/3: 9.D.4.a*			
J-106	Does each IS have an Approval to Operate (ATO) that is within three years?	6/3: 9.D.4.a			
J-107	If an IS does not have an ATO, has an Interim ATO (IATO) been issued and is it current? (Indicate why an IATO is in place rather than ATO.)	6/3: 9.D.4.c			
J-108	Are all of the technical and non-technical requirements in place and functioning properly? If not, are they clearly addressed in the approved SSP?	6/3: 9.F			

K. TRANSMISSION					
K-1	Does the PSO approve all couriering of SAP material via commercial aircraft?	6/0: 5-400b			
K-2	Is classified program material prepared, reproduced and packaged by program briefed personnel in an approved SAPF?	6/0: 5-401			
K-3	Has a suspense system been established to track transmitted documents until a signed copy of the receipt is returned?	6/0: 5-401b			
K-4	Are opaque inner and outer covers used when transmitting program material outside the facility?	6/0: 5-401c			
K-5	Are detailed courier instructions provided to couriers when hand-carrying SAP material?	6/0: 5-402			
K-6	When couriering SAP material, are travel anomalies reported to the PSO/CPSO as soon as practical?	6/0: 5-402			
K-7	Has written authorization been received, through the PSO or designee, to transmit TS information outside the facility?	6/0: 5-402			
K-8	Is a courier authorization letter provided to the individual hand-carrying SAP material?	6/0: 5-402			
K-9	*Is Top Secret material transmitted only by authorized means?*	*6/0: 5-402* *6/0: 5-403* *6/0: 5-404*			
K-10	Is the appropriate warning notice added to all classified program or program related material on the inner container/wrapping when transmitting material outside the program facility?	6/0: 5-402c(1)			
K-11	Is classified SAP information electronically transmitted only on approved secure communication channels authorized by the PSO?	6/0: 5-403			
K-12	Are only program briefed personnel designated to receive US Registered Mail, USPS Express Mail, US Certified Mail or material delivered by messenger?	6/0: 5-404e(3)			
K-13	Are reports made of any problem, mis-delivery, loss, or other security incident encountered during the transmission via USPS immediately to the PSO?	6/0: 5-404f			
K-14	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: 5-404g			
K-15	Are two program briefed personnel destroying accountable classified program material?	6/0: 5-702			
K-16	Are external receipts and dispatch records executed and maintained IAW Appendix C (five year period)?	6/0: Appendix C			

L. SECURITY EDUCATION					
L-1	Have ALL individuals received initial and refresher training as needed, and annual awareness training covering IS security requirements and agreed in writing via an IS User Agreement to abide by those requirements?	6/0: 3-100 6/3: 2.B.6.c(13) 6/3: 8.B.1.c(2)			
L-2	*Are program personnel aware of program security requirements?*	*6/0: 3-100*			
L-3	Has an in-depth and, on-going security education program been developed?	6/0: 3-100			
L-4	Have security training and briefings been specifically tailored to the unique security requirements of each program?	6/0: 3-100			
L-5	Does the SAP specific security training cover all required items IAW JAFAN Edition-SAP Form 17?	6/0: 3-100			
L-6	Is a record maintained documenting refresher training?	6/0: 3-100, Table 1			
L-7	Has a program specific initial indoctrination been developed?	6/0: 3-100, Table 1			
L-8	Does every accessed person receive an annual refresher briefing and on-going specialized training that contains a minimum of those elements outlined in the SAP From 17?	6/0: 3-100, Table 1			
L-9	Is computer security refresher training conducted at least annually?	6/0: 3-100, Table 1			
M. CONTRACTING					
M-1	Do all contractors (prime and sub) have valid facility clearances to the level of classified information involved in their work, and has that been verified in coordination with the PSO?	6/0: 7-101			
M-2	Has the storage capability level and access level to classified been verified in coordination with the PSO?	6/0: 7-102			
M-3	Is subcontractor program access pre-coordinated with the PSO?	6/0: 7-102			
M-4	Has a security requirements agreement been prepared that specifically addresses those enhanced security requirements that apply to the subcontractor?	6/0: 7-102			
M-5	Does the security requirements agreement include all required items? Format 13?	6/0: 7-102			
M-6	Has a DD Form 254 been prepared for each subcontractor or consultant?	6/0: 7-102			
M-7	Has the PSO approved all DD Form 254s for subcontractors?	6/0: 7-103			

N. GUARD FORCE					
N-1	Does the response force respond to alarms at **CLOSED** storage SAPFs within **15** minutes?	6/9: 3.1.1.1			
N-2	Does the response force respond to alarms at **OPEN** storage SAPFs within **5** minutes?	6/9: 3.1.2.1			
N-3	Are response force personnel properly trained and post instructions adequate, available and appropriate?	6/9: Annex B			
N-4	Are response force personnel properly equipped, to include adequate communications?	6/9: Annex B			
N-5	Are alarms installed, maintained and monitored by U.S. citizens who have been subjected to a trustworthiness determination?	6/9: Annex B			

O. SPECIAL EMPHASIS ITEMS

APPENDIX G
SPECIAL ACCESS PROGRAM FORMATS

NUMBER	TITLE	DATE
SAP Format 1, (JAFAN EDITION)	**Program Access Request (PAR)** *(*supercedes all previous editions; insert in JAFAN 6-4 as a page change)*	**Dec 07**
SAP Format 2 (JAFAN EDITION)	**Special Access Program Indoctrination Agreement (SAPIA)** *(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)*	**Dec 07**
SAP Format 5	**Inadvertent Disclosure Statement**	**Jan 98**
SAP Format 6	**Notification of Foreign Travel** *(Note: SCI Comparable Form may be used- DoD 5105.21-M-1, Appendix I, Atchs 8 & 9 – Foreign Travel/Foreign Contact Questionnaires are included)*	**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**	**Jun 07**
SAP Format 19	**Special Access Program Inspection**	**Dec 07**
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**
SAP Format 703	**SAP Cover Sheet – Top Secret (Orange) (U)**	**Jun 07**
SAP Format 704	**SAP Cover Sheet – Secret (Red) (U)**	**Jun 07**
SAP Format 705	**SAP Cover Sheet – Confidential (Blue) (U)**	**Jun 07**
SAP Format 703a	**SAP Record of Access-Continuation Sheet**	**Jun 07**

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

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** ☐ Yes ☐ No	**7. SSAN**
8. Date of Birth (YYMMDD)	**9. State/Country of Birth**		**10.** ☐ Military ☐ Government Civilian ☐ Contractor		**11. Date Needed By**
12. Position Description/Job Title			**13.** ☐ Full Time ☐ Temporary *(Period of access)* ☐ 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)*
☐ In Progress (Date Initiated/Submitted: _____ (YYMMDD)
(include additional information in the "Remarks" section below as needed)
☐ Current ☐ 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)*
☐ Acceptable DCII check results ☐ Acceptable JPAS check results
☐ Referred to next Tier Review Official level

25. Justification (CLASSIFICATION) *(include detailed justification as to how this candidate will support and contribute to the program)* *(CONTINUE ON SEPARATE SHEET IF NECESSARY)*

26. Billet Number *(if any)*:			
27. Requestor ***(Government/Contractor)***			
Typed Name/Title/Organization	Signature		Date
28. Additional Coordination *(As Necessary)*			
Typed Name/Title/Organization	Signature	☐ Concur ☐ Non-Concur	Date
29. Government SAP Security Officer/Contractor Program Security Officer (GSSO/CPSO)			
Typed Name/Title/Organization	Signature	☐ Concur ☐ Non-Concur	Date
30. Government/Contractor Program Manager (GPM/CPM)			
Typed Name/Title/Organization	Signature	☐ Concur ☐ 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	☐ First Tier Eligible ☐ First Tier Ineligible	Date
32. SECOND TIER REVIEW OFFICIAL (TRO) *(Typed Name/Title/Organization)*	Signature	☐ Concur ☐ Non-Concur	Date
33. THIRD TIER REVIEW OFFICIAL (TRO) *(Typed Name/Title/Organization)*	Signature	☐ Concur ☐ Non-Concur	Date
34. Government Program Security Officer (PSO) *(Government Only)*			
Typed Name/Title/Organization	Signature	☐ Concur ☐ Non-Concur	Date
35. SAP Central Office (SAPCO) *(Government Only) (If SAPCO Waiver Required)*			
Typed Name/Title/Organization	Signature	☐ Waiver - Approved ☐ Waiver - Disapproved	Date
36. Access Approval Authority (AAA) *(Government Only)*			
Typed Name/Title/Organization	Signature	☐ Access Approved ☐ 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," December 2007 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.

16a SIGNATURE		**b. DATE** (YYYYMMDD)
17. 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):

_____
Signature of Individual Briefed

DEBRIEF Date_____

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

_____
Signature of Individual Debriefed

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

_____ _____
Signature of Briefing 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)

NOTIFICATION OF FOREIGN TRAVEL

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

1. BACKGROUND:

   a. Travel outside of the United States is a matter of security interest in view of the clearances you hold. Such travel includes points in Canada, the Caribbean, Mexico, and Europe, as well as more distant places.

   b. Knowledge of your whereabouts is needed primarily for personal protection and as a guide in locating you should an official search be required. Your itinerary should be adhered to as closely as possible.

   c. If major changes are made or if your estimated return date is extended by 24 hours or more, please advise Security accordingly to forestall any unnecessary concern as to your whereabouts. Contact Security upon your return for a debriefing. Any incidents of an intelligence nature which may have occurred must be reported.

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

a. THIS TRAVEL IS: ☐ OFFICIAL ☐ PERSONAL

b. _____
NAME (Last, First, MI) SSAN

_____
HOME ADDRESS HOME TELEPHONE

_____
ORGANIZATION WORK TELEPHONE

c. PERSON WHO KNOWS YOUR PLANS AND WHEREABOUTS:

_____
NAME (Last, First, MI) HOME TELEPHONE

_____
HOME ADDRESS WORK TELEPHONE

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

PLACE	DATE(S)	CARRIER	CONTACTS

Expected date of return to the US _____

TRAVELER'S SIGNATURE _____ DATE _____

SECURITY CONCUR _____

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)

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)

DATE/TIME: _____ **CONTROL #** _____ **PRECEDENCE** _____

FROM: _____ **OFFICE SYMBOL** _____ **PHONE#** _____

TO: _____

INFO: _____

SUBJECT: VISIT NOTIFICATION

1. ( ) The following individual(s) will visit _____

on date(s) indicated for the purpose of _____.

Point(s) of contact is/are _____

(U) NAME	(U) SSAN	(U) CLEARANCE AND INVESTIGATION	(C/SAR) PROGRAM/ LEVEL OF ACCESS	(U/HVSACO) DATE(S) OF VISIT

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

PRIVACY ACT STATEMENT

AUTHORITY: **10 U.S.C. 3101 & EO 9397**

PRINCIPAL PURPOSE: **FOR GRANTING VISIT APPROVAL TO A CLASSIFIED PROGRAM FACILTY AND TO AUTHORIZE ACCESS TO PROGRAM MATERIAL.**

ROUTINE USE: **TO RECORD VISIT APPROVAL. USE OF SSAN IS NECESSARY TO MAKE POSITIVE IDENTIFICATION OF THE INDIVIDUAL AND RECORDS.**

DISCLOSURE IS VOLUNTARY; FAILURE TO PROVIDE THE INFORMATION AND SSAN COULD RESULT IN APPROVAL BEING DENIED.

Derived From:
Declassify On:

SENT BY: _____

SAP Format 7, "Visit Notification," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

TSCM Request (U)

(Date of Request)

(U) FACILITY _____
(Organization/Company Name)

(U) STEET _____
(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)

(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** _____

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

Derived From:
Declassify On:

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

(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)

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

Computer Security

☐ JAFAN 6/3 (IA Operating Procedures)		
☐ Data Transfers (High to Low transfers)		
☐ Password Protection		
☐ 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: _____

_____ _____

Printed Name Organization/Firm

_____ _____

Signature Location

_____

Program Security Officer (PSO)

SAP Format 17, "Refresher Training Record," June 2007 PREVIOUS EDITIONS ARE OBSOLETE (File in Individual Personnel Records)

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

(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:
☐ Government ☐ Prime Contractor ☐ Subcontractor

CPSO/GSSO:

PSO:

5. INSPECTION DATES:

Last Insp: (To-From)

Current Insp: (To-From)

6. SCOPE OF ACTIVITY:
☐ Active ☐ Inactive ☐ Close Out

7. NUMBER OF PERSONS ACCESSED:

SECRET	TOP SECRET	TOTAL

8. NUMBER OF DOCUMENTS:
TOP SECRET: SECRET: CONFIDENTIAL:
Total:

SECTION II – INSPECTION SUMMARY

9. TYPE: ☐ Full-Scope ☐ Re-inspection ☐ Core Compliance ☐ Close Out ☐ Unannounced

10. OVERALL RATING: ☐ Excellent ☐ Satisfactory ☐ Marginal ☐ Unsatisfactory

11. DEFICIENCIES: ☐ No Deficiencies | Findings | Deviations | Corrected-On-The-Spot

12. INSPECTOR NAMES/AGENCIES: *SEE ATTACHED REPORT* | Time Expended: ☐ Days ☐ Hours

13. PERSONNEL OUTBRIEFED: *SEE ATTACHED REPORT*

SECTION III – FUNCTIONAL AREAS INSPECTED

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

SECTION IV - REPORT PROCESSING

14. CORRECTIVE ACTION REPORT:
☐ Required →
☐ 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," December 2007 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 on 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 couriering 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

H. If you arrive at your destination after working hours, make prior arrangements to secure the material in an approved SAP facility. If your 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

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

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

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

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

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)*
_____Currrent _____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*

TOP SECRET

Special Access Required

THIS IS A COVER SHEET
FOR TOP SECRET // SAR INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF NATIONAL SECURITY OF THE UNITED STATES. HANDLING, STORAGE, REPRODUCTION, AND DISTRIBUTION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

RECORD OF ACCESS

Full Name (Printed)	Signature	Office/Activity	Date

Note: Use SAP Format 706, "Record of Access-Continuation Sheet" to record additional names.

CONTACT _____

AT TEL: ( ) _____

TO VERIFY SPECIAL ACCESS / HANDLING INSTRUCTIONS / STORAGE REQUIREMENTS.

(THIS COVER SHEET IS UNCLASSIFIED)

TOP SECRET

Special Access Required

SAP Format 703 – June 2007

SECRET

Special Access Required

THIS IS A COVER SHEET
FOR SECRET // SAR INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF NATIONAL SECURITY OF THE UNITED STATES. HANDLING, STORAGE, REPRODUCTION, AND DISTRIBUTION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

CONTACT _____

AT TEL: ( ) _____

TO VERIFY SPECIAL ACCESS / HANDLING INSTRUCTIONS / STORAGE REQUIREMENTS.

(THIS COVER SHEET IS UNCLASSIFIED)

SECRET

Special Access Required

SAP Format 704 – June 2007

CONFIDENTIAL
Special Access Required

THIS IS A COVER SHEET
FOR CONFIDENTIAL // SAR INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF NATIONAL SECURITY OF THE UNITED STATES. HANDLING, STORAGE, REPRODUCTION, AND DISTRIBUTION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

CONTACT _____

AT TEL: ( ) _____

TO VERIFY SPECIAL ACCESS / HANDLING INSTRUCTIONS / STORAGE REQUIREMENTS.

(THIS COVER SHEET IS UNCLASSIFIED)

CONFIDENTIAL
Special Access Required

SAP Format 705 – June 2007

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

TOP SECRET ACCESS RECORD – CONTINUATION SHEET (SAP FORMAT 703a)

FULL NAME	SIGNATURE	OFFICE / ACTIVITY	DATE

SAP Format 703a, "Access Record – Continuation Sheet," June 2007 Page _____ of _____

Document Control Number: _____

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

Appendix H – SAP National Interest Determination Request (SAMPLE)

MEMORANDUM FOR ASSISTANT SECRETARY OF THE XXXXXXXXXXX
(THROUGH XXXX/XXXXX)

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, XXXXXXXXX. XXXXXXXXX, XXXXXXXXX, SAF/GC; Approval XXXXX - XXXXX.*

(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)

***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, XXXXXXXXX. XXXXXXXXX, XXXXXXXXX, 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)

Tab A

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

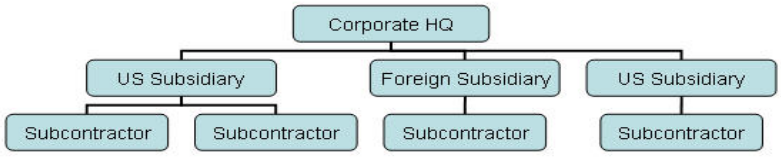
Tab B
(Full company identification & foreign ownership synopsis)

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)

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.)

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.)

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.)

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)

Tab G

(Proposed NID Approval / Disapproval Letter (XXXXX))