

Chapter 1

General Provisions and Requirements

Section 1. Introduction

1-100. Purpose.

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

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

1-101. scope.

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

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

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

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

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

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

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

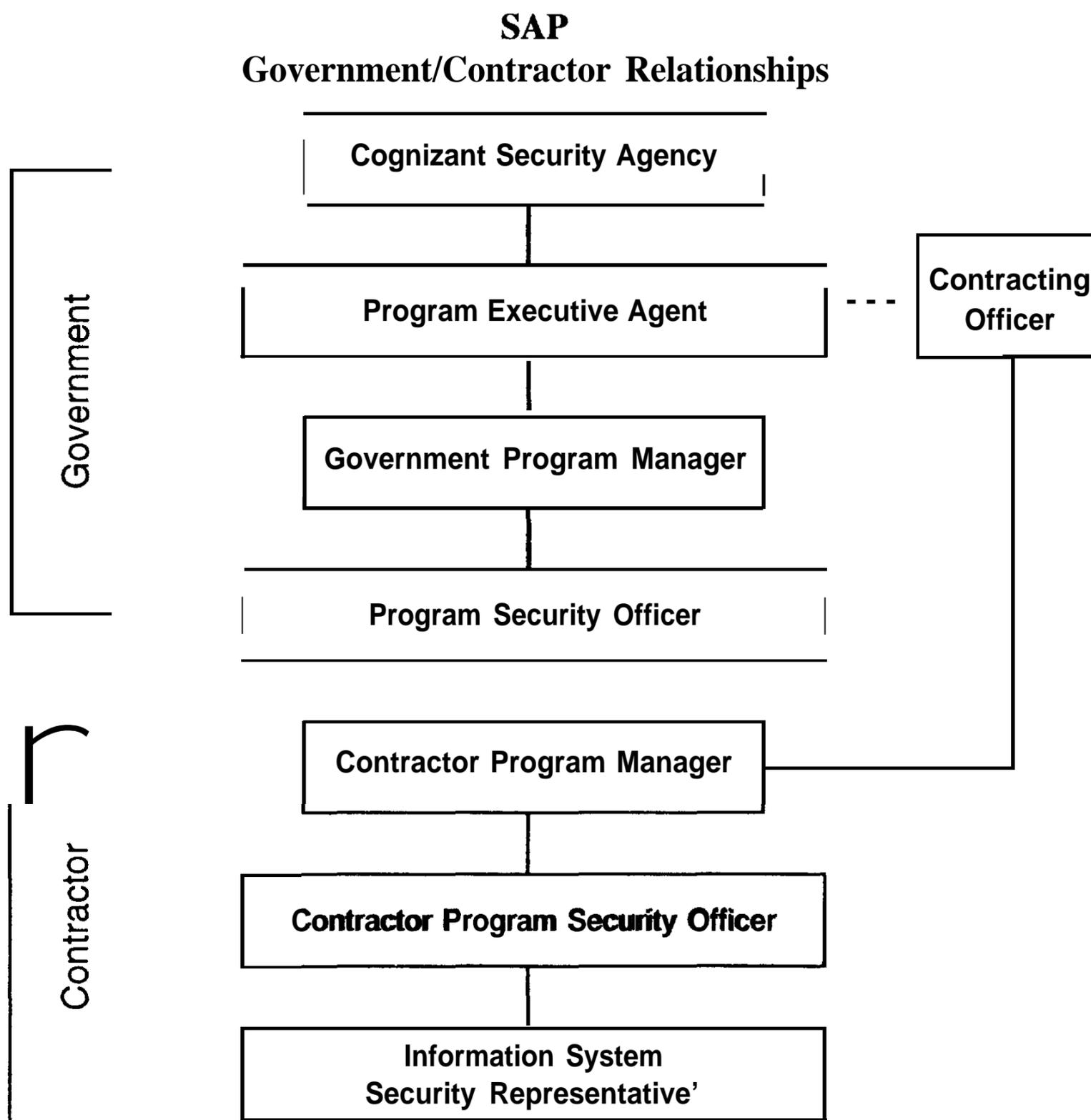
1-106. **Waivers and Exceptions.** The purpose of having a waiver and exception policy is to ensure that deviations from established SAP criteria are systematically and uniformly identified to the Government Program Manager (GPM). Every effort will be made to avoid

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

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

1-107. Special Access Programs Categories and Types.

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



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

Section 2. General Requirements

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

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

- (1) Overall Program management.
- (2) Execution of the statement of work, contract, task orders and all other contractual obligations.

b. The CPSO oversees compliance with SAP security requirements.

The CPSO will:

- (1) *Possess a personnel clearance and Program access at least equal to the highest level of Program classified information involved.*
- (2) *Provide security administration and management for his/her organization.*
- (3) *Ensure personnel processed for access to a SAP meet the prerequisite personnel clearance and/or investigative requirements specified.*
- (4) *Ensure adequate secure storage and work spaces.*
- (5) *Ensure strict adherence to the provisions of the NISPOM and its Supplement.*
- (6) *When required, establish and oversee a classified material control program for each SAP.*
- (7) *When required, conduct an annual inventory of accountable classified material*
- (8) *When required, establish a SAPF.*

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

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

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

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

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

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

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

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

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

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

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

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

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

1-206. Security Reviews.

- a. **General.** The frequency of Industrial Security Reviews (e.g., Reviews, evaluations, and security surveys) is determined by the **NISPOM** and will be conducted by personnel designated by the CSA.
- b. **Joint Efforts.** In certain cases, an individual Program may be a joint effort of more than one component of the U.S. Government or more than one element of the same component. In such a case, one element will, by memorandum of agreement, take the lead as the Cognizant Security Agency and may

have security review responsibility for the Program facility. In order to ensure the most uniform and efficient application of security criteria, review activities at contractor facilities will be consolidated to the greatest extent possible.

- c. **Prime Contractor Representative.** A security representative from the prime contractor may be present and participate during reviews of subcontractors, but cannot be the individual appointed by the CSA to conduct security reviews specified in paragraph 1-206a.
- d. **Review Reciprocity.** In order to ensure the most uniform and efficient application of security reviews, review **reciprocity** at contractor facilities will be considered whenever possible.
- e. **Contractor Reviews.** When applicable, the U.S. Government may prescribe the intervals that the contractor **will** review their systems.
- f. **Team Reviews.** Team Reviews may be conducted by more than one PSO based on mutual consent and cooperation of both the Government and the contractor.

Section 3. Reporting Requirements

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

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

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

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

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

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

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

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

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

a. **Security Violations and Infractions**

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

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

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

- (1) If during emergency response situations, guard personnel or local emergency authorities (e.g., police, medical, fire, etc.) inadvertently gain access to Program material, they should be interviewed to determine the extent of **the exposure**. If circumstances **warrant**, a preliminary inquiry will be conducted. **When** in doubt, contact the PSO for advice.
- (2) ***Refusal to sign an inadvertent disclosure oath will be reported by the CPSO to the PSO.***
- (3) ***Contractors shall report all unauthorized disclosures involving RD or Formerly Restricted Data (FRD) to Department of Energy (DOE) or Nuclear Regulatory Commission (NRC) through their CSA.***