Student Guide

SAP Security Roles and Responsibilities

Introduction

As a new employee working on a Special Access Program, or SAP, you are quickly becoming familiar with the specific functional requirements of your job. But there's a lot more going on in a SAP beyond the actual work of the program.

Security, for one, is an essential component of protecting SAP information. Security plans and standard operating procedures must be created, approved, and administered. Personnel must be cleared to the appropriate level and properly trained. Facilities must be accredited. Visitors must be approved. Information must be safeguarded. But who is responsible for making sure these things happen? Who will you go to when you have questions about SAP security?

Who is in charge of security at your SAPF?

Overview of SAP Security Roles

The day-to-day operations of SAPs rely on both government and contractor personnel. The Program Security Officer, or PSO, is the government security professional responsible for all aspects of SAP security. The Government SAP Security Officer, or GSSO, and the Contractor Program Security Officer, or CPSO, provide hands-on security administration and management at the organizational level, whether at a government or a contractor facility.

Every SAP has only one PSO. However, a SAP that is large and complex enough may have multiple GSSOs and CPSOs subordinate to the PSO.

PSO Overview

Appointed in writing by the appropriate Cognizant Authority SAP Central Office, or CA SAPCO, or its service component designee, the PSO oversees and implements SAP security requirements for a specific SAP, sub compartment, project, geographical location, or agency or organization. With responsibilities encompassing all security disciplines, the PSO administers the security policies for the SAP and exercises full authority of SAP security on behalf of the CA SAPCO or its designee.

Program Security Officer (PSO)

Appointment: Appointed in writing by the CA SAPCO or its designee

Role: Oversees and implements SAP security requirements

General Responsibilities:

- Administers security policies for the SAP
- Exercises authority on behalf of CA SAPCO or its designee

PSO Duties and Responsibilities

The PSO security responsibilities fall into four broad categories. These principles include but are not limited to: administration, personnel security, physical security, and security education. Review each category.

Administration

PSO administrative responsibilities cover all duties related to compliance with SAP laws and security requirements in order to ensure a secure environment for the SAP. Specific tasks include approving standard operating procedures and providing instructions for implementing other SAP security guidelines.

- Ensure adherence to applicable laws as well as national, DoD, and other security SAP policies and requirements such as DoD Special Access Program (SAP) Security Manuals: DoDM 5205.07, Volumes 1 – 4
- Work with the SAP government program manager (GPM) to ensure a secure environment to facilitate the successful development and execution of a SAP
- Exercise approval authority for standard operating procedures (SOPs), security plans, and/or security documentation
- Provide detailed instructions and procedures in accordance with the program’s security classification guide (SCG), SOPs, and applicable marking guides
- Approve mode for transmission and transportation
- Provide detailed courier instructions to program-briefed couriers
- Approve all couriering of TS SAP material
- Notify and report security violations to the government program manager (GPM) with copy to the appropriate CA SAPCO
- Determine if an inquiry is required

Personnel Security

PSO personnel security responsibilities address action that must be taken when adverse or questionable information is discovered on a cleared employee.

- Take immediate action when new adverse or questionable information is discovered regarding an individual with current access

- Provide oversight for Program Access Requests (PARs)
- Ensure that Access Eligibility Reviews are accomplished to determine that candidates are eligible for access to SAP information
- Ensures that a SAP trained and knowledgeable GSSO or CPSO is assigned to serve as the SAP security official at each organization or facility

Physical Security

PSO physical security responsibilities address all high-level issues related to the facility, including certifying accesses and accrediting SAP facilities.

- Certify accesses to the facility
- Accredit SAP facilities (SAPF) when designated by the CA SAPCO as a SAPF accrediting official.
- Conducts or verifies that all approved SAPFs are properly inspected for security compliance
- Verify that configuration management policies and procedures for authorizing the use of hardware and software on an IS are followed
- Approve Secure Encryption Devices
- During Staff Assistance Visit (SAV) the PSO or designee will review security documentation and provide assistance and direction as necessary.

Security Education

The primary PSO security education responsibility is to approve the Security Education, Training and Awareness, or SETA, program for each assigned SAP. Note that the SETA program may be documented in a standalone document or incorporated into the facility’s standard operating procedures.

- Approve the Security Education, Training and Awareness (SETA) program of assigned SAP
- May be documented in a standalone document or incorporated into the facility’s SOPs
- Brief SAP-accessed individuals
- Provide necessary country-specific threat and defensive information to be used during foreign travel awareness briefings upon request

GSSO and CPSO Overview

The GSSO and CPSO perform essentially the same function in providing security administration and management for their respective facilities. Both positions are appointed in writing; however, the GSSO is appointed in writing by the Government Program Manager (GPM); whereas the CPSO is appointed by his or her Contractor Program manager (CPM), with copies of the appointment letter provided to the

PSO. Both perform under the guidance of the PSO to oversee the day-to-day security administration, management, and operations for his or her assigned SAP, and both are responsible for creating and maintaining a secure environment for the execution of a SAP. The general responsibilities of the GSSO and CPSO are quite similar, with a few notable differences. Take a moment to review them. Note that both the GSSO and CPSO must hold a security clearance equal to or greater than the highest clearance level of the SAP.

Government SAP Security Officer (GSSO)

Appointment: Appointed by the Government Program Manager (GPM)

Role

- Oversee security administration, management, and operations of SAP facility
- Create and maintain secure environment for execution of SAP

General Responsibilities

- Coordinate with SAP GPM and PSO
- Coordinate security matters with the PSO as applicable

Contractor Program Security Officer (CPSO)

Appointment: Appointed in writing by CPM, with copy provided to PSO

Role

- Oversee security administration, management, and operations of SAP facility
- Create and maintain secure environment for execution of SAP

General Responsibilities

- Coordinate with contractor program manager (CPM) and PSO
- Perform security duties and functions
- Oversee compliance with SAP security requirements

GSSO and CPSO Duties and Responsibilities

The GSSO and CPSO security responsibilities can be grouped into five categories: administration, personnel security, physical security, security education, and storage and handling. Review each category.

Administration

GSSO and CPSO administrative responsibilities cover all duties related to compliance with SAP policies and requirements, management of information and information systems, and adherence to SAP communications requirements.

- Ensure adherence to applicable laws as well as national, DoD, and other SAP security policies and requirements such as DoD Special Access Program (SAP) Security Manuals: DoDM 5205.07, Volumes 1 - 4
- When required, ensure that contract-specific SAP security requirements such as TEMPEST and Operations Security (OPSEC) are accomplished
- Prepare SOPs and forward the proposed SOPs and SOP changes to the PSO for approval
- Provide detailed instructions and procedures in accordance with the program's SCG, SOPs, and applicable marking guides
- Oversee an information management system for the SAP to facilitate the control of requisite information within the SAP
- Ensure information systems (IS) are in accordance with DoD Joint Special Access Program Implementation Guide (JSIG)
- Ensure adherence to special communications requirements, capabilities, and procedures within the SAPF, including briefings, debriefings, and foreign travel briefings
- Oversee transmission of SAP material
- Develop a transportation plan and forward to PSO for approval

Personnel Security

GSSO and CPSO personnel security responsibilities address SAP Nomination Process (SAPNP), program indoctrination, and foreign travel by program personnel.

- Ensure that personnel processed for access to a SAP meet the prerequisite SAPNP requirements
- Provide initial program indoctrination of employees after access approval; rebrief and debrief as required
- Review all proposed foreign travel itineraries of program-accessed personnel
- Conduct pre and post-travel briefings/debriefings
- Evaluate foreign travel trends for SAP-accessed personnel and have accessible
- Receive/forward reportable information on SAP-accessed

individuals such as personnel changes and derogatory information

Physical Security

GSSO and CPSO physical security responsibilities address all issues related to the facility, including maintaining a secure workspace, which may include a Special Access Program Facility, and overseeing self-inspections and visitor access. CPSOs are also responsible for certifying SAP accesses for visits between the prime contractor and any subcontractors.

- Ensure adequate secure storage and workspace
- When required, establish and maintain a SAPF in accordance with 5205.07, Volume 3 and ICD 705
- Ensure that all self-inspections are conducted
- Establish and oversee a visitor control program
- When properly trained and designated by the CA SAPCO, may perform SAPF Accrediting Officials (SAO) functions
- Certify SAP accesses to the facility for visits between a prime contractor and the prime's subcontractors (CPSO only)

Security Education

GSSO and CPSO security education responsibilities address issues related to security education, training, and awareness of all personnel working within the SAP, including providing overall management of the SAP SETA programs and ensuring that requirements and briefings are tailored to the needs of the individual SAP.

- Provide overall management and direction for assigned SAP SETA programs
- Ensure the SETA program meets specific and unique requirements of individual SAPs
- Establish security training and briefings specifically tailored to the unique requirements of the SAP
- Deliver country-specific threat/defensive briefs to personnel travelling to foreign countries
- Deliver annual refresher training covering the topics outlined on the SAP Refresher Training Record

Storage and Handling

GSSO and CPSO storage and handling responsibilities address the storage and handling of materials and documents related to the SAP, including overseeing classified material control, conducting annual inventories, and providing courier instructions.

- When required, establish and oversee a classified material control program for each SAP
- When required, conduct annual inventory of accountable classified

material*

- Maintain Control log for all SAP material that is not accountable
- Monitor reproduction and/or duplication and destruction capabilities of SAP information, including preparing written reproduction procedures
- Establish and oversee specialized procedures for transmission of SAP material to and from program elements
- Provide detailed courier instructions to program-briefed couriers

**Note: Not all SAP classified material is accountable; non-accountable material does not need to be inventoried.*

Knowledge Check

Select the best response for each question below, then check your answers in the answer key on the following page.

1. Who prepares a SAP's standard operating procedures (SOPs) and submits them for approval?

   ○ Program Security Officer (PSO)

   ○ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

2. Who verifies that configuration management policies and procedures for authorizing the use of hardware and software on an Information Systems are followed?

   ○ Program Security Officer (PSO)

   ○ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

3. Who reviews all proposed foreign travel itineraries of program-accessed personnel?

   ○ Program Security Officer (PSO)

   ○ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

4. Who establishes security training and briefings specifically tailored to the unique requirements of the SAP?

   ○ Program Security Officer (PSO)

   ○ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

5. Who reports security violations to the government program manager (GPM)?

   ○ Program Security Officer (PSO)

   ○ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

6. Who ensures adequate secure storage and workspace for the SAP?

   ○ Program Security Officer (PSO)

   ○ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

Answer Key

Select the best response for each question below, then check your answers in the answer key on the following page.

1. Who prepares a SAP's standard operating procedures (SOPs) and submits them for approval?

○ Program Security Officer (PSO)

◉ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

Feedback: *The GSSO/CPSO prepares a SAP's SOPs and submits the proposed SOPs and SOP changes to the PSO for approval.*

2. Who verifies that configuration management policies and procedures for authorizing the use of hardware and software on an Information Systems are followed?

◉ Program Security Officer (PSO)

○ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

Feedback*: The PSO certifies accesses to the facility and accredits SAPFs.*

3. Who reviews all proposed foreign travel itineraries of program-accessed personnel?

○ Program Security Officer (PSO)

◉ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

Feedback*: The GSSO/CPSO reviews all proposed foreign travel itineraries of program-accessed personnel.*

4. Who establishes security training and briefings specifically tailored to the unique requirements of the SAP?

○ Program Security Officer (PSO)

◉ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

Feedback*: The GSSO/CPSO establishes security training and briefings specifically tailored to the unique requirements of the SAP.*

5. Who reports security violations to the government program manager (GPM)?

   ◉ Program Security Officer (PSO)

   ○ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

***Feedback**: The PSO reports security violations to the GPM and sends a copy to the appropriate service-component CA SAPCO.*

6. Who ensures adequate secure storage and workspace for the SAP?

   ○ Program Security Officer (PSO)

   ◉ Government SAP Security Officer (GSSO)/Contractor Program Security Officer (PSO)

***Feedback**: The GSSO/CPSO ensures adequate secure storage and workspace for the SAP.*