Special Access Program Security Annual Refresher

Student Guide

September 2017

Center for Development of Security Excellence

Lesson 1: Course Introduction

Welcome

Throughout our nation's history, our military and strategic advantage has relied upon the quiet work of sensitive programs and operations. These programs have revolutionized industries and changed technology. They have made the impossible, possible. Each program came with its own unique challenges. And each required the dedication of people like you to safeguard its many secrets. Together, these programs have played a crucial role in the defeat of great powers and have changed history.

We refer to these programs as Special Access Programs, or SAPs. Because the United States has placed its trust in you, you have been given access to a special access program. Whether you've had access to a SAP or SAPs for several years or just received access in the past year, you know that when you protect SAP information and materials, you are protecting our nation's security along with the warfighters defending the American way of life. In this course, you will review the types of SAPs and SAP facilities, or SAPFs, and the various security requirements and procedures for safeguarding SAPs.

Objectives

Here are the course objectives. Take a moment to review them.

- Recognize purpose, categories and protection levels of Special Access Programs (SAPs) and types of SAP facilities (SAPFs)
- Identify the security procedures for SAPFs
- Identify the personnel security requirements for SAPs
- Select the proper methods for safeguarding SAP material
- Recognize threats that can affect SAPs
- Recognize Operations Security (OPSEC) requirements for SAPs
- Identify security compliance and inspection requirements for SAPs

Pre-Test/Post-Test

This course includes a pre-test which will test your current knowledge of the topics covered in this annual refresher. The pre-test is divided into sections. Each section corresponds to a lesson in this course. If you choose to take the pre-test, and you pass a section with a minimum score of 80%, you will not be required to take the corresponding lesson for that section. If you fail to pass a section on the pre-test, you will be required to complete that lesson of this course. In addition, everyone who

takes this course is required to take a post-test which covers the entire course content. The pre-test is available from the course menu.

Lesson 2: What Are SAPs and SAP Facilities (SAPFs)?

Introduction

In this lesson, we'll explore why we have SAPs, how they are categorized, what protection levels they have and the types of SAP facilities.

Objectives

Here are the lesson objectives. Take a moment to review them.

- Identify the purpose of SAPs
- Distinguish between the three SAP categories
- Distinguish between the three SAP protection levels
- Distinguish between the five types of SAP facilities

Purpose of SAPs

Overview

Policy guidance at the executive and DoD levels direct why we have SAPs and how they are to be protected.

Executive Order, or E.O., 13526, Classified National Security Information, states that DoD SAPs must be established for a specific class of classified information that imposes additional safeguarding and access requirements that exceed those normally required for information at the same classification level.

DoDD 5205.07, Special Access Program Policy, states that DoD SAPs must be established and maintained when absolutely necessary to protect the most sensitive DoD capabilities, information, technologies, and operations or when required by statute.

Additional SAP Policy Guidance

DoDM 5205.07, Special Access Program Policy Manual, Volumes 1-4, cover general procedures, personnel security, physical security and marking requirements for protecting SAPs.

The DoD Joint SAP Implementation Guide (JSIG) provides standardized cybersecurity related policy, procedures, and implementation guidance for use in the management of all networks, systems, and system components at all classification levels under the purview of the cognizant SAP Authorizing Official (AO).

DoDI 5205.11 provides for management, administration, and oversight of DoD SAPs and Title 10, Section 119, of the U.S. Code provides requirements for congressional oversight of special access programs.

DoD Joint SAP Implementation Guide (JSIG)

The security policy and procedures contained in this document are to be used by all personnel with a responsibility for protecting the confidentiality, integrity, and availability of DoD SAP information, information systems, and networks. This document applies to the DoD SAP Community and all networks, information systems, and applications for which the cognizant SAPCO has management or oversight responsibility regardless of the physical location. This includes Service elements, contractor sites, and DoD organizations that connect to a SAP-managed network which includes weapons systems, test equipment and multifunction devices such as printer-copier-fax-scanners.

Types of SAPs

SAP Categories

In what kind of SAP do you work? SAPs are categorized based on what type of programs they encompass. Some SAPs encompass acquisition programs of sensitive technology to include research, development, testing and evaluation, modification, or procurement activities which ensure the U.S. maintains its leading technological edge. Some SAPs protect the planning for, execution of, and support to especially sensitive military operations to ensure they are completed without disclosure. These SAPs may protect organizations, property, operational concepts, plans, or activities. Other SAPs protect the planning and execution of especially sensitive intelligence (SI) or counterintelligence (CI) operations or collection activities which keeps us ahead of our adversaries.

SAP Protection Levels

Do you know the protection level of your SAP? A protection level communicates how a SAP is acknowledged and protected. Although the specific program details of all SAPs are very closely protected, there are SAPs whose mere existence is closely guarded and others whose existence may be publicly acknowledged to a certain extent.

A SAP that is acknowledged is one whose existence may be openly recognized. Its purpose may be identified. However, the details of the program – including its technologies, materials, and techniques - are classified as dictated by their vulnerability to exploitation and the risk of compromise. Therefore, individuals may disclose that they work for a SAP on their resume or to family members or friends, but may not disclose the specifics of their SAP to any of those individuals. However, prior to disclosing, discuss with your security officer.

An unacknowledged SAP is one whose existence and purpose are protected. As with acknowledged SAPs, the details, technologies, materials and techniques of unacknowledged SAPs are classified. Under extremely limited circumstances, unacknowledged SAPs may also be waived.

Waived SAPs are unacknowledged SAPs for which the Secretary of Defense (SECDEF) has waived applicable Congressional reporting requirements to select committee members. Waived SAPs also have more restrictive access controls.

Types of SAP Areas

SAP Types Overview

Just as there are different types of SAPs, there are also different types of SAP areas. In what type of SAP area are you currently working?

A SAP Facility (SAPF)? A SAP Working Area (SAPWA)? A SAP Compartmented Area (SAPCA)? A Temporary SAP Facility (T-SAPF)? Or, a SAP Temporary Secure Working Area (SAPTSWA)? It is important to know your SAP facility type so that you know what can and cannot be done with SAP information in your facility.

A SAPF is an accredited area, room, group of rooms, building, or installation where SAP materials may be stored, used, discussed, manufactured, or electronically processed. The SAPF Accrediting Official (SAO) will inspect any SAP area before accreditation. Periodic re-inspections will be conducted based on threat, physical modifications, sensitivity of SAPs, and past security performance, but will be conducted no less frequently than every 3 years. Inspections, announced or unannounced, may occur at any time.

A SAPWA is used for discussing, handling, or processing SAP information however, storage is not authorized. A SAPWA is accredited with periodic re-inspections conducted no less frequently than every 3 years.

A SAP Compartmented Area (SAPCA) is used when different compartmented programs share the same SAPF or Sensitive Compartmented Information Facility, or SCIF, necessitating additional physical or operations security safeguards because not all personnel are cross-briefed. A SAPCA is approved for discussion, processing, manufacturing, testing and storage of SAP information. A SAPCA may be accredited with periodic re-inspections conducted at least every 3 years.

A T-SAPF is used for temporary periods of contingency operations, emergency operations, and tactical military operations. Accreditation for use shall not exceed 1 year without mission justification and approval of the SAO. T-SAPFs are approved for discussion, processing, manufacturing, testing and storage of SAP information.

A SAPTSWA is limited to less than 40 hours per month and the accreditation is limited to 12 months or less. SAP information may be discussed and processed or handled but storage is not authorized in a SAPTSWA. The SAPTSWA must be sanitized after each use and can be used for other non-SAP meetings. However, access to this area is limited to personnel with a minimum of U.S. Secret access, and the area will be secured appropriately per SAO approved methods.

Review Activities

Review Activity 1

Question 1 of 3. You are working on the drawings for a new military drone? In what type of SAP are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acquisition
- ○ Operations and Support (O&S)
- ○ Intelligence

Question 2 of 3. You are taking aerial pictures of a foreign manufacturing facility. In what type of SAP are you most likely working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acquisition
- ○ Operations and Support (O&S)
- ○ Intelligence

Question 3 of 3. While huddled in a military tent in a war zone in a foreign country, you are discussing your strategic and tactical plans with squadron leaders. In what type of SAP are you operating?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acquisition
- ○ Operations and Support (O&S)
- ○ Intelligence

Review Activity 2

Question 1 of 3. Your SAP has the most restrictive congressional reporting requirements. For what type of SAP are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acknowledge
- ○ Unacknowledged
- ○ Unacknowledged – Waived

Question 2 of 3. You told your spouse that you are working on a Special Access Program but you did not provide any specific details about the program. For what type of SAP are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acknowledge
- ○ Unacknowledged
- ○ Unacknowledged - Waived

Question 3 of 3. The mere existence of the SAP you are working on is classified but it has the same congressional reporting requirements as a SAP whose purpose is openly known. For what type of SAP are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acknowledge
- ○ Unacknowledged
- ○ Unacknowledged - Waived

Review Activity 3

Question 1 of 3. The SAP facility in which you are working was set up for the next six months for an emergency military operation. In what type of SAP facility are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Special Access Program Facility (SAPF)
- ○ Special Access Program Working Area (SAPWA)
- ○ Special Access Program Compartmented Area (SAPCA)
- ○ Temporary Special Access Program Facility (T-SAPF)
- ○ Special Access Program Temporary Secure Working Area (SAPTSWA)

Question 2 of 3. 3 You occasionally work in a SAP area that does not allow storage of SAP information, and is occasionally used by SCI briefed individuals for classified meetings. In what type of SAP facility are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Special Access Program Facility (SAPF)
- ○ Special Access Program Working Area (SAPWA)
- ○ Special Access Program Compartmented Area (SAPCA)
- ○ Temporary Special Access Program Facility (T-SAPF)
- ○ Special Access Program Temporary Secure Working Area (SAPTSWA)

Question 3 of 3. Your program is located in a room within a SAPF shared by other programs. In what type of SAP facility are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Special Access Program Facility (SAPF)
- ○ Special Access Program Working Area (SAPWA)
- ○ Special Access Program Compartmented Area (SAPCA)
- ○ Temporary Special Access Program Facility (T-SAPF)
- ○ Special Access Program Temporary Secure Working Area (SAPTSWA)

Lesson 3: Security Procedures for SAP Facilities (SAPF)

Introduction

In this lesson, we'll review the requirements for bringing items and people into SAP facilities and the procedures for visits, meetings, conferences and discussions in SAP facilities.

Objectives

Here are the lesson objectives. Take a moment to review them.

- Identify requirements for bringing items into a SAP facility
- Recognize procedures for visits, meetings, conferences and discussions in SAP facilities

Bringing Items into SAP Facilities

Requirements

Due to electronic monitoring threats associated with certain devices and proximity to SAP information technology networks, some electronic devices are prohibited from being introduced into a SAPF. Although this list does not include every prohibited device, it does include: personal computer systems or laptops, cell phones and other portable electronic devices (PEDs) including Government issued phones and devices, fitness trackers, and MP3 players, smart watches and/or reminder recorders, or other wireless 2 way devices, and any device with recording capability, such as cameras, video equipment and tape recorders. Digital media (i.e., magnetic tapes, CDs and DVDs) must be authorized through the PSO or designee prior to being introduced into the SAPF. All SAP areas must have procedures for inspecting personal belongings and vehicles at the entry and exit points to the building or site or at other designated areas.

Visitors to SAP Facilities

Prior to Visit

When a visitor is coming to a government or contractor SAPF, the request for the visit must be formally transmitted via a SAP Visit Request or other electronic means approved by the Government Program Manager (GPM) or contractor Program Manager (CPM) as appropriate or their designee. The security officer must receive the visit request in sufficient time to verify its accesses and transmit it to the appropriate facility prior to the visit. If the visitor's requisite SAP accesses cannot be verified, the visitor will not be allowed into the SAPF.

As a minimum, the Government SAP Security Officer (GSSO) or Contractor Program Security Officer (CPSO) from the departure location will provide each authorized courier with a copy of Department of Defense (DD) Form 2501, "Courier Authorization," and detailed instructions. Visitors who courier

classified material must provide their travel itinerary, storage requirements, and emergency contact information to their GSSO or CPSO and to the destination GSSO or CPSO.

At Visitor Check-In

When a visitor arrives at a government or contractor SAPF, he or she must provide an acceptable form of identification which must be validated by SAP security personnel. Security will ask the visitor if they have any electronic devices and, if so, they will secure those devices for the visitor. The visitor will sign in and out on the visitor log. Unless a PSO approved electronic visitor record is on file, the security officer will maintain segregated visitor logs for non-briefed and SAP accessed personnel.

Security will alert other personnel in the facility of the incoming visitor and allow personnel sufficient time to secure their area, such as doors, documents, printers, and discussions, before the visitor enters the area. The number of escorts for the visitor will depend on the standard operating procedure (SOP) of the SAPF and the ability to closely monitor visitor activities.

Meetings and Conferences

Remember, SAP meetings and conferences may only be held in SAP Facilities approved for discussions. The meeting host must validate the appropriate SAP access of all attendees and must establish and announce the common level of the classified information and SAP program to be discussed among attendees. Don't forget that non-SAP individuals may not enter into Special Access Programs Facilities (SAPFs) without prior SAP Central Office (SAPCO) and SSO approval. And finally, remember that all classified material generated or distributed at the meeting, such as notes, minutes, and summaries, must be gathered at the end of the meeting and prepared for storage, electronic transmittal, or destruction.

Discussion Areas

You may recall that procedures for SAP discussions are similar to those for meetings and conferences. The discussion host must validate SAP accesses of all attendees and announce the SAP common levels of the classified information and SAP program to be discussed prior to discussions. You may use white noise generators to meet acoustical requirements and cease discussions and processing when the door is opened. As with meetings and conferences, you must control all SAP materials and notes used and gather them for secure transmission through SAP systems, courier, or fax.

You must verify the courier card or letter for those departing the SAP area to other accredited spaces with SAP materials. Also, remember receipts are required if there is any physical transfer of Top Secret SAP custody. And finally, you must sanitize the room after use to ensure all SAP information is removed, including from trash cans, all notes are gathered, white boards are erased, and so on.

Review Activities

Review Activity 1

Who would approve temporary use of prohibited items in a SAP facility?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ PSO or GPM
- ○ PSO or SAO
- ○ GPM or CA SAPCO

Review Activity 2

Question 1 of 3. You must use white noise generators during SAP discussions to meet acoustical requirements if the area does not meet the requirement.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 2 of 3. All SAP materials must be removed from areas or rooms after SAP meetings, conferences and discussions and prepared for secure transmission, storage or destruction.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 3 of 3. Visitors may enter a SAPF without a Visit Request as long as they have an escort.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Lesson 4: Personnel Security Requirements

Introduction

In this lesson, we'll review the personnel security requirements for special access programs.

Objectives

Here is the lesson objective. Take a moment to review it.

- Identify the personnel security requirements for SAPs

SAP Nomination, Indoctrination, and Debriefing

Requirements

Before you are given access to your SAP, the Special Access Program Personnel Security Official, or SPO, is responsible for the completeness and accuracy of information submitted in the nominated individuals' packages. Once approved, the indoctrination briefing takes place. Finally, when you leave the SAP, a SAP exit debriefing is executed.

Remember, by signing the SAPIA in both the indoctrination briefing and the debriefing, you have agreed to protect SAP information for the rest of your life, while you have access to the SAP and even after you no longer have access to the SAP.

SAP Nomination Process

The Special Access Program Personnel Security Official (SPO) will make the initial eligibility determination and/or recommendation in accordance with the SAP Nomination Process (SAPNP) by reviewing the Pre-screening Questionnaire (PSQ). The Program Security Officer (PSO) evaluates the recommendation and makes a recommendation to the Access Approval Authority (AAA). The AAA then approves or disapproves your Program Access Request (PAR). For additional information, please refer to DoDM 5205.07, Volume 2, Enclosure 4.

Indoctrination Briefing

After the AAA approved your Program Access Request, or PAR, you were formally indoctrinated into the SAP by reading and signing the Special Access Program Indoctrination Agreement (SAP Indoctrination Agreement). After signing the SAP Indoctrination Agreement, you should have reviewed your SAP's Security Classification Guides (SCGs) and Standard Operating Procedures (SOPs).

SAP Exit Debriefing

When you leave your SAP, you must execute the debriefing acknowledgement portion of the SAP Indoctrination Agreement. Then your SAP Indoctrination Agreement will be forwarded to

the Program Security Officer, or PSO, where it will be destroyed 5 years after the SAP is terminated or in accordance with agency directives. Remember, by signing the SAP Indoctrination Agreement in both the indoctrination briefing and the debriefing, you have agreed to protect SAP information for the rest of your life.

Reporting Requirements

Overview

As you know, you have access to one or more SAPs because the United States Government has put its trust in you. This relationship obligates you to report certain events and incidents to your security office, which range from specific information about your personal life to security incidents that have caused the loss or compromise of classified information.

Remember, any change which affects your responses to the Pre-Screening Questionnaire (PSQ) must be reported on the applicable PSQ templates. PSQ's need to be re-validated annually.

Let's review other types of information that you, as an individual with SAP access, are required to report. Each person in this fictional conference room has SAP access. Read each of the scenarios to hear their stories and decide if the information you learn must be reported or not.

Woman 1 Scenario:

Yesterday Paula Noble forgot to check under the table in a SAP conference room when sanitizing the area after a meeting. Another team met afterwards in that conference room and that team found a SAP document under the table related to the SAP program Paula is working on.

Does this incident require reporting?

- ○ Yes
- ○ No

Feedback: *Yes, this incident must be reported. You must report to your Program Security Officer, or PSO, Government SAP Security Officer, or GSSO, or contractor program security officer, or CPSO, immediately when you become aware of any known or suspected compromises of classified information or security incidents. Similarly, you must also report any suspicious contacts where any person attempts to obtain classified information from you or another person.*

Woman 2 Scenario:

Shannon O'Connor recently got married but she did not take her new husband's last name.

Is Shannon required to report her marriage?

- ○ Yes
- ○ No

Feedback: *Yes, Shannon is required to report her marriage whether she changes her last name or not. In fact, everyone who has SAP access is required to report any changes in personal status such as marriage, separation, divorce, foreign cohabitants and citizenship. Potentially adverse involvement with law enforcement, such as arrests and drug use, as well as changes in financial status, such as credit judgments, bankruptcy, garnishments, and repossessions, must also be reported.*

Man 1 Scenario:

Scott Tully just informed his supervisor that he no longer wishes to work on Special Access Programs contracts.

Is Scott's supervisor required to report this information about Scott or can his supervisor just transfer Scott to another area working on unclassified work and not report it?

- ○ Yes
- ○ No

Feedback: *Yes, Scott's supervisor is required to report this information. In fact, you must report to your PSO, GSSO, or CPSO immediately, when any employee refuses to sign a SAP Indoctrination Agreement (SAPIA) or when any employee says they do not wish to perform on classified work.*

Man 2 Scenario:

On Friday evening, Raul DeGuzman attended a work-related cocktail party at a local hotel. While at the party, a Russian man approached Raul and engaged him in conversation. After the conversation ended, Raul's co-worker, Jack Kelly, told him that the Russian man is believed to work for the Russian Foreign Intelligence Entity.

Is Raul required to report his contact with this Russian man?

- ○ Yes
- ○ No

***Feedback**: Yes, Raul is required to report this foreign contact. Everyone with SAP access must report foreign contacts with known or suspected Foreign Intelligence Officers or contacts which suggest you may be targeted for exploitation by a Foreign Intelligence Entity. In addition, foreign contacts where you or your spouse cohabitate or have a continuing relationship must also be reported.*

Man 3 Scenario:

Not only is Howard Brewer a well-respected employee, but he is also a great husband because he is taking his wife to Hawaii to celebrate their 30th anniversary.

Was Howard required to report that he was taking this trip?

- ○ Yes
- ○ No

Feedback: *No, Howard is not required to report his trip to Hawaii because it is within the U.S. However, Howard Brewer and all personnel who have SAP access are required to report all foreign travel prior to departure. An exception to this rule is that same day travel does not need prior notification but must be reported immediately upon return. In addition, all suspicious contacts on any trip must be reported upon return.*

Review Activities

Review Activity 1

Which of the following items are allowed into SAP facilities if processed and approved by the PSO or CA SAPCO?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Review of SAPs Standard Operating Procedures
- ☐ Acknowledgement that requirement to protect SAP information is a lifelong obligation
- ☐ Signing of debriefing acknowledgement portion of SAP Indoctrination Agreement
- ☐ Destruction of SAPIA 5 years after program is terminated or in accordance with agency directives

Lesson 5: Information Security Requirements

Introduction

As you know, additional protection is provided to SAP information through classification management and marking, above and beyond what is provided to classified information. In this lesson, you will review what classification management is and how SAP information is protected with SAP marking and release requirements.

Objectives

Here is the lesson objective. Take a moment to review it.

- Recognize the classification, marking, and release requirements for SAP material

Protecting SAP Material

Classification

As you know, only an Original Classification Authority (OCA) may classify material in accordance with Executive Order 13526, National Security Information. The OCA's decisions are documented in the Security Classification Guide, or SCG, so the SCG becomes the authoritative document for determining if information is classified or not. Agencies must establish procedures to ensure SCGs are reviewed, updated, and revalidated every 5 years.

Derivative classification occurs when individuals who handle SAP information incorporate, paraphrase, restate, or generate in new form information that is already classified, and mark the newly developed material consistent with the classification markings that applied to the source information. This also includes the classification of information based on classification guidance. Derivative classifiers must receive training at least every 2 years.

Normally unclassified administrative aspects of a program are protected within SAP channels to protect a sensitive organizational relationship or simply the existence of an Unacknowledged SAP. If details were revealed, they could expose the intended SAP objectives or even the existence of the SAP. To prevent the revelation of an Unacknowledged SAP, use the "Unclassified Handle Via Special Access Channels Only" handling caveat on documents and keep information within SAP control channels on security approved SAP communications systems only.

Marking

As you know, all classified material must be properly marked with the appropriate classification levels derived from the program's SCG. You can find marking guidance for SAP materials in DoDM 5205.07, Volume 4, DoD SAP Security Manual: Marking. Let's review each type of marking: overall

classification or banner markings, portion markings, derivative classification and declassification markings.

Overall Classification or Banner Markings

Top and Bottom Banner Marking Example:

TOP SECRET//SAR-RED CAR/SAR-TIN BAKER//WAIVED

[document body]

TOP SECRET//SAR-RED CAR/SAR-TIN BAKER//WAIVED

Overall classification or banner markings are located at the top and bottom of each page in the document. Mark each page on the top and bottom with the highest level of the page. Make them in larger font than the rest of the page or the highest overall of the entire document depending on your program procedures. Spell out Special Access Required or use acronym "SAR" and include the program nickname or code word. This example has two program nicknames, which are RED CAR and TIN BAKER. Use a hyphen to separate the acronym and program's nickname or code word. Include the dissemination control, if assigned. In this example, the dissemination control is WAIVED. Do not use program identifiers (PIDs) in the banner. PIDs are only used in the portion markings.

Portion Markings

Portion Marking Example:

TOP SECRET//SAR-RED CAR/SAR-TIN BAKER//WAIVED

[Date of origin]

MEMORANDUM FOR SAP DOCUMENT PREPARERS

From: Director of SAPCO, MDA

SUBJECT: (U) Markings for a SAP Document

(U//FOUO) This sample memorandum highlights markings for classified documents containing SAP information

(S//SAR-RC) This section demonstrates how to mark a paragraph that contains SAP information from one Secret program. The portion marking reflects the highest classification level in the portion or paragraph.

(TS/SAR-RC/SAR-TBK//WAIVED) This section demonstrates how to mark a paragraph that contains SAP information from two programs. The portion marking reflects the highest classification level in the portion or paragraph. Additionally, since TBK is a Waived SAP, the dissemination control is also reflected in the portion marking.

(U//FOUO) Portion markings for the Subject and Attachments indicate the classification of the subject or attachment title; not the classification of the document. Also note that Document Control information is reflected in the lower right corner for SAP documents requiring formal accountability.

Signature Block

Attachment:
Tab A: (U) Quad Chart

[Classification authority block]

TOP SECRET//SAR-RED CAR/SAR-TIN BAKER//WAIVED

Portion markings are located at the beginning of each paragraph. Mark each paragraph with the highest classification for that paragraph. For classified information related to the SAP, mark SAR and the assigned program identifier, or PID, which is the abbreviation for the program's nickname or code work. Also use a hyphen to separate the SAR acronym and the PID. Include the dissemination control, if there is one. In this example, WAIVED is the dissemination control. Also, portion mark titles of memoranda. Note that charts, graphs and images must also be portion marked within their boundary.

Derivative Classification and Declassification Markings

Derivative Classification and Declassification Markings Example:

TOP SECRET//SAR-RED CAR/SAR-TIN BAKER//WAIVED

[Date of origin]

MEMORANDUM FOR SAP DOCUMENT PREPARERS

From: Director of SAPCO, MDA

SUBJECT: (U) Markings for a SAP Document

(U//FOUO) This sample memorandum highlights markings for classified documents containing SAP information

(S//SAR-RC) This section demonstrates how to mark a paragraph that contains SAP information from one Secret program. The portion marking reflects the highest classification level in the portion or paragraph.

(TS/SAR-RC/SAR-TBK//WAIVED) This section demonstrates how to mark a paragraph that contains SAP information from two programs. The portion marking reflects the highest classification level in the portion or paragraph. Additionally, since TBK is a Waived SAP, the dissemination control is also reflected in the portion marking.

(U//FOUO) Portion markings for the Subject and Attachments indicate the classification of the subject or attachment title; not the classification of the document. Also note that Document Control information is reflected in the lower right corner for SAP documents requiring formal accountability.

Signature Block

Attachment:
Tab A: (U) Quad Chart

Classified by: David L. Smith, PSO
Derived from: RC SCG dated 20081128: TBK SCG dated 20090415
Declassify on: 20511231 (per FSE dated 20150306)

TOP SECRET//SAR-RED CAR/SAR-TIN BAKER//WAIVED

Classification authority block is located together near the bottom of the document. On the Classified by line, include the name, title and organization of the derivative classifier. On the Derived from line, include the detailed title and date of the source document. Or if there are multiple sources, list all sources on the front or at the back of the document. On the Declassify on line, list the source document declassification date per file series exemption (FSE) if multiple documents are utilized use the most restrictive date. For material dated prior to January 1, 1982, declassify on December 31, 2031. For material dated on or after January 1, 1982, declassify on December 31 of the year the document is 50 years old unless previously reviewed or extended.

Release of SAP Information

Don't forget that you may not release SAP information to the public without written SAP Central Office, or SAPCO, approval. All material proposed for release must be submitted through the program security officer, or PSO, to the Government Program Manager, or GPM, 60 days before the proposed release date. SAP briefed personnel who write a book or article, post a blog, or give a speech must request a security review of the material and receive written authorization from the SAPCO. Public disclosure approval of SAP information does not automatically mean the information is now declassified nor does it authorize individuals to confirm, deny, or disclose that information. Remember, your requirement to protect SAP is a lifelong obligation.

Review Activities

Review Activity 1

Question 1 of 3. Per E.O. 13526, who is authorized to determine the classification of SAP material?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Derivative Classifier
- ○ Original Classification Authority (OCA)

Question 2 of 3. Whose classification decisions are recorded in the Security Classification Guide (SCG) for a SAP?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Derivative Classifier
- ○ Original Classification Authority (OCA)

Question 3 of 3. Who must receive training every two years?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Derivative Classifier
- ○ Original Classification Authority (OCA)

Review Activity 2

Question 1 of 3. Which type of marking utilizes the program identifier (PID) abbreviation?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Overall classification or banner marking
- ○ Portion marking
- ○ Classification Authority Block

Question 2 of 3. Where do you indicate who classified the document?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Overall classification or banner marking
- ○ Portion marking
- ○ Classification Authority Block

Question 3 of 3. In what marking must you include the highest overall classification of a page?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Overall classification or banner marking
- ○ Portion marking
- ○ Classification Authority Block

Review Activity 3

For what types of publications must you request SAPCO approval before releasing any SAP information?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Books
- ☐ Articles
- ☐ Blog posts
- ☐ Speeches

Lesson 6: Safeguarding SAP Information

Introduction

In this lesson, we'll review the transmission requirements and the requirements for handling SAP material which includes control, accountability, reproduction and destruction of SAP material.

Objectives

Here are the lesson objectives. Take a moment to review them.

- Identify the transmission requirements for SAP material
- List the handling requirements to include control, accountability, reproduction and destruction of SAP material

Transmission Requirements

Control

Transmission methods vary by classification level. You may transmit Top Secret information through authorized systems, such as secure telephones and classified networks; secure fax; and hand-carry with two persons, unless otherwise authorized by the PSO.

Secret information and below may be transmitted the same ways that Top Secret may be transmitted except hand-carry may be done with just one person. When approved by the PSO, a USPS mailing channel may be established to ensure mail is received only by appropriately cleared and accessed personnel. Secret and below information may also be transmitted via United States Postal Service (USPS) Priority Express Mail, and USPS Registered mail.

Confidential information may be sent via USPS Certified mail.

Finally, US Government approved contract carriers may be used with Program Security Office, or PSO, approval and can only be used within the continental United States (CONUS).

DoDM 5205.07, Volume 1, Enclosure 5

SAP information will only be transmitted outside the SAPF using one of the methods identified. The GSSO or CPSO will oversee transmission of SAP material. The order of precedence for transmission processes is:

1) Cryptographic communications systems (i.e., secure facsimile, Information systems).
2) Courier.
3) PSO approved government or commercial carrier for SECRET SAP material and below.
4) Defense Courier Service for TOP SECRET SAP material.
5) United States Postal Service (USPS) registered mail or US Express Mail for SECRETSAP material and below within the continental United States (CONUS).
6) USPS certified mail for CONFIDENTIAL SAP material and below within CONUS.

Secure Telephone

Never use unsecured phone lines to discuss SAP information or to even try to talk about SAP information without really specifying the SAP information. You must always use approved secure telephones for the appropriate level of classification for which they are authorized. So, for example, do not discuss TOP SECRET SAP information on a secure phone only authorized for SECRET SAP information. Always be aware of your environment to ensure no one is eavesdropping on your conversation. Verify who you are talking to. For example, get the individual's information to verify their program access before discussing SAP information with them. Finally, contact your security team for training and any additional requirements.

Classified Networks

Data transfer is the movement of electronic information between systems or media of different classification levels which requires special prior approval and must be performed by trained and certified individuals who follow approved procedures and software tools. You may transmit classified SAP information via e-mail only over a classified network that has been accredited for SAP. You may NOT transmit classified SAP information and Handle Via Special Access Channel Only (HVSACO) information over an unapproved information system, to include the SECRET Internet Protocol Router Network (SIPRNET) and/or the Joint Worldwide Intelligence Communications System (JWICS). See your PSO or CA SAPCO for specific classified network procedures.

Courier

All personnel must possess a valid courier authorization letter or card approved by the PSO. Couriers must be accessed to the level of SAP being couriered. Top Secret Special Access Required, or SAR, material and all classified media requires a two-person courier team unless one courier has otherwise been approved by the PSO. The CA SAPCO defines the local area and may modify this requirement. For local travel, SAP material may be hand-carried using a locked container as the outer wrapper and have an attached tag or label with the individual's name,

organization, and telephone number. Couriered material must have a cover sheet, be properly marked, be receipted, and be double-wrapped or put into an authorized courier bag.

Handling Requirements

Control

To control SAP information, you must maintain records detailing the receipt, dispatch, and destruction of items. You must also ensure proper physical storage in approved security containers.

Recall that all Top Secret collateral and SAP information is considered "accountable." However, SAP material, hardware, equipment, and media that is "not accountable" is controlled by the procedures implemented through policy, training, and awareness that regulate and monitor the introduction and exit of all controlled items. Controls also include identifying and documenting SAP material including the custodian, date created and destroyed; as well as the classification, program sensitivity, item type and content. Finally, at least on an annual basis you must assess the need for all the controlled items and items no longer required must be destroyed.

Accountability

An accountability system, approved by the PSO, must be developed and maintained for the following SAP classified information: all Top Secret SAP material, media, hardware, equipment; Secret SAP material, media, hardware, equipment when directed by the CA SAPCO; and all other classified media when directed by the CA SAPCO.

Accountable SAP material is entered into an accountability system whenever it is received, generated, reproduced, or dispatched either internally or externally to other SAPFs. The accountability system is designed to record all transactions of handling, receipt, generation, reproduction, dispatch, or destruction. The accountability system assigns individual responsibility for all accountable information. When SAP material is received with the originator's accountability control number, the accountability system will include the originator's accountability control number. If an automated system is used, it will have a backup.

The accountability system will have at the minimum:

1) Classification
2) Originator of the item
3) Title and description of item
4) Custodian assigned
5) Date of product
6) Control number (maintained in consecutive number series)
7) Copy number
8) Page count
9) Disposition and date
10) Destruction date
11) Internal and external receipt records

Reproduction

SAP reproduction is authorized on specifically approved copy equipment within SAP areas only. Approved copiers have a sign posted stating the highest level of information authorized and who is authorized to reproduce such material. Be sure to follow all posted signs above the copier! Note, however, that Unclassified HVSACO material CANNOT be copied on unclassified copiers. Reproduced material is subject to the same rules as other documents and must be documented in a reproduction log, then protected, marked, and accounted for appropriately.

Destruction

Destruction is the process of physically damaging media so that it is not usable and there is no known method of retrieving the data. This may include degaussing, incineration, shredding, grinding, embossing, chemical immersion, etc. All sanitization and destruction procedures require Authorizing Official (AO) approval, and must be in accordance with the Program SCG or CA SAPCO. SAP destruction requirements include single person, two-person integrity (TPI) destruction and burn bags.

DoDM 5205.07, Volume 1, distinguishes between non-accountable SAP material destruction and accountable material destruction. Non-accountable SAP material may be destroyed by a single SAP-briefed employee with access to the level of material being destroyed. This includes Top Secret working papers that have not been brought into formal accountability.

Accountable SAP material destruction requires using two SAP-briefed employees with access to the level of material being destroyed. Another distinction is that non-accountable SAP material does not require a destruction certificate, unless the Program SCG directs otherwise. Accountable SAP material does require destruction logs maintained by your PSO or Top Secret Control Officer, or TSCO, per your SOP in accordance with DoD policies. Use of burn bags for destruction may be utilized where authorized and in accordance with the Program SOP.

Review Activities

Review Activity 1

Question 1 of 4. At which of the classification levels is it permitted to transmit SAP information via USPS Priority Mail Express with SAPCO approval?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential

Question 2 of 4. At which classification level(s) is it permitted to transmit SAP information via secure fax?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential

Question 3 of 4. At which classification level(s) is it permitted to transmit SAP information via USPS Certified mail?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential

Question 4 of 4. At which classification level(s) is it permitted to transmit SAP information via a USG approved contract carrier with PSO approval and only within CONUS?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential

Review Activity 2

Question 1 of 4. All Top Secret collateral and SAP information is considered "accountable."

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 2 of 4. SAP Accountability System is required for Top Secret SAP documents only.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 3 of 4. Identification and documentation of SAP materials includes the custodian, date created/destroyed classification, program sensitivity, item type and content.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 4 of 4. The accountability system is designed to record all transactions of handling, receipt, generation, reproduction, dispatch, or destruction.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Review Activity 3

Question 1 of 4. Any copier located in the program office can be used for Top Secret, Secret, and Confidential SAP documents.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 2 of 4. Unclassified Handle Via Special Access Channels Only (HVSACO) material can be copied on unclassified copiers.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 3 of 4. Accountable SAP material destruction requires using two SAP-briefed employees with access to the level of material being destroyed.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 4 of 4. Non-accountable SAP material typically does not require a destruction certificate.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Lesson 7: Threats and Other Security Requirements

Introduction

In this lesson, we'll explore threats that can affect SAPs, and operations security (OPSEC) requirements for SAPs. We'll then examine security compliance inspection requirements for SAPs.

Objectives

Here are the lesson objectives. Take a moment to review them.

- Recognize potential threats that can affect SAPs
- Recognize Operations Security (OPSEC) requirements for SAPs
- Identify security compliance and inspection requirements for SAPs

Threats and Operations Security

Overview

Are you giving away more unclassified information than needed? Adversaries piece together sensitive unclassified information from information you reveal. You can prevent adversaries' ability to piece together a puzzle by limiting unclassified disclosure via internet/social media and securing your credentials when departing your work site. Always be conscious of your discussions in unclassified areas. Do not include, or even allude to, classified and or sensitive information concerning programs, program activities, and operations, whether on a resume, in a personnel review, or in a publication.

> "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy."
> Al-Qaeda training manual recovered in Afghanistan

OPSEC Process

1. Identification of Critical Information:

   Information concerning sensitive activities, whether classified or unclassified, which is vitally needed by adversaries or competitors for them to plan and act effectively.

   Indicators are detectable actions that can be heard, observed, or imaged. Obtained by an adversary, they could result in adversary knowledge or actions harmful to friendly intentions. They include such things as personnel or material actions and movements that can be observed, public release conversations or documents, and habitual procedures when conducting a given type of operation

or test. All detectable indicators that convey or infer critical information must be identified and protected if determined vulnerable.

2. Analysis of Threats:

   Process in which information about a threat or potential threat is subjected to systematic and thorough examination in order to identify significant facts and derive conclusions.

   Threat analysis is an examination of an adversary's technical and operational capabilities, motivation, and intentions to detect and exploit security vulnerabilities. A determination will need to be made as to who would want this technology, who would want to discredit this Project, who would like to cause harm to the Project participants, or who would like to do other nefarious activities directed at the Project.

3. Analysis of Vulnerabilities:

   Process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a safeguards and security system to protect specific targets from specific adversaries and their acts.

   Actions and things that can be observed or other data that can be interpreted or pieced together to derive critical information must be identified. These potential vulnerabilities must be matched with specific threats. Once it is determined what an adversary needs to know and where that information is available, it is necessary to determine if it is possible for the adversary to acquire and exploit the information in time to capitalize on it. If so, vulnerability exists.

4. Assessment of Risks:

   Evaluation of potential threats against a safeguard and security interest and the countermeasures necessary to address potential vulnerabilities.

   Included in the assessment of an adversary's capability is not only his ability to collect the information but also his capability to process and exploit (evaluate, analyze, interpret) in time to make use of the information. This process should result in a list of recommendations along with an estimate of the reduced impact upon the operation as achieved through their application. The decision maker can then weigh the cost of recommended OPSEC countermeasures in terms of resources and operational effectiveness against the impact of the loss of critical program information.

5. Application of Countermeasures:

   Anything that effectively negates an adversary's ability to exploit vulnerabilities.

   The most effective countermeasures are simple, straightforward, procedural adjustments that effectively eliminate or minimize the generation of indicators. Following a cost-benefit analysis, countermeasures are implemented in priority order to protect vulnerabilities having the most impact on the Project, as determined by the appropriate decision maker.

Threats

Would you recognize a threat from the insider? What would you do? Espionage is the act or practice of spying or of using spies to obtain secret information, about another government or a business competitor. It can be perpetrated by personnel within your organization as well as by external domestic and foreign spies.

Infamous spies have done great damage to our national security, yet each one thought the rules didn't apply to them. John Anthony Walker helped the Soviets decipher 1 million encrypted naval messages. Aldrich Ames provided information leading to the compromise of at least 100 Intel operatives and the execution of 10 sources. Ana Montes disclosed the location of a clandestine Army camp directly resulting in the death of Green Beret SSG Gregory A. Fronius. Chelsea Manning released approximately 750,000 classified and sensitive documents to the Internet. Espionage is punishable by fines and/or imprisonment!

Title 18 U.S. Code

"Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States classified information…shall be fined under this title or imprisoned"

Title 50 U.S. Code

"It shall be unlawful…to communicate in any manner…to any foreign government, any information of a kind which shall have been classified…punishable by fines and or imprisonment"

Threat Reporting

Let's examine four common but highly effective techniques for gathering foreign intelligence. The request for information is one cheap and easy technique that carries with it the idea that if enough people are solicited, eventually you'll find a nugget of information that can connect the dots. Another technique is the poking and prodding that comes with suspicious network activity. These attacks are the fastest growing method of operation for foreign entities. The academic solicitation technique uses students, professors, scientists or researchers as collectors improperly attempting to obtain sensitive or classified information. Finally, elicitation and recruitment is a seemingly non-threatening and natural manner used by the spy to spot and collect information.

Report to your security officer contacts, activities, indicators, and behaviors that signify potential foreign intelligence threats against DoD or its personnel, information or materiel, facilities, activities, and national security.

Security Compliance and Inspection Requirements

Core Compliance Inspections

Inspections are conducted to validate that SAP security processes and procedures are in compliance with the governing DoD policies and to ensure that the risk of compromise to SAP information is at a minimum. Core compliance inspections are conducted at a minimum of every 2 years at the direction of the inspection official. They include the Self-inspection Checklist, Core functional areas (CFAs) and Special Emphasis Items (SEIs).

CFAs will confirm that Top Secret SAP data and materials are properly accounted for, and that all personnel have completed their security, education, training and awareness annual training. CFAs will also confirm that the Special Access Program Nomination Process, or SAPNP, to determine personnel suitability was completed within the 365-day window and the SAP Pre-Screening Questionnaire, or PSQ, has been updated on an annual basis. If a SAP inspection report identified an acute or critical vulnerability in a Program, then as part of security management and oversight, inspectors will ensure the corrective action plan was executed. Another CFA deals with cybersecurity inspection to ensure that all media is controlled within the SAPF. Finally, as part of the physical security review, they will ensure the SF 702, Security Container Checksheet, is completed as required.

Common inspection problems vary from program to program and year to year. Be cognizant of your program's common inspection problems. Your PSO/GSSO/CPSO will provide you the specifics of your programs common problem areas.

In the third area of core compliance inspections, the CA SAPCO will annually determine the SEIs and report to the DoD SAPCO. Subcontractor DD Form 254 and Assured File Transfer, for example, are items that may require additional review of the current policy and procedures in operation by the unit or agency.

SETA: Security, Education, Training and Awareness
Annual training is recorded in the SAP training record template posted at http://www.dss.mil/documents/isp/SAP_Training_Record_Template.pdf
SAPNP: Special Access Program Nomination Process – a standardized security management process that applies enhanced security procedures to determine personnel suitability for access to DoD SAPs. SAPNP process includes: SAP Nomination Requirements; SAP Nomination Packages; SAP Nomination Review Process; and SAP Access Decision.
CA SAPCO: Cognizant Authority Special Access Program Central Office
PSO: Program Security Officer
GSSO: Government SAP Security Officer
CPSO: Contractor Program Security Officer
PSQ: SAP Prescreening Questionnaire

Fraud, Waste, Abuse, and Corruption (FWAC)

Breach of Classified Systems Involving SAPs ... Nuclear Surety ... Unauthorized Disclosures ... Security Violations/Compromise ... Intelligence Oversight ... Violations that should be reported for classified complaints must be done via SECURE means. However, it is imperative that you do not discuss classified information on any DoD Fraud, Waste, Abuse, and Corruption Hotline and do not use other advertised FWAC hotlines when SAP information may be revealed. Talk to your PSO/GSSO/CPSO in order to obtain the number of the FWAC Hotline that you should be using for your program.

Review Activities

Review Activity 1

Which of the following are measures to prevent adversaries from piecing together sensitive unclassified information?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Limit unauthorized disclosure via the Internet and social media
- ☐ Be conscious of discussion in unclassified areas
- ☐ Secure credentials when departing the work site
- ☐ Do not include, or even allude to, classified and or sensitive information in a resume, personnel review, or publication
- ☐ Determine whether anyone around you might be interested in the technical and operational activities of your program prior to discussing them.

Review Activity 2

Which of the following are core functional area activities for SAP compliance inspections?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☐ TS SAP data and materials are properly accounted for
- ☐ Personnel completion of the required annual education and awareness training
- ☐ Completion of Special Access Program Nomination Process within 365 days and update annually
- ☐ Ensure execution of the corrective action plan resulting from a SAP inspection report as part of security management and oversight
- ☐ Conduct a cybersecurity inspection to ensure all media is controlled
- ☐ Ensure the SF 702, Security Container Checksheet, is completed

Lesson 8: Course Conclusion

Course Summary

Summary

In this course, you reviewed the types of SAPs and SAP facilities and the security requirements and procedures you must follow to protect SAPs.

Always refer to your individual SAP for program-specific security requirements.

Lesson Review

Here is a list of the lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: What Are SAPs and SAP Facilities?
- Lesson 3: Security Procedures for SAP Facilities
- Lesson 4: Personnel Security Requirements
- Lesson 5: Information Security Requirements
- Lesson 6: Safeguarding SAP Information
- Lesson 7: Threats and other Security Requirements
- Lesson 8: Course Conclusion

Lesson Summary

Congratulations! You have completed the *Special Access Program Security Annual Refresher* course.

You should now be able to perform all of the listed activities.

- Recognize purpose, categories and protection levels of Special Access Programs (SAPs) and types of SAP facilities (SAPFs)
- Identify the security procedures for SAPFs
- Identify the personnel security requirements for SAPs
- Select the proper methods for safeguarding SAP material
- Recognize threats that can affect SAPs
- Recognize Operations Security (OPSEC) requirements for SAPs
- Identify security compliance and inspection requirements for SAPs

To receive credit for this course, you *must* take the *Special Access Program Security Annual Refresher* post-test. You will have three chances to pass the post-test with a score of 80% or higher and receive a certificate of completion.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

Question 1 of 3. You are working on the drawings for a new military drone? In what type of SAP are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ Acquisition (correct response)
- ○ Operations and Support (O&S)
- ○ Intelligence

Feedback: *Programs that involve sensitive military technology, such as drones, fall under the Acquisition SAP category.*

Question 2 of 3. You are taking aerial pictures of a foreign manufacturing facility. In what type of SAP are you most likely working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acquisition
- ○ Operations and Support (O&S)
- ⦿ Intelligence (correct response)

Feedback: *Programs that protect the planning and execution of especially sensitive intelligence or counterintelligence operations or collection activities fall under the Intelligence SAP category.*

Question 3 of 3. While huddled in a military tent in a war zone in a foreign country, you are discussing your strategic and tactical plans with squadron leaders. In what type of SAP are you operating?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acquisition
- ⦿ Operations and Support (O&S) (correct response)
- ○ Intelligence

Feedback: *Programs that ensure sensitive military operations are completed without disclosure fall under the Operations and Support SAP category.*

Review Activity 2

Question 1 of 3. Your SAP has the most restrictive congressional reporting requirements. For what type of SAP are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acknowledge
- ○ Unacknowledged
- ⦿ Unacknowledged – Waived (correct response)

Feedback: *Unacknowledged waived SAPs are unacknowledged SAPs for which the Secretary of Defense has waived applicable Congressional reporting requirements to select committee members.*

Question 2 of 3. You told your spouse that you are working on a Special Access Program but you did not provide any specific details about the program. For what type of SAP are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ Acknowledge (correct response)
- ○ Unacknowledged
- ○ Unacknowledged – Waived

Feedback: *Individuals who work in Acknowledged SAPs may acknowledge that they work for a SAP in general, such as to friends and family or in their resume, but they may not disclose program specifics.*

Question 3 of 3. The mere existence of the SAP you are working on is classified but it has the same congressional reporting requirements as a SAP whose purpose is openly known. For what type of SAP are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Acknowledge
- ⦿ Unacknowledged (correct response)
- ○ Unacknowledged - Waived

Feedback: *The existence, purpose and specific details of Unacknowledged Special Access Programs are classified but their congressional reporting requirements are the same as those for Acknowledged Special Access Programs.*

Review Activity 3

Question 1 of 3. The SAP facility in which you are working was set up for the next six months for an emergency military operation. In what type of SAP facility are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Special Access Program Facility (SAPF)
- ○ Special Access Program Working Area (SAPWA)
- ○ Special Access Program Compartmented Area (SAPCA)
- ⊙ Temporary Special Access Program Facility (T-SAPF) (correct response)
- ○ Special Access Program Temporary Secure Working Area (SAPTSWA)

Feedback: *T-SAPFs are used for contingency operations, emergencies, and tactical military operations of less than 1 year.*

Question 2 of 3. 3 You occasionally work in a SAP area that does not allow storage of SAP information, and is occasionally used by SCI briefed individuals for classified meetings. In what type of SAP facility are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Special Access Program Facility (SAPF)
- ○ Special Access Program Working Area (SAPWA)
- ○ Special Access Program Compartmented Area (SAPCA)
- ○ Temporary Special Access Program Facility (T-SAPF)
- ⊙ Special Access Program Temporary Secure Working Area (SAPTSWA) (correct response)

Feedback: *A SAPTSWA is used less than 40 hours per month and is approved for less than 1 year. SAP information may be discussed and processed or handled but may not be stored in a SAPTSWA.*

Question 3 of 3. Your program is located in a room within a SAPF shared by other programs. In what type of SAP facility are you working?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Special Access Program Facility (SAPF)
- ○ Special Access Program Working Area (SAPWA)
- ⊙ Special Access Program Compartmented Area (SAPCA) (correct response)
- ○ Temporary Special Access Program Facility (T-SAPF)
- ○ Special Access Program Temporary Secure Working Area (SAPTSWA)

Feedback: *A SAPCA is used when different compartmented programs share the same SAPF or SCIF, necessitating additional physical or operations security safeguards because not all personnel are cross-briefed. A SAPCA is approved for discussion, processing, manufacturing, testing and storage of SAP information. A SAPCA may be accredited with periodic re-inspections conducted at least every 3 years.*

Lesson 3 Review Activities

Review Activity 1

Who would approve temporary use of prohibited items in a SAP facility?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ PSO or GPM
- ⦿ PSO or SAO (correct response)
- ○ GPM or CA SAPCO

Feedback: *The PSO or SAO may approve prohibited items for special circumstances.*

Review Activity 2

Question 1 of 3. You must use white noise generators during SAP discussions to meet acoustical requirements if the area does not meet the requirement.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ True (correct response)
- ○ False

Feedback: *True. Use white noise generators during SAP discussions to meet acoustical requirements.*

Question 2 of 3. All SAP materials must be removed from areas or rooms after SAP meetings, conferences and discussions and prepared for secure transmission, storage or destruction.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ True (correct response)
- ○ False

Feedback: *True. All SAP materials must be removed from areas or rooms after SAP meetings, conferences and discussions and prepared for secure transmission, storage or destruction.*

Question 3 of 3. Visitors may enter a SAPF without a Visit Request as long as they have an escort.

Select True or False. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ True (correct response)
- ○ False

Feedback: *True. If the visitor's requisite SAP accesses cannot be verified, the visitor will not be allowed into the SAPF.*

Lesson 4 Review Activity

Review Activity 1

Which of the following items are allowed into SAP facilities if processed and approved by the PSO or CA SAPCO?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Review of SAPs Standard Operating Procedures
- ☑ Acknowledgement that requirement to protect SAP information is a lifelong obligation (correct response)
- ☐ Signing of debriefing acknowledgement portion of SAP Indoctrination Agreement
- ☐ Destruction of SAP Indoctrination Agreement 5 years after program is terminated or in accordance with agency directives

Feedback: *All of these are part of either the SAP indoctrination briefing or debriefing but only acknowledgement of your lifelong obligation to protect SAP is covered in both.*

Lesson 5 Review Activities

Review Activity 1

Question 1 of 3. Per E.O. 13526, who is authorized to determine the classification of SAP material?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Derivative Classifier
- ⦿ Original Classification Authority (OCA) (correct response)

Feedback: *Only the OCA is authorized to classify SAP material.*

Question 2 of 3. Whose classification decisions are recorded in the Security Classification Guide (SCG) for a SAP?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Derivative Classifier
- ⦿ Original Classification Authority (OCA) (correct response)

Feedback: *The OCA's classification decisions are recorded in the SCG for a SAP. Derivative classifiers use the SCG to derivatively classify new documents.*

Question 3 of 3. Who must receive training every two years?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ Derivative Classifier (correct response)
- ○ Original Classification Authority (OCA)

Feedback: *Derivative classifiers must receive derivative classification training every 2 years.*

Review Activity 2

Question 1 of 3. Which type of marking utilizes the program identifier (PID) abbreviation?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Overall classification or banner marking
- ⦿ Portion marking (correct response)
- ○ Classification Authority Block

Feedback: *You must include the PID in the SAP portion marks.*

Question 2 of 3. Where do you indicate who classified the document?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Overall classification or banner marking
- ○ Portion marking
- ⦿ Classification Authority Block (correct response)

Feedback: *You list the name, title and organization of the derivative classifier in the Classification Authority block under Classified by.*

Question 3 of 3. In what marking must you include the highest overall classification of a page?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ Overall classification or banner marking (correct response)
- ○ Portion marking
- ○ Classification Authority Block

Feedback: *You must include the highest level of classification on a page in the banner marking.*

Review Activity 3

For what types of publications must you request SAPCO approval before releasing any SAP information?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☑ Books (correct response)
- ☑ Articles (correct response)
- ☑ Blog posts (correct response)
- ☑ Speeches (correct response)

Feedback: *You must request SAPCO approval before releasing any SAP information to the public in any form, whether it is in a book, an article, a blog post, and speech or any other form of disclosure to the public.*

Lesson 6 Review Activities

Review Activity 1

Question 1 of 4. At which of the classification levels is it permitted to transmit SAP information via USPS Priority Mail Express with SAPCO approval?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Top Secret
- ☑ Secret (correct response)
- ☑ Confidential (correct response)

Feedback: *Secret and Confidential SAP material can be transmitted via USPS Priority Mail Express with SAPCO approval.*

Question 2 of 4. At which classification level(s) is it permitted to transmit SAP information via secure fax?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☑ Top Secret (correct response)
- ☑ Secret (correct response)
- ☑ Confidential (correct response)

Feedback: *SAP information may be transmitted via secure approved fax machine at all three levels.*

Question 3 of 4. At which classification level(s) is it permitted to transmit SAP information via USPS Certified mail?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Top Secret
- ☐ Secret
- ☑ Confidential (correct response)

Feedback: *Confidential SAP information may be sent via USPS Certified mail.*

Question 4 of 4. At which classification level(s) is it permitted to transmit SAP information via a USG approved contract carrier with PSO approval and only within CONUS?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Top Secret
- ☑ Secret (correct response)

☑ Confidential (correct response)

Feedback: *Secret and Confidential SAP material can be transmitted via USG approved contract carriers with PSO approval and can only be used within CONUS.*

Review Activity 2

Question 1 of 4. All Top Secret collateral and SAP information is considered "accountable."

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

⦿ True (correct response)

○ False

Feedback: *All Top Secret collateral and SAP information is considered "accountable" according to DoDM 5205.07.*

Question 2 of 4. SAP Accountability System is required for Top Secret SAP documents only.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

○ True

⦿ False (correct response)

Feedback*: The SAP Accountability System is required for all Top Secret SAP material, media, hardware, equipment; Secret SAP material, media, hardware, equipment when directed by the CA SAPCO; and all other classified media when directed by the CA SAPCO.*

Question 3 of 4. Identification and documentation of SAP materials includes the custodian, date created/destroyed classification, program sensitivity, item type and content.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

⦿ True (correct response)

○ False

Feedback: *Identification and documentation of SAP materials includes the custodian, date created/destroyed classification, program sensitivity, item type and content.*

Question 4 of 4. The accountability system is designed to record all transactions of handling, receipt, generation, reproduction, dispatch, or destruction.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ True (correct response)
- ○ False

Feedback: *The accountability system is designed to record all transactions of handling, receipt, generation, reproduction, dispatch, or destruction.*

Review Activity 3

Question 1 of 4. Any copier located in the program office can be used for Top Secret, Secret, and Confidential SAP documents.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ⦿ False (correct response)

Feedback: *Only approved copiers have a sign posted stating the highest level of information authorized.*

Question 2 of 4. Unclassified Handle Via Special Access Channels Only (HVSACO) material can be copied on unclassified copiers.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ⦿ False (correct response)

Feedback: *Unclassified HVSACO material CANNOT be copied on unclassified copiers.*

Question 3 of 4. Accountable SAP material destruction requires using two SAP-briefed employees with access to the level of material being destroyed.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ True (correct response)
- ○ False

Feedback: *Accountable SAP material destruction requires using two SAP-briefed employees with access to the level of material being destroyed.*

Question 4 of 4. Non-accountable SAP material typically does not require a destruction certificate.

Select True or False for the statement. Then check your answer in the Answer Key at the end of this Student Guide.

- ⦿ True (correct response)
- ○ False

Feedback: *Non-accountable SAP material does not require a destruction certificate, unless the Program SCG directs otherwise.*

Lesson 7 Review Activities

Review Activity 1

Which of the following are measures to prevent adversaries from piecing together sensitive unclassified information?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☑ Limit unauthorized disclosure via the Internet and social media (correct response)
- ☑ Be conscious of discussion in unclassified areas (correct response)
- ☑ Secure credentials when departing the work site (correct response)
- ☑ Do not include, or even allude to, classified and or sensitive information in a resume, personnel review, or publication (correct response)
- ☐ Determine whether anyone around you might be interested in the technical and operational activities of your program prior to discussing them.

Feedback: *You can prevent adversaries' ability to piece together a puzzle by limiting unauthorized disclosure via internet/social media and securing your credentials when departing your work site. Always be conscious of your discussions in unclassified areas. Do not include, or even allude to, classified and or sensitive information concerning programs, program activities, and operations, whether on a resume, in a personnel review, or in a publication.*

Review Activity 2

Which of the following are core functional area activities for SAP compliance inspections?

Select all that apply; then check your answer in the Answer Key at the end of this Student Guide.

- ☑ TS SAP data and materials are properly accounted for (correct response)
- ☑ Personnel completion of the required annual education and awareness training (correct response)
- ☑ Completion of Special Access Program Nomination Process within 365 days and update annually (correct response)
- ☑ Ensure execution of the corrective action plan resulting from a SAP inspection report as part of security management and oversight (correct response)
- ☑ Conduct a cybersecurity inspection to ensure all media is controlled (correct response)
- ☑ Ensure the SF 702, Security Container Checksheet, is completed (correct response)

Feedback: *All of these are core functional area activities addressed in SAP compliance inspections*