Student Guide

Course: Special Access Program (SAP) Overview

Lesson 1: Course Introduction

1. Course Information

Purpose	Provide an overview of the SAP environment, including its history and purpose, lifecycle, approval process, and roles and responsibilities.
Audience	Military, civilian, and contractor personnel working in support of DoD Special Access Programs (SAPs)
Pass/Fail %	80%
Estimated completion time	90 minutes

2. Course Overview

Special Access Programs, referred to as SAPs, aim to protect national security by employing enhanced security measures to strictly enforce need-to-know. They also have safeguarding and access requirements that exceed those normally required for information at the same classification level.

In this course, you will learn why we have SAPs, how they are authorized, and the basics of how they operate. This course will look at the policy documents governing SAPs and the many agencies and individuals involved in SAP oversight and support.

3. Course Objectives

Here are the course objectives:

- Identify the definition, purpose, and history of SAPs
- Identify key SAP policy documents
- Identify the categories and types of SAPs
- Identify the steps in the SAP approval process
- Identify the roles and responsibilities involved in the SAP approval process
- Identify the steps in the SAP lifecycle (establishment, management and administration, apportionment, and disestablishment)
- Identify operations, oversight, and support roles and responsibilities

4. Course Structure

This course is organized into the lessons listed below:

- Course Introduction
- Introduction to Special Access Programs
- SAP Lifecycle and Structure
- SAP Approval
- SAP Operations
- Course Conclusion

Student Guide

Course: Special Access Program (SAP) Overview

Lesson 2: Introduction to Special Access Programs

Introduction

Throughout our nation's history, our military and strategic advantage hasrelied 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 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.

Objectives

The lesson objective is:

- Identify the definition, purpose, and history of Special Access Programs (SAPs)

What are Special Access Programs?

1. Definition

Executive Order 13526, "Classified National Security Information," defines a SAP as "a program established for a specific class of classified information that imposes safeguarding and access requirements exceeding those normally required for information at the same classification level."

SAPs are established only when the program is required by statute, or upon the finding of exceptional vulnerability of, or threat to, specific information, and if the normal criteria for determining access to information classified at the same level are insufficient.

SAPs use the standard levels of classified information; that is, Top Secret, Secret, and Confidential. SAPs also require an assigned nickname and/or codeword and identification of any special handling procedures.

In simplest terms, a SAP is a classified program with enhanced safeguarding and access requirements.

2. History of SAPs

SAPs have existed for many years, though they have not always been called SAPs. It was not until the 1980s that their existence was publicly acknowledged.

They were originally established to protect DoD acquisition programs and often used to hide sensitive operations. Through the 1980s, these programs were referred to as "Black Programs" and were generally restricted to protecting DoD acquisition programs. They were "Black Programs" due to the fact they were close-hold, people were unaware of their existence, and were conducted in tight-knit organizations.

When a controversial covert special operations activity called "Yellow Fruit" became public in the 1980s, it became apparent that there was a need to significantly increase the oversight of these programs.

During the 1990s, the term *Special Access Program* replaced *Black Program*. SAP security procedures were modified to include the protection of not just DoD acquisition programs, but also intelligence programs and operations and support programs.

a. Greenbrier Hotel

The Greenbrier Hotel is located in the mountains of West Virginia. Built at the request of Congress in the late 1950s and early 1960s, the hotel's purpose was to function as a safe haven for members of Congress in the event of a nuclear attack on the U.S.

Its construction posed many challenges and serves as an example of the unique challenges facing SAP security officials as they strive to protect SAP assets.

Greenbrier Hotel:
- Construction: Began 1958, completed 1961
- Cost: $86,000,000
- Public became aware: 1992

Unique program challenges:
- 50,000 tons of concrete used
- Removal of several tons of dirt and rock
- Movement of underground rivers
- Excessive noise around site
- 1,000+ personnel involved

b. Black Programs

Up through the 1980s, SAPs were referred to as Black Programs. They largely protected DoD acquisition programs. Well-known Black Programs include Skunk Works, the code name for Lockheed Martin's Advanced Development Programs. Skunk Works is responsible for the design of many famous and technologically advanced aircrafts, including the F-117A Nighthawk stealth fighter.

Black Programs (1980s):
- Protected DoD acquisition programs
- Example: Skunk Works and the F117A stealth fighter

c. Yellow Fruit

Yellow Fruit was the code name for a U.S. Army operation that was conducting work for the Army and Iran Contra. However, allegedly illegal misuse of funds drew the attention of not only the Army's Joint Chief of Staff, but Congress as well.

The operation led to investigations about the mismanagement of some $300 million in black operations funds over a five-year period. Investigations into the spending led to the court martial of three Army officers and a sergeant. In the most severe punishment, one of the accused was sentenced to 10 years in prison, fined $50,000, ordered to forfeit over $35,000 in salary, and dismissed from the service. Military court later reversed the conviction, citing little guidance from higher echelons concerning the handling of funds.

Following the Yellow Fruit operation and controversy, oversight for SAPs increased significantly.

Yellow Fruit:
- Alleged illegal use of funds
- Investigation led to court martial and imprisonment of personnel
- Further investigation revealed lack of oversight
- Led to greater oversight of SAPs

d. Special Access Programs (SAPs)

During the 1990s, Black Programs became SAPs. Security procedures were modified significantly and included increased oversight. SAP operations expanded to include intelligence and operations and support programs in addition to acquisition programs.

During 1990s, SAP security procedures were modified:
- Increased oversight
- Inclusion of intelligence and operations and support programs

Why Do We Have SAPs?

1. Misperceptions versus Reality

In 1983, an Army civilian stumbled onto billing irregularities at a U.S. intelligence front company that was handling secret supplies for Central America. The discovery led to the uncovering of the Yellow Fruit operation.

Given the circumstances of operations like Yellow Fruit, it is not surprising that misperceptions about SAPs exist. There are several common misperceptions about SAPs.

First, many believe SAPs are used as a means to hide money spent on certain programs. SAPs are *not* a place to hide money; they are used to ensure the security and accountability of a specific project is maintained to the highest level.

Another misperception is that SAPs are used to avoid taxpayer scrutiny. That is also not true. In fact, taxpayer understanding and awareness is often a key to an acknowledged program's success.

SAPs are also believed to lack Congressional oversight. However, following Yellow Fruit, Congressional oversight increased significantly and now requires reports on every DoD SAP be submitted to Congress annually.

2. Importance

Designed and built so that it cannot be detected by radar, the F-117A stealth fighter dramatically changed U.S. strategic advantage. During Operation Desert Storm, the F-117A made up only two percent of the sorties, yet accounted for forty percent of the bomb damage. The importance and power of what can be accomplished through the use of SAPs *should not* be understated.

SAPs are important for several reasons. Some SAPs protect technology breakthroughs and ensure the U.S. maintains its leading technological edge. Some SAPs ensure once we discover and exploit an adversary's vulnerabilities, the knowledge of the exploitation remains secure and the adversary does not develop a countermeasure. Some SAPs also ensure sensitive operational plans are completed without disclosure. Of equal importance, some SAPs protect intelligence information, which is often the key to a successful mission. Reducing the amount of intelligence gathered on U.S. forces significantly enhances our success on the battlefield.

3. Goals

In 1987, the USSR began deployment of the MiG-29 to its allies. It bore a striking resemblance to the U.S. F-15. In fact, we have several examples of the Russians emulating U.S. military jets. *How does this happen?*

In the late 1970s and early 1980s, the U.S. spent well over a million dollars developing the technology to allow aircraft to transport the space shuttle. Just a few years later, the Russians "borrowed" our technology, requiring far less research and development dollars. *How did this happen?*

In 2001, former FBI agent Robert Hanssen was arrested for selling American secrets to Russia. During his liaison with the DoD, Mr. Hanssen had access to SAPs. However, because of the accountability mechanism built into the SAP environment, it could easily be determined when and to what programs Mr. Hanssen had access. Such measures are essential to knowing the people involved in your programs and help facilitate damage assessment when necessary.

We have established SAPs due in part for the need for enhanced measures to protect our national security. SAPs employ enhanced security measures beyond those required in baseline regulations and directives. To protect the work of SAPs, the number of personnel who have access to a SAP is kept to an absolute minimum. If an individual will not materially and directly contribute to a SAP, that person is not authorized access. Access to SAPs is not granted on a convenience basis. In addition, records of individuals who have or have had access to a SAP are maintained. This record-keeping capability far exceeds what is required for collateral programs. An individual's *need-to-know* is a key piece of maintaining the security of SAPs.

Need-to-know

1. What is Need-to-know?

Brian Patrick Regan, a retired U.S. Air Force Sergeant, asked questions about information he did not need to know about, and subsequently sold detailed, comprehensive classified documents and photos containing U.S. reconnaissance mission information to China, Iraq, and Libya. This act caused a grave risk of death to U.S. Air Force reconnaissance pilots.

Need-to-know is a fundamental principle in the protection of classified information and the protection of SAPs. It is not enough just to have the appropriate clearance and formal approval to access a SAP. In addition, a person must have a need- to-know that pertains to the specific information.

Take a look at the formal definition of need-to-know: Determination made by an authorized holder of classified information that a prospective recipient requires access in order to perform or assist in a lawful and authorized governmental function.

The *authorized holder of classified information* is you. You are responsible for determining whether someone does or does not legitimately *require access* to the information you have in order to perform or assist in a lawful and authorized governmental function.

You must also make sure that person has the *appropriate clearance* for the information. You are obligated to ask for sufficient information so you can make an informed decision whether or not to share your classified information with the requestor. Don't assume when someone asks you for information that he or she has a legitimate need-to-know.

Verify that individual needs the information specifically to do their work, they have the appropriate clearance, and that someone in a position of authority has given them the permission to access the information. If you are unsure of someone's need-to-know, withhold your information until you can establish the need-to-know is legitimate.

2. Sample Situations

Consider this situation: Ted tells you he is working as a database administrator on a project similar to yours. Ted is curious to see if your project uses some of the same data as his, and he asks to see your database, which is classified.

Does Ted have a valid need-to-know?

No. Ted does *not* have a valid need-to-know that would justify his seeing your classified materials. Even though he is working on a similar project, he has no need to work with your information as part of his job, and no one has authorized him to see it. Sharing it with him could compromise the information. You don't know what he will do with it.

Now consider this: Ann's supervisor tells you that Ann has been assigned to your project as a technical writer and will need access to all your project materials. Ann later asks to see your project plan, which is classified.

Does Ann have a valid need-to-know?

Yes. Ann *does* have a valid security clearance and need-to-know, because she has been authorized by her supervisor to work on your project and to have access to all of your project materials, whether classified or not. Because her supervisor has told you directly about this authorization, there is no reason to suspect that Ann will compromise the information.

Review Activity 1

Which of the following do SAPs aim to achieve? *Select all that apply; then check your answers in the Answer Key at the end of this Student Guide.*

- ☐ Protect technological breakthroughs
- ☐ Cover exploitation of adversary vulnerabilities
- ☐ Protect sensitive operational plans
- ☐ Reduce intelligence on U.S. force capabilities

Review Activity 2

You are preparing to start work on a SAP. How much do you know about these programs? *Select True or False for each statement; then check your answer in the Answer Key at the end of this Student Guide.*

	True	False
The SAP for your project was likely formed to hide the money that will be spent.	○	○
Because you will be working on a SAP, you can expect the oversight to be much greater than the collateral programs you've worked on in the past.	○	○
You should expect to work using enhanced security measures.	○	○
Access to your program will be kept to an absolute minimum.	○	○

Answer Key

Review Activity 1

Which of the following do SAPs aim to achieve?

- ☑ Protect technological breakthroughs
- ☑ Cover exploitation of adversary vulnerabilities
- ☑ Protect sensitive operational plans
- ☑ Reduce intelligence on U.S. force capabilities

Review Activity 2

	True	False
The SAP for your project was likely formed to hide the money that will be spent.	○	●
Because you will be working on a SAP, you can expect the oversight to be much greater than the collateral programs you've worked on in the past.	●	○
You should expect to work using enhanced security measures.	●	○
Access to your program will be kept to an absolute minimum.	●	○

Student Guide

Course: Special Access Program (SAP) Overview

Lesson 3: SAP Lifecycle and Structure

Introduction

Objectives

Special Access Programs (SAPs) can vary widely in the types of missions and operations they fulfill. However, all DoD SAPs must be categorized by type and they all follow the same lifecycle. This lesson will familiarize you with types of SAPs and the SAP lifecycle.

The lesson objectives are:

- Identify the protection levels and categories of SAPs
- Identify the steps in the SAP lifecycle

SAP Regulatory Structure

Oversight

As you learned earlier in this course, the Yellow Fruit investigation led to many changes in how the U.S. deals with its most sensitive operations and programs. Following the Yellow Fruit episode, new measures and safeguards were put in place, including expanded oversight measures. As a result, the oversight provided to DoD SAPs is *much* more significant than that given to collateral programs. SAP oversight is outlined in Section 119, Title 10 United States Code, and includes the requirement to report annually to Congress.

Section 119 of Title 10 specifies the types of reports that are submitted to Congress as well as the frequency with which they are submitted.

Existing SAPs must submit a report to Congress no later than March 1 of each year.

Reports for existing SAPs include:

- The estimated total budget requested for the current and next fiscal years
- A brief description of the program, including the numbers of individuals involved
- A brief discussion of the major milestones for the SAP, such as current issues or significant changes
- The actual cost of the program for each previous fiscal year

New or proposed SAPs must submit a SAP Listing to Congress no later than February 1 of each year. The report includes:

- Notice of the designation of the program as a SAP and the justification for such designation
- The current estimate of the total cost for the program
- Identification of existing programs or technologies that are similar to the new SAP's technology or mission

Types of SAPs

1. Protection Levels

SAPs are categorized both by how they are protected and acknowledged, referred to as a SAP *protection level*, and by the *type* of program they encompass, referred to as a SAP *category*. Every SAP within the DoD will fall under both a protection level and a category.

A *protection level* communicates how the 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.

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. The funding for acknowledged SAPs is generally unclassified.

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 as dictated by their vulnerability to exploitation and the risk of compromise. The program funding for unacknowledged SAPs is often classified, unacknowledged, or not directly linked to the program.

Under extremely limited circumstances, unacknowledged SAPs may also be *waived*. Waived SAPs are unacknowledged SAPs for which the Secretary of Defense has waived applicable reporting requirements under Section 119, Title 10 U.S. Code. Waived SAPs have *more* restrictive reporting requirements and access controls.

2. SAP Categories

While all SAPs fall under a protection level, all SAPs also fall under one of three possible categories. As with protection levels, the category to which a SAP is assigned impacts its oversight and operation. You'll learn more about that later in this course.

For now, you should know approximately 75 to 80 percent of all DoD SAPs are *acquisition* SAPs. Acquisition SAPS are established to protect sensitive research, development, testing and evaluation, modification, and procurement activities. They involve buying or building something, such as a weapons system or aircraft. The vast majority of SAPs are acquisition SAPs. Other SAPs are *intelligence* SAPs. Intelligence SAPs are established primarily to protect the planning and execution of especially sensitive intelligence or CI operations or collection activities. They are generally associated with the intelligence community. Finally, *operations and support* SAPs are established primarily to protect the planning for execution of and support to especially sensitive military operations. They often involve the use of soldiers, sailors, airmen, and marines and they may protect organizations, property, operations, concepts, plans or activities.

SAPs are referred to using both their protection level and category; you may see acknowledged acquisition SAPs, unacknowledged intelligence SAPs, unacknowledged waived operations, and support SAPs, or any other combination.

SAP Lifecycle

1. Overview

All SAPs within the DoD follow the same lifecycle regardless of their category or protection level. SAPs begin in the *establishment* phase. In this phase, it is determined whether or not extra protection is warranted to establish a Prospective SAP (PSAP). The establishing SAPCO must notify the Director, DoD SAPCO, in writing of the decision to create a PSAP. Here, documents are created to ensure the SAP's protection, and the program's eligibility to become a SAP is evaluated through the approval process.

Once approved, the SAP operates within the *Management and Administration* phase. It is here that the work of the SAP is accomplished as long as there is a continued need for the SAP. The SAP continues to follow the appropriate processes and procedures throughout its operation.

Annually, one of three things will happen to every SAP within the DoD: revalidation, apportionment and deapportionment, or disestablishment. Once a SAP is no longer needed, it moves to the *disestablishment* phase.

a. Establishment

When a program is initially considered for SAP eligibility, the first consideration is to determine if it meets the basic SAP requirements.

The criteria outlined in DoDM 5200.01, Volume 1, DoD Information Security Program, is utilized.

Historical examples and past lessons learned should be evaluated. Operations Security (OPSEC) must be considered. For example, what would happen if the enemy got a hold of the program's information or technology? What kind of damage would it do?

If it is determined that the threat to the program is exceptional and enhanced security measures are necessary, the program can move to the next phase of the lifecycle.

b. Management and Administration

Once the program is granted approval as a SAP, it moves to the *Management and Administration* phase. Here, the SAP's work is accomplished. This is the day-to-day operation of the SAP. The program undergoes inspections, audits, and internal control. Each year one of three things will happen to every DoD SAP: the SAP will be revalidated and continue its work, apportioned, or transitioned to the *Disestablishment* phase.

c. Apportionment

Apportionment means that a SAP or section of a SAP has been formally included in the Integrated Joint Special Technical Operations (IJSTO) process for Combatant Commands use during deliberate planning, crisis action response, and operational employment.

During the SAP *Apportionment* phase, the DoD Component and PSA SAPCOs nominate SAP capabilities to be apportioned into IJSTO when they are deemed operational capability or no later than 18 months prior to plan IOC.

The *Apportionment* phase has the following: a program Quad Chart, a program fact sheet, indoctrination briefing, an SCG, a written legal review, and a PID and nickname.

d. Disestablishment

Once the SAP is no longer needed, it is disestablished. This may be due to the program transitioning to a collateral program or by being absorbed into another existing SAP. Disestablishment includes ensuring the SAP's information and related SAPs are protected, a disestablishment plan is developed, a debrief of personnel, and a closeout inspection are conducted.

Review Activity 1

Program XYZ involves the gathering of information regarding active terrorist groups. There have been public hearings regarding the purpose of this SAP. This is most likely an example of what type of SAP?

Select the best answer; then check your answers in the Answer Key at the end of this Student Guide.

- ○ Acknowledged Acquisition
- ○ Unacknowledged Acquisition
- ○ Acknowledged Intelligence
- ○ Unacknowledged Intelligence
- ○ Acknowledged Operations and Support
- ○ Unacknowledged Operations and Support

Review Activity 2

Program ABC is in the process of developing a super-secret new technology that could completely revolutionize the way that wars are fought. The name of the program remains classified and its funding is associated with a different program. This is most likely an example of what type of SAP?

Select the best answer; then check your answers in the Answer Key at the end of this Student Guide.

- ○ Acknowledged Acquisition
- ○ Unacknowledged Acquisition
- ○ Acknowledged Intelligence
- ○ Unacknowledged Intelligence
- ○ Acknowledged Operations and Support
- ○ Unacknowledged Operations and Support

Review Activity 3

Program Alpha exists to provide logistical assistance to a covert military operation in a turbulent foreign country. Its funding is classified and the program is subject to stricter reporting requirements and access controls. This is most likely an example of what type of SAP?

Select the best answer; then check your answers in the Answer Key at the end of this Student Guide.

- ○ Acknowledged Acquisition
- ○ Unacknowledged Acquisition
- ○ Acknowledged Intelligence
- ○ Unacknowledged Intelligence
- ○ Acknowledged Operations and Support
- ○ Unacknowledged Operations and Support

Review Activity 4

Match each phase of the SAP lifecycle on the left to its matching description on the right; then check your answers in the Answer Key at the end of this Student Guide.

A. Management & Administration	___	…Extra protection warranted?
B. Establishment	___	…continued need? Processes followed?
C. Apportionment	___	…proper measures in place? Approval received?
D. Disestablishment	___	…program no longer needed?

Answer Key

Review Activity 1

Program XYZ involves the gathering of information regarding active terrorist groups. There have been public hearings regarding the purpose of this SAP. This is most likely an example of what type of SAP?

- ○ Acknowledged Acquisition
- ○ Unacknowledged Acquisition
- ◉ Acknowledged Intelligence
- ○ Unacknowledged Intelligence
- ○ Acknowledged Operations and Support
- ○ Unacknowledged Operations and Support

Review Activity 2

Program ABC is in the process of developing a super-secret new technology that could completely revolutionize the way that wars are fought. The name of the program remains classified and its funding is associated with a different program. This is most likely an example of what type of SAP?

- ○ Acknowledged Acquisition
- ◉ Unacknowledged Acquisition
- ○ Acknowledged Intelligence
- ○ Unacknowledged Intelligence
- ○ Acknowledged Operations and Support
- ○ Unacknowledged Operations and Support

Review Activity 3

Program Alpha exists to provide logistical assistance to a covert military operation in a turbulent foreign country. Its funding is classified and the program is subject to stricter reporting requirements and access controls. This is most likely an example of what type of SAP?

- ○ Acknowledged Acquisition
- ○ Unacknowledged Acquisition
- ○ Acknowledged Intelligence
- ○ Unacknowledged Intelligence
- ○ Acknowledged Operations and Support
- ◉ Unacknowledged Operations and Support

Review Activity 4

Match each phase of the SAP lifecycle on the left to its matching description on the right; then check your answers in the Answer Key at the end of this Student Guide.

A. Management & Administration	B	…Extra protection warranted?
B. Establishment	A	…continued need? Processes followed?
C. Apportionment	C	…proper measures in place? Approval received
D. Disestablishment	D	…program no longer needed?

Student Guide

Course: Special Access Program (SAP) Overview

Lesson 4: SAP Approval

Introduction

Objectives

Before becoming a Special Access Program (SAP), a program must follow a standard process to ensure it meets SAP requirements. In this lesson, you will learn about SAP approval and about the roles and responsibilities involved.

The lesson objectives are:

- Identify the steps in the SAP approval process
- Identify the roles and responsibilities involved in the SAP approval process

SAP Approval Overview

1. SAP Approval Authorities

Due to their importance and the sensitivity of their operations, SAPs are approved only at the highest levels. Unless otherwise directed by the President of the United States, only the Secretaries of State, Defense, Energy, Homeland Security, and the Director of National Intelligence, and the Attorney General (or their principal deputies) are authorized to approve SAPs.

Although all of these agencies have SAPs, they do not all establish and operate them in the same way as the Department of Defense, but they do work together. In cases of joint programs, the host activity ensures regulatory requirements are met by the other involved agencies.

This lesson focuses on the implementation of SAPs within the Department of Defense, which has designated primary and direct responsibility for SAPs to the Deputy Secretary of Defense (DEPSECDEF).

2. Approval Process

When the need for a SAP is identified, there is a specific process the program must follow before becoming a SAP. The initial need for a SAP can be identified and initiated anywhere: within the government, which includes civilians and warfighters alike, or within industry. Whether identified by government or industry, each need is first assessed.

When it is determined enhanced security measures are required, it is then the Establishment process begins. The program is referred to as a prospective SAP (PSAP). Upon PSAP approval enhanced security measures may be applied for a period not to exceed 210 days.

While in the Establishment phase, all documents required for a program to be approved as a SAP are developed. Together, these documents make up the SAP Approval package. Once all the documents are developed, the Approval Package is sent to the SAP Oversight Committee (SAPOC) for concurrence or non-concurrence.

Then the SAP approval package goes to Congress for formal approval. Let's take a closer look at the entities involved in this process.

Roles in SAP Approval

1. Overview

Even though the Deputy Secretary of Defense approves every SAP within the Department of Defense, the process relies upon several entities. The SAP governance structure is comprised of the SAPOC, the SRG, and the SSWG. The governance process relies upon personnel making the determination that the need for a SAP exists. You learned about this in an earlier discussion of the SAP lifecycle. Next, the process relies upon the examination into and justification for the need for a SAP. If the need is justified, then it moves into the Establishment phase, also called a PSAP.

During the Establishment phase, all the required documents to identify how that widget or piece of technology is going to be protected are developed. Once all the documents are developed, they are packaged together and sent to the SAPOC for concurrence. Finally, once a SAP is approved by the SECDEF/DEPSECDEF, Congress needs to be notified.

We'll look at each of these entities and the roles they play in a moment. A job aid that describes these roles at a high level is available at the end of the lesson.

2. Component-Level SAP Central Office

When the need for a SAP is initially identified, it is the component-level Special Access Program Central Office, also referred to as SAPCO, which assesses the need.

Component-level SAPCOs exist for:

- Each military component
- The Joint Chiefs of Staff
- The Defense Advanced Research Projects Agency (DARPA)
- The Missile Defense Agency (MDA)

Each component-level SAPCO is responsible for all SAPs under their purview.

3. OSD-level SAP Central Office

DoD SAPs are categorized and managed by the Under Secretaries of Defense. Each OSD-level SAP Central Office is established to assist the Deputy Secretary of Defense in overseeing DoD SAPs. Each Under Secretary serves as the oversight authority for a specific category of SAPs: acquisition, intelligence, or operations and support.

All acquisition SAPs are assigned to the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. All intelligence SAPs are assigned to the Office of the Under Secretary of Defense for Intelligence. Finally, all operations and

support SAPs are assigned to the Office of the Under Secretary of Defense for Policy.

4. Senior Review Group (SRG)

The Senior Review Group is a senior executive service-level working group that is responsible for ensuring SAPs aren't duplicated across the various SAP categories.

Senior Review Group members include:

- Chair: Under Secretary of Defense for AT&L
- Vice Chair: The Director, DoD SAPCO
- Executive Secretary: The Deputy Director, DoD SAPCO
- General Membership: The SRG comprises the primary or alternate members, designated in writing by each SAPOC member. Only designated SRG members have voting rights within this body; however, in the case of the Army, Navy, and Air Force, only one individual will represent their respective Under Secretary and Vice Chief of Staff (one vote per Military Department). Additional appropriately cleared personnel may attend if approved by the SRG Chair.

5. Senior SAP Working Group

The Senior SAP Working Group (SSWG) is a new group added to serve as the senior program protection forum to coordinate, deconflict, and integrate special programs; address SAP policy, oversight, and management, and provide recommendations to the SRG. The members are listed below. Also note the SSWG Chair may approve additional attendance of appropriately cleared personnel.

Senior SAP Working Group Members include:

- Director, DoD SAPCO – Chair
- SAPCO Directors of the USD (I), USD (AT&L), Army, Air Force, Navy, Marine Corps, JS, DARPA, and MDA
- The principal-appointed representatives from the offices of the DCAPE; the DoD CIO; the USD(C)/CFO and the GC, DoD

6. Special Access Program Oversight Committee (SAPOC)

Chaired by the Deputy Secretary of Defense, the SAPOC is where the formal SAP approval decision is made. SAPOC members are considered super users and have access to all DoD-approved SAPs. With exception of the Vice Chairman of the Joint Chiefs of Staff, all committee members are appointed officials of the DoD.

SAPOC members include:

- Chair: The DepSecDef
- Vice-Chair: The USD(AT&L)
- Executive Secretary: The Director, DoD SAPCO
- General Membership
    - USD(P)
    - USD(Comptroller)/Chief Financial Officer, DoD (USD(C)/CFO)
    - USD(I)
    - Under Secretary of Defense for Personnel and Readiness
    - Vice Chairman of the Joint Chiefs of Staff
    - Assistant Secretary of Defense for Networks & Information Integration [ASD(NII)]/DoD Chief Information Officer (DoD CIO)

- General Counsel of the Department of Defense (GC, DoD)
- Director, Cost Assessment and Program Evaluation (DCAPE)
- Under Secretaries for the Departments of the Army, Navy, and Air Force
- Vice Chiefs of Staff of the Army and the Air Force
- Vice Chief of Naval Operations
- Assistant Commandant of the Marine Corps

7. DoD SAP Central Office

Once an agreement has been reached, it is the DoD SAPCO that communicates this concurrence to Congress for approval. The DoD SAPCO serves many functions. The SAPCO develops, coordinates, and publishes policy and is the main point of contact for DoD SAP resources.

The director of the DoD SAPCO is the head of the Acquisition SAPCO, the Under Secretary of Defense for Acquisition, Technology, and Logistics. In addition to the executive secretary serving on the SAPOC, the SAPCO director is also the primary point of contact with agencies of the executive branch, Congress, and the DoD components on all issues relating to DoD SAPs. This ensures that the DoD speaks to Congress about SAPs using one voice.

When concurrence has been reached by the SAPOC, it is the DoD SAPCO that notifies Congress.

8. Congressional Committees

While Congress is notified of all approved SAPs, not *all* members of Congress have access to SAP information. Only members of the Authorization and Appropriations Committees and their Defense Subcommittees are authorized access to SAPs. The appropriate intelligence committees receive notification of approved intelligence SAPs.

Authorization Committees:

- House Armed Services Committee (HASC)
- Senate Armed Services Committee (SASC)

Appropriations Committees:

- House Appropriations Committee (HAC)
- Senate Appropriations Committee (SAC)
- Defense Subcommittees of HAC and SAC

Intelligence Committees:

- House Permanent Select Committee on Intelligence (HPSCI)
- Senate Select Committee on Intelligence (SSCI)

Roles in SAP Approval Job Aid

Role	Responsibility
Component-Level SAPCO	• Manage and oversee SAPs • Maintain records and list of SAP facilities • Each SAPCO is responsible for all the SAPs under their purview • Exist for: – Each military component – Joint Chiefs of Staff – Defense Advanced Research Projects Agency (DARPA) – Missile Defense Agency (MDA)
Office of the Secretary of Defense-Level SAPCO	Each OSD-level SAP Central Office: • Is the oversight authority for the SAP category under their purview • Is established to assist the Deputy Secretary of Defense in overseeing DoD SAPs • Serves as the oversight authority for a specific category of SAPs: Acquisition, Intelligence, or Operations and Support • All Acquisition SAPs are assigned to the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L) • All Intelligence SAPs are assigned to the Office of the Under Secretary of Defense for Intelligence (USDI) • All Operations and Support SAPs are assigned to the Office of the Under Secretary of Defense for Policy (USDP)
Senior Review Group	• Is the principal working-level body executing the governance process and performing oversight and management of DoD SAPs. • Unanimous recommendations of the SRG may be forwarded directly to the DepSecDef for decision.
SAPOC	• Is chaired by the Deputy Secretary of Defense • Is where the formal SAP approval decision is made
DoD SAP Central Office	• Develops, coordinates, and publishes policy • Is principal DoD point of contact for all SAP resources • Director serves as Executive Secretary SAPOC • Is the DoD SAP legislative liaison • Ensures “one voice” to Congress
SAP Senior Working Group	• Serves as the senior program protection forum to coordinate, deconflict, and integrate special programs • Addresses SAP policy, oversight, and management • Provides recommendations to the SRG

Review Activity 1

Match each role of SAP approval on the left to its matching description on the right, then check your answers in the Answer Key at the end of this Student Guide.

A. Component-level SAP Central Offices	__ DoD SAP legislative liaison that notifies Congress of SAP approval
B. Special Access Program Oversight Committee (SAPOC)	__ Ensure there are no duplicative efforts across SAPs
C. Senior Review Group (SRG)	__ The final SAP approving body chaired by the Deputy Secretary of Defense
D. DoD Special Access Central Office (SAPCO)	__ Exercise oversight authority for the specific SAP category under their purview
E. Authorization, Appropriations, and Intelligence Congressional	__ Congressional committees granted SAP access
F. OSD-level SAP Central Offices	__ Exist for each military component, the Joint Chiefs of Staff, Defense Advanced Research Projects Agency (DARPA), and Missile Defense Agency (MDA)

Answer Key

Review Activity 1

A. Component-level SAP Central Offices	D DoD SAP legislative liaison that notifies Congress of SAP approval
B. Special Access Program Oversight Committee (SAPOC)	C Ensure there are no duplicative efforts across SAPs
C. Senior Review Group (SRG)	B Functions as the SAP governance, management, and oversight committee and will advise the SecDef and DepSecDef
D. DoD Special Access Central Office (SAPCO)	F Exercise oversight authority for the specific SAP category under their purview

E. Authorization, Appropriations, and Intelligence Congressional	E	Congressional committees granted SAP access
F. OSD-level SAP Central Offices	A	Exist for each military component, the Joint Chiefs of Staff, Defense Advanced Research Projects Agency (DARPA), and Missile Defense Agency (MDA)

Student Guide

Course: Special Access Program (SAP) Overview

Lesson 5: SAP Operations

Introduction

Objectives

The requirements that all Special Access Programs (SAPs) must follow are outlined in several policy documents. There are SAP personnel that work to ensure these policies are carried out. In this lesson, you will learn about these policies and about the roles and responsibilities of the personnel who enforce them.

The lesson objectives are:

- Identify key SAP policy documents
- Identify SAP operations, oversight, and support roles and responsibilities

SAP Oversight

1. Audits and Inspections

As you learned earlier, Section 119, Title 10 United States Code: SAPs Congressional Oversight, requires SAPs to report to Congress annually. It also subjects SAPs to oversight in the form of inspections and audits.

SAPs are subject to the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS). SAPs are also subject to the Defense Contract Management Agency policies. SAPs may be audited against these regulations or may be subjected to other audits and inspections as appropriate. These audits may be conducted by many entities, including the Government Accountability Office, the DoD Inspector General, or the Defense Contract Audit Agency.

2. Oversight and Support Agencies

There are several agencies that provide oversight and support to ensure that SAPs are operating properly and to help them prepare for inspections and audits, as well as reporting to Congress.

These agencies include the Defense Contract Audit Agency, the Defense Security Service, the Defense Logistics Agency, and the DoD Inspector General, among others, including:

- National Reconnaissance Office
- Missile Defense Agency
- National Security Agency
- Defense Intelligence Agency

Many of these agencies have staff specifically dedicated to providing support to SAPs. Different SAPs may receive oversight and support from other agencies, depending on their function and the agencies with which they interact. It is important to note that the agencies represented here are not the *only* agencies that provide oversight and support to SAPs.

SAP Roles and Responsibilities

1. Component-Level SAP Central Offices

As you will recall, each DoD component has a Special Access Program Central Office (SAPCO) that is responsible for coordinating and performing oversight of SAPs within their respective components. A SAPCO for the Joint Chiefs of Staff coordinates unified commands.

Each component-level SAPCO is responsible for the overall management of SAPs under its authority. This includes administering SAPs and maintaining records, including maintaining a list of all SAP facilities the SAPCO manages.

2. Key Roles

The day-to-day operations of SAPs rely on both government and contractor personnel. They also depend on personnel with technical knowledge of SAP operations and personnel responsible for maintaining SAP security. Program managers and security officials play key roles in ensuring a program's security.

a. Government Program Manager (GPM)

A senior government program official, the Government Program Manager is responsible for all aspects of the SAP.

b. Contractor Program Manager (CPM)

The Contractor Program Manager is the government program manager's industry equivalent. This individual is responsible for the program's overall management within the contractor facility and is responsible for executing all contractual obligations.

c. Program Security Officer (PSO)

The Program Security Officer (PSO) is a government security professional who is responsible for all aspects of security. The PSO is appointed in writing by the SAP Central Office (SAPCO), and exercises all authorities for security policies and requirements on behalf of the SAPCO or service component designee. A SAP has only one PSO. A SAP that is large and complex enough may have multiple Contractor Program Security Officers (CPSOs) and Government SAP Security Officers (GSSOs) subordinate to the PSO.

d. Government SAP Security Officer (GSSO)

Service components appoint a Government SAP Security Officer (GSSO) at all government program facilities. The GSSO provides security administration and management based on guidance provided by the PSO.

The GSSO has specific duties and responsibilities:

- Coordinate with the PSO and GPM to create a secure environment to facilitate the successful development and execution of a SAP at each organization or location where SAP information is stored, accessed, or SAP-accessed personnel are assigned
- Are responsible for security management, to include SETA, and operations within their assigned activity, organization, or office.
- Adhere to applicable laws as well as national, DoD, and other security SAP policies and requirements
- Coordinate SAP security matters with the PSO and GPM
- Establish, conduct, and document initial, event-driven, and annual refresher training for all assigned SAP-accessed individuals
- Conduct an annual self-inspection, document the self-inspection, and submit to the PSO a corrective action plan that identifies actions to establish compliance

e. Contractor Program Security Officer (CPSO)

The Contractor Program Security Officer (CPSO) is the government SAP security officer's industry equivalent. The CPSO provides security administration and management as directed by the PSO.

The CPSO has specific duties and responsibilities:

- Coordinate with the PSO and CPM to create a secure environment to facilitate the successful development and execution of a SAP at each organization or location where SAP information is stored, accessed, or SAP-accessed personnel are assigned
- Are responsible for security management, to include SETA, and operations within their assigned activity, organization, or office.
- Adhere to applicable laws as well as national, DoD, and other security SAP policies and requirements
- Coordinate SAP security matters with the PSO and CPM
- Establish, conduct, and document initial, event-driven, and annual refresher training for all assigned SAP-accessed individuals
- Conduct an annual self-inspection, document the self-inspection, and submit to the PSO a corrective action plan that identifies actions to establish compliance

Governing Policy

1. Overview

There are many policies that govern the operations of SAPs. Some policies form the foundation of SAP policy, but don't directly address specific SAP procedures. They focus on the relationship of SAPs to DoD and the government in general. Other policies are targeted directly at the SAP community.

A job aid is located at the end of this lesson that describes these policies at a high level.

2. Foundational Policy

There are several policies, regulations, and baseline documents that establish the security protection standards for classified information released and disclosed to agencies, organizations, and contractors participating in the administration of classified programs. Together, these have been used as the foundation for SAP policy.

Executive Order 13526, "Classified National Security Information," is the foundation of national policy for classified information. This Executive Order directs the Information Security Oversight Office (ISOO) under the direction of the National Archives, to develop implementing guidance. They issued ISOO Directive No. 1, "Classified National Security Information," which sets forth more specific guidance to agencies on the implementation of the Executive Order.

The DoD has implemented national policy guidance on classified information in several documents:

- DoD 5220.22-M: National Industrial Security Program Operating Manual (NISPOM) establishes the standard procedures and requirements for all government contractors, with regard to classified information.
- DoDM 5200.01, Volumes 1-4, DoD Information Security Program, prescribes the defined procedures for the DoD Information Security Program.
- DoD 5200.2-R, Personnel Security Program, outlines the responsibilities of personnel to safeguard classified information.
- DoD 5200.8-R, Physical Security Program, implements the policies and minimum standards for the physical security of DoD installations and resources.
- DoD Directive 5205.2E, DoD Operations Security (OPSEC) Program, implements policy, assigns responsibilities, and provides procedures for managing DoD operations security (OPSEC) programs.

While all of these documents provide foundational guidance for SAPs, let's take a closer look at the policies that more directly address these programs.

3. SAP-Focused Policy

As you learned earlier in this course, Section 119, Title 10 United States Code: SAP Congressional Oversight, outlines SAP oversight and reporting requirements.

DoDI 5205.11, Management, Administration, and Oversight of DoD SAPs, is the implementing document for the DoDD 5205.07. It disseminates policy, assigns responsibilities, and prescribes procedures for implementation and use in the management, administration, and oversight of all DoD SAPs.

In addition, the DoD published DoD Manual 5205.07, Volumes 1-4 which provides additional guidance and applies to all DoD SAPs

- Volume 1 assigns responsibilities; implements policy established in DoD Instruction or DoDI (Dee-oh-Dee-Eye) 5205.11 and describes the general procedures for the administration of DoD SAP security.

- Volume 2 assigns responsibilities and provides procedures for personnel security for DoD SAPs.

- Volume 3 implements policy established in DoDI (Dee-oh-Dee-Eye) 5205.11 and assigns responsibilities and provides procedures for physical security for DoD SAPs.

- Volume 4 provides guidance and procedures for the application of control markings on DoD SAP information.

The DoD Manuals were published by the DoD and applies to all DoD SAPs. It standardizes the foundational SAP security guidance throughout the DoD, outlining the minimum security procedures for DoD SAPs. This policy applies to all Industry as well as to all non-DoD organizations that require access to DoD SAPs.

SAP Applicability

Having standard SAP practices that are applied uniformly across all service branches enable individuals to move between SAPs. This is known as *reciprocity*.

Reciprocity applies to DoD SAPs of the *same* sensitivity level, as long as the individual has a valid need-to-know and meets all requirements. In addition, reciprocity applies to contractor facilities that have been approved for SAP access. That is, if a contractor facility has been approved to work on a Navy SAP, that facility does not need to be approved separately in order to work on an Army SAP.

The use of reciprocity allows DoD SAPs to simplify the process and save time and money.

To be eligible for reciprocity, individuals must:

- Have a valid need-to-know
- Meet all requirements

Applies to:

- Personnel security clearances

- Facility security clearances
- SAP access
- Administrative review process
- Inspections

Special Access Program (SAP) Guidance and Policy Job Aid

Special Access Program (SAP) Foundational Policy and Guidance The following policies form the foundation of Special Access Program policy, but don't directly address specific Special Access Program procedures. They focus on the relationship of Special Access Programs to the Department of Defense (DoD) and the government in general.	
Policy	**Description**
Executive Order 13526 - Classified National Security Information	• Prescribes a uniform system for classifying, safeguarding, and declassifying national security information • Directs the Information Security Oversight Office (ISOO) to develop implementing guidance
Information Security Oversight Office (ISOO) 32 CFR Parts 2001 and 2003 Classified National Security Information; Final Rule	• Defines specific guidance to agencies on the implementation of the Executive Order 13526
DoD 5220.22-M: National Industrial Security Program Operating Manual (NISPOM)	• Establishes the standard procedures and requirements for all government contractors with regard to protection of classified information in the interest of national security
DoDM 5200.01-M, Volume 1-4, Information Security Manual	• Prescribes the defined procedures for the DoD Information Security Program
DoD 5200.02-R: Personnel Security Program	• Outlines the responsibilities of personnel to safeguard classified information
DoD 5200.08-R: Physical Security Program	• Implements the policies and minimum standards for the physical security of DoD installations and resources
DoDD 5205.02E: DoD OPSEC Program	• Implements policy, assigns responsibilities, and provides procedures for managing DoD operations security (OPSEC) program

Special Access Program (SAP) Specific Policy and Guidance The following policies are targeted directly at the Special Access Program (SAP) community.	
Policy	**Description**
Section 119, Title 10 United States Code: Special Access Programs Congressional Oversight	• Outlines SAP oversight and reporting requirements
DoDD 5205.07, Special Access Program Policy	• Outlines policy and responsibilities on the oversight and management of all DoD Special Access Programs (SAPs)
DoDI O-5205.11, Management, Administration, and Oversight of DoD Special Access Programs	• Implements DoD Directive 5205.07 • Disseminates policy, assigns responsibilities, and prescribes procedures for implementing and using in the management, administration, and oversight of all DoD SAPs
DoD Directive 5205.07, Volumes 1-4	• Implements policy established in DoDD 5205.07, assign responsibilities, and provide security procedures for DoD SAP information

Review Activity 1

How well do you understand SAP roles and responsibilities? *Select all that apply; then check your answers in the Answer Key at the end of this Student Guide.*

1. You need to get in touch with your program's Government Program Manager (GPM). Who should you contact?

   - ❍ Maria: Individual appointed by the contractor, who performs security duties and functions at the facility
   - ❍ John: The senior manager for industry, who executes all contact obligations
   - ❍ Saul: Government official who exercises authority on behalf of the SAP Central Office (SAPCO)
   - ❍ Louise: The senior government official with ultimate program responsibility

2. You need to get in touch with your program's Contractor Program Security Officer (CPSO). Who should you contact?

   - ❍ Maria: Individual appointed by the contractor, who performs security duties and functions at the facility
   - ❍ John: The senior manager for industry, who executes all contact obligations
   - ❍ Saul: Government official who exercises authority on behalf of the SAP Central Office (SAPCO)
   - ❍ Louise: The senior government official with ultimate program responsibility

3. You need to get in touch with your program's Program Security Officer (PSO). Who should you contact?

   - ❍ Maria: Individual appointed by the contractor, who performs security duties and functions at the facility
   - ❍ John: The senior manager for industry, who executes all contact obligations
   - ❍ Saul: Government official who exercises authority on behalf of the SAP Central Office (SAPCO)
   - ❍ Louise: The senior government official with ultimate program responsibility

4. You need to get in touch with your program's Contractor Program Manager (CPM). Who should you contact?

   - ❍ Maria: Individual appointed by the contractor, who performs security duties and functions at the facility
   - ❍ John: The senior manager for industry, who executes all contact obligations
   - ❍ Saul: Government official who exercises authority on behalf of the SAP Central Office (SAPCO)
   - ❍ Louise: The senior government official with ultimate program responsible

Answer Key

Review Activity

1. You need to get in touch with your program's Government Program Manager (GPM). Who should you contact?

   - ❍ Maria: Individual appointed by the contractor, who performs security duties and functions at the facility
   - ❍ John: The senior manager for industry, who executes all contact obligations
   - ❍ Saul: Government official who exercises authority on behalf of the SAP Central Office (SAPCO)
   - ⊙ Louise: The senior government official with ultimate program responsibility

2. You need to get in touch with your program's Contractor Program Security Officer (CPSO). Who should you contact?

   - ⊙ Maria: Individual appointed by the contractor, who performs security duties and functions at the facility
   - ❍ John: The senior manager for industry, who executes all contact obligations
   - ❍ Saul: Government official who exercises authority on behalf of the SAP Central Office (SAPCO)
   - ❍ Louise: The senior government official with ultimate program responsibility

3. You need to get in touch with your program's Program Security Officer (PSO). Who should you contact?

   - ❍ Maria: Individual appointed by the contractor, who performs security duties and functions at the facility
   - ❍ John: The senior manager for industry, who executes all contact obligations
   - ⊙ Saul: Government official who exercises authority on behalf of the SAP Central Office (SAPCO)
   - ❍ Louise: The senior government official with ultimate program responsibility

4. You need to get in touch with your program's Contractor Program Manager (CPM). Who should you contact?

   ❍ Maria: Individual appointed by the contractor, who performs security duties and functions at the facility
   ⊙ John: The senior manager for industry, who executes all contact obligations
   ❍ Saul: Government official who exercises authority on behalf of the SAP Central Office (SAPCO)
   ❍ Louise: The senior government official with ultimate program responsibility

Student Guide

Course: Special Access Program (SAP) Overview

Lesson 6: Course Conclusion

Course Summary

As you've learned in this course, SAPs aim to protect national security by employing enhanced security measures to strictly enforce need-to-know and have safeguarding and access requirements which exceed those normally required for information at the same classification level.

In this course, you learned why we have SAPs, how they are authorized, and the basics of how they operate. You learned about the policy documents that govern SAPs and the many agencies and individuals involved in SAP oversight and support.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- Introduction to Special Access Programs
- SAP Lifecycle and Structure
- SAP Approval
- SAP Operations
- Course Conclusion

Course Objectives

You should now be able to:

- ✓ Identify the definition, purpose, and history of SAPs
- ✓ Identify key SAP policy documents
- ✓ Identify the categories and types of SAPs
- ✓ Identify the steps in the SAP approval process
- ✓ Identify the roles and responsibilities involved in the SAP approval process
- ✓ Identify the steps in the SAP lifecycle (establishment, management and administration, apportionment, and disestablishment)
- ✓ Identify operations, oversight, and support roles and responsibilities

Conclusion

Congratulations. You have completed the Special Access Program Overview course. To receive course credit, you *MUST* take the Special Access Program Overview examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.