OPSEC Fundamentals for OPSEC Practitioners Course

Student Guide

November 2025

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Course Overview

OPSEC in Personal Life, Work, and Military

We practice Operations Security (OPSEC) in our daily lives all the time, probably without ever thinking of it.

Have you ever contacted your post office to request a mail hold when you go on a lengthy vacation, so the buildup of mail doesn't indicate to others that you are away from home? You performed OPSEC!

Do you shred your bank or credit card statements before throwing them away to prevent dumpster divers from getting your personal information? You performed OPSEC!

Have you ever set up light timers to go on when you are not home, so it doesn't appear like your home is vacant? You performed OPSEC!

Every day, individuals unknowingly share small pieces of information; harmless on their own but potentially damaging when pieced together by an adversary. These everyday decisions show how OPSEC helps us protect information.

These same principles apply in the workplace and across the Department of Defense. For example, Charlie, a contractor, takes home documents marked Controlled Unclassified Information (CUI) to finish some work and stores them overnight in an unlocked briefcase. This creates a risk of unauthorized disclosure, which could compromise sensitive information and potentially impact national security. Documents containing CUI must always be properly stored and protected to prevent unauthorized access.

Dana, a government employee, also compromises OPSEC in a different way. She casually mentions her organization's upcoming shipment of sensitive equipment in an email to a friend. While it may seem harmless, this message unintentionally reveals critical details such as the type of equipment, shipping routes, dates, and methods that could be exploited if intercepted. To protect mission-related operations, it's essential to avoid discussing sensitive logistics or capabilities with anyone who isn't authorized to receive that information, especially in private messages or informal conversations.

OPSEC Objectives

Welcome to the OPSEC Fundamentals for OPSEC Practitioners course. The examples just shared demonstrate the importance of applying OPSEC principles in personal and professional settings.

In this course you will learn the principles of OPSEC. The course will focus on the historical events that helped shape the OPSEC program, what OPSEC is and how it differs from military deception, relevant policies for implementing the OPSEC program, and how OPSEC is integrated with other security disciplines.

Take a moment to review the course objectives:

- Recognize the principles of OPSEC.
- Describe the historical events that helped shape the OPSEC program.
- Distinguish between OPSEC and military deception.
- Identify the main OPSEC policy documents.
- Describe how and why OPSEC is integrated with counterintelligence and all other security disciplines.

Lesson 2: History and Evolution of OPSEC

Introduction

Lesson Overview

Welcome to the History and Evolution of OPSEC lesson. In this lesson, you will learn about the origins and evolution of Operations Security (OPSEC) within the DOD.

By the end of this lesson you will be able to recognize the mission failures during the Vietnam War that led to the formal establishment of OPSEC in DOD policy, and understand how the OPSEC program has developed and adapted over time. Take a moment to review the lesson objectives.

- Recognize mission failures during the Vietnam War that led to OPSEC being formally established in DOD policy.
- Recognize how the OPSEC program has evolved since the Vietnam War.

Historical Foundations of OPSEC

Protecting private, seemingly inconsequential information from those without a need to know is just a common-sense security practice that humanity has been doing since the dawn of time. While not always referred to as “OPSEC,” the idea of protecting information about battlefield activities dates back to the earliest human conflicts. It is reflected in the following examples.

- General Sun Tzu, a Chinese general and military strategist, wrote about the importance of achieving the element of surprise on the battlefield way back in the 5th Century.
- George Washington, the first president of the United States, is quoted as saying during the Revolutionary War, “Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion.”
- In World War II, the poster with the slogan “Loose Lips Sink Ships” warned service members to “beware of unguarded talk.” The phrase originated on propaganda posters and was created by the War Advertising Council. This type of poster was part of a general campaign to advise servicemen and other citizens to avoid careless talk that might undermine the war effort.

Vietnam War

Origins of Operations Security

The practice of OPSEC has evolved over time, influenced by key military conflicts, intelligence operations, government policies, and technology. Operations security, as we have come to know and understand it, began during the Vietnam War. This need became evident through vulnerabilities exposed during key campaigns, such as Operation Rolling Thunder and Operation Arc Light.

Operations Rolling Thunder

Operation Rolling Thunder was a sustained bombing campaign against North Vietnam. Over time, U.S. military leaders saw that compromised information was jeopardizing missions and endangering lives. These disclosures allowed the enemy to anticipate airstrikes, reducing their impact and revealing the need for stronger operational security.

Operation Arc Light

Operation Arc Light used B-52 bombers for strategic strikes in Vietnam. However, predictable flight paths and unsecured communications sometimes allowed enemy forces to detect the missions in advance, reducing their effectiveness. These compromises further underscored the importance of improving operations security to protect mission success and personnel.

Operation Purple Dragon (1966)

Due to vulnerabilities like those you just learned about during the Vietnam War, U.S. military forces noticed that adversaries were successfully predicting American military actions. The problem was so extensive that in 1966, the Joint Chiefs of Staff initiated a classified study known as Operation Purple Dragon to investigate how adversaries were gaining intelligence on U.S. operations.

Through the course of their investigation, the team behind Operation Purple Dragon discovered that the Viet Cong were not decrypting our secure communications, but that U.S. forces were inadvertently revealing vital information to the enemy. The U.S. troops were not varying their tactics and plans; they were using the same refueling routes and using the same bombing routes – indicators of critical information.

When the enemy sees you refueling your plane every time before a planned operation, what does that indicate? It indicates that an operation is in the very near future. When you use the exact same bombing route over and over, the enemy is bound to catch on and start to move people, weapons, and other assets from the impacted area. Bombing raids were less successful than anticipated.

JCS Publication 18 (1973)

Based on these findings, the team recommended corrective actions to local commanders to reduce vulnerabilities. Their efforts proved highly effective, and to describe this new approach, they coined the term "operations security."

After the Vietnam War ended in 1973, the Joint Chiefs of Staff (JCS) adopted the OPSEC instruction developed by the Operations Security unit within the Pacific Command, or CINCPAC OPSEC Branch, and published it as JCS Publication 18, “Doctrine for Operations Security.”

Purple Dragon identified five key steps to performing OPSEC: identify critical information, analyze the threat, analyze the vulnerabilities, assess the risk, and apply countermeasures. Purple Dragon was so successful, that the Joint Staff then made OPSEC mandatory for all U.S. combatant commands.

From the Cold War to the Present

NSDD 298 (1988)

In 1988, at the height of the Cold War, President Ronald Reagan, recognizing the importance of OPSEC beyond the military community, signed the first National-level OPSEC policy. National Security Decision Directive (NSDD) 298 was short, and conceived during a time when traditional Human Intelligence, HUMINT, Signals Intelligence, SIGINT, and counterintelligence Tactics, Techniques, and Procedures (TTPs) were in play. Society was not yet tethered to computers or armed with cellphones.

NSDD 298 designated the National Security Agency (NSA) as the Executive Agency for OPSEC training and established the Interagency OPSEC Support Staff to develop and provide that training.

NSDD 298 applied to Federal Departments and Agencies who identified as having national security missions. The policy didn’t apply to all Federal Departments and Agencies—only those who identified as having national security missions, and many organizations did not include themselves in that category. NSDD 298 served as the national OPSEC policy for nearly 33 years.

Effort to Update NSDD 298 (2019)

In early 2019, the National Security Council began a multi-agency effort, that DOD was a big part of, to update the National OPSEC policy. The focus of the update was to bring OPSEC out of the Cold War and into the great power competition of today.

The Cold War was a period of global geopolitical rivalry between the United States and the former Soviet Union (USSR) which lasted from 1947 until the dissolution of the Soviet Union in 1991. The term Cold War is used because there was no direct fighting between the two superpowers.

During the Cold War, information was a key commodity. It was vital to know what the adversary was up to, and the hi-tech surveillance that is used today was not available. Instead of trusting technology, states relied on spies: people who infiltrated enemy territory and tried to discover information while staying undetected.

The 2019 update effort was intended to update NSDD 298 to better protect our national interests against the adversaries and capabilities we face today, not the ones we faced 30 years ago. Threats from our adversaries have evolved over the years due to new, disruptive, and emerging technologies and advancements in data aggregation and analysis. Information is still a key commodity, and it's a lot easier to gather now.

There also needed to be a fundamental change in culture to understand that OPSEC is not just for forward deployed uniformed soldiers. "Operations" does not just refer to "military operations." Operations also encompass day-to-day office and administrative operations, acquisition-related operations, contracting operations, budget planning operations, supply chain/risk management operations, and research and development operations.

OPSEC is not just for the military. OPSEC is everyone's responsibility.

NSPM 28 (2021)

The new OPSEC policy, National Security Presidential Memorandum (NSPM) 28, was signed by President Trump on January 13, 2021. NSPM 28 is the current National-level OPSEC policy, and it has five key changes and updates from the original policy.

Change 1

The most significant change from the old policy to the new one is that the new policy applies to all Federal Departments and Agencies— which is over 300 different organizations! This means departments and agencies that previously did not consider themselves to have "national security" missions, are now directed to have OPSEC Programs as well.

Foreign adversaries are trying to get a military, political, diplomatic, economic, or technological advantage over the United States, so they are going after

information from all U.S. federal departments and agencies. Yet another indication that OPSEC is not just applicable to military matters.

Change 2

NSPM 28 directs the integration of OPSEC with counterintelligence and all other security disciplines. While some departments and agencies choose to interpret this to mean that all OPSEC programs should be organizationally placed with their counterintelligence and other security disciplines, DOD policy leaves that to the Component head and the Commander's discretion.

Within the Office of the Secretary of Defense (OSD) OPSEC Policy is functionally placed with the Under Secretary of Defense for Intelligence and Security, and then again under the Director for Defense Intelligence Counterintelligence, Law Enforcement, and Security. This further reinforces OPSEC's function as a security discipline.

Change 3

NSPM 28 reaffirms that OPSEC is a security function, which underscores more of the rationale for ensuring OPSEC is integrated with other security disciplines and missions.

Change 4

NSPM 28 made a major structural change to the U.S. government's OPSEC oversight. It disbanded the former Interagency Operations Security Support Staff, IOSS, at NSA and created a new National-level OPSEC Program Office under the Office of the Director of National Intelligence (ODNI) at the National Counterintelligence and Security Center.

The new National Operations Security Program (NOP) is a new office operating under a completely different charter. It should go without saying, but the NOP is a National-level office outside of the DOD. No one in the DOD should contact the NOP Office before going through their own OPSEC Chain of Command for questions regarding OPSEC policy, training, or resources.

In addition, NOP-provided OPSEC training does not meet minimum DOD training requirements. While students may take NOP courses, the training is not sufficient on its own. For more information you can reference the "Use of National Operations Security Program Office Training for DOD Operations Security Workforce" document in the course Resources.

Change 5

The new policy replaces the term “OPSEC Process” with “OPSEC Cycle.” While updating the term “process” to “cycle” might seem like a small change, it was done to emphasize that the OPSEC Cycle is a series of continuous actions, it’s not a one-and-done task.

This modification is intended to change how people think about OPSEC and encourage people to see OPSEC as a continuous effort. The OPSEC Cycle describes the same five actions as the original “process,” just repeated in a continuous cycle.

You will learn more about the steps of the OPSEC Cycle in the next lesson.

Review Activities

Knowledge Check – 1

Which of the following Vietnam War events contributed to the creation of “operations security”?

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

- ☐ Operation Rolling Thunder indicated that the encryption methods were not protecting battlefield communications.
- ☐ Operation Rolling Thunder indicated that compromised information was jeopardizing missions.
- ☐ Operation Arc Light indicated that there were classified documents leaked to the press before the mission.
- ☐ Operation Arc Light indicated that enemy forces were able to detect missions in advance.

Knowledge Check – 2

What were some of the driving forces that contributed to the 2019 update of NSDD 298?

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

- ☐ The need to make the National Security Agency (NSA) the Executive Agency for OPSEC training
- ☐ The rise of advanced technologies and increased reliance on digital information

- ☐ The need to expand OPSEC to all Federal Departments and Agencies
- ☐ The shift from Cold War-era threats to modern day threats

Knowledge Check – 3

Which of the following key OPSEC updates were introduced in NSPM 28?

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

- ☐ NSPM 28 shifted OPSEC oversight to the Department of Homeland Security.
- ☐ NSPM 28 reaffirms that OPSEC is a security discipline.
- ☐ NSPM 28 indicates OPSEC applies to all Federal Departments and Agencies.
- ☐ NSPM 28 directs the integration of OPSEC with counterintelligence and all other security disciplines.

Lesson 3: OPSEC Today

Introduction

Lesson Overview

Welcome to the OPSEC Today lesson. This lesson explores the modern role of Operations Security (OPSEC) in safeguarding critical information from unauthorized disclosure and how to identify critical information. It also covers the components of the OPSEC Cycle, including the purpose of each step and the benefits of applying the cycle in practice. Lastly, it highlights the distinction between OPSEC and military deception. Take a moment to review the lesson objectives.

- Define what OPSEC is, including its purpose and how it protects critical information from unauthorized disclosure.
- Given a scenario, identify critical information.
- Describe the OPSEC Cycle components including the purpose of each component and the benefits of applying the OPSEC Cycle.
- Given an activity, determine whether the activity is an OPSEC activity or a deception activity.
- Recognize that deception activities need additional authorizations and have additional requirements.

OPSEC and Critical Information

OPSEC Defined

OPSEC is a security discipline designed to deny adversaries the ability to collect, analyze, and exploit information that might provide an advantage against the United States.

OPSEC helps prevent the inadvertent disclosure of critical information including details about your intentions, capabilities, and activities that unauthorized individuals could exploit to compromise or disrupt your mission. What qualifies as critical information varies by organization and mission.

Critical Information Defined

The whole point of OPSEC is to protect critical information. So, what is critical information? The DOD Dictionary of Military and Associated Terms defines critical information as “Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.”

Such information, if revealed to an unauthorized recipient, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources. What is sensitive on one mission might be completely harmless in another mission. Effective OPSEC means evaluating the unique risks of each mission and protecting information accordingly.

As you will see later in this lesson, OPSEC itself is in fact a cycle of repeating actions you will need to take to ensure that critical information is protected.

Impact of OPSEC Failure

Let’s look at an example that shows how not having an OPSEC plan can have an impact on the compromise of critical information. The Manta Ray is a prototype Unmanned Underwater Vehicle (UUV) built by Northrop. This project was part of the Defense Advanced Research Projects Agency’s (DARPA’s) Manta Ray Program, which began in 2020 with the goal of advancing technologies for a “new class” of autonomous UUVs that could be used by the Navy for long-range and long-duration missions.

Satellite images taken in November 2023 and April 2024, that were available through Google Earth, show the Manta Ray docked at the Port Hueneme naval base in California. The sighting went viral online, sparking widespread curiosity. It appears that measures to protect critical information related to the Manta Ray development were either not in place or not properly carried out.

If the intent was to keep images of the developing technology concealed from public release, storing the vessel in broad daylight was clearly not a good idea. A simple tarp large enough to cover the dock would likely have prevented images from being taken and uploaded on Google Maps.

While attempts were made to remove or alter the image, scrubbing the image after the fact had the unintended consequence of bringing more attention to it. Taking proactive steps to protect sensitive details about the Manta Ray development could have prevented the compromise of critical information.

The OPSEC Cycle

How does OPSEC prevent the disclosure of critical information?

How does OPSEC prevent the disclosure of critical information? OPSEC is a cycle that examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by adversaries.

OPSEC prevents inadvertent disclosure of critical information through a continuous cycle of assessment involving five core steps. First, it identifies critical information and indicators (CII) by determining what adversaries can observe. Next, it analyzes threats, assessing who potential adversaries are, their intent, ability to collect information, and opportunities to act. This cycle then examines vulnerabilities and indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. After that, it assesses risks by determining which of these represent an unacceptable risk. Finally, it selects and executes countermeasures to eliminate or reduce risks to an acceptable level.

All elements of the cycle are needed to conduct an OPSEC analysis.

Identification of CII

Critical information indicators are clues or pieces of observable data that could lead an adversary to infer critical information. Such information, if revealed to an unauthorized recipient, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources. To illustrate how this applies in practice, consider the following example.

Identification of CII – Example

Consider this scenario. The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) is funding quantum research at Patriotic University, USA. Specifically, the students in the funded research team are developing quantum algorithms.

Information about the specific algorithms being researched, their intended applications, for example, breaking encryption and optimization problems, and their performance characteristics are considered OPSEC critical information because knowing these details could allow adversaries to anticipate future vulnerabilities or develop countermeasures.

This information will be compiled in a Critical Information and Indicators List (CIIL).

Analysis of Threat

Threat information is necessary to develop appropriate countermeasures to protect critical information and indicators. The threat analysis includes identifying potential adversaries and their associated capabilities and intentions to target critical information and indicators through collection, analysis, and exploitation. Consider the following example.

Analysis of Threat – Example

Continuing from our previous example, unauthorized recipient X, a known foreign intelligence entity, is interested in quantum research being funded by OUSD(R&E) at Patriotic University USA. X is part of a sophisticated intelligence apparatus assessed to be quite adept in intelligence tradecraft.

Analysis of Vulnerabilities

An OPSEC vulnerability exists when the unauthorized recipient is capable of collecting critical information or indicators, analyzing it, and then acting quickly enough to impact friendly objectives. Conducting exercises, red teaming, a practice of adopting an adversary's perspective, and analyzing operations can help identify vulnerabilities. Consider the following example.

Analysis of Vulnerabilities – Example

Continuing from our previous example, the CIIL specific to OUSD(R&E)'s quantum research was shared with the funded academic research team at Patriotic University USA. Vulnerability analysis revealed that the students in the funded research team lack OPSEC Awareness training. Additionally, foreign students, some assessed to be non-traditional collectors, have access to the research facilities and computers. A non-traditional collector is an individual who is not a trained spy or official employee of a foreign government but is expected to work in the best interest of their homeland.

Assessment of Risk

The risk assessment evaluates the likelihood that an adversary will collect critical information and how damaging its exposure would be to the mission. Determining the level of risk is a key element of the OPSEC cycle and provides justification for using countermeasures. Once the risk level is determined, consider the cost, time, and effort required to implement OPSEC countermeasures to mitigate risk. Consider the following example.

Assessment of Risk – Example

Continuing from our previous example, after each item on the CIIL was evaluated against the threat, vulnerability, and impact, four items were assessed at high risk, eleven items were assessed at medium high risk, and three items were assessed at medium low or low risk. Overall, fifteen were assessed with a high or medium high risk rating. The OUSD(R&E) OPSEC practitioner recommends enacting countermeasures to safeguard the 15 CIIL items assessed as most at risk.

Apply Countermeasures

Countermeasures are designed to prevent an unauthorized recipient from detecting critical information, provide an alternative interpretation of critical information or indicators, or deny the unauthorized recipient's collection system. If the amount of risk is determined to be unacceptable, countermeasures are then implemented to mitigate risk or to establish an acceptable level. Consider the following example.

Apply Countermeasures – Example

Continuing from our previous example, as the academic research team at Patriotic University, USA is assessed to have the highest vulnerabilities, all participants must complete the following mandatory training before starting research: Cyber Awareness Challenge, Counterintelligence Awareness and Reporting, Insider Threat Awareness, OPSEC Awareness, Introduction to Information Security, Unauthorized Disclosures of Classified and Controlled Unclassified Information (CUI) training.

An OPSEC Program Plan will be developed and provided to the Patriotic University Quantum Research Team. All members must read and sign it, indicating that they know they may not discuss the CIIL-associated information and data verbally, electronically, or in writing outside of an appropriate workplace or environment, and only within the presence of individuals who have a verifiable need-to-know. In addition, team members indicate that they understand that they must report unauthorized disclosures upon recognition of a leak, in order to mitigate further spread of nonpublic information.

Benefits of Applying OPSEC Cycle

The OPSEC Cycle helps identify critical information that could compromise operations if exposed and analyzes potential adversaries and their capabilities to help anticipate and counter emerging threats. It also provides a structured and systematic approach to protecting critical information and helps ensure the success of missions and operations.

Overall, it enables organizations to effectively manage risks. Assessing risks can help leaders make decisions that balance operational needs with security requirements.

OPSEC Versus Military Deception

Differences Between OPSEC and Military Deception

Now that you understand the importance of protecting critical information, it's important to also understand the methods used to safeguard it. This includes knowing the difference between OPSEC and DOD deception.

OPSEC is a security discipline, whereas deception is an operational activity governed by a separate policy from OPSEC. The objective of OPSEC is to prevent adversaries from gaining access to critical information that could disclose operational intentions, with the ultimate goal of denying the enemy critical information. In contrast, deception activities are designed to intentionally mislead adversaries about DOD capabilities, intentions, or operations.

Example

Let’s use the example of a project manager overseeing the rollout of a new government IT system. The project includes sensitive timelines, vendor partnerships, and cybersecurity features.

OPSEC: To protect critical information, the project manager must restrict access to the project schedule and system architecture, use secure file-sharing platforms for contractor communications, and avoid discussing project milestones in common areas or during virtual meetings without proper clearance. The goal is to prevent external vendors, hackers, or the public from gaining details that could lead to a security breach or sabotage.

DOD Deception: In a DOD deception effort, the project manager can publish a general project update with broad, vague descriptions of the system features and publicly reference an outdated implementation timeline, knowing the actual launch date is weeks earlier. The goal is to prevent competitors from figuring out the real scope of the system and trying to underbid or interfere.

DOD Military Deception Policy

DOD Instruction S-3604.01, Department of Defense Military Deception, is classified; however, at the unclassified level you should be aware that DOD deception activities must be approved and comply with applicable U.S. law and other Presidential and DOD policies.

Also, DOD deception activities must not explicitly or implicitly target, mislead, or attempt to influence congress, the public, or news media of the United States.

Refer to the course Resources to view the policy.

Review Activities

Knowledge Check – 1

Which of the following statements define OPSEC?

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

- ☐ OPSEC is a cycle used to identify and protect critical information from adversaries.
- ☐ OPSEC is only used to classify information at the national level.
- ☐ OPSEC eliminates the need for physical security measures.
- ☐ OPSEC involves analyzing operations and activities to determine what information could be valuable to adversaries.

Knowledge Check – 2

You work in the Human Resources office of a defense agency. Your team handles employee records, onboarding documentation, and travel plans for new hires. Which of the following pieces of information in the HR files may be considered critical information under OPSEC?

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

- ☐ Travel plans related to mission activities
- ☐ Deployment assignments
- ☐ Employee job titles and departments they are joining
- ☐ Special access designations (e.g., Special Access Program [SAP])

Knowledge Check – 3

Which of the following best describes the purpose of the Analysis of Threat step in the OPSEC Cycle?

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

- ○ Identify DOD activities, intentions, capabilities, or limitations that an unauthorized recipient seeks to gain an advantage
- ○ Identify potential adversaries and their associated capabilities and intentions to collect, analyze, and exploit critical information and indicators
- ○ Assess the unauthorized recipient's ability to exploit vulnerabilities that would lead to the exposure of critical information and the potential impact it would have on the mission
- ○ Design countermeasures to prevent an unauthorized recipient from detecting critical information

Knowledge Check – 4

Which of the following are benefits to applying the OPSEC Cycle?

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

- ☐ Elimination of the need for traditional physical security measures
- ☐ Prevention of all insider threats
- ☐ Protection of critical information from unauthorized access
- ☐ Improved risk management through regular identification and prioritization of threats

Knowledge Check – 5

In the same defense agency, teams are using multiple strategies to protect mission information. One team is implementing physical security measures to safeguard information while another team is disseminating false information about troop movements and mission plans. Which of the following best describes each activity?

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

- ○ The team that is implementing physical security measures is using a deception activity and the team disseminating false information is using an OPSEC activity

- ○ The team that is implementing physical security measures is using an OPSEC activity and the team disseminating false information is using a deception activity
- ○ Both activities are deception activities because they involve manipulating information
- ○ Both activities are OPSEC activities because they help protect critical information

Knowledge Check – 6

In the previous question, one team was implementing physical security measures to safeguard information while another team was disseminating false information about troop movements and mission plans. Which of the following best describes requirements for these strategies?

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

- ○ The team disseminating false information must receive additional authorizations and follow additional requirements.
- ○ The team implementing physical security measures must receive additional authorizations and follow guidelines in DOD Instruction S-3604.01.
- ○ Both strategies must follow the guidance in DODM 5205.02.
- ○ Both strategies require formal approval.

Lesson 4: OPSEC Policy and Integration with Other Security Disciplines

Introduction

Lesson Overview

Welcome to the OPSEC Policy and Integration with Other Security Disciplines lesson. In this lesson you will learn to recognize the key policy requirements involved in implementing an effective Operations Security (OPSEC) program, identify the requirements for training individuals on critical information, identify how OPSEC is integrated in other security disciplines, and describe the purpose and benefits of OPSEC working groups. Take a moment to review the lesson objectives.

- Recognize the key policy requirements for implementing the OPSEC program.
- Given a plan for training individuals on their organization's critical information, identify whether the training meets requirements.
- Given a scenario related to a specific security discipline, identify OPSEC's role in protecting critical information.
- Describe the purpose and benefits of OPSEC working groups.

OPSEC Policies

OPSEC Implementation Policies

As we discussed earlier, the development of national level OPSEC policy began with the first National Security Decision Directive, NSDD 298, signed in 1988, and continued with National Security Presidential Memorandum (NSPM) 28, issued in 2021, which extended OPSEC requirements to all federal agencies.

Now, let's explore two policies that are foundational documents for the implementation and governance of Operations Security (OPSEC) in the Department of Defense. DODD 5205.02E, a DOD Directive, establishes the policy and responsibilities for the implementation of the OPSEC policy program. This directive provides a framework to ensure that critical information and indicators of DOD operations, activities and capabilities are protected from unauthorized recipient exploitation.

DODM 5205.02, a DOD Manual, provides detailed procedures and implementation guidance for carrying out the OPSEC program.

You can find a link to both of these documents in the course Resources.

OPSEC Program Requirements

The following key policy points highlight how these documents guide OPSEC integration, training, program management, and oversight.

According to the documents, all Office of the Secretary of Defense (OSD) and DOD missions, functions, programs, and activities shall be protected by an OPSEC program. OPSEC shall be considered across the entire spectrum of DOD missions, functions, programs, and activities.

OPSEC and other security missions shall be closely coordinated to ensure the protection of personnel and the security of information and activities. Head of DOD and OSD Components shall establish OPSEC programs with full-time OPSEC program managers and practitioners to promote an understanding and practice of OPSEC among all personnel.

Overall, DOD and OSD must integrate OPSEC across all activities, with dedicated staff ensuring coordination with other security efforts and promoting awareness among all personnel.

OPSEC Training Requirements

In addition, these policy documents provide guidance on OPSEC training requirements. To ensure the effective protection of critical information, it is essential that individuals in key roles receive appropriate training in OPSEC.

Personnel such as OPSEC program managers and practitioners, information operations (IO) professionals, public affairs personnel, contracting specialists, and those responsible for reviewing and approving information for public release must receive specialized OPSEC training tailored to their specific responsibilities.

In addition to specialized training for these roles, all members of the general workforce are required to complete OPSEC Awareness training upon initial entry into duty, including those entering through accession programs such as basic training, commissioning sources, and internships. All members of the workforce must refresh this training on an annual basis.

General Workforce Training Content

DODM 5205.02 specifies that the initial OPSEC Awareness training must include an explanation of what OPSEC is, why it’s important, or its purpose, what kinds

of threats exist, what the organization considers to be critical information, and what each individual's role is in protecting that information.

General organizational orientations may need to be supplemented by job-specific training in the work center, targeted toward specific critical information and vulnerabilities associated with the work.

DODM 5205.02 requires annual refresher OPSEC training that reinforces understanding of OPSEC policies and procedures, critical information, and procedures covered in initial and specialized training. In addition, refresher training should also address the threat and techniques employed by adversaries attempting to obtain classified and sensitive information.

Training on Critical Information

According to DOD policy, your organization's critical information must be taught during initial and annual training, or it does NOT meet the bare minimum training requirements. Because critical information is specific to your organization, this means it is unlikely that generic standalone computer-based-training is going to meet that threshold.

As an OPSEC program manager or practitioner, you'll need to get inventive with your training techniques; this could mean monthly in-person new-employee OPSEC training briefings, or working with your local Public Affairs and media support staff to film OPSEC training that goes over the critical information and how to protect it and make the link available on a Common Access Card, or CAC-accessible firewall protected site.

OPSEC Assessments

Beyond training, OPSEC program effectiveness must also be measured through OPSEC assessments, as required by DOD guidance. An OPSEC Assessment is an evaluation of your OPSEC program and is used to determine the likelihood that critical information can be protected based on the procedures currently in place. You will learn more about conducting OPSEC Assessments in the OPSEC Analysis Training course.

Integration of OPSEC

OPSEC Integration with Security Disciplines

As you recall, NSPM 28 reaffirms that OPSEC is a security discipline, which underscores the rationale for ensuring OPSEC is integrated with other security disciplines and missions.

Security disciplines include:

- Personnel Vetting: Ensures individuals are vetted, trustworthy, and reliable for access to classified information or sensitive duties
- Physical Security: Safeguards personnel, facilities, and resources from unauthorized access, damage, or loss through physical protective measures;
- Information Security: Protects classified information from unauthorized disclosure through proper classification and handling procedures
- Cybersecurity: Protects DOD information systems and networks from digital threats and cyberattacks
- Special Access Program (SAP) Security: Provides enhanced protection for highly sensitive programs requiring extraordinary security measures
- Counterintelligence Security: Identifies, assesses, and counters threats posed by foreign intelligence entities and insider espionage to protect national security information and operations
- Insider Threat: Detects, deters, and mitigates risks posed by trusted individuals who may intentionally or unintentionally harm national security through unauthorized disclosure, sabotage, or other malicious acts
- Industrial Security: Oversees the protection of classified information in the hands of cleared defense contractors.

Operations Security identifies and protects critical information to prevent adversaries from exploiting U.S. military operations and although OPSEC is distinct from the other security disciplines, it overlaps with all of them—meaning, while OPSEC's primary focus is to protect critical information from adversaries, it requires coordination across multiple areas of security.

Example of OPSEC Integration with Security Discipline

Let's examine an example demonstrating how organizational OPSEC Programs are integrated with Agency and Department Counterintelligence and Security Programs – in this case, Physical Security (PhysSec).

Physical Security personnel determine how many security guards a building needs, the locations they will be posted, and their duty hours and rotation schedules. This is critical information. OPSEC must also be practiced in order to keep the critical information about the details of those plans from being inadvertently disclosed to an unauthorized recipient who wants nefarious access to the building.

OPSEC Integration with Activities and Operations

As we just discussed, at the national policy level, NSPM 28 directs OPSEC to be integrated with counterintelligence and all other security disciplines. In addition, DODM 5205.02 also directs the heads of the DOD Components to "integrate OPSEC in all activities and operations that prepare, sustain, or employ U.S. Armed Forces during war, crisis, or peace including, but not limited to, research, development, test, and evaluation; special access programs; DOD contracting; treaty verification; nonproliferation protocols; international agreements; force protection; and release of information to the public."

OPSEC does not just apply to uniformed military members. Since the rest of DOD exists as a supporting function to our military, it's important to protect critical information we are privy to so as not to compromise any future DOD activities.

OPSEC Working Groups

Because OPSEC must be considered across the entire spectrum of DOD missions, functions, programs, and activities, it's critical that coordination happens at the organizational level. One effective way to ensure this integration is through the establishment of an OPSEC Working Group.

An OPSEC working group brings together experts from various backgrounds to ensure a comprehensive, proactive approach to protecting critical information. It is comprised of Subject Matter Experts (SMEs) for each aspect of the mission or organization. This allows for information sharing between organizations, offices, and mission partners. Collaboration among the working group members ensures sustained vigilance against threats.

Depending on the circumstances of the OPSEC working group, working group members may include:

- Critical Infrastructure Protection (CIP) Planners
- Public Affairs
- Counterintelligence Representatives
- Cybersecurity Specialists
- Insider Threat Program Managers
- Budget Representatives
- Others as needed

Now that we've covered the purpose and composition of an OPSEC Working Group, let's see what this might look like in a department.

Working Group Example

Consider this scenario. Gwen in the Human Resources (HR) office noticed that job postings were unintentionally revealing sensitive details about leadership changes and deployment schedules. In response, the HR office formed an OPSEC working group focusing on securing personnel data and ensuring HR processes don't expose operational information that could be exploited by adversaries.

OPSEC working group members included the HR Director who will ensure OPSEC is integrated into HR policies and operations, OPSEC Practitioner who provides guidance on protecting critical information, Public Affairs who can review job postings and public communication, and Information Security Personnel who can ensure the HR databases are secured.

Review Activities

Knowledge Check – 1

Which of the following are key policy requirements for implementing the OPSEC program?

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

- ☐ All OSD and DOD Components must post incident reports publicly for accountability
- ☐ All OSD and DOD Components must identify and remove traditional security roles that are redundant with OPSEC personnel roles
- ☐ All OSD and DOD missions, functions, programs, and activities must be protected by an OPSEC program
- ☐ All OSD and DOD Components must establish OPSEC programs with full-time OPSEC program managers and practitioners

Knowledge Check – 2

Carol, a Security Practitioner, has developed a plan to train new and existing personnel in her department on critical information. Which of the following training activities best meets policy requirements?

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

- ○ Carol will train all personnel once a year focusing on what critical information is.
- ○ Carol will train new personnel during initial training and all personnel annually thereafter focusing on what critical information is.
- ○ Carol will train all personnel once a year focusing on what is considered critical information in the department.
- ○ Carol will train new personnel during initial training and all personnel annually thereafter focusing on what is considered critical information in the department.

Knowledge Check – 3

Now that Carol knows what training activities she must perform, what training methods will best comply with policy requirements?

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

- ○ Carol distributes a slide deck via email that details the organization's critical information
- ○ Carol conducts a small group training session with tailored instruction on her organization's critical information
- ○ Carol provides learners with an online training course on OPSEC that addresses critical information without local content
- ○ Carol conducts a small group training session where she provides generic information on critical information

Knowledge Check – 4

Steve, a logistics coordinator, has access to unit deployment schedules and vehicle movement data. His coworker noticed that he has been downloading large amounts of planning documents to a personal thumb drive, outside of his normal duties. His pattern of behavior raises concerns. In this insider-threat scenario, what best describes OPSEC's primary role in protecting critical information?

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

- ○ OPSEC requires immediate public disclosure of the incident to preserve transparency
- ○ OPSEC requires issuing insider-threat alerts to all personnel whenever suspicious downloads occur
- ○ OPSEC includes analyzing observable behaviors (e.g., transfers to thumb drives) that might reveal critical information, and implementing countermeasures
- ○ OPSEC mandates installation of computer tools to track unusual online activities

Knowledge Check – 5

Which of the following best describes the purpose and benefits of forming an OPSEC working group?

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

- ○ To assemble subject matter experts from different disciplines to enforce physical security measures like badge-access systems
- ○ To assemble subject matter experts from different disciplines to create standardized OPSEC policies
- ○ To assemble subject matter experts from different disciplines to conduct surveillance and audits for the OPSEC program
- ○ To assemble subject matter experts from different disciplines to identify mission-critical information, assess vulnerabilities, and determine countermeasures, as needed

Lesson 5: Course Conclusion

Conclusion

Lesson Review

This course introduced the principles of OPSEC. It focuses on the historical events that helped shape the OPSEC program, relevant policies for implementing the program, and how OPSEC is integrated with other security disciplines.

Course Summary

Congratulations! You have completed the *OPSEC Fundamentals for OPSEC Practitioners* course.

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

- Recognize the principles of OPSEC.
- Describe the historical events that helped shape the OPSEC program.
- Distinguish between OPSEC and military deception.
- Identify the main OPSEC policy documents.
- Describe how and why OPSEC is integrated with counterintelligence and all other security disciplines.

To receive course credit, you must take the *OPSEC Fundamentals for OPSEC Practitioners* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Knowledge Check – 1

Which of the following Vietnam War events contributed to the creation of "operations security"?

- ☐ Operation Rolling Thunder indicated that the encryption methods were not protecting battlefield communications.
- ☑ Operation Rolling Thunder indicated that compromised information was jeopardizing missions. (correct response)
- ☐ Operation Arc Light indicated that there were classified documents leaked to the press before the mission.
- ☑ Operation Arc Light indicated that enemy forces were able to detect missions in advance. (correct response)

***Feedback**: During Operation Rolling Thunder it was discovered that compromised information was jeopardizing missions while Operation Arc Light indicated that enemy forces were able to detect missions in advance.*

Knowledge Check – 2

What were some of the driving forces that contributed to the 2019 update of NSDD 298?

- ☐ The need to make the National Security Agency (NSA) the Executive Agency for OPSEC training
- ☑ The rise of advanced technologies and increased reliance on digital information (correct response)
- ☐ The need to expand OPSEC to all Federal Departments and Agencies
- ☑ The shift from Cold War-era threats to modern day threats (correct response)

***Feedback**: The shift from Cold War-era threats to modern day threats and the rise of advanced technologies and increased reliance on digital information both contributed to the 2019 update of NSDD 298.*

Knowledge Check – 3

Which of the following key OPSEC updates were introduced in NSPM 28?

- ☐ NSPM 28 shifted OPSEC oversight to the Department of Homeland Security.
- ☑ NSPM 28 reaffirms that OPSEC is a security discipline. (correct response)
- ☑ NSPM 28 indicates OPSEC applies to all Federal Departments and Agencies. (correct response)
- ☑ NSPM 28 directs the integration of OPSEC with counterintelligence and all other security disciplines. (correct response)

Feedback*: NSPM 28 reaffirms that OPSEC is a security discipline, indicates that OPSEC applies to all Federal Departments and Agencies, and directs the integration of OPSEC with counterintelligence and all other security disciplines.*

Lesson 3 Review Activities

Knowledge Check – 1

Which of the following statements define OPSEC?

- ☑ OPSEC is a cycle used to identify and protect critical information from adversaries. (correct response)
- ☐ OPSEC is only used to classify information at the national level.
- ☐ OPSEC eliminates the need for physical security measures.
- ☑ OPSEC involves analyzing operations and activities to determine what information could be valuable to adversaries. (correct response)

Feedback*: OPSEC is a cycle used to identify and protect critical information from adversaries and involves analyzing operations and activities to determine what information could be valuable to adversaries.*

Knowledge Check – 2

You work in the Human Resources office of a defense agency. Your team handles employee records, onboarding documentation, and travel plans for new hires. Which of the following pieces of information in the HR files may be considered critical information under OPSEC?

- ☑ Travel plans related to mission activities (correct response)
- ☑ Deployment assignments (correct response)
- ☐ Employee job titles and departments they are joining

- ☑ Special access designations (e.g., Special Access Program [SAP]) (correct response)

***Feedback**: Travel plans related to mission activities, deployment assignments, and special access designations may all provide valuable insight that adversaries could exploit.*

Knowledge Check – 3

Which of the following best describes the purpose of the Analysis of Threat step in the OPSEC Cycle?

- ○ Identify DOD activities, intentions, capabilities, or limitations that an unauthorized recipient seeks to gain an advantage
- ⊙ Identify potential adversaries and their associated capabilities and intentions to collect, analyze, and exploit critical information and indicators (correct response)
- ○ Assess the unauthorized recipient's ability to exploit vulnerabilities that would lead to the exposure of critical information and the potential impact it would have on the mission
- ○ Design countermeasures to prevent an unauthorized recipient from detecting critical information

***Feedback**: Analysis of Threat involves identifying potential adversaries and their associated capabilities and intentions to collect, analyze, and exploit critical information and indicators.*

Knowledge Check – 4

Which of the following are benefits to applying the OPSEC Cycle?

- ☐ Elimination of the need for traditional physical security measures
- ☐ Prevention of all insider threats
- ☑ Protection of critical information from unauthorized access (correct response)
- ☑ Improved risk management through regular identification and prioritization of threats (correct response)

***Feedback**: Protection of critical information from unauthorized access and improved risk management through regular identification and prioritization of threats are both benefits of applying the OPSEC Cycle.*

Knowledge Check – 5

In the same defense agency, teams are using multiple strategies to protect mission information. One team is implementing physical security measures to safeguard information while another team is disseminating false information about troop movements and mission plans. Which of the following best describes each activity?

- ○ The team that is implementing physical security measures is using a deception activity and the team disseminating false information is using an OPSEC activity
- ⊙ The team that is implementing physical security measures is using an OPSEC activity and the team disseminating false information is using a deception activity (correct response)
- ○ Both activities are deception activities because they involve manipulating information
- ○ Both activities are OPSEC activities because they help protect critical information

Feedback*: The team that is implementing physical security measures is using an OPSEC activity and the team disseminating false information is using a deception activity.*

Knowledge Check – 6

In the previous question, one team was implementing physical security measures to safeguard information while another team was disseminating false information about troop movements and mission plans. Which of the following best describes requirements for these strategies?

- ⊙ The team disseminating false information must receive additional authorizations and follow additional requirements. (correct response)
- ○ The team implementing physical security measures must receive additional authorizations and follow guidelines in DOD Instruction S-3604.01.
- ○ Both strategies must follow the guidance in DODM 5205.02.
- ○ Both strategies require formal approval.

Feedback*: The team disseminating false information must receive additional authorizations and follow additional requirements.*

Lesson 4 Review Activities

Knowledge Check – 1

Which of the following are key policy requirements for implementing the OPSEC program?

- ☐ All OSD and DOD Components must post incident reports publicly for accountability
- ☐ All OSD and DOD Components must identify and remove traditional security roles that are redundant with OPSEC personnel roles
- ☑ All OSD and DOD missions, functions, programs, and activities must be protected by an OPSEC program (correct response)
- ☑ All OSD and DOD Components must establish OPSEC programs with full-time OPSEC program managers and practitioners (correct response)

***Feedback**: All OSD and DOD missions, functions, programs, and activities must be protected by an OPSEC program and all OSD and DOD Components must establish OPSEC programs with full-time OPSEC program managers and practitioners.*

Knowledge Check – 2

Carol, a Security Practitioner, has developed a plan to train new and existing personnel in her department on critical information. Which of the following training activities best meets policy requirements?

- ○ Carol will train all personnel once a year focusing on what critical information is.
- ○ Carol will train new personnel during initial training and all personnel annually thereafter focusing on what critical information is.
- ○ Carol will train all personnel once a year focusing on what is considered critical information in the department.
- ⊙ Carol will train new personnel during initial training and all personnel annually thereafter focusing on what is considered critical information in the department. (correct response)

***Feedback**: Carol will train new personnel during initial training and all personnel annually thereafter focusing on what is considered critical information in their department.*

Knowledge Check – 3

Now that Carol knows what training activities she must perform, what training methods will best comply with policy requirements?

- ○ Carol distributes a slide deck via email that details the organization's critical information
- ⊙ Carol conducts a small group training session with tailored instruction on her organization's critical information (correct response)
- ○ Carol provides learners with an online training course on OPSEC that addresses critical information without local content
- ○ Carol conducts a small group training session where she provides generic information on critical information

***Feedback**: Conducting a small group training session with tailored instruction on your organization's critical information meets policy requirements.*

Knowledge Check – 4

Steve, a logistics coordinator, has access to unit deployment schedules and vehicle movement data. His coworker noticed that he has been downloading large amounts of planning documents to a personal thumb drive, outside of his normal duties. His pattern of behavior raises concerns. In this insider-threat scenario, what best describes OPSEC's primary role in protecting critical information?

- ○ OPSEC requires immediate public disclosure of the incident to preserve transparency
- ○ OPSEC requires issuing insider-threat alerts to all personnel whenever suspicious downloads occur
- ⊙ OPSEC includes analyzing observable behaviors (e.g., transfers to thumb drives) that might reveal critical information, and implementing countermeasures (correct response)
- ○ OPSEC mandates installation of computer tools to track unusual online activities

***Feedback**: OPSEC includes analyzing observable behaviors (e.g., transfers to thumb drives) that might reveal critical information, and implementing countermeasures.*

Knowledge Check – 5

Which of the following best describes the purpose and benefits of forming an OPSEC working group?

- ○ To assemble subject matter experts from different disciplines to enforce physical security measures like badge-access systems
- ○ To assemble subject matter experts from different disciplines to create standardized OPSEC policies
- ○ To assemble subject matter experts from different disciplines to conduct surveillance and audits for the OPSEC program
- ⊙ To assemble subject matter experts from different disciplines to identify mission-critical information, assess vulnerabilities, and determine countermeasures, as needed (correct response)

Feedback*: The purpose of OPSEC working groups is to assemble subject matter experts from different disciplines to identify mission-critical information, assess vulnerabilities, and determine countermeasures, as needed.*