OPSEC Awareness for Military Members, DoD Employees, and Contractors Course

Course Introduction

This presentation provides OPSEC awareness for military members, government employees, and contractors. The training provides information on the basic need to protect critical and sensitive unclassified and controlled unclassified information (CUI) to ensure safe and successful operations and personal safety.

Objectives

Protecting critical and sensitive information is essential to protecting the success of your organization and missions, and to protecting the lives of U.S. service members, DoD employees, and contractors.

Learning Objectives: After completing this training you will be able to:

- Define Operations Security (OPSEC)
- Identify critical information
- Describe the five-step OPSEC Process
- Recognize indicators and how they may lead an adversary to discover classified and unclassified critical information
- Apply appropriate countermeasures to protect critical information

What is Operations Security (OPSEC)?

OPSEC isn't just a set of rules that tells you what you should or shouldn't say:

- It's a process; a method of denying critical information to an adversary.
- A five-step process to identify, control and protect critical information and analyze friendly actions and indicators that would allow adversaries or potential adversaries to identify and exploit vulnerabilities.

Five-Step OPSEC Process

Department of Defense (DoD)

DoD leaders at all levels have the responsibility to integrate the five-step OPSEC process into the planning, execution, and assessments of their organizations day-to-day activities and operations.

Step 1 – Identify Critical Information

Let's review the five-step process.

Step 1 - Identify Critical Information

Within the Department of Defense critical information is information that the organization has determined is valuable to an adversary. This information will vary based on the organization's role. It is best identified by the personnel responsible for planning and executing the organization's mission.

Do you know what information must be protected? Do you understand why this information needs to be protected?

Step 1 - Identify Critical Information: What is Critical Information?

Critical information is unclassified or controlled unclassified information (CUI) about DoD activities, intentions, capabilities, or limitations.

- It includes indicators, which are specific facts (like puzzle pieces) that an adversary seeks to collect, analyze, and exploit in order to gain some type of an advantage (military, economic, geopolitical, etc.).
- It is sometimes revealed by publicly available information.

Step 1 - Identify Critical Information: Examples of Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI): Unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy.

Examples of CUI

- Pre-decisional information and meeting minutes
- Investigation documents
- Inspection reports
- Agency budgetary information
- Procurement bids/proposals
- Personally Identifiable Information (PII)
- Information protected under Privacy Act of 1974

Step 1 - Identify Critical Information: Examples of Critical Information

Adversaries collect information pertaining to U.S. DoD activities and technology to further their own agendas. Even pieces of unclassified information can hold great value to an adversary. Some examples of critical information are:

- Deployment dates and location
- Military operations
- Acquisition

- Agency Program of Instructions (POI)
- Position, mission capabilities and limitations

Additional examples include:
- Training operations and missions
- Schedules and travel itineraries
- Usernames, passwords, network details
- Social security number, credit cards, banking information

Adversaries can put together small details and indicators, called "aggregation," to deduce enough information about day-to-day activities or U.S. military plans and operations to do us harm.

Step 2 – Identify Threats

Let's review Step 2 of the five-step process.

Step 2 - Identify Threats

Within the Department of Defense threat information is necessary to develop appropriate countermeasures. The threat analysis includes identifying potential adversaries and their associated capabilities and intentions to collect, analyze, and exploit critical information and indicators. Organizations should seek support from their security, intelligence, and counterintelligence experts.

As an individual, whether you are at work, or outside of work, try and answer these questions. Who is an adversary? What are the adversaries' intentions? What is the adversary capable of doing?

Step 2 - Identify Threats: What is a Threat?

A threat is an adversary that has the capability + intent to take any actions detrimental to the success of DoD activities or operations.

An adversary is an individual, group, organization, or government that must be denied critical information (*DoDM 5205.02 "DoD Operations Security (OPSEC) Program Manual").*

Common examples of adversaries are sworn enemies, foreign governments, or terrorists, however, a threat can be anyone with the intent and capability to take actions detrimental to the success of DoD activities and operations.

Step 2 - Identify Threats: How is Information Collected?

Threats and adversaries can be anyone with the intent and capability to take actions detrimental to the success of DoD activities and operations. Adversaries exploit many vulnerabilities to collect our information. It is an individual responsibility to be aware of these threats. Some

examples of collection include:

- Observation of our actions to detect patterns to predict behavior
- Using the internet to collect data from social media sites (web pages, blogs, chat groups)
- Interception of our unsecured communications (phone calls - work or personal), unencrypted e-mails etc.
- Using people to collect information, listening to conversations in public, social engineering, etc.
- Going through our trash (at work and at home)
- Geolocation tracking of DoD personnel and their devices to collect patterns of life and deviations from that pattern

Step 3 – Analyze Vulnerabilities

Let's review Step 3 of the five-step process.

Step 3 - Analyze Vulnerabilities

Within the Department of Defense an OPSEC vulnerability exists when the adversary is capable of collecting critical information to exploit our vulnerabilities. Organizations are required to conduct assessments, exercises, and analyze operations to help identify vulnerabilities.

As an individual, whether you are at work, or outside of work, try and answer this question. What weaknesses can an adversary exploit to uncover critical information?

Step 3 - Analyze Vulnerabilities: What is a Vulnerability?

A vulnerability exists when the adversary is capable of collecting critical information or indicators analyzing it, and then acting quickly enough to impact friendly objectives.

An indicator is data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities.

Step 3 – Analyze Vulnerabilities: What are Vulnerabilities?

Critical information indicators often reveal small portions of information about a mission. They provide one piece of a larger puzzle. Adversaries capable of collecting, analyzing, and acting in time to impact friendly objectives create an OPSEC vulnerability. If adversaries collect and interpret enough indicators, they'll have a pretty good picture of the mission.

In short, they are clues that an adversary can interpret to uncover critical information. Look at these examples of vulnerabilities:

- Forgetting to remove your ID badge when you leave your facility
- Posting or sending sensitive information over the web (family members locations during deployment)
- Discussing sensitive (agency operational procedures) information in public, or over the

telephone

- Photos you take with your smartphones and load to the Internet that have been geotagged
- Using a device, application, or services with geolocation capabilities (e.g., fitness trackers, smartphones, tablets, smartwatches, and related software applications)

Step 4 – Assess Risks

Let's review Step 4 of the five-step process.

Step 4 - Assess Risks

Within the Department of Defense determining the level of risk is a key element of the OPSEC process. It involves assessing the adversary's ability to exploit vulnerabilities that would lead to the exposure of critical information and the potential impact it would have on the mission. It provides justification for the use of countermeasures based on a cost benefit analysis to mitigate risk.

As an individual, whether you are at work, or outside of work, try and answer these questions. If an adversary exploits a vulnerability, how will that affect the mission? What will be the overall impact of the adversary learning our critical information?

Step 4 - Assess Risks: Risk Assessment

Risk assessment is the process of evaluating risks to information based on susceptibility to collection and the anticipated severity of loss.

Step 4 - Assess Risks: How to Assess Risks?

Risk is the likelihood that an adversary will effectively collect, analyze, and exploit your critical information, thus having some level of impact on the mission, operation, or activity.

A risk assessment is a decision-making step to determine if a countermeasure needs to be assigned to a vulnerability based on the level of risk this vulnerability poses.

Step 5 – Apply OPSEC Countermeasures

Let's review Step 5 of the five-step process.

Step 5 - Apply OPSEC Countermeasures

Within the Department of Defense after conducting the risk assessment if the amount of risk is determined to be unacceptable, countermeasures are then implemented to mitigate risk or to establish an acceptable level. Countermeasures should be coordinated and integrated within other core program areas if applicable.

As an individual, whether you are at work, or outside of work, try and answer this question. How can I protect critical information?

Step 5 - Apply OPSEC Countermeasures: What are Countermeasures?

Countermeasures are designed to prevent an adversary from detecting critical information, provide an alternative interpretation of critical information or indicators (deception), or deny the adversary's collection system.

Step 5 - Apply OPSEC Countermeasures: How do I Apply Countermeasures?

Countermeasures are designed to prevent an adversary from detecting critical information. As an individual identify and implement actions you can take at, or outside of work to protect critical information. Look at some of the examples listed below:

- Think before you act by asking how can this information be used against me?
- Know what your agency considers critical information.
- Safeguard all sensitive, unclassified information.
- Understand OPSEC and data aggregation.
- Be aware of your surroundings.
- Use Social Media with caution by limiting the amount of personal information posted.
- Be aware the photos you take with your smartphones and load to the internet may have been geotagged.
- Be aware of information you are putting out in emails, online, phone conversations, photos and open unsecure conversations in public.
- Be aware of, or disable geolocation capabilities on devices or applications.
- Don't discuss details, such as:
    - Time lines, detailed locations, or movements
    - Limitations or capabilities
    - Specific names, ranks, job titles, or budgets
    - Current or future operations
    - Security procedures

If you identify any possible vulnerability to your organization's mission, you have the responsibility to report it.

Contact your Agency Security Manager or OPSEC Manager Representative if you have any questions or need additional information on OPSEC.

Summary

You should now be able to:

- Define Operations Security (OPSEC)
- Identify critical information
- Describe the five-step OPSEC Process
- Recognize indicators and how they may lead an adversary to discover classified and unclassified critical information
- Apply appropriate countermeasures to protect critical information