

OPSEC FUNDAMENTALS

I. OPERATIONS SECURITY (OPSEC)

NSDD-298 required that all executive departments and agencies with national security missions, and the contractors that support them, establish OPSEC programs.

The goal of OPSEC is to control information about your capabilities and intentions in order to keep them from being exploited by your adversary.

A. Definition of OPSEC

OPSEC is a systematic, proven process to identify, control and protect generally sensitive but *unclassified* information about a mission, operation or activity, and, thus, denying or mitigating an adversary's ability to compromise or interrupt that mission, operation or activity.

If an adversary has knowledge regarding your capabilities, interests, intentions, plans, or procedures, then he has an opportunity to exploit your vulnerabilities.

B. Definition of OPSEC terms.

Critical information includes specific facts about friendly intentions, capabilities, operations, and other activities vitally needed by adversaries for them to plan and act effectively, so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

Adversary is anyone who contends with, opposes or acts against your interest and must be denied critical information.

Threat is the capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of friendly activities or operations.

Indicators are observable or detectable activities or information that can be pieced together to reveal sensitive information regarding your operation.

Vulnerability is a weakness that can be exploited by an adversary to obtain your critical information, and it can be present in any facet of your operations.

Risk is the probability an adversary will compromise your critical information, and the impact this would have if the adversary is successful.

Countermeasure is *anything* that effectively negates or reduces an adversary's ability to exploit our vulnerabilities.

C. Describe how OPSEC fits into your organization.

OPSEC allows you to look at your operation from both the friendly and adversary perspectives.

II. OPSEC PROCESS

A. Definition of the OPSEC Process.

The **OPSEC process** is designed to determine how adversaries could collect information regarding a specific operation, activity, or project so that countermeasures can be implemented to prevent exploitation of associated critical information. The OPSEC process is often described as having five steps.

1. Identify the five steps of the OPSEC Process.

- Identify Critical Information
- Analyze the Threat
- Assess Risk
- Apply Countermeasures
- Analyze Vulnerabilities

Critical information is developed from analyzing both friendly and adversary strategies to achieve their objectives.

Threat is defined as the capability of an adversary, coupled with his intentions, to acquire and exploit critical information. Threat requires both intent and capability. If one or the other is not present, there is no threat. **In order to analyze the threat, you need to identify**

- What the adversary already knows.
- What the adversary needs to know to be successful.
- The adversary's intent and capability.
- Potential adversaries to your mission, operations, or activity.
- Where the adversary is likely to look to obtain the information.

Vulnerability exists when critical information is susceptible to exploitation by an adversary.

- An indicator includes any detectable activity and/or information that, when looked at by itself or in conjunction with something else, points to a vulnerability or critical information item that can be exploited by an adversary.

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

- You assess vulnerability in conjunction with the threat's intent and capability - is he willing to exploit your vulnerability and does he have the means to do so? Then, you determine the impact this would have on your mission if the threat was successful in exploiting the vulnerability. This determines the level of risk. You then decide if the resultant level of risk warrants the application of a countermeasure.

Risk has three components: Threat X Vulnerability X Impact = Risk (TxVxI-R)

- **Threat** is the adversary's intent and capability,
- **Vulnerability** is the weakness that provides the adversary's opportunity, and
- **Impact** is the potential negative consequences inflicted upon your mission.

Countermeasure is anything that effectively reduces an adversary's ability to exploit vulnerabilities. The following are examples of countermeasures...

- Changes in procedure
- Controlling Dissemination
- Cover and Deception
- Speed of execution
- Awareness training

III. APPLICATION OF OPSEC

Effective implementation of OPSEC policies and countermeasures will have a positive effect on most organizations and workplaces. Below are various **applications** of the OPSEC Process.

- **Day-to-Day Operations:** News releases, responses to requests, communications, and habits of your employees, people who come and go from your facility, and training are all activities which should include OPSEC.
- **Contingencies:** A contingency is a temporary period of adjustment to your normal work routine to cover some unique event. Remember, the adversary could be tipped off to a new activity by any detectable and observable change in the normal daily routine.
- **Planning:** You need to identify the responsibilities for all OPSEC actions in your plans, including identification of critical information, threat assessment, vulnerabilities, risk assessment, and countermeasure requirements. Being able to track this process allows you to detect any OPSEC problem very early, which can greatly minimize the damage an adversary can do.
- **Surveys:** Surveys look at the effectiveness of all existing countermeasures, identify any vulnerability, and assess the risks. Surveys focus on a specific activity or event a team who mirror the adversary's approach to intelligence collection conduct the surveys, so that a certain level of realism can be attained.

Benefits to you program by applying OPSEC to Day-to Day operations

- Incorporating OPSEC into operation planning provides for early detection of OPSEC problems.
- Incorporating OPSEC into your day-to-day operations makes OPSEC second nature to your employees.

WHAT IS OPSEC

An analytic *process* by which an organization can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.