LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

NOVEMBER 2025

OPERATIONS SECURITY (OPSEC)

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 a method of denying critical information to an adversary.
- OPSEC involves 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.

Step 1: Identify Critical Information. 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. 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 2: Identify Threats. Threat analysis reveals information that 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.

- 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.
- 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 operations.

Step 3: Analyze Vulnerabilities. When the adversary is capable of collecting critical information to exploit our vulnerabilities, it is vital that we understand what those vulnerabilities are. 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?

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

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com

- 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 4: Assess Risks. 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 to 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?

- **Risk assessment** is the process of evaluating risks to information based on susceptibility to collection and the anticipated severity of loss.
- 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 Countermeasures. After conducting the risk assessment, if the amount of risk is determined to be unacceptable, countermeasures are 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?

- **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.

- **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.

Examples:

- 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, posts, phone conversations, photos, and open unsecure conversations in public.
- Be aware of or disable geolocation capabilities on devices and 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 vulnerabilities to your organization's mission, you have a responsibility to report them.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com