What is OPSEC?

Operations Security (OPSEC) is an analytical process used to deny an adversary information - generally unclassified - about our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning process or operations. OPSEC does not replace other security disciplines - it supplements them.

OPSEC - A New Mindset

Our attention to security must change now. The events of September 11, 2001, proved there is a demonstrated and known threat. How many times have we heard that terrorism is a threat? But, most of us thought it could only happen elsewhere - not in America.

Unfortunately, we have suffered other terrorist attacks in recent years - such as the Oklahoma City and USS Cole attacks. In these cases, the adversaries were successful because they knew our vulnerabilities. Americans at large provided much of what was used against us. The only thing our enemies brought to the table was their personal agenda and their resolve.

As Federal employees, we are the representatives of the people. The American people trust us to do our jobs and keep them safe. The mishandling of information can put everything at risk and cost the lives of many Americans.

Why is it important to learn about OPSEC?

The information that is used against us often is not classified; it is information that is openly available to anyone who knows where to look and what to ask.

OPSEC is a tool that our adversaries believe in and one that we in the U.S. Government need to understand and integrate into our daily routines. Our work is information, and not all of it is classified. What we don't always realize is how much we are giving away by our predictable behavior, casual conversations, routine acquisitions and Internet information. We must be careful of what we are revealing - failure to do so could provide our adversaries with the information they need to execute additional terrorist acts.

What can I do to help thwart any future attempts to harm the U.S.?

We can all incorporate OPSEC into our everyday work routine. Practicing operations security will help you accomplish your goals. When you do something, ask yourself, "What could an adversary glean from the knowledge of this activity? Is it revealing information about what we do and how we do it?" It is helpful to view yourself and what you're doing as an adversary would. For example, what can be gained by observing your actions or reading what you place on a web site?

What are OPSEC indicators?

What do people observe about your schedule? What do you do when you go to work? What are you revealing by your predictable routines and the way you do business? These are indicators. OPSEC helps people identify the indicators that are giving away information about missions, activities, and operations.

Who is the adversary?

Let's not focus strictly on terrorists right now. Remember that there are other adversaries - for example, foreign intelligence services that continue to collect information on us that could be used to hurt us in the future. We sometimes only focus on what just happened - but it is a certainty that our adversaries will continually look for and find any weak links.

What are the capabilities of the adversary?

We can never underestimate the capabilities or strength of conviction of terrorists or any other adversary. Nothing is more dangerous than people who are willing to die for a cause.

What is the risk?

Everything we do involves risk. The application of the OPSEC process develops effective countermeasures to help us accomplish our missions by analyzing and minimizing the risk.

Our enemy took us by surprise and the country will never be the same. To bring the enemy to justice, we need to maintain the element of surprise. Every aspect of our operations is more sensitive than ever before. We must rededicate ourselves to our mission and our country to help ensure that it does not happen again. Security must be incorporated into every aspect of our jobs. If we are not vigilant in protecting critical information, it will happen again. The future of America depends on changing the way we look at security. OPSEC can make the difference. It is essential that it be understood and incorporated into everything we do.

The OPSEC Process

1 Identify Your Critical Information

What do you want to protect?

Why do you want to protect it?

Is it governed by a regulatory requirement?

Can it be defined as sensitive but unclassified?

Examples of potential critical information:

- Travel itineraries
- Operations planning information
- Employee addresses
- Employee phone lists
- Budget information
- Entry/Exit security procedures

2 Analyze the Threat

Who wants the sensitive information?

Is there more than one adversary?

What is their objective?

What will they do to get to your sensitive information?

What methods will they use to get it?

There are 2 elements of threat:

- Intent
- Capability

3 Analyze the Vulnerabilities

How is your information vulnerable?

How is it protected or not protected?

Or, is it properly protected?

Examples of vulnerabilities:

- Critical information posted on the Internet
- Non-secure communications

4 Assess the Risk

Is the risk great enough to do something about the threat?

How would the loss of sensitive data affect your operations?

What would be the cost of losing sensitive information?

Risk is determined by analyzing 3 factors:

- Threat
- Vulnerability
- Impact

5 Develop and Apply Countermeasures

What countermeasures will block access to your information? Adopt measures specific to your operation.

Examples of countermeasures:

- Limit web page access
- Shred sensitive hard copy
- Sanitize bulletin boards
- Monitor public conversations
- Do not use e-mail to discuss sensitive operations
- Training and awareness

U.S. DEPARTMENT OF HOMELAND SECURITY

Department of Homeland Security
Office of Security
Phone: (202) 447-5010
E-mail: OfficeofSecurity@dhs.gov

What OPSEC Means to You

Office of Security
Operations Security (OPSEC) Program

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security