OPSEC Countermeasures

Below are some basic OPSEC practices that can reduce your risk of accidentally disclosing critical information:

Do:

- Know the critical information for your programs and activities.
- Properly handle and destroy all classified and sensitive unclassified information.
- Remember: phone, fax, and radio communications can be intercepted.
  - ◊ Always use the most secure means to transmit information.
  - ◊ Be aware of your surroundings.
- Observe the Need-to-Know (NTK) principle.
  - ◊ Share critical and sensitive information only with those who have a NTK.
  - ◊ Only discuss critical or sensitive information in suitable locations such as your office or a conference room.
- Put your federal credential or badge away or lock it up when you are away from SNL.

Don't:

- Respond to (but report) unsolicited requests from any source.
- Reveal critical and sensitive information on social networking sites.
- List (try to avoid) your employment at SNL (Facebook, Twitter, etc.).
- Put critical and sensitive information in blue/yellow recycling or trash bins.
- Post critical and sensitive information on walls, bulletin boards, or SNL websites.

OPSEC Program Office

SNL's OPSEC Program Office is here to help. We offer the following services to all organizations at SNL:

- OPSEC awareness and training.
- OPSEC reviews and assessments.
- Assistance with identifying operational vulnerabilities.
- Assistance in selecting countermeasures to mitigate risks.

The OPSEC Program Office is here to support your organization—not criticize. We're here to help you find facts—not faults!

Security& YOU
Think. Assess. Protect.

OPSEC's Internal SNL Website
security.sandia.gov
search "OPSEC"

OPSEC Hotline
505-844-OPSEC

Security Connection
505-845-1321

U.S. DEPARTMENT OF ENERGY
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multiprogram laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2014-20431 M

Exceptional service in the national interest

Sandia National Laboratories

A Guide to OPERATIONS SECURITY

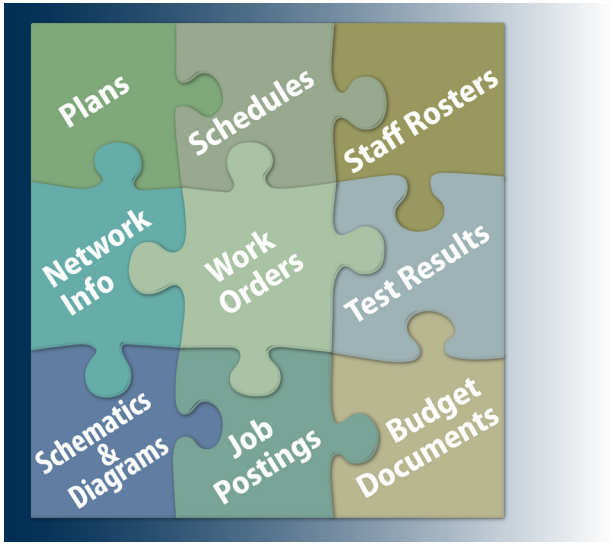
OPSEC

What is OPSEC?

Operations Security or OPSEC is an analytical process used to deny or delay our adversaries of SNL's critical information. Using OPSEC enhances mission success. OPSEC is not just a program—it supplements SNL's security disciplines by using the five-step process. It is a requirement per DOE Order 471.6, Information Security.

Information Collection

Collecting information is much like assembling a jigsaw puzzle. Each piece of the puzzle could be an item of information that is not classified or sensitive by itself, but when combined with other pieces of the puzzle, creates a complete picture that could damage SNL or its customers. Our adversaries do not need all the pieces to understand the whole picture.



Workplace OPSEC Practices

The easiest way for adversaries to gain valuable information about SNL is through our carelessness. Adversaries can piece together information from bits of a conversation overheard in a public setting, or from an article in the Lab News or web page. We need to understand the value of all kinds of critical and sensitive information and take steps to protect it.

OPSEC Five-Step Process

Everyone needs to be aware of the OSPEC process and practice it in daily operations. The steps below will help you incorporate OPSEC practices in your organization's programs and activities:

1. Determine Critical Information.

Critical information is any information—classified or unclassified—that adversaries need in order to cause damage to SNL. What information do you need to protect? Do you have unclassified information that needs to be protected from unlimited release? Knowing what needs to be protected is the first step in determining how to keep your information safe. The SNL Critical Information List is located on the OPSEC website and organized by sensitive programs and activities.

2. Analyze the Threat.

Who wants your critical information? The OPSEC Program publishes a list of potential threats to SNL. Current threats are:

- Foreign Intelligence Services
- Insiders
- Cyber Hackers
- Terrorists
- Criminals
- Disturbed Persons
- Violent Activists

3. Determine Vulnerabilities.

How can adversaries obtain SNL's critical information? Studying your operations from an adversarial perspective will help you determine how well your critical information is protected.

4. Analyze the Risk.

What are the consequences if SNL critical information is lost? Estimating the potential effects of compromised vulnerabilities and doing a cost-benefit analysis can help you make the right decisions about what OPSEC countermeasures to implement.

5. Develop and Implement Countermeasures.

What measures are needed to protect SNL's critical information? You can determine what actions will be most effective for minimizing the risks to your organization by using the information identified in steps 1-4.