THE PROCESS OF OPSEC

1. IDENTIFY CRITICAL INFORMATION

The first step in the OPSEC process is to determine which information is critical to the organization. Critical information is that which would harm the organization's ability to effectively carry out normal operations if obtained by an adversary. Usually, this information includes the core secrets of an organization and can vary from one organization to the next.

2. ANALYZE THE THREAT

Once the critical information is identified, the next step is to determine the individuals or groups that represent a threat to that information. There may be more than one adversary, and different pieces of information may be targeted by different groups. In this stage, the adversary's capabilities, use for the information, and resources must also be analyzed.

3. ANALYZE THE VULNERABILITIES

In this phase, "think like the wolf" and view the organization from an adversary's perspective. The vulnerabilities of the organization must be thoroughly explored, especially in terms of physical safeguards, network/electronic safeguards, and personnel training.

4. ASSESS THE RISKS

For each vulnerability, the threat must be matched. At this point, each vulnerability is assigned a risk level. This is an unmitigated risk level, meaning that any corrective factors are not included in the analysis.

5. APPLY THE COUNTERMEASURES

Beginning with high-risk vulnerabilities, a plan is put in place to mitigate the risk factors. The most important element of this step is to develop a plan to lower or eliminate the risk or remove the threat's access to the resource.

COUNTERMEASURES

Countermeasures are any steps taken to mitigate the risk and reduce the loss of critical information. Examples of countermeasures you should employ include:

- Properly shred classified and sensitive information, including PII
- Use appropriately encrypted radios, telephones, faxes, and email communications
- Never speak about classified or sensitive information in public
- Always apply the need-to-know principle
- Think before you speak
- Adhere to all security and IA policies and procedures

OPSEC

OPSEC focuses on identifying and safeguarding sensitive or critical information, whether it's about you, your family, your coworkers, your overall mission, or your day-to-day operations. Whether we realize it or not, every day there are adversaries, such as terrorists, spies, and criminals, trying to gain this information. They piece together bits of data, especially unclassified open-source information, to determine the big picture related to our missions. Use of OPSEC every day can help make sure this does not happen. Your understanding and use of sound OPSEC practices may save lives. . . including your own!

CRITICAL INFORMATION

Your critical information is any information that you or your mission manager considers sensitive. Here are some examples:

- Names and photos of you, your family, and coworkers
- User names, passwords, computer and networking information
- Personnel information, including rosters, clearance level, personal addresses and phone numbers
- Operational, security, and logistical data
- Mission capabilities or limitations
- Schedules and travel itineraries
- Social Security numbers, credit card numbers, and banking info
- Building plans
- Budget information

THE THREAT

An adversary is any person or group that collects information about the Navy or Marine Corps and intends to use that information to cause harm to operations and assets and includes foreign intelligence organizations, terrorist groups, lone criminals, and organized criminal enterprises.

Adversaries may use multiple methods to collect information:

- Searching trash containers
- Monitoring radio frequencies, cellphones, wireless devices, email, faxes, and telephones
- Monitoring and exploiting the Internet and SNS
- Elicitation
- Eavesdropping and electronic surveillance

OPSEC process retrieved from http://www.opsecprofessionals.org/process.html

FEB12

STAY ALERT
USE OPSEC
YOU NEVER KNOW
WHO'S THERE

Operations Security (OPSEC)
A Guide to Protecting DON Missions,
Operations, and Personnel

NCIS

YOU NEVER KNOW WHO'S OUT THERE! PROTECT DON MISSIONS, OPERATIONS, AND PERSONNEL ... USE OPSEC

HOW TO KEEP YOUR INFO LOCKED

OPSEC AND SOCIAL NETWORKING SITES

Social networking sites, such as Facebook and Twitter, are great ways to connect with people, share information, and market products and services. However, these sites can also provide adversaries with the critical information they need to disrupt your mission and harm you, your coworkers, and even your family members. Think before your post! Remember, your information could become public at any time due to hacking, configuration errors, social engineering, or the business practice of selling or sharing user data.

SNS SAFETY CHECKLIST ✓

PERSONAL INFORMATION – DO YOU:

✔ Keep sensitive, work-related information OFF your profile?

✔ Keep your plans, schedules, and location data to yourself?

✔ Protect the names and information of coworkers, friends, and family members?

✔ Tell friends to be careful when posting photos and information about you and your family?

POSTED DATA – BEFORE POSTING, DID YOU:

✔ Check all photos for indicators of work-related information in the background and reflective surfaces?

✔ Check file names and file tags for sensitive data (your name, organization, and other details)?

PASSWORDS – ARE THEY:

✔ Unique from your other online passwords?

✔ Sufficiently hard to guess?

✔ Adequately protected (not shared or given away)?

SETTINGS AND PRIVACY – DID YOU:

✔ Carefully look for and set all of your privacy and security options?

✔ Determine both your profile and search visibility?

✔ Sort "friends" into groups and networks and set access permissions accordingly?

✔ Verify through other channels that a "friend" request was actually from your friend?

✔ Add new "untrusted" people with the lowest permissions and accesses to the group?

SECURITY – REMEMBER TO:

✔ Use and keep security software (anti-virus, anti-spyware, anti-phishing and firewalls) updated.

✔ Beware of links, downloads, and attachments just as you would in emails.

✔ Beware of "apps" or plug-ins, which are often written by unknown third parties that could use them to access your data and friends.

✔ Look for HTTPS and the lock icon that indicate active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

REMEMBER:

➜ Unclassified information is important, too – pieced together, it can reveal the whole picture.

➜ Adversaries do not have to follow legal procedures to collect information.

➜ Protecting DON information is everyone's responsibility.

➜ Practicing good OPSEC will help safeguard DON personnel, missions, and facilities.

THINK YOU ARE SAFE?

- A U.S. government official on sensitive travel to Iraq created a security risk for himself and others by tweeting his location and activities every few hours.
- According to the Al Qaeda Handbook, terrorists search online for data about "Government personnel, officers, important personalities, and all matters related to them (residences, work place, times of leaving and returning, children, places visited.)"
- Several kidnappings, rapes and murder cases were linked to social networking sites (SNS) where the victims first connected with their attackers.
- SNS have become a haven for identity thieves and con artists trying to use your information against you.
- A family on vacation kept friends up-to-date via online profiles; their home was burglarized while they were away.

The Al Qaeda manual that was recovered in Afghanistan points to the criticality of unclassified information. The manual states that by "using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." *–John Ashcroft, former U.S. Attorney General*

24/7 ANONYMOUS **TIP** SUBMISSION
TEXT • WEB • SMARTPHONE APP

REPORT IT! Phone 1-800-543-6289 | Web www.ncis.navy.mil | Text "NCIS "+ your tip info to CRIMES (274637)