Protect our Critical Information

Why OPSEC?

Our adversaries are **constantly** *collecting*, *compiling* and *analyzing* seemingly harmless pieces of information they obtain from open sources and other observable activities. The OPSEC process should be used to slow the flow of information of potential intelligence value where it can be readily collected.

Our adversaries routinely use our own information against us for sabotage, espionage, subversion and terrorism efforts. Poorly executed OPSEC enables adversarial activities, including:

❑ **Target selection for "spear-phishing" campaigns often enabling penetration of our networks**:

- ➢ *Exploitation of our networks for information*
- ➢ *Implant software on our networks in preparation for further operations*
- ➢ *Attack or degrade our networks, and ultimately our operational capabilities, in time of crisis*

❑ **Intelligence collection designed to**:

- ➢ *Enhance their military, economic or political situation*
- ➢ *Enable terror or criminal activities*
- ➢ *Degrade our mission effectiveness*
- ➢ *Shorten system combat-effective life*
- ➢ *Support adversary R&D efforts aimed at eliminating our technological advantage*
- ➢ *Force changes in program direction forcing significant delays and co$t*
- ➢ ***Kill***, ***Counter***, *or* ***Clone*** *our technologies & capabilities*

"…we have helped our adversaries by not following the OPSEC process. Technologies and concepts we have worked long and hard to develop have found their way into foreign weapon systems. Our adversaries are able to develop and field advanced and capable weapon systems at reduced costs and in shorter time than ever before, because of their ability to glean information, often from open sources."

Oct 2010, "Message from the Commander ", NAVAIR Vector Newsletter, by VADM David Architzel (USN RET), NAVAIR Commander, May 2010 – Sep 2012

For More OPSEC Information

Access the link below to view the video, "OPSEC Awareness for Military Members, DOD Employees and Contractors":

http://cdsetrain.dtic.mil/opsec/index.htm

For OPSEC questions, contact the RED-INC Facility Security Officer (FSO):

Valerie James
301-737-4361
valerie.james@red-inc.us

NAVAIR Operations Security (OPSEC)

Information Pamphlet

What is OPSEC?

A proven analytical process used to deny an adversary information, generally unclassified, concerning friendly intentions and capabilities by identifying, controlling, and protecting **indicators** associated with planning processes or operations.

✓*OPSEC does not replace other security disciplines - it supplements them.*

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*

Protect our Critical Information

Critical Information

One of the toughest aspects of OPSEC is simply defining your critical information, or what you need to protect

DoD Definition *- Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.*

Working Definition *- Any information that you or your organization considers sensitive and of potential intelligence value to an adversary. Such as:*

- *Mission capabilities or limitations*
- *Operational characteristics*
- *Operational, security, and logistical data and procedures*
- *Testing schedules & objectives*
- *Travel itineraries*
- *Building plans*
- *Budget information*
- *User names, passwords, computer and networking information*
- *Personnel information anything considered or containing PII, including; organizational charts, rosters, clearance levels, personal addresses/email addresses, phone numbers, photos, etc*

THE OPSEC PROCESS

1. IDENTIFY CRITICAL INFORMATION

What do we want to protect?

The first step in the OPSEC process is to determine which information is critical to the organization. Critical Information, obtained by our adversaries, effects the organization's ability to effectively carry out normal operations, as well as negatively affect our technological, operational or competitive advantage. NAVAIR maintains a general Command Critical Information list, programs should develop a tailored version.

2. ANALYZE THE THREAT

Who wants it & could they get it?

Once critical information is identified, the next step is to determine the individuals or groups that represent a threat to that information. An adversary must have both the capability and intent to collect the information to be considered a threat. Information sharing and evolving cyber threats adds complexity.

3. ANALYZE THE VULNERABILITIES

How could they get it?

In this phase, 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 observable activities. Look for the nexus between the previously identified threats and your vulnerabilities.

4. ASSESS THE RISKS

What are the consequences of loss?

*Risk is determined by analyzing **threat**, **vulnerability** and **impact.** Ultimately it comes down to asking whether the risk is great enough to enact appropriate countermeasures?*

5. APPLY THE COUNTERMEASURES

What reduces/eliminates vulnerabilities?

What solutions can we employ to reduce risks to an acceptable level, whether by eliminating indicators or vulnerabilities, disrupting the effective collection of information, or by preventing the adversary from accurately interpreting the data?

Countermeasures - *Anything that reduces the level of risk to your operation*

- Countermeasures need not be exotic or expensive; simply smarter
- Countermeasures may focus on:
  1. *Reducing the level of threat posed by an adversary,*
  2. *Reducing or eliminating a vulnerability,*
  3. *Or reducing the amount of potential impact caused by compromise of your critical information*
- Following a cost-benefit analysis, countermeasures are implemented in priority order to ensure the success
- Frequently a combination of low cost countermeasures provides the best overall protection
- All possibilities should be considered and the potential effectiveness of each should be evaluated
- Again, weigh the cost/effort versus the benefit

OPSEC Policy & Guidance:

- **NSDD 298**, *"National Operations Security Program"*, 22 Jan 1988
- **DoD Directive 5205.02 E**, *DoD Operations Security (OPSEC) Program"* , 20 June 2012
- **JP 3-13.3**, *"Operations Security"*, 4 Jan 2012
- **NTTP 3-54M/MCWP 3-40.9** *"Operations Security"*, Mar 2009
- **DoD 5205.02-M**, *"DoD Operations Security (OPSEC) Program Manual"*, 3 Nov 2008
- **DoD Instruction 8550.01**, *"DoD Internet Services and Internet-Based Capabilities"*, 11 Sep 2012
- **OPNAV Instruction 3432.1A**, *"Operations Security"*, 4 Aug 2011