Operations Security
(OPSEC)
• Background
• What is it?
• Why do we need it?
• Who should use it?
• Goal
• Key Terms
• The 5-Step Process
• OPSEC Applications
OPSEC Background

• National Security Decision Directive (NSDD) 298, identified and formalized the five-step OPSEC process.
• NSDD 298 required all executive departments and agencies, with national security operations, and the contractors that support them, to establish OPSEC programs.
• Interagency OPSEC Support Staff (IOSS) was established to direct and support this directive.
What is OPSEC?

Definition:
A systematic proven process to identify, control and protect generally sensitive but unclassified information about a mission, operation or activity and thus denying or mitigating an adversary’s ability to compromise or interrupt that mission, operation or activity.
Why do we need OPSEC?

- To ensure mission effectiveness
- To protect critical information
- To protect the integrity of a mission
- To maintain an element of surprise

*OPSEC looks at critical information from both a friendly and adversary perspective.*
Who should use OPSEC?

OPSEC can be used by the military, government institutions, corporations, schools, communities and individuals.

OPSEC can be used for but not limited to the following:

• Planning and Forecasting special events
• Special Training Exercises
• Standard Operating Procedures
• Methods, Sources, and Technical Tradecraft
• At home and on vacation
• Contracts/Bidding Processes
• Software and Source Code
OPSEC Goal

To control information about your organization’s capabilities and intentions in order to keep them from being exploited by your adversaries.

*OPSEC does not replace other security disciplines; it supplements them.*
Key Terms

1. **Critical Information** – Specific facts about friendly operations, needed by an adversary, in order to plan, act and guarantee failure of your mission.

2. **Adversary** – An opponent who opposes your interest and who must be denied critical information of your mission (the bad guy).

3. **Threat** – The capability and intent of an adversary to undertake actions that will be detrimental to the success of your operation.

4. **Indicator** – Observable activities or clues that can reveal sensitive information about your operation. Indicators can be exploited by an adversary and used to their advantage.
5. **Vulnerability** – A weakness that can be exploited by an adversary to obtain critical information about your mission.

6. **Risk** – The probability that an adversary will compromise your critical information, and the impact the act will have on your mission.

7. **Countermeasure (CM)** – Anything that effectively negates or reduces an adversary’s ability to exploit your vulnerabilities.
The 5 Steps of OPSEC

The OPSEC 5-Step Process provides: a holistic picture, a systematic process for mission success and an analytical methodology for assessing critical information.

1) Identify Critical Information
2) Analyze Threats
3) Analyze Vulnerabilities
4) Assess Risk
5) Apply Countermeasures
Step 1. Identify Critical Information

Critical Information is developed from analyzing both friendly and adversary strategies to achieve objectives.
Step 2. Analyze the Threat

- Identify the potential adversary(s)
- Identify intent and capabilities
- Identify what the adversary(s) already knows (public information)
- Identify what the adversary(s) needs to know
- Identify where the adversary(s) may look to obtain critical information of your operation
Step 3. Analyze Vulnerabilities

Some examples of vulnerabilities are:

- Lack of training
- Use of non-secure communications
- Publishing VIP itineraries
- Poor system design
Step 3. Analyze Vulnerabilities (cont’d)

Three indicator categories that can lead to vulnerabilities or reveal critical information:

1. Patterns and daily routines can establish a profile
2. Sudden change in normal conduct; deviations
3. Tip-off indicators show an adversary where to focus attention
Step 4. Assess Risk

Risk has three components:

** All Three Components Must Be Present For Risk To Exist **

Threat $\times$ Vulnerability $\times$ Impact = Risk

- **Adversary’s intent**
- **Weakness giving adversary an opportunity**
- **Negative consequences on a mission**

**All Three Components Must Be Present For Risk To Exist**
Step 4. Assess Risk (cont’d)

Risk Assessment is the decision-making step, once a vulnerability has been detected, to determine if countermeasures should be applied.

Two methods used to assess risk:

1. **Intuitive Reasoning Approach** – gained from personal experience

2. **Committee Approach** *(preferred method)* – several people look at the same problem and determine the answer collectively
Step 5. Apply Countermeasures

Examples of Countermeasures:


2. Limit distribution to **ONLY** those who need it for operational use.

3. Cover and Deception can conceal the nature of the mission, but is difficult to implement and sustain - also very costly.

4. Accelerate the schedule.

5. Awareness training for all personnel. Know and understand the threat and how to protect critical information from potential adversaries.
A combination of low-cost countermeasures are the best overall protection.

** ALWAYS weigh the Cost vs. the Benefit **
OPSEC Applications

• Benefit day-to-day operations by making OPSEC practices ‘second nature’ to all personnel.
• Lessen contingencies by reducing indicators and avoiding tip-offs.
• Increase early detection when used in the planning phase of a task.
• Allows for change in procedures over time, through surveys.
“The number of known adversaries conducting research on information attacks is increasing rapidly and includes intelligence services, criminals, industrial competitors, hackers and disgruntled or disloyal insiders.”

- George Tenet  
  (Former Director, CIA)
REMEMBER

Protecting **YOUR** information is **YOUR** responsibility!!

“In wartime, the truth is so precious that it must be protected by a bodyguard of lies.”

– Winston Churchill