



Security Awareness Training



So What Is OPSEC?

“Operations Security”

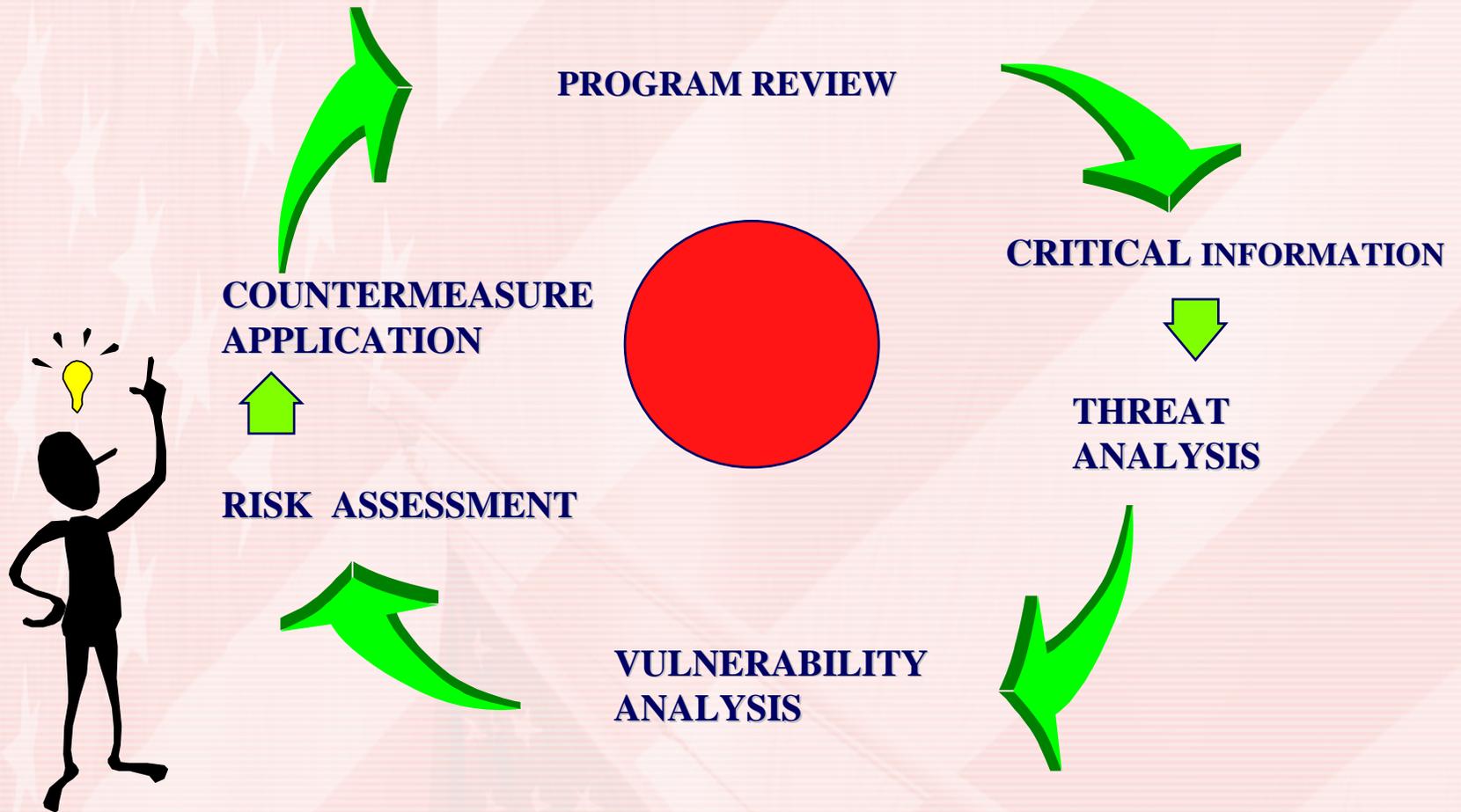
OPSEC deals primarily with protecting sensitive but unclassified information that can serve as indicators about our mission, operations and capabilities

- A Five Step Process

- 1. Identify Critical Information (CI)
- 2. Analyze the threat to the CI
- 3. Determine OPSEC vulnerabilities
- 4. Determine the acceptable level of risk
- 5. Implement appropriate countermeasures



The OPSEC Process





You already practice OPSEC at home

When most of us leave home for vacation, we take actions to protect our homes while we're away.

We may:

- Stop newspaper deliveries
- Have the yard mowed
- Buy light timers
- Have a neighbor get the mail
- In short, we want our houses to look like someone is home



What is Critical Information?

- Critical Information (CI) is information which can potentially provide an adversary with knowledge of our intentions, capabilities or limitations. It can also cost us our technological edge or jeopardize our people, resources, reputation and credibility.
- Controlled unclassified information, is often identified as Critical Information.



Information Designations

- For Official Use Only (FOUO)
 - Non-classified but sensitive DoD information
 - Some CAP missions are designated FOUO
 - CAP radio frequencies are designated FOUO
- Other agencies use similar designations
 - Sensitive But Unclassified (SBU)
 - Law Enforcement Sensitive (LES)
 - Trusted Agent – Eyes Only, etc.



Control of Critical Information

- Regardless of the designation, the loss or compromise of sensitive information could pose a threat to the operations or missions of the agency designating the information to be sensitive.
- Sensitive information may not be released to anyone who does not have a valid "need to know".



Examples of Critical Information

- Deployments
 - Chaplain or other support requested of CAP
- Technology
 - Capabilities of SDIS, ARCHER
- Exercises
 - CAP participation in DoD exercises
- Missions
 - Planned intercept missions
 - Law enforcement support missions
 - Major event support like the Super Bowl or Olympics
- Communications
 - Frequencies and access tones
- Locations of Resources
 - Airplanes, Vehicles, Repeater Sites, etc.



The Threat

Others constantly study us
to determine our weaknesses

- Their Tools:
 - HUMINT
 - Human Intelligence
 - SIGINT
 - Signals Intelligence
 - COMMINT
 - Communications Intelligence
 - ELINT
 - Electronic Intelligence
 - Many more "INTs"





HUMINT – You could be a target!

Watch what you say to:

- The public/media
- Friends
- Professional Colleagues outside of CAP/DoD

Places to be especially wary

- At work
- Bars and restaurants
- Conventions/symposiums

Don't try to impress people with your knowledge

- Loose Lips Sink Ships!



SIGINT, COMMINT, ELINT

Americas enemies actively target US military communications systems

- CAP performs non-combat *military missions* and operates *on military frequencies*
- CAP is entrusted with more sensitive military information than you may think
- Don't assume we're immune because we're out of the mainstream military presence
 - For that reason we can actually be *MORE* vulnerable
- Watch what you transmit on:
 - Radios, phones, Fax, and email



Vulnerability: Public Web Sites

Publicly accessible web sites will NOT contain:

- For Official Use Only (FOUO) Information
 - Such as CAP frequencies
- Sensitive Information
- Plans
- Planned Deployments
- Personal Information
 - SSANs
 - Home phone numbers



Marking Documents

- Documents containing FOUO info must be marked

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Information contained in this document is designated by the Department of Defense (DoD) as For Official Use Only (FOUO) and may not be released to anyone without the prior permission of NHQ CAP and/or CAP-USAF

- Examples of CAP FOUO documents:
 - Exercise or operational plans
 - Lists of CAP radio frequencies or access tones



Marking Documents

- Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings that alert the holder or viewer that the material contains FOUO information.
- Each part of electrically transmitted messages containing FOUO information shall be marked appropriately. Messages containing FOUO information shall contain the abbreviation "U//FOUO" before the beginning of the text.



Protection of FOUO Information

- FOUO information should be stored in locked desks, file cabinets, bookcases, locked rooms, or similar items, unless Government or Government-contract building security is provided.
- FOUO documents and material may be transmitted via first-class mail, parcel post or -- for bulk shipments -- fourth-class mail.
- Electronic transmission of FOUO information (voice, data or facsimile) should be by approved secure communications systems whenever practical.



It's Everyone's Responsibility

- The purpose of the security program is to protect against unauthorized disclosure of official information. Keep your information secure at all times.
- OPSEC is mostly common sense. If we all take the time to learn what information needs protecting, and how we can protect it, we can continue to execute our mission effectively.



Disclosure of Information

Disclosure of information, quite simply is when information passes from one party to another.

When dealing with sensitive information, it is the responsibility of the party possessing the information to ensure it is not disclosed to parties who do not have a need for or a right to the information.





Authorized Disclosure

Disclosure of sensitive information is authorized only when the party receiving the information can be properly identified and has a "need to know."

"Need to Know" does not mean, because a person holds a high management position, he or she automatically needs access to the information.





Unauthorized Disclosure

Unauthorized disclosure of sensitive information is when the party receiving the information does not have a "Need to Know."

In most cases, unauthorized disclosures are **unintentional** and due to poor planning or a failure to think by the possessing party.





Unaware of Surroundings

One of the leading causes of unintentional disclosures is simply people not being aware of what is happening around them.

Discussing sensitive information when you are unsure or unaware of your surroundings can quickly lead to this information being disclosed to the wrong people.

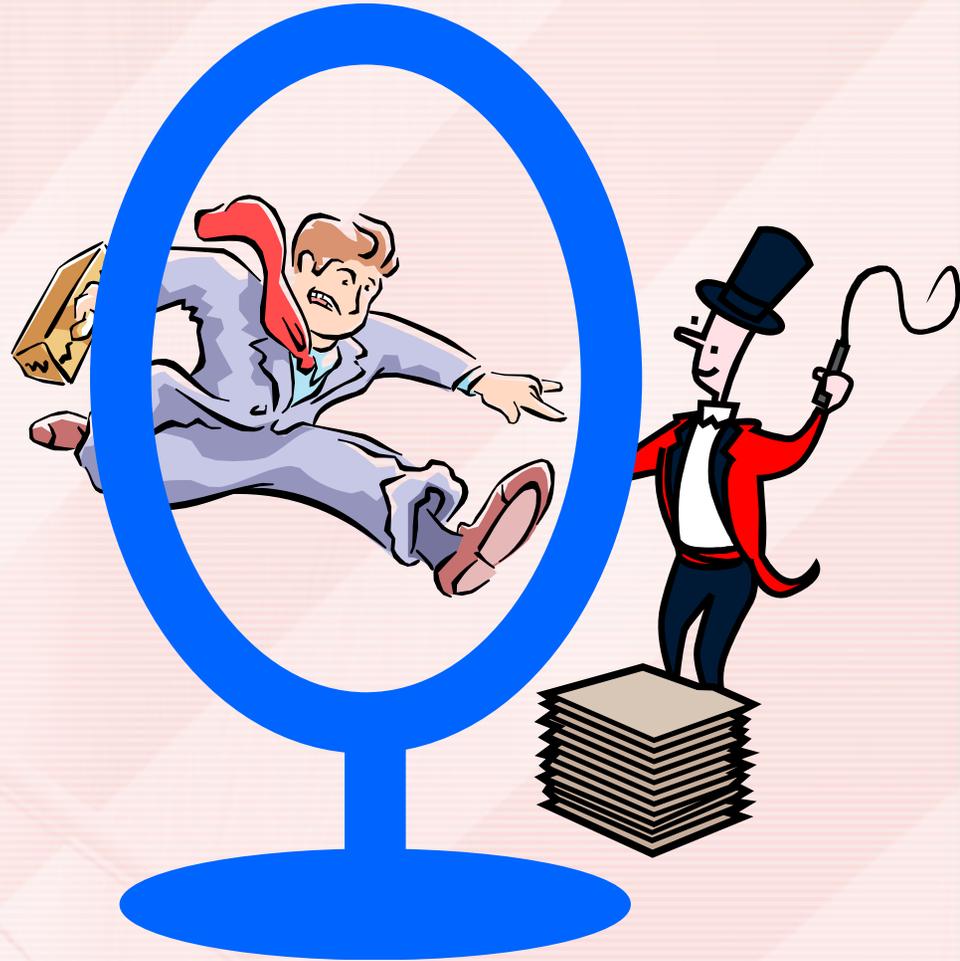




Awe Of Position

We all want to please our commanders, and work very hard each day to do so.

However, even if a superior officer requests something that is sensitive in nature, we must still make sure they meet all the requirements for access to this information just like everyone else.





The “Message”

- Operations Security is everyone’s business
- Good OPSEC saves lives and resources
- Always use common sense and stay alert
- Only release info to those with a valid need-to-know
- Identify vulnerabilities to your commander



The Bottom Line

- OPSEC is a time-tested process that analyzes threats, identifies Critical Information, and develops appropriate countermeasures
- OPSEC is used by all of us in everyday life
- OPSEC is not so much a bunch of security rules, but a common-sense approach to viewing your operations through the adversary's eyes
- OPSEC increases opportunities for mission success by protecting Critical Information
- You are the key to making OPSEC work!



Success Means...

- Being effective in helping defend our homeland
- Keeping CAP and Air Force people alive and safe
- Helping America keep its technological and military advantage
- Helping preserve freedom and liberty