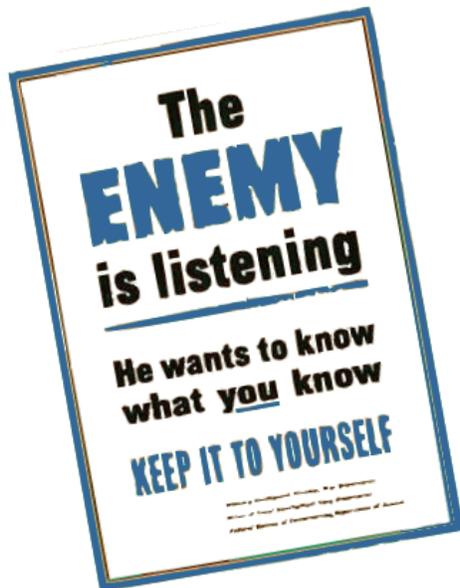


Chapter 8

OPERATIONAL SECURITY

Intelligence collection and analysis is very much like assembling a picture puzzle. Intelligence collectors are fully aware of the importance of obtaining small bits of information (or "pieces" of a puzzle) from many sources and assembling them to form the overall picture. Intelligence collectors use numerous methods and sources to develop pieces of the intelligence puzzle . . . their collection methods range from sophisticated surveillance using highly technical electronic methods to simple visual observation of activities (these activities are referred to as "indicators"). Information may be collected by monitoring radio and telephone conversations, analyzing telephone directories, financial or purchasing documents, position or "job" announcements, travel documents, blueprints or drawings, distribution lists, shipping and receiving documents, even personal information or items found in the unclassified trash.

The premise of OPSEC is that the accumulation of one or more elements of sensitive/unclassified information or data could damage national security by revealing classified information. The goal of OPSEC, as a "countermeasures" program, is to deny an adversary pieces of the intelligence puzzle.

There is nothing new about the principles underlying OPSEC. In fact, we can trace OPSEC practices back to the colonial days and the Revolutionary War. George Washington, our first president, was a

known OPSEC practitioner. General Washington was quoted as saying, "Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion."

However, OPSEC, as a methodology, originated during the Vietnam conflict when a small group of individuals were assigned the mission of finding out how the enemy was obtaining advance information on certain combat operations in Southeast Asia. This team was established by the Commander-in-Chief Pacific, and given the code name "PURPLE DRAGON."

It became apparent to the team that although traditional security and intelligence countermeasures programs existed, reliance solely upon them was insufficient to deny critical information to the enemy--especially information and indicators relating to intentions and capabilities. The group conceived and developed the methodology of analyzing U.S. operations from an adversarial viewpoint to find out how the information was obtained.

The team then recommended corrective actions to local commanders. They were successful in what they did, and to name what they had done, they coined the term "operations security."

OPSEC and Government Activities

Over the years it became increasingly apparent that OPSEC had uses in virtually every government program that needed to protect information to ensure program effectiveness. OPSEC professionals modified and improved techniques based on experience gained with many different organizations and in areas such as military combat operations.

Today, OPSEC is as equally applicable to an administrative or research and development activity as it is to a combat operation. If OPSEC is not integrated into sensitive and classified activities, chances are that our adversaries will acquire significant information about our capabilities and limitations. It probably would have been difficult for the "Purple Dragon" team to foresee that, 20 years later, the methodology they developed would become a national program.

OPSEC at Home

You have probably been practicing OPSEC in your personal life without knowing it! When you are getting ready to go on a trip have you ever:

- Stopped the delivery of the newspaper so that they would not pile up outside and send a signal that you are not home?
- Asked your neighbor to pick up your mail so the mailbox would not fill up, also indicating that you are away?
- Connected your porch lights and inside lights to a timer so they would go on at preset times to make it look like someone is home?
- Left a vehicle parked in the driveway?

Connected a radio to a timer so that it comes on at various times to make it sound like that someone is inside? Well, guess what you did? You practiced OPSEC!

The critical information here is obvious - we do not want anyone to know the house is unoccupied. None of the actions (countermeasures) listed above directly conceal the fact that your residence is unoccupied. A newspaper on the lawn or driveway does not necessarily mean no one is at home. Newspapers in the yard or driveway are only an indicator to the adversary. That indicator, combined with other indicators, (no internal lights at night, mail stuffed in the mailbox, etc.) will provide the adversary with the information needed to reach a conclusion with an acceptable level of confidence. In this case, the more indicators that the adversary is able to observe, the greater the level of confidence in his/her conclusion. When you eliminate these indicators, you have a much better chance of ensuring that your home is not burglarized while you are away.

The same holds true at your place of work. We must protect our critical information and eliminate indicators available to the adversary.

The Five-Step OPSEC Process

1. Identification of the critical information to be protected
2. Analysis of the threats
3. Analysis of the vulnerabilities
4. Assessment of the risks
5. Application of the countermeasures

Identification of Critical Information

Basic to the OPSEC process is determining what information, if available to one or more adversaries would harm an organization's ability to effectively carry out the operation or activity. This critical information constitutes the "core secrets" of the organization, i.e., the few nuggets of information that are central to the organization's mission or the specific activity. Critical information usually is, or should be, classified or least protected as sensitive unclassified information.

Analysis of Threats

Knowing who the adversaries are and what information they require to meet their objectives is essential in determining what information is truly critical to an organization's mission effectiveness. In any given situation, there is likely to be more than one adversary and each may be interested in different types of information. The adversary's ability to collect, process, analyze, and use information, i.e., the threat, must also be determined.

Analysis of the Vulnerabilities

Determining the organization's vulnerabilities involves systems analysis of how the operation or activity is actually conducted by the organization. The organization and the activity must be viewed as the adversaries will view it, thereby providing the basis for understanding how the organization really operates and what are the true, rather than the hypothetical, vulnerabilities.

Assessment of Risks

Vulnerabilities and specific threats must be matched. Where the vulnerabilities are great and the adversary threat is evident, the risk of adversary exploitation is expected. Therefore, a high priority for protection needs to be assigned and corrective action taken. Where the vulnerability is slight and the adversary has a marginal collection capability, the priority should be low.

Application of the Countermeasures

Countermeasures need to be developed that eliminate the vulnerabilities, threats, or utility of the information to the adversaries. The possible countermeasures should include alternatives that may vary in effectiveness, feasibility, and cost. Countermeasures may include anything that is likely to work in a particular situation. The decision of whether to implement countermeasures must be based on cost/benefit analysis and an evaluation of the overall program objectives.

OPSEC Laws

The First Law of OPSEC

If you don't know the threat, how do you know what to protect? Specific threats may vary from site to site or program to program. Employees must be aware of the actual and postulated threats. In any given situation, there is likely to be more than one adversary, although each may be interested in different information.

The Second Law of OPSEC

If you don't know what to protect, how do you know you are protecting it? The "what" is the critical and sensitive, or target, information that adversaries require to meet their objectives.

If you are not protecting it (the critical and sensitive information), the adversary wins! OPSEC vulnerability assessments, (referred to as "OPSEC assessments" - OA's - or sometimes as "Surveys") are conducted to determine whether or not critical information is vulnerable to exploitation. An OA is a critical analysis of "what we do" and "how we do it" from the perspective of an adversary. Internal procedures and information sources are also reviewed to determine whether there is an inadvertent release of sensitive information

Designations

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.

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".

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

What type of information may be critical in the Civil Air Patrol? As a new member, you may be very surprised by the sensitive information that is entrusted to the Civil Air Patrol by the military and other government agencies.

Critical information may be in the form of more obvious CAP operations such as area surveillance, planned aerial intercepts, law enforcement support, homeland security support and DoD exercises. However other information may be deemed critical such as chaplain deployments, technological capabilities (i.e. SDIS and ARCHER), communication frequencies and the location of aircraft, vehicles and repeaters.

The Threat

Others are constantly trying to determine our weaknesses. Some forms of intelligence gathering are:

- HUMINT - Human Intelligence
- SIGINT - Signals Intelligence
- COMMINT – Communications Intelligence
- ELINT - Electronic Intelligence

Americas enemies actively target US military communications systems. 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.

**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



She never had a clue that she was the enemy's source to!

Rules for FOUO Documentation

At some point in your CAP career, you will most likely create documentation that is designated as FOUO. So as an originator of the documentation you must know some of the rules.

First, any documentation that is classified as FOUO will contain the following:

Paper documents such as exercises or operational plans or list of CAP radio frequencies and access tones are examples of FOUO documentation.

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 documentation and material may be transmitted via first-class, parcel post or forth-class mail (for bulk shipments).

In the age of electronics, there are many other considerations for operational security. Any non-paper documents such as slides, films, or computer media also need to be clearly marked as FOUO.

Electronic transmissions or email messages must also be appropriately marked. The abbreviation "U//FOUO" must be at the beginning of the text. This will notify the recipient immediately upon reading the message that they must take care with its contents. Publicly accessible web sites will NOT contain:

- For Official Use Only (FOUO) Information
- Sensitive Information
- Plans
- Planned Deployments
- Personal Information

Such information will be in a secured section of the website that will require a password to enter the site. You should make all personal attempts to secure your password information that may allow for someone else to access the FOUO information.

Summary

The purpose of the security program is to protect against unauthorized disclosure of official information. Keep your information secure at all times.

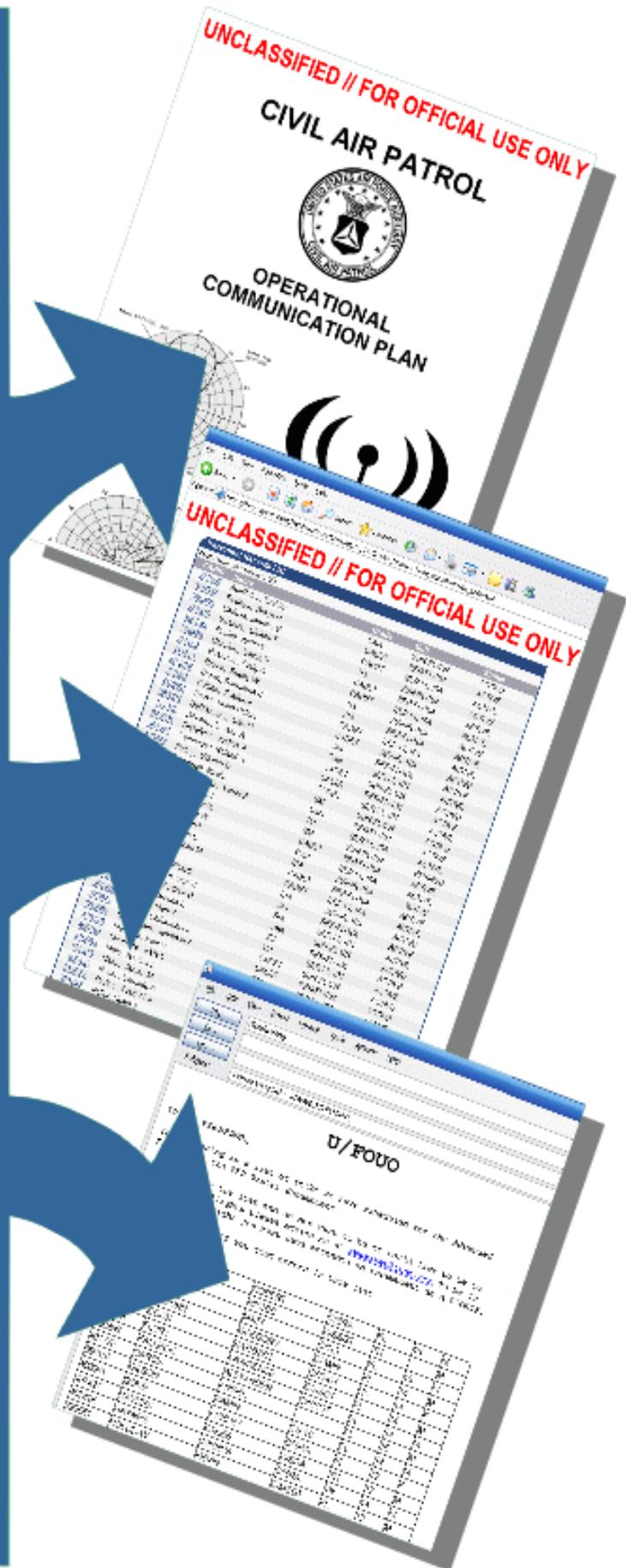
OPSEC is mostly common sense. If we all take the time to learn what information needs protecting, and how we can protect it, we can continue to execute our mission effectively.

No matter what the form the document takes, whether paper or electronic, information that is not for the public eye must be labeled as For Official Use Only or FOUO.

Paper documents such as exercises or operational plans or list of CAP radio frequencies and access tones are examples of FOUO documentation.

Publicly accessible web sites containing For Official Use Only (FOUO) Information, Sensitive Information, Plans, Planned Deployments and Personal Information will be in a secured section of the website that will require a password to enter the site. You should make all personal attempts to secure your password information that may allow for someone else to access the FOUO information.

Electronic transmissions or email messages must also be appropriately marked. The abbreviation "U//FOUO" must be at the beginning of the text. This will notify the recipient immediately upon reading the message that they must take care with its contents.



SUMMARY EXERCISE

1. The goal of OPSEC, as a "countermeasures" program, is to deny an adversary pieces of the intelligence puzzle.
 - a. True
 - b. False
2. Name the five-step OPSEC process.
 - a. _____
 - b. _____
 - c. _____
 - d. _____
 - e. _____
3. The first law of OPSEC is _____.
 - a. secure all documents
 - b. to know you threat
 - c. don't talk at all
 - d. place FOUO in all documents
4. "For Official Use Only" documents are considered classified or secret.
 - a. True
 - b. False
5. You are evolved with an operation due to you specialty qualification. This assignment was given to you by a higher headquarters. Your immediate commander approaches you and orders you to fill him in on the details since no one told him anything. Do you tell him as you have been ordered to do so?
 - a. Yes. You have been given a direct order.
 - b. Yes. Your commander must always be aware of you actions.
 - c. No. Direct your commander to the information officer.
 - d. No. It is apparent that he may not have the need to know. You should contact the operation coordinator and in form them of the request.
6. All electronic messages must have the designation U//FOUO in the subject line regardless of the content.
 - a. True
 - b. False
7. Name a couple of types of information should be designated as "For Official Use Only"?
 - a. _____
 - b. _____
8. What is the purpose of the security program?
 - a. To secure all documents from new members.
 - b. To protect against unauthorized disclosure of official information.
 - c. To prevent the media from finding out what Civil Air Patrol does.
 - d. To prevent the use all of Civil Air Patrol information from being used by the public.
9. Civil Air Patrol radio frequencies are no different than those used by amateur radio operators and are not considered sensitive information.
 - a. True
 - b. False
10. When trusted with sensitive information, it is you responsibility to secure that information and not spread it to others who do not have the need to know whether written or verbally.
 - a. True
 - b. False

NOTES
