Operations Security (OPSEC)

Welcome to the Department of the Air Force Operations Security Training

Air Force OPSEC: Protecting the Mission!

Operations Security

Overview

In this lesson you will learn:

- The definitions of OPSEC, critical information, and an OPSEC threat
- The purpose of OPSEC in the workplace
- The means by which our adversaries collect critical information
- Protecting Controlled Unclassified Information (CUI) from Unauthorized Disclosures (UD)
- Points of contact to report possible OPSEC vulnerabilities

Operations Security

Why This Training? Why now?

The Department of Defense's ability to effectively protect its sensitive information has been significantly hampered recently due to ongoing unauthorized disclosures of sensitive operational information.

The loss of our sensitive information, even unclassified small bits of information, has a direct and negative impact on our ability to effectively execute operations while ensuring our personal remain safe.

This training will address these concerns along with new guidance regarding how OPSEC relates to DoD guidance on Unauthorized Disclosures (UD) of Controlled Unclassified Information (CUI).

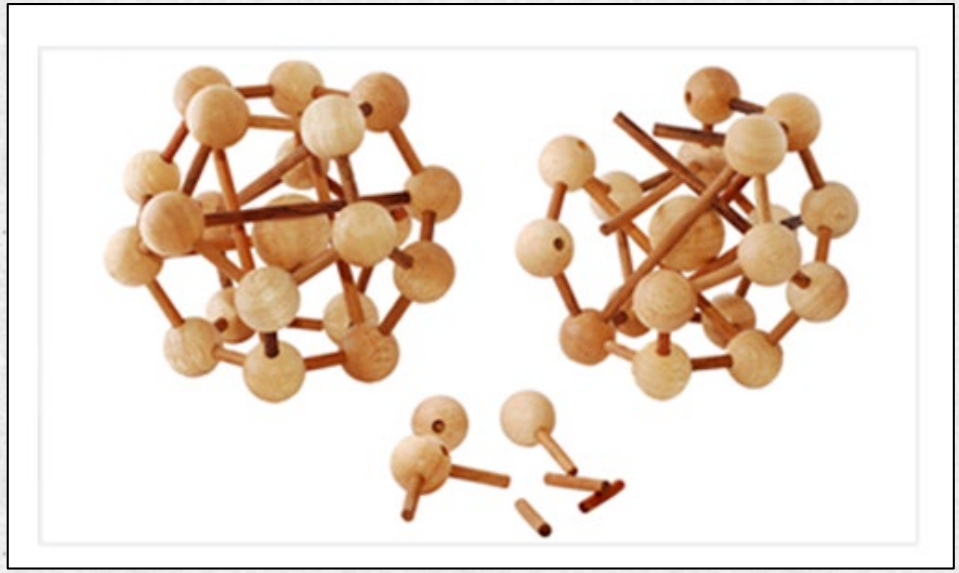
Operations Security

OPSEC

America's adversaries collect information pertaining to U.S. military activities and technology to further their own agendas.

Even pieces of unclassified information can hold great value to an adversary.

By putting together enough small details and indicators, an adversary may piece together enough about U.S. military plans and operations to do us harm.



Operations Security

OPSEC Defined

Operations Security (OPSEC) is a capability that uses a process to preserve friendly essential secrecy by identifying, controlling and protecting critical information and indicators that would allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities. Reference: AFI 10-701, OPSEC

In other words, OPSEC's desired effect is to influence the adversary's behavior and actions by protecting friendly operations and activities.

Operations Security

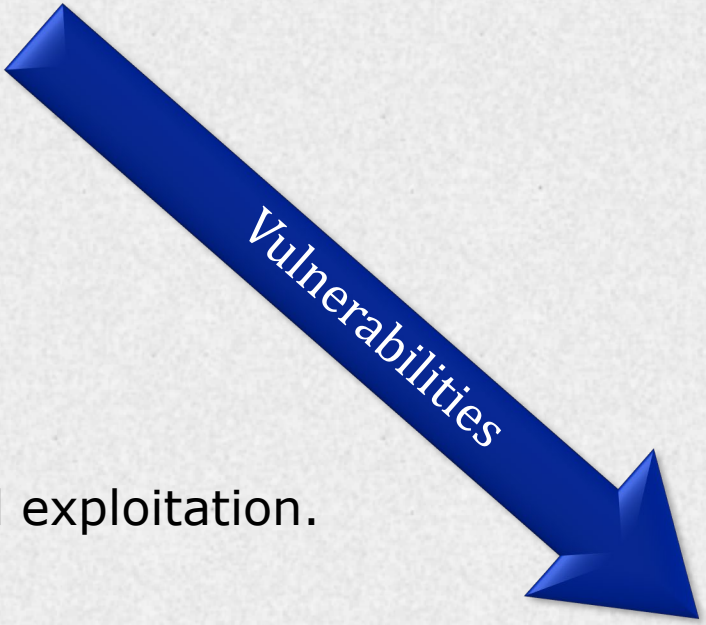
What is the purpose of OPSEC in your workplace?

Reduce vulnerabilities to

Air Force operations

from adversary

collection and exploitation.



Operations Security

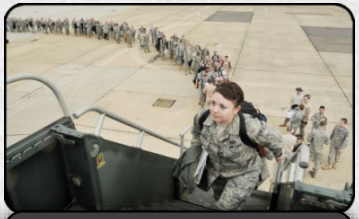
Critical Information

Critical information includes specific facts (like puzzle pieces) about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively.

Determine what information, if available to one or more adversaries, would harm the Air Force's ability to effectively carry out its missions.

Can you name an example of critical information?

Air Show Location and Dates



Deployment Dates and Location

Rank / Promotion

Training Dates

Operations Security

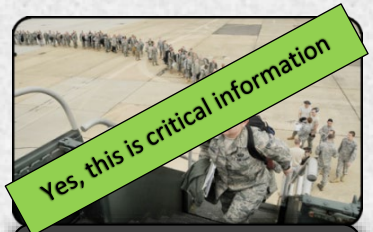
Critical Information

Critical information includes specific facts (like puzzle pieces) about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively.

Determine what information, if available to one or more adversaries, would harm the Air Force's ability to effectively carry out its missions.

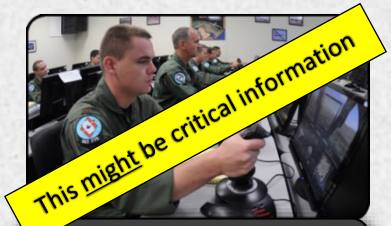
Can you name an example of critical information?

Air Show Location and Dates



Deployment Dates and Location

Rank / Promotion



Training Dates

Operations Security

Critical Information about your unit you must protect includes:

172 AIRLIFT WING OPSEC CRITICAL INFORMATION LIST

1. Planned missions, flying schedules, deployment/routes and operating locations
2. Deployment dates, times, missions, and locations
3. Combat readiness and capabilities of ground security forces
4. Information revealing specific combat or combat support capabilities
5. Deployment taskings, capabilities, requirements, equipment, personnel and status
6. Specific operation mission nature and objectives
7. Combat readiness and capabilities of aircraft and aircrews
8. Capabilities, configuration, security measures, limitations, vulnerabilities, status, upgrades or proposed changes to communication systems – to include networks, transmission systems, relay stations and associated equipment
9. Specific User IDs/passwords, network paths, IP addresses, nodes or links for mission specific requirements)
10. Equipment amount, configuration and capabilities/limitations
11. Discussion of C-17 strengths, weaknesses, limiting factors and operational status
12. Information protected under the Privacy Act of 1974, specifically PII of others, SSN, personal information
13. TDY orders revealing specific dates and locations
14. Association of call signs with unit, geographical location, mission or type aircraft
15. Alert status/response times
16. Technical system architecture, capabilities, vulnerability information, and security assessment reports related to C2 systems.
17. Specific aspects and changes in relation to FPCON/INFOCON changes
18. Overall organization effectiveness/shortfalls and limiting factors
19. Specific equipment inventory lists to include types of video, radio or security systems utilized
20. Unit Manning levels to include personnel shortages/deficiencies
21. Security clearance access/eligibility levels of personnel
22. Recall activation plans/procedures
23. Training and readiness status/deficiencies
24. Immunization/medical requirements/health status and deficiencies

Operations Security

Threats

An OPSEC threat is **an adversary** that has the **capability + intent** to take any **actions detrimental** to the success of **our activities or operations.**

Adversaries exploit many vulnerabilities to collect our information

- ✓ They use the internet to glean data from web pages, blogs, chat groups, and social media postings.
- ✓ They use people to collect information — informers, listening to conversations in public, social engineering, etc.
- ✓ They can easily intercept our unsecured communications — your unsecure phone call, unencrypted e-mails, radios, etc.
- ✓ They can gain information from going through our trash and recycling where we work and live.
- ✓ They can observe our actions to detect patterns to predict behavior.

Operations Security

What countermeasures will protect our critical information?

- ✓ Know what your unit considers critical information.
- ✓ Encrypt all e-mails with sensitive information.
- ✓ Ensure all information is reviewed by Public Affairs for OPSEC concerns before it is released to the public (in any fashion).
- ✓ Properly destroy any papers with sensitive information.
- ✓ Don't discuss sensitive information with someone not authorized to know the information.
- ✓ Be cautious of sensitive discussions in public (in-person and online).
- ✓ Remain vigilant for attempts to oversee or gain your sensitive data.
- ✓ Understand your stereotyped operations can be exploited.
- ✓ Others as directed by your Commander/Director

Operations Security & CUI

What is Controlled Unclassified Information(CUI)?

In addition to classified information, certain types of unclassified information also require application of access and distribution controls and protective measures for a variety of reasons. Such information is referred to collectively as CUI. There are multiple categories of data that fall under the designation of CUI.

How does it relate to OPSEC?

Remember when we discussed critical information earlier? Your organization's critical information (identified through the OPSEC process) falls within a specific category of CUI.

Unauthorized Disclosures

What is an Unauthorized Disclosure (UD) of CUI?

A communication or physical transfer of CUI to an unauthorized recipient.

How does an Unauthorized Disclosure, or UD, relate to OPSEC?

When we lose our critical information (or their associated indicators that point to our critical information) it is considered an **Unauthorized Disclosure**. Under the CUI program, any loss of CUI must be reported.

Operations Security

Reporting OPSEC Concerns

If you identify an Unauthorized Disclosure or detect a possible vulnerability to your organization's mission, you have the responsibility to report it.

Contact your unit OPSEC Signature Manager, your supervisor or your commander.

Primary OPSEC Signature Manager
Name: Capt Ryan Gressett
Phone: (601) 405-8747

Alternate OPSEC Signature Manager
Name: 1Lt Corey Harris
Phone: (601) 405-8073

Knowledge Check

Knowledge Check

True or False

OPSEC is a process used to identify, analyze, and control critical information indicating friendly actions associated with military operations and other activities.

- ❑ True
- ❑ False

Knowledge Check

True or False

OPSEC is a process used to identify, analyze, and control critical information indicating friendly actions associated with military operations and other activities.

- ❑ True
- ❑ ~~False~~

Knowledge Check

What is the purpose of Operations Security (OPSEC) in the workplace?

- ❑ Reduce vulnerabilities to AF missions
- ❑ Protect classified information
- ❑ Reduce insider threat
- ❑ Deter adversaries who try to access our computer networks

Operations Security

Knowledge Check

What is the purpose of Operations Security (OPSEC) in the workplace?

- ❑ Reduce vulnerabilities to AF missions
- ~~❑ Protect classified information~~
- ~~❑ Reduce Insider Threat~~
- ~~❑ Deter adversaries who try to access our computer networks~~

Knowledge Check

An adversary with the capability and intent to undertake any actions detrimental to the success of programs activities or operations describes _____.

- ❑ OPSEC
- ❑ INFOSEC
- ❑ An OPSEC threat
- ❑ Critical information

Knowledge Check

An adversary with the capability and intent to undertake any actions detrimental to the success of programs activities or operations describes _____.

- ~~OPSEC~~
- ~~INFOSEC~~
- An OPSEC threat
- ~~Critical information~~

Operations Security

Summary

In this lesson you learned:

- The Definitions of OPSEC, critical information, and an OPSEC threat.
- The purpose of OPSEC in the workplace.
- The means by which our adversaries collect critical information.
- Protecting Controlled Unclassified Information (CUI) from Unauthorized Disclosures (UD).
- Points of contact to report possible OPSEC vulnerabilities.

Congratulations, you have completed OPSEC training!