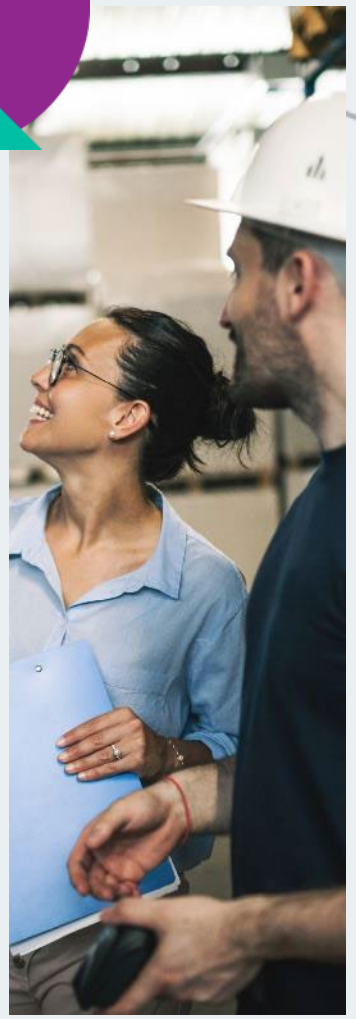
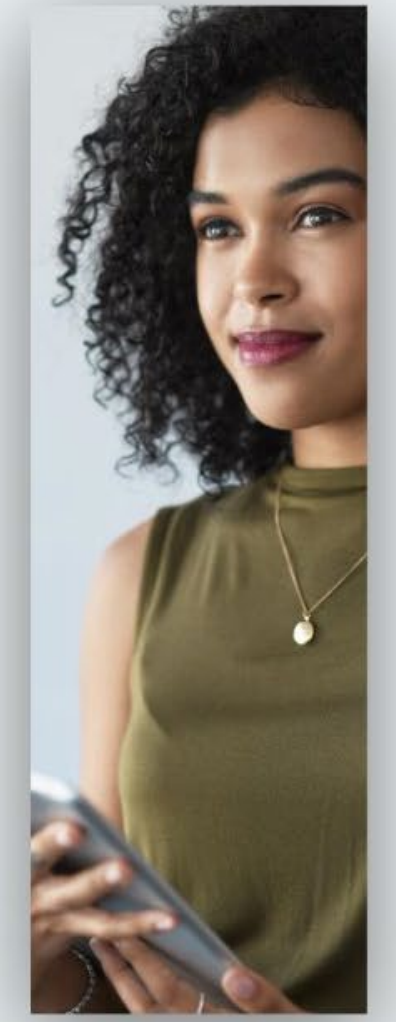
OPSEC for ALL

Protecting yourself and your critical information



This briefing is UNCLASSIFIED
in its entirety
October 25, 2022

What is Operations Security (OPSEC)?



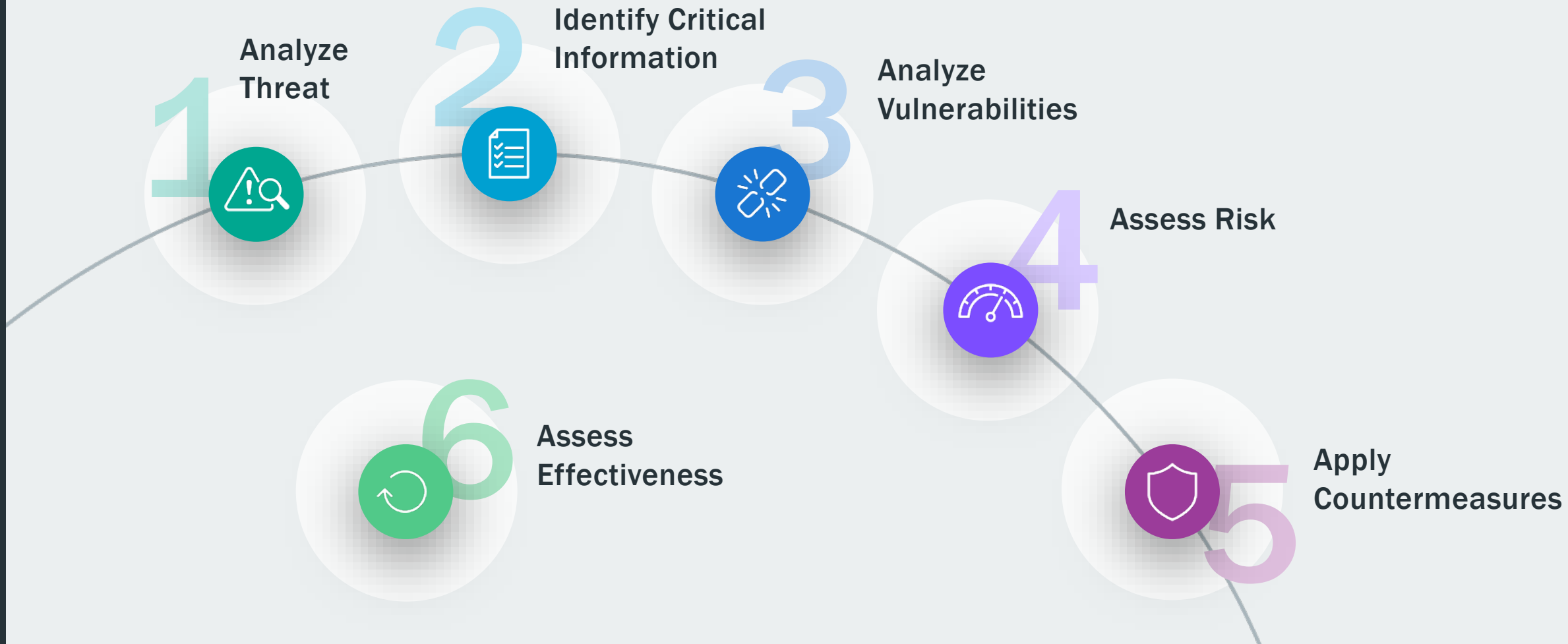
Using best practices to identify and protect your critical information.

What is Operations Security (OPSEC)?

The Importance of OPSEC

Understanding how a threat could potentially exploit vulnerabilities to compromise your personal information and learning different countermeasures to prevent it are key to ensuring critical information doesn't land in the adversary's hands.

The OPSEC Cycle



ANALYZE THREAT

What is a Threat?

A threat is an adversary who has the intent and capability to compromise your mission or sensitive activities.

ANALYZE THREAT

What is an Adversary?

An adversary, or bad actor, is an individual, group, organization, or government that threatens to compromise your interests, missions, and sensitive information.

IDENTIFY CRITICAL INFORMATION

What is Critical Information?

Details about your intentions, capabilities, and activities that an adversary can exploit to compromise or interrupt your mission.

IDENTIFY CRITICAL INFORMATION

How do Adversaries Collect Critical Information About You?

Open sources such as the internet, news outlets, professional journals, and social media.

Casual conversation or by eavesdropping at places frequented by you.

Social engineering tactics to trick you into providing sensitive information.

IDENTIFY CRITICAL INFORMATION

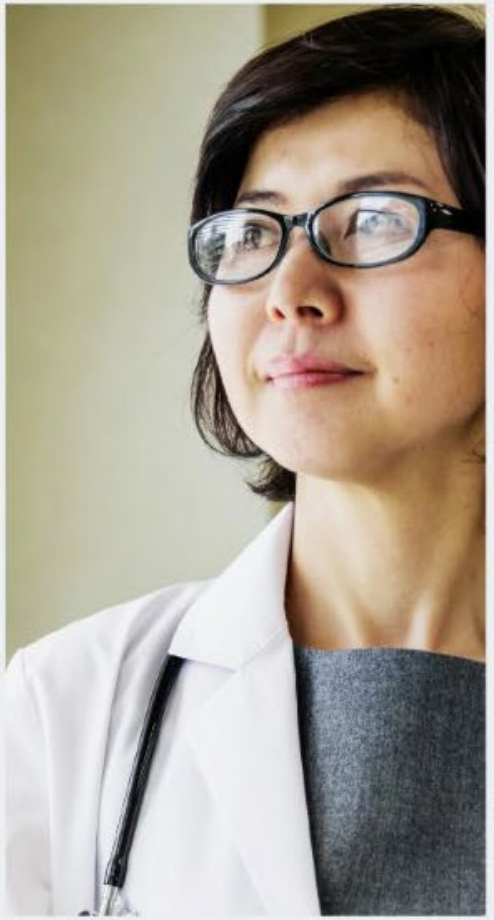
Ask Yourself This…

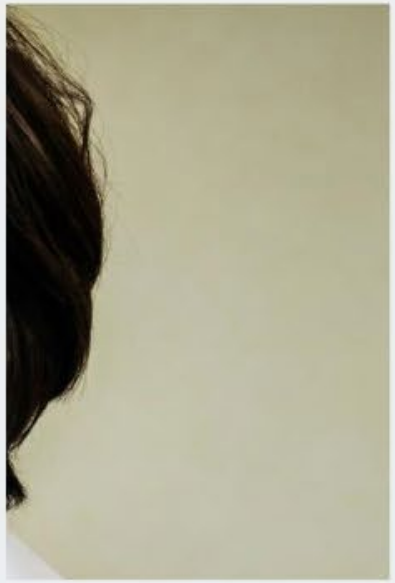
- What is the mission or project?
- How can the adversary use the information?
- Would the information support an adversary's strategy or activities?
- How long does the information need to be protected?

IDENTIFY CRITICAL INFORMATION

Know What to Protect

A critical information list (CIL) is a list of your critical information such as capabilities, activities, limitations and intentions. Critical Information can also include personal items such as PII, health information, and travel plans.





IDENTIFY CRITICAL INFORMATION

Keeping Critical Information Safe

Refer to your CIL when sharing information in these unsecure instances;

- Unencrypted email
- Social media posts
- Public conversations, or even at home with family and friends
- Travel planning
- Requests for personal information

ANALYZE VULNERABILITIES

Vulnerabilities Can be Observed in Many Ways

An adversary can detect a vulnerability by observing an activity, such as security procedures you follow when entering a building.

- Physical environment/work area
- Office operating procedures
- Outdated computer software

ANALYZE VULNERABILITIES

Hacked Within Minutes

ANALYZE VULNERABILITIES

Common Vulnerabilities

- Use of email, social media, and the internet
- Access to mail, trash, and recyclables
- Predictable patterns and procedures
- Lack of awareness of threats and vulnerabilities
- Increased connectivity on insecure devices

ANALYZE VULNERABILITIES

Indicators are Clues

Indicators may reveal sensitive information and activities such as:

- Sudden changes in procedures
- Staging of cargo or vehicles
- Presence of specialized equipment
- Increased security measures
- Personal behavior/actions

ANALYZE VULNERABILITIES

Data Aggregation

Data aggregation is combining information from multiple sources.

ASSESS THE RISKS

What is Risk?

Risk is the likelihood that an adversary will get your critical information.

ASSESS THE RISKS

Don’t Risk Your Information

APPLY COUNTERMEASURES

Use Countermeasures to Reduce Risk

Countermeasures reduce the likelihood that critical information will be lost. These include educating yourself on threats and vulnerabilities, using traditional security precautions (physical, personal, cyber, etc.), and enforcing policies.

APPLY COUNTERMEASURES

Stay Safe

Assessing the risks and taking the precautions could be the difference in protecting your critical information and your safety.

OPSEC Every Day

Knowing the risks, reducing your vulnerabilities and taking the correct countermeasures will help to keep you and your critical information safe.

For additional resources
Operations Security (odni.gov)
Or you can reach us at
NOP@DNI.GOV

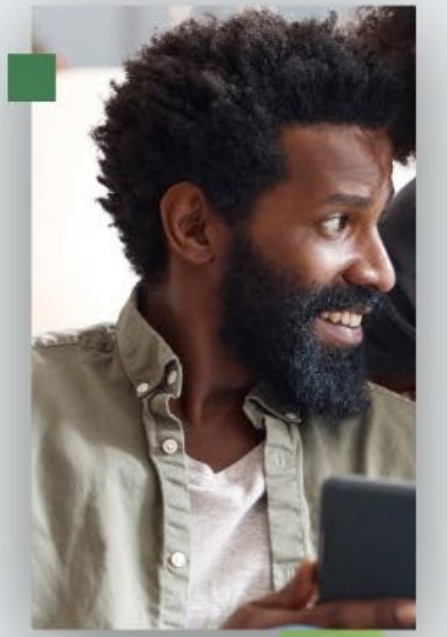
OPSEC & Your Family

Many family members inadvertently provide critical information without even knowing. When your critical information is exposed to the wrong person, it can endanger your family.

Talk to Your Family about OPSEC

Define what and who could be a threat. Make sure your family understands the vulnerabilities and risks of over-sharing information and that even children can be potential targets or victims.

A burglary happens every 26 seconds



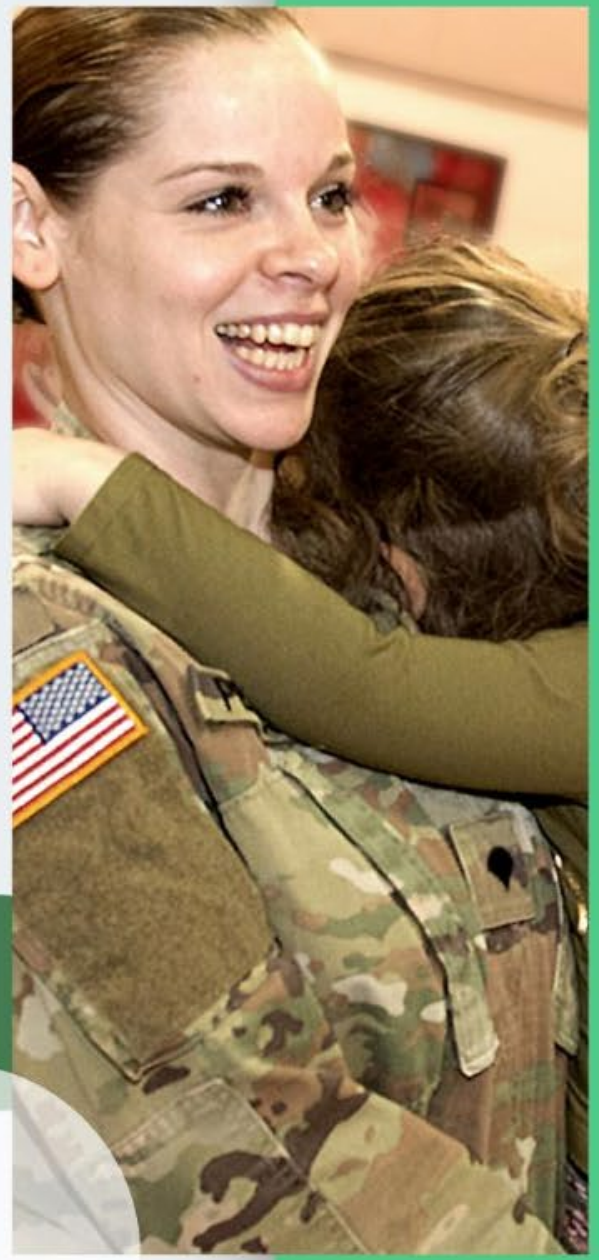
Awareness Starts at Home

- Threats come from criminals, identity thieves, and pedophiles.
- Talking about work, school, and social schedules can expose critical information.
- Social media posts, discussions in public and items left in cars are all types of vulnerabilities.
- Understand the risk that an adversary could gain your critical information if you are overly sharing it.

Awareness Starts at Home

Protect Your Family

- Schedules can reveal your whereabouts, don’t overly share them.
- Leaving items in your car makes you a target for theft.
- Using the Post Office’s indoor drop box can reduce your likelihood of mail theft.
- Remember to always lock your house and car.



OPSEC & Your Connected Devices

Did you know, that the average household has at least 10 devices connected to the internet. Do you think they are all secure?

Beware of Hackers Inside Your Home

Connected devices will reach 75 billion by 2025

With so many different devices being connected in your home network, there are even more vulnerabilities and risks of being hacked.

The Internet of Things (IOT) is billions of devices around the world that are connected to the internet through sensors or Wi-Fi. These include smart devices such as watches, thermostats, doorbell cameras and baby monitors.

Be Aware of What You Can't See

- Threats come from malicious cyber actors.
- Critical Information includes PII, financial info, schedule and photos/videos.
- Not changing your default passwords, using insecure networks and not allowing updates/patches are all examples of vulnerabilities.
- Understand the risk that an adversary could gain your critical information if you do not disconnect your devices.

Be Aware of What You Can’t See

Protect Your Home Network

- Install the latest router firmware.
- Change your home network password when connecting a new device.
- Use strong passwords.
- Encrypt and hide your network.
- Change passwords regularly, especially Wi-Fi.
- Turn off connected devices when not in use.

OPSEC & Work From Home

Cyber attacks are increasing as more employees have the ability to telecommute.

Don’t Let Your Guard Down

Working from home has become the new normal. Yet remembering to take precautions is challenging in addition to the stress of work life balance. Extra attention needs to be given to setting up secure environments.

Adversaries are targeting employees who work from home by using different methods and types of software to gain access to your company’s sensitive information. Most at home cyber attacks occur when employees click on bad links and Phishing emails.

Nearly 60% of the data breaches are due mainly to human error,

Keep Your Workspace Safe

- Threats come from bad actors, identity thieves, industrial spies, cyber criminals.
- Critical Information includes your personal information and the organization’s critical information list.
- Using Public Wi-Fi, unpatched operating systems and software, weak passwords, unsecure teleworking location are all vulnerabilities.
- Understand the risk that an adversary could gain your critical information if you do not secure your remote workspace.

Keep Your Workspace Safe

Protect Your Remote Workspace

- Beware of your surroundings if you are teleworking from different locations and always use a virtual private network (VPN).
- Stay focused and check the content and recipient before sending data.
- Participate in information systems security and general awareness training.
- Implement the required measures to protect your company’s systems and information such as installing approved software updates.
- Turn off home virtual assistance when not needed.

OPSEC & Engaging in Social Media

Everything you post on Social Media is out on the Internet and up for grabs by the adversary.

How Much Information are You Really Sharing?

Social media-enabled cybercrimes generate $3.25+ billion in global revenue per year

What you or your family and friends share on social media can provide the adversary with important information about our connections, habits, and careers. This can support their efforts of elicitation, recruitment, social engineering, targeting, and more - putting us, our families, our organizations, and our missions at risk.

Shared Awareness

- Threats come from criminals, hackers, nation states, economic competitors, and terrorists.
- PII, financial or account information, personal and professional schedules, job details, sensitive or proprietary information, and official capabilities, activities, or limitations.
- Oversharing, lax privacy settings, and clicking on scam links are examples of vulnerabilities.
- The risks associated with social media will have a lot to do with how much information you share.

Shared Awareness

Protect Your Social Media Accounts

- Posting personal details can give too much information to the wrong people.
- Use the highest privacy setting available.
- Be selective with fiend/connection requests.
- Turn off location settings feature.
- Avoid clicking on suspicious messages or links.
- Report any scam posts or messages.
- Use unique passwords for all your accounts.

OPSEC Every Day

Knowing the risks, reducing your vulnerabilities and taking the correct countermeasures will help to keep you and your critical information safe.

For additional resources
Operations Security (odni.gov)
Or you can reach us at
NOP@DNI.GOV