FY23 Operations Security (OPSEC)

Introduction

- **Command Training Officers and OPSEC Officers shall supplement this brief with the below information in order to satisfy annual training requirements per SECNAVINST 3070.2A, 9 May 2019. Ensure:**
  - **All members of the command understand and are familiar with the contents of their command's Critical Information List (CIL)**
    - **Specific contents not to be disclosed to the public or anyone without the need-to-know**
    - **Responsibilities for safeguarding, sending and destroying critical information (CI)**
  - **Local threat or adversary (include collection methods)**
  - **Social media awareness and other command specific vulnerabilities**
  - **Risk mitigation efforts or countermeasures**
- **Efforts shall be made to reach and educate family members.**
- **All assigned personnel shall receive OPSEC training as part of their onboarding process prior to accessing DON networks/accounts.**

"Bumper stickers" like this are placed within this presentation as placeholders to discuss the above information.

References

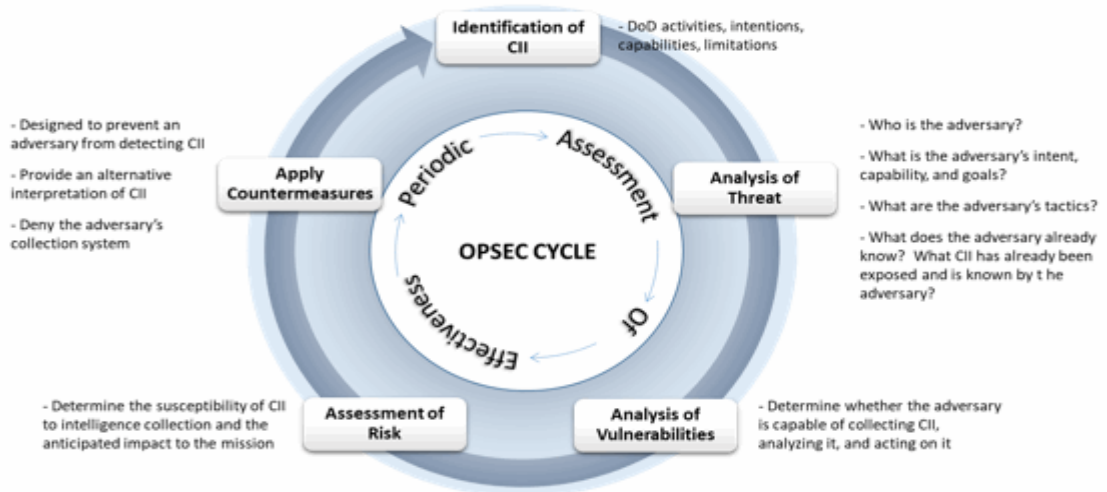
- National Security Presidential Memorandum (NSPM-28), 13 January 2021 National OPSEC Program
- Department of Defense Directive (DoDDir 5205.02 (series)), OPSEC
- Department of Defense Instruction (DODI 8170.01 (series)), Online Information Management and Electronic Messaging
- Department of Defense Instruction (DODI 5200.48 (series)), Controlled Unclassified Information (CUI)
- Secretary of the Navy Instruction (SECNAVINST 3070.2 (series)), OPSEC
- Chief of Naval Operations Instruction (OPNAVINST 3070.X (series)), OPSEC
- Navy Tactics, Techniques and Procedures (NTTP 3-13.3M), OPSEC
- DoDD 3115.18 DOD Access to and Use of Publicly Available Information (PAI)
- Deputy Security of Defense Memorandum, 03 August 2018, Use of Geolocation-Capable Devices, Applications, and Services
- Navy Social Media Handbook
- Command Policy

Agenda

- The definition of OPSEC
- The continuous OPSEC cycle
  - Critical Information and indicators
    - Operational Aspects
  - Threat
  - Vulnerabilities
    - Geo-tagging
    - Commercial Applications
    - Social Media
  - Risk
  - Countermeasures
  - Assessment of Effectiveness
- Controlled Unclassified Information
- Publicly Available Information

Operations Security

- Operations Security (OPSEC) is a continuous cycle that identifies unclassified critical information and indicators (CII), analyzes potential threats and vulnerabilities, assesses risks, and develops countermeasures to safeguard CII.
- Is an operations function and security discipline that depends on successfully implementing the OPSEC cycle.
- The continuous cycle includes:
  - Identify critical information and indicators
  - Analyze threat
  - Analyze vulnerabilities
  - Assess risk
  - Apply countermeasures
  - Periodic Assessment



Critical Information

- Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively against our operations.
- Every command member must be familiar with the organization's critical information list (CIL) per SECNAVINST 3070.2A.
  - Discuss the contents of the command's CIL
  - Discuss where to find or locate the command's CIL
- Critical information and indicators will derive from the operational aspects that are associated with your command or organization.

Discuss your Command's (Organization, program, element, activity) Critical Information

Operational Aspects

- Are pieces of information that relate to, or derive from the command's operations:
  - Presence: Where your unit is currently operating
  - Capability: The unique abilities your unit lends to the operation
  - Strength: The number of units or personnel coupled with the ability to withstand great force
  - Intent: What your unit plans to do
  - Readiness: Level of preparedness to execute
  - Timing: Specific timeliness of events
  - Location: Where your unit will deploy (specific locations)
  - Method: The way your mission will be executed

Think about which operational aspects are associated with your command and are the most significant?

Indicators

- Friendly, detectable actions that potentially reveal critical information:
  - Longer working hours
  - Rehearsals
  - Sudden changes in procedures
  - Troop or stores on-loads
  - Large troop movements
  - Uniform emblems/logos

- Not all indicators can be protected
  - For example, on-loads that must occur during the day.
- Not all indicators are necessarily bad.
  - For example, external cameras indicate monitoring, and may thwart adversarial action.

Threat or Adversary

- An adversary must have intent and capability to undertake any action detrimental to the success of our activities or operations.
- Common collection methods / capabilities:
  - Open source or Publically Available Information (PAI)
    - Data aggregation from multiple sources
    - Ubiquitous Technical Surveillance (UTS). The widespread collection of data through visual, imagery electronic communications, financial transactions, domestic and overseas travel and online presence.
  - Human Intelligence (face-to-face and on-line interaction)
  - Signals Intelligence (collection of electronic signals)
  - Geospatial Intelligence (overhead or satellite)
  - Measures and Signatures Intelligence (technically derived signatures)

Discuss your organization's most realistic threat or adversary

What are adversaries looking for?

- Operational aspects, critical information and indicators.
- Present, future or sensitive operations:
  - Times of operational events
  - Participating units
  - Projected locations
- Information about military facilities:
  - Critical Infrastructure details
  - Sensitive activities
  - Specific dates and times of operations
- Technology:
  - Newly developed and tested
  - Capabilities and limitations

You may choose to discuss how and where to obtain threat information for your location or command.

Vulnerabilities

- Is a weakness an adversary can exploit to gain our critical information.
- Anything that makes our critical information susceptible to intel collection.
- Common vulnerabilities include:
  - Lack of awareness on our part (everything we do is important)
  - Poor policy enforcement (lack of shred or electronic device policies)
  - Unsecure communications (are almost always being monitored)
  - Social engineering (in-person or on-line interaction with collectors)
  - Printed or recycled paper not shredded or reviewed for critical information
  - Our own predictable actions, patterns or routines
  - Geo-location devices in operational areas **
  - Use of unapproved commercial applications for official business **
  - Social media posts revealing too much information **

** additional slides

Geo-Location Devices

- Geotagging: Location / GPS data embedded in photos.
- Default feature in most smart phones and digital cameras.
  - Provides latitude/longitude/altitude
  - Device details and access to information depending on Terms of Services (ToS) and what you accept
- Information can potentially be retrieved from posted digital photos.
- Several "Check-in" features on applications.
- Even when disabled, location data is still saved and may be automatically uploaded when the device is connected.
- Per DEPSECDEF Memo dated 3 Aug 2018, DoD personnel are prohibited from using geolocation features and functionality on both non-government and government-issued devices, applications, and services while in locations designated as operational areas (OAs), unless authorized by Combatant Commanders or their designees after a threat-based OPSEC survey is conducted.

Applications (Apps)

- Per DODI 8170.01, Do not use non-DoD-controlled electronic messaging services to process non-public DoD information, regardless of the service's perceived appearance of security (e.g., "private" Instagram accounts, "protected" tweets, "private" Facebook groups, "encrypted" WhatsApp messages).
- Use of commercial applications for official Navy business is a constant and growing vulnerability.
- Just because commercial applications are available, it does not mean they should be used for military business.
- WhatApp, Slack, GroupMe, Facebook Messenger and several others, and new ones in the future, are not authorized unless approved by DOD prior to use for military business.
- When in doubt, ask your Immediate Senior in Command.

Social Media

- Social media and information in the PAI space is playing an increasingly important role in U.S. military information operations, because people around the world, including civilian populations, U.S. allies, and adversaries, use social media and PAI platforms to share and gain information and persuade others.
- Our adversaries work tirelessly to gain the competitive advantage by accessing sensitive operational and proprietary information on our ships, submarines, aircraft, installations, business processes and our most important asset, our people.
- Non-state adversaries have an asymmetric advantage, low cost of entry and the relative operational agility with which they can access and utilize new technologies.

Social Media – Do's & Don'ts

Do

- Utilize appropriate privacy settings
- Verify all friend requests
- Know who is following you
- Verify links before clicking
- Review your family's security settings & what they post about you and the Navy
- Understand the risks of geo-tagging
- Understand the terms of services, and you may no longer "own" the information once posted

Don't

- Depend on default security or privacy settings
- Trust add-on's or applications
- Discuss personal information, work details, or answer questions from strangers
- Take the bait by correcting other's posts or incorrect information
- "Check in" to places
- Think you have any "RIGHT" to privacy on the Internet

Remember – the internet is FOREVER

Risk

- The probability an adversary will gain knowledge of our critical information, and the impact it will have on our operations if they successfully use that information against us.
- Impact: The potential cost if our critical information is compromised:
  - Loss of lives
  - Mission failure
  - Loss of money
  - Loss of time
- How much are we willing to accept by disclosing critical information, displaying indicators, or not properly identifying vulnerabilities?
- Commanding Officers must determine the acceptable level of risk if critical information is exploited and potentially acted upon.

Countermeasures

- Anything that effectively negates or reduces an adversary's ability to exploit vulnerabilities or collect and process critical information:
- For most vulnerabilities, there is likely an inexpensive countermeasure.
- Training is one of the most effective countermeasures, when adhered to and policies are followed.
- Per NSPM-28, Identity Management (IdM) means an OPSEC capability that seeks to mitigate risks to personnel, organizations, missions, and capabilities through the discovery, examination, analysis, assessment, and management of an individual's or organization's identity elements, characteristics, or other attributes in public or non-public records and databases or in social media or other unstructured data sources.
- Effective countermeasures will Influence or manipulate an adversary's perception, causing them to:
  - Take no action
  - React too late
  - Take the wrong action

Assessment of Effectiveness

- The periodic assessment determines if anything has changed in the cycle.
- Are your countermeasures effective or ineffective, or are additional countermeasures still required?
- If an area within the cycle requires attention, address the change and continue with the cycle, constantly assessing your OPSEC posture, especially as missions change.
- The operational and information environment is constantly evolving and changing, which requires the OPSEC posture to keep pace in maintaining essential secrecy and protecting critical information and indicators.
- The key takeaway: The OPSEC cycle is not a “one and done” requirement.

Controlled Unclassified Information

- CUI is unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government policy.
- The DoD CUI Program website provides relevant information on the DoD CUI Registry, training, policy and desktop aids to properly mark and control DOD material (https://www.dodcui.mil/). Criteria for marking material CUI under the DoD OPSEC category is that the information should be identified on the command/organization/agency/unit/program OPSEC Critical Information List (CIL) or as designated by a senior official. This process identifies unclassified information that must be protected. It almost always results from a command/organization/agency/unit/program official OPSEC program, or is otherwise commonly approved for use by the Senior Official.
- Not all CUI is Critical Information, however all Critical Information is CUI.
- Guidance for CUI, to include its proper destruction, is provided in DOD Instruction 5200.48.

Publicly Available Information

- Disclosures occur when personnel share information in the PAI space with individuals they don't know, like on their social media pages or Apps.
- Personnel who publish in the PAI environment shall at a minimum:
  - Ensure all information about any DoD, military and Navy activity and event is approved for public release prior to sharing publicly.
  - Not discuss details of command tactics, techniques or procedures (TTPs) in any social media forum.
  - Not discuss details, capabilities or functions of weapon systems unless specifically authorized.
  - Not provide information of ship / unit locations, itineraries, current or future deployment dates, present or future operational information, unless specifically authorized.
  - Not post any unauthorized pictures, videos, maps, diagrams that identify weapon systems, computer systems, sensitive compartments, radar / sonar, or any other equipment that can compromise capabilities or TTPs.
- Refer to DOD Directive 3115.18, DOD Access to and Use of Publicly Available Information (PAI)

Summary

- The definition of OPSEC
- The continuous OPSEC cycle
  - Critical Information and indicators
    - Operational Aspects
  - Threat
  - Vulnerabilities
    - Geo-tagging
    - Commercial Applications
    - Social Media
  - Risk
  - Countermeasures
  - Assessment of Effectiveness
- Controlled Unclassified Information
- Publicly Available Information

Questions

NAVY_OPSEC@us.navy.mil
757-203-3656
www.navifor.usff.navy.mil/opsec
Naval Information Forces
ATTN: Naval OPSEC Support Team
115 Lake View Parkway
Suffolk, Virginia 23435

Summary

Congratulations!
You have completed this training.

Please continue to obtain your certificate of completion.