|  |  |
| --- | --- |
|  | **Facilitator speaking points**   * This column provides the facilitator speaking points for the audience.   Recommend removing bumper stickers and implementing command information prior to delivery to the command |
|  | Per SECNAVINST 3070.2A, 9 May 2019, commands shall include, at a minimum:   * A tailored, command-specific training program that ensures all assigned personnel are aware of the contents of their Critical Information (CIL) and their specific responsibilities for safeguarding critical information. * All assigned personnel must receive OPSEC training as part of their onboarding process prior to approving personnel for access to DON networks, and at least annually. This training shall include, at a minimum, the unit’s CIL; social media awareness and vulnerabilities; local threats; how to protect, transmit, and destroy controlled unclassified information; risks and guidance pertaining to geolocation-capable devices, applications, and services; and OPSEC review procedures for public release. * All training must be formally documented, maintained, and available online for higher command review. Family outreach shall also be performed to educate the families of assigned personnel about OPSEC principles and concerns.   **Do not read** (This training will cover the majority of the above information, however, some information must be covered by local commands, like your organizations critical information and local threat. Bumper stickers are added as reminders to consult with the command OPSEC Officer for supplemental information.) |
|  | * Changes from previous OPSEC training include: * Department of Defense Instruction (DODI 8170.01 (series)), Online Information Management and Electronic Messaging. This directive provides guidance on the use of online information, to include the use of commercial applications (Apps), which pose a significant OPSEC concern. * Department of Defense Instruction (DODI 5200.48 (series)), Controlled Unclassified Information (CUI). CUI is an Information Security program, but clearly aligns with OPSEC and the protection of critical information. For CUI, contact your Information Security Team. * Per SECNAVINST 3070.2A, CUI must be covered as part of your annual OPSEC training. |
|  |  |
|  | * Detailed information about the cycle is provided throughout this training. * 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. |
|  | * The OPSEC cycles begins with identifying the command’s critical information. These are unclassified, 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. * **Specifically discuss, and or show 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 of operations** that are associated with your command or organization. |
|  | * The eight operational aspect of operations are **Presence, Capability, Strength, Intent, Readiness, Timing, Location and Method.** * Discuss which operational aspects relate to your organization, followed by the critical information associated with each operational aspects. * For example:   + A large naval base cannot protect **Presence** or **Location**, but may need to protect critical information related to **Readiness**.   + Disclosing the percentage of a crew that is infected with COVID could divulge **Capability** and **Readiness** of the unit. |
|  | * Indicators are the detectable actions we disclose that may lead an adversary to our critical information and impending operations. * Discuss how these examples can be an indicator. What could they mean? * For example: * Your unit was all of a sudden working until the middle of the night. What could that possibly mean? Would an adversary want to investigate this further? * Huge stores on-loads on a pier could indicate a ship getting underway for a major deployment. * Discuss what could be good indicators in the military. A large security presence with heavy weapons could indicate safeguarding something or someone important. The weapons could possibly keep the adversary from trying to access that area. * Not all indicators can be eliminated or controlled but can still convey information to our adversaries if they are watching. * For example: * A significant on-load aboard an amphibious ship, of both a large number of Sailors and Marines would indicate an Amphibious Readiness Group (ARG) will get underway. |
|  | * Unfortunately, we deal with unpredictable, unconventional threats/adversaries to today’s world, not to mention Great Power Competitors (GPC) like Russia and China. * One of our primary threats in the United States is foreign intelligence Entity **(FIE)** (spies trying to gather information). They are very active, especially in the DC metro area and near military bases. Why are they specifically active in these locations? * FIE also spend resources collecting and/or stealing U.S. intellectual property, often times resulting in the loss of Billions annually. After all, what is easier, developing technology from scratch, or just stealing it and replicating it? * Threat information can be obtained from either a command’s S2/N2 shop or any local NCIS area office. Much of what NCIS provides is available from the NCIS MTAC site or other on line sites. * Discuss the local adversary and not only what they’re collecting, but how. Are they collecting using one or more of the common collections methods of:   + OSINT or Opens Source Intelligence   + HUMINT or Human Intelligence   + SIGINT or Signals Intelligence   + GEOINT or Geospatial Intelligence   + MASINT or Measures and Signatures Intelligence * Although not one of the “traditional” adversary collections methods above, CYBER is a common collection method. * Discuss how adversaries aggregate information from multiple sources. * Ubiquitous Technical Surveillance (UTS) defines the collection of technical information from the multitude of on-lines services ranging from the Internet of Things (IoT), smart devices, artificial intelligence (AI) and more. Expect to see and learn more about UTS in the coming years. |
|  | * As previously discussed, it’s not only important to protect our critical information, but also know which adversary is attempting to collect your critical information. * Think about what you do on a day-to-day basis, and determine if anything you do is something valuable to an adversary. Think about what information you exchange on unclassified, unprotected networks or even social media platforms. * Why is this information important? Discuss why the adversary would want to know these things. How could they use this information to their advantage? |
|  | * Vulnerabilities are weaknesses an adversary can exploit to collect critical information. A vulnerability is anything that makes our critical information susceptible to intelligence collection. * These are the most common vulnerabilities discovered during annual assessments of organizations. * Lack of awareness- Many just are not aware of the vulnerabilities when posting information. * Poor policy enforcement- Policies are only as good as how they are enforced. An all shred policy is great as long as everyone participates. No cell phone policy in the spaces for security purposes must be enforced. * Consider unsecure communications as being monitored. Many believe cell phones are secure. Most communications used today are not secure. * Social engineering. We are naturally friendly and like to talk about our work or personal experiences. Don’t share this information with strangers, regardless of how harmless they may seem. * Trash. Be sure to shred/burn all personal or official correspondence, to include junk mail. * We are creatures of habit, and very predictable in our daily routines and pattern of live. Become more unpredictable. * Geo-location or GPS remains a big vulnerability, especially when Sailors are located in operational areas (OA). * The unauthorized use of commercial applications (Apps) is a growing vulnerability throughout the DOD. * Social media. There are billions of users, and none of the sites are 100 percent secure. Essentially, you could be posting information to billions. |
|  | * + Geotagging: Location/GPS data embedded in photos.   + Location/GPS settings are normally defaulted ON in most smart phones and digital cameras. Most users leave this feature on because it also provides mapping instructions while driving and provides a host of other benefits. Do understand that latitude/longitude/altitude will be imbedded in digital photos…….where the photo was actually taken.   + Device details and access to information may also be enabled depending on the Terms of Service (ToS) and what you accept on different applications   + Information can potentially be retrieved from posted digital photos   + There are several “Check-in” features on applications, too many to list.   + 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. |
|  | * + 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 plays an important role in U.S. military information operations (IO). * Adversaries and criminals use social media and publically available information (PAI) platforms to share, gather and aggregate information and persuade others. * The rapid growth of the communication technologies that support social media and PAI platforms provides our adversaries an asymmetric advantage. * Low cost of entry, relative operational agility and easy access to new technologies makes it increasingly difficult to counter nefarious efforts. * While there are compelling national security reasons to field a social media and PAI space analysis capability, the U.S. Department of Defense (DoD) must do so both while navigating U.S. law and cultural norms and under conditions of great uncertainty. * Amid quickly evolving technologies and communication trends, there is a risk that DoD could invest in soon-to-be obsolete capabilities or encounter other challenges in building its analytic capacity and applying it in an effective and practical manner. |
|  | * This slide shows some basic Social Media Do’s and Don’ts   **DO**   * Utilize appropriate security and privacy settings – this will help minimize your digital footprint and access to your information * Verify all friend requests – if you do not know who is sending you the request, do not accept it. It very well could be a GPC actor or criminal. * Know who is following you – same as before * Verify links before clicking – ensure you are not a target of phishing or spearfishing, or receive a virus or malware thru the link. * Review your family’s security settings and what they post about you and the Navy. Talk to your family and ensure they know the risks. * Understand the risks associated with geo-tagged information. * Completely review and understand the terms of services of each platform you socialize on.   **DON’T**   * Depend on security or privacy settings – typical default settings do not have the user’s privacy in mind. * Trust Add-On’s or Applications – verify before adding, that it will not change your security setting and/or it’s not malicious. * Discuss personal/work details or answer questions from strangers – GPC actors are known to target military members and solicit technical information. * Correct other’s Posts – this could be a baiting opportunity to solicit information. * “Check-In” to places – people who know where you are, also know where you are not, like your home. * Think you have any “RIGHT” to privacy on the Internet, because you do not. |
|  | * Risk is the probability an adversary will gain knowledge of your critical information, and the impact it will have on your mission if they are successful. * When assessing risk, you must think about how it could impact the lives of personnel, the mission, how much the organization stands to lose in money, and time lost as a result of the mission being impacted. * How much are we willing to accept by disclosing critical information, displaying indicators, or not properly identifying vulnerabilities? * Much like ORM and safety, Commanding Officers must determine the acceptable level of risk if critical information is exploited and potentially acted upon. |
|  | * Countermeasures will effectively negate or reduce 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. * Think back to the list of vulnerabilities on previous slides. Remember “Lack of awareness” is a common vulnerability? We cannot just keep shrugging our shoulders when we violate policy or just say we were not aware of something. * How can you mitigate this particular vulnerability? Training! Providing regular awareness training so personnel have a better understanding of what information to protect, and how to protect it. * 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. The Navy as a service does not have a dedicated IdM program, but there are certain elements within the service that have adopted this program for the protection of its personnel. * Effective countermeasures will Influence or manipulate an adversary’s perception, causing them to: * Take no action * React too late * Take the wrong action |
|  | * A periodic assessment is conducted to evaluate whether or not any measures or countermeasure you enacted are effective. * 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. |
|  | * CUI is unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government policy. * Examples of CUI include: * Pre-decisional information and meeting minutes * Investigation documents * Inspection reports * Agency budgetary information * Procurement bids/proposals * Personally Identifiable Information (PII) * 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. |
|  | * OPSEC disclosures occur when personnel share operations/critical information with people they don’t know, like on their social media pages or applications. * 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) |
|  |  |
|  | * Add command information * The Naval OPSEC Support Team is always available to support the fleet. * Visit the NOST website for additional OPSEC information. |