**OPSEC Awareness Month Training 2: Identifying and Protecting Critical Information**

Welcome to the second OPSEC training for OPSEC Awareness Month. Last training we covered the overall concept of how OPSEC best practices preserve lethality along with OPSEC terminology, including CIILs. Now we will dive deeper into identifying critical information and protecting it through our command’s Critical Information and Indicators List (CIIL).

(Lines starting with \*\* are to be asked as questions to help guide discussion in your command trainings prior to reading the provided answers in the following bullets)

**\*\* What is a CIIL, can anyone recall from its introduction last training?**

* A list of critical information and indicators for a specific command or organization, overseen by the command OPSEC Program Manager. (SECNAVINST 3070.2A)
* This document identifies specific information and indicators that, if compromised, could have a significant negative impact on mission effectiveness or national security. It serves as a guide for protecting this information from unauthorized disclosure

**\*\* Who here knows where our command CIIL is?**

* Provide location for soft/hard copies to training attendees
* CIIL should be posted around the command this IAW OAM messaging, see poster format on NOST site for further assistance

**\*\* What is Controlled Unclassified Information (CUI)?**

* CUI is sensitive government information that isn't classified but still needs protection. Command CUI can be found on your CIIL. It encompasses various types of information, including (but not limited to):
  + Personally Identifiable Information (PII): This includes names, social security numbers, addresses, and other data that can be used to identify individuals.
  + Financial information: Budgetary data, contract details, and other sensitive financial records.
  + Export controlled information: Technical data subject to export restrictions.
  + Privacy Act information: Information protected by the Privacy Act of 1974.
  + Proprietary information: Trade secrets or other confidential business information.
  + Law enforcement sensitive information: Information related to ongoing investigations or law enforcement operations.

**\*\* Why do we protect critical information?**

* Unclassified but sensitive information is collected in aggregate by bad actors in an attempt to gain access to a larger, and generally more classified picture of DoD activities planning and execution.

Conduct training on your command CIIL and answer questions as they arise to provide clarification to the items listed