**OPSEC Awareness Month Training 1: Preserving Lethality**

Welcome to OPSEC Awareness Month. The Department of the Navy’s goal is to stress the importance of proper OPSEC practices and to provide in-depth refresher trainings over the coming months to introduce a greater level of knowledge and understanding to all DoN Personnel. OPSEC is vital to remain the most powerful military force in the world, enabling us to preserve lethality.

 (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 Operations Security (OPSEC)?**

* A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

**\*\* Why is OPSEC important?**

* OPSEC is essential for Military operations to assist:
* Mission Success: OPSEC is critical for protecting military operations, troop movements, and sensitive intelligence from enemy detection and exploitation. This helps ensure mission success and minimize casualties.
* Protection of National Security: OPSEC safeguards critical infrastructure, national secrets, and other vital assets from sabotage, espionage, and terrorist attacks.
* Maintaining a Strategic Advantage: By protecting sensitive information and operational plans, OPSEC helps maintain a strategic advantage over adversaries.

Please familiarize your commands with the following OPSEC vocabulary and definitions:

* **Critical Information** - Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment. (JP 3-13)
* **Indicators** - Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (JP 3-13)
* **Information Environment (IE)** - The aggregate of social, cultural, linguistic, physiological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information including individual, organizations, and systems that collect, process, disseminate, or use information. (JP 3-04).
* **OPSEC Measures** - actions to conceal or protect critical information and indicators from disclosure, observation or recognition and are generally defensive in nature (NTTP 3-13.3)
* **OPSEC Countermeasures** - planned offensive actions taken to affect adversary collection, analysis, delivery, or interpretation of information by the adversary FIE (NTTP 3-13.3)
* **Critical Information and Indicator List** – A list of critical information and indicators for a specific command or organization, overseen by the command OPSEC Program Manager. (SECNAVINST 3070.2A)