OPERATIONS SECURITY (OPSEC)

THIS PRODUCT WAS PUBLISHED BY NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE & THE NATIONAL OPERATIONS SECURITY PROGRAM (NOP) OFFICE

Understanding OPSEC

National OPSEC Awareness Month, January 2023, Bulletin 1

National Operations Security (OPSEC) Awareness Month is an opportunity for government agencies, public and private-sector entities, and individuals to reflect on ways to mitigate the various vulnerabilities, risks, and threats to their organizations. This year, the National OPSEC Program (NOP) is focusing on familiarizing personnel with the elements of an effective OPSEC program, to include an emphasis on implementation of the OPSEC cycle.

The term OPSEC was coined by the U.S. military following the realization during the Vietnam War that the enemy was piecing together seemingly innocuous, unprotected information to learn about U.S. military operations in advance. Predictable behavior, lack of communications discipline, and unnecessary sharing of information resulted in the collection and exploitation of information by the enemy. Today, OPSEC is a systematic and proven security discipline for denying adversaries the ability to collect, analyze, and exploit information, including capabilities and intentions. OPSEC has been applied effectively throughout various industries and sectors, not just in the military.

Much of today's intelligence comes from the collection and analysis of open source data, while a smaller percentage comes from clandestine collection efforts, such as human spies, intercepted communications, etc. When an adversary such as a foreign nation, corporate competitor, criminal enterprise, or terrorist group gathers a sufficient amount of unprotected information pertaining to operations, capabilities, or other critical information, the outcome can be disastrous.

Taking appropriate steps to make it harder for adversaries and rivals to collect unclassified and seemingly innocent information can exponentially improve an organization's overall security. The mere process of identifying key data, anticipating the motives and goals of potential adversaries, and actively seeking out threat information increases the likelihood of thwarting efforts to acquire more sensitive but unclassified data. Understanding the likelihood and impact of disclosure, coupled with the implementation of tangible countermeasures to limit vulnerabilities and reduce risk are all part of the OPSEC Cycle. Ultimately, OPSEC is a continuous cycle that should be part of your overall efforts to protect your organization.

OPSEC principles and tactics protect not just organizations, but also individuals, their families, and other loved ones. From a personal perspective, general OPSEC principles help protect private information, and can ingrain security principles and healthy skepticism as individuals navigate everyday situations. In modern society, individuals face a variety of potential risks related to technology, personal security, and finances. The same OPSEC mindset and process that protects major corporations, government agencies, and military units can help individuals reduce their own vulnerabilities.

During National OPSEC Awareness Month, please take the opportunity to learn more about OPSEC, understand its role in securing your organization, and how that understanding can benefit you personally. Our second OPSEC Awareness Month bulletin will feature a more detailed explanation of the OPSEC Cycle.

For more information, tools, and awareness materials from the National OPSEC Program Office, please visit the following link: National Operations Security Program Office (NOP) (dni.gov)