NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

OPERATIONS SECURITY (OPSEC)

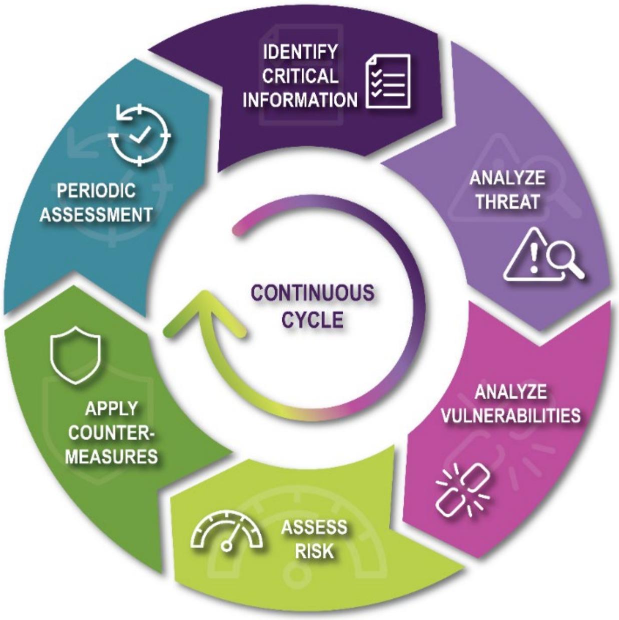
THIS PRODUCT WAS PUBLISHED BY NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE & THE NATIONAL OPERATIONS SECURITY PROGRAM (NOP) OFFICE

Understanding OPSEC - The OPSEC Cycle

National OPSEC Awareness Month, January 2023, Bulletin 2

Operations Security (OPSEC) isn't rocket science, nor should it be. Most of us apply OPSEC principles in our daily lives without realizing it. Whenever an individual identifies personal information that needs to be protected in order to limit risk, they are practicing OPSEC. Not sharing Social Security numbers or other personally identifiable information (PII) — knowing adversaries can use this data to commit identity theft — is common sense, but it is also the first step of the OPSEC Cycle. The threat of information loss/compromise can also be applied to departments/agencies, businesses, corporations, and any other organization, thereby compelling the need to implement the OPSEC Cycle and a robust OPSEC program.

As detailed below, the first step in the OPSEC Cycle involves identifying critical information. Critical information is that which you determine is important to your organization, and if exposed, could be useful by itself or in aggregate to a known or unknown adversary. Critical information does not necessarily mean classified information. Examples of critical information include research and development, proprietary operational information, PII, financial information, and more.



Once you have identified critical information, evaluate potential threats. A threat is anyone with the intent and capability to cause harm. Next, examine the vulnerabilities of your organization (i.e., how your critical information is protected and any weaknesses in that protection), then think about the level of risk your organization faces. The risk equation is calculated as risk = threat (x) vulnerability (x) impact. There are many nuances to the equation and you should evaluate threats in relation to specific vulnerabilities.

For example, if the impact of losing all of your employees' or clients' PII to criminals is high (e.g., it could bankrupt the business), if you are vulnerable due to antiquated cyber protections, and if hackers have tried to access that information previously (the threat), the risk of losing that data should be taken very seriously. However, the risk can be mitigated by developing and deploying countermeasures. In our scenario, countermeasures could include encrypting files containing PII, using multi-factor authentication for employees to access pay statements or other personnel information, not using social security numbers as employee IDs, and providing OPSEC awareness training/resources to employees. Not all countermeasures require expensive solutions and, in fact, many are low- or no-cost to your organization.

During National OPSEC Awareness Month, take the opportunity to learn about OPSEC, understand its role in securing your organization, and how that understanding can benefit you personally.

The National OPSEC Program Office provides OPSEC resources and awareness materials year round. Please visit the following link: National Operations Security Program Office (NOP) (dni.gov)

For more information on Operations Security (OPSEC) please visit www.NCSC.gov