Relationship of OPSEC to other Security Programs

Proficiency Code: A

Operation Security (OPSEC) is the process of identifying critical information and analyzing friendly actions attendant to military operations and activities. In other words, OPSEC denies adversaries critical information and observable indicators about friendly forces and actions. OPSEC serves to identify any unclassified activity or information that, when associated with other activities or information, can reveal protected information about friendly operations or activities. Activities disseminated in the form of a critical information list to help ensure military personnel and media are aware of non-releasable information.

OPSEC is an information-related capability (IRC) that preserves friendly essential secrecy by using a process to identify, control, and protect critical information and indicators that, if compromised, would allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities leading to increased risk or potential mission, function, program, or activity failure or the loss of life. OPSEC's desired effect is to influence the adversary's behavior and actions by reducing the adversary's ability to collect and exploit critical information and indicators about friendly activities.

COMSEC is part of the overall OPSEC program. COMSEC seeks to deny unauthorized people information of intelligence value that they might receive by intercepting and analyzing it. The Air Force Cyberspace Defense Analysis (CDA) weapon system conducts Defensive

To enhance the effectiveness and understanding of OPSEC, the AF provides awareness, education, and training to all AF personnel (e.g., military, DAFC, contractors, family members). Additionally, the AF conducts internal and external assessments utilizing tools and capabilities such as the AF OST, Cyberspace Defense Analysis (CDA) Weapon System (WS), and Enterprise Protection Risk Management (EPRM)

Cyberspace Operations by monitoring, collecting, analyzing, and reporting on sensitive information released from friendly unclassified systems, such as computer networks, telephones, email, and USAF Websites. CDA is vital to identifying OPSEC disclosures. This weapon system grew from OPSEC programs designed to identify vulnerabilities for commanders in the field

Additional Information:

AFI 10-701