Principles

Proficiency Code: A

Communication Security (COMSEC) refers to measures and controls taken to deny unauthorized persons information derived from information systems (IS) of the United States Government related to national security and to ensure the authenticity of such ISs. COMSEC protection results from applying security measures of cryptosecurity, transmission security (TRANSEC), and emission security (EMSEC) to communications and information systems (CIS) generating, handling, storing, processing, or using classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes applying physical security measures to COMSEC information or materials.

The COMSEC program design allows it to detect and correct procedural weaknesses that could expose critical information. COMSEC is part of the overall Operation Security (OPSEC) program. COMSEC seeks to deny unauthorized people information of intelligence value that they might receive by intercepting and analyzing it.

Threat to information systems

Hostile information operations/information cyber-warfare activities pose the greatest threats to an organization's mission critical information via its CISs. Use of commercial hardware and software, in combination with extensive network connectivity, provides many potential avenues for information operations/information cyber-warfare attacks. Such attacks, including introduction of malicious codes (malware), trap doors, or viruses, could result in disabling operations, unauthorized monitoring, and denial or manipulation of communications and information. Various techniques can jam or spoof communications or otherwise degrade or deny access to CISs. Additionally, CISs are vulnerable to espionage and sabotage (especially from individuals who have legitimate access to the system or the physical plant in which it is housed), and to physical damage or destruction. Further, Telecommunications Electronic Material Protected From Emanating Spurious Transmissions (TEMPEST) hazards (compromising emanations or unintentional signals) that, if intercepted and analyzed, would disclose the information transferred, received, handle, or otherwise processed by an information-processing system.

Secure national security systems are vitally important to the operational effectiveness of the warfighter. The Air Force COMSEC program meets Public Law, National, and DOD requirements to secure or protect classified and sensitive information processed using Air Force information systems.

Additional Information:

AFMAN 17-1302-O (Digital Order via WMS)