Protective Measures

Proficiency Code: A

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.

Computer Security (COMPUSEC) is an Information Assurance (IA) discipline identified in AFI 33–200, Information Assurance (IA) Management. Compliance ensures appropriate implementation of measures to protect all Air Force information system resources and information against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuses, or release to unauthorized persons.

Information Assurance defined

Adequate security of Air Force information and supporting IT assets is a fundamental management responsibility. The Air Force implements and maintains the IA Program to secure its information and IT assets. The effective employment of the Air Force's core IA disciplines of COMSEC, COMPUSEC, and EMSEC meets the objectives below.
Objectives

The IA Program ensures Air Force ISs operate securely by protecting and maintaining the confidentiality, integrity, and availability of IS resources and information processed through the system's life cycle. The program also protects information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

Information Assurance Program

The Air Force IA Program synchronizes and standardizes the IA requirements of Air Force ISs through:

- IA integration on all AF enterprise Architecture.
- Coordination of all projects through Lead Command management.
- Streamlining Air Force IT and NSS acquisition through the IT Lean Process IAW AFI 63–101 and 33–210.
- Clear assignment of Air Force organizational and IT level roles and responsibilities.
- Development and management of a professional IA workforce.

Computer security defined:

The objective of COMPUSEC is to ensure the employment of countermeasures to protect and maintain the confidentiality, integrity, availability, and nonrepudiation of AF IS resources and information processed throughout the system’s life cycle.

The framework of the Air Force COMPUSEC IA program consists of a cyclic sequential security management model for risk management. This model is specific to information processed on Air Force computing systems and incorporates strategy, policy, awareness/training, implementation, assessment, remediation, and mitigation controls.

Air Force ISs and devices include but are not limited to: Stand-alone systems, Platform Information Technology (PIT) systems, IS components of systems where Platform Information Technology interconnections (PITI) exist, modeling and simulation systems/networks, ISs connected to external networks via authorized Internet service providers (ISP), ISs providing the management infrastructure, connections/interfaces with other ISs.