

COMPIANCE WITH THIS PUBLICATION IS MANDATORY

Unit Computer Security (COMPUSEC)



Manager's Handbook

Introduction

Congratulations on your appointment as the Computer Security (COMPUSEC) Manager of your unit. At the 159th Fighter Wing, the terms COMPUSEC Manager and Unit Workgroup Manager (WGM) are synonymous. The person appointed as the WGM also performs the functions of the Unit COMPUSEC Manager. It is a very important job and requires your continuous attention.

Automated Information Systems (AIS) and the information they process are critical to our USAF mission. These systems must be treated the same way as any other critical mission resource. Today, most USAF career fields rely on computerized systems to accomplish their missions and many people rely on computers to do their daily jobs.

As COMPUSEC Manager you will provide direction and assistance to the personnel within your unit. It is your job to monitor compliance to ensure measures are taken to protect all Air Force information system resources and information effectively. You will also provide assistance in applying the appropriate levels of protection against threats and vulnerabilities, prevent denials of service, corruption, compromise, fraud, waste and abuse.

MSgt Tiffanni L. Beckham
Wing Information Assurance Manager

COMPUSEC Objectives

The objectives of the COMPUSEC program are to protect and maintain the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle. Security disciplines such as COMPUSEC, Information Security (INFOSEC), Emission Security (EMSEC), and Communications Security (COMSEC) all contribute to provide safeguards to protect information. Administrative and managerial activities that implement the safeguards are known as controls. Each safeguard and its associated control constitute a countermeasure. We apply countermeasures to achieve four main objectives:

- ☐ **Availability** ensures computer resources are available to authorized users when needed. This means unexpected or unscheduled downtime is reduced as much as possible.
- ☐ **Integrity** is comprised of two parts: data and system integrity. Data integrity ensures data is not accidentally or maliciously modified, altered or destroyed. System integrity ensures the system performs its intended function in an unimpaired manner.
- ☐ **Confidentiality** ensures that only those with the proper clearance, authorization, and need-to-know are allowed access to sensitive information.
- ☐ **Accountability** ensures that all security-relevant actions on the base network are traceable to a single user who is accountable for those actions.

Roles & Responsibilities

Designated Approval Authority (DAA) - The DAA has the overall responsibility for the operation of an AIS within a specified environment. This is done by formally "accrediting" systems before placing them

into operation. In addition the DAA approves AIS security policies, certification plans, and operating procedures to ensure the secure operation of the AIS. The DAA is further responsible for approving security requirements documents, Memorandums of Agreement, and deviations from the security policy. The wing commander is the DAA for the 159th Fighter Wing Wide Area Network.

Wing Information Assurance (IA) Office – The IA office implements the COMPUSEC program for the wing commander. The IA office assists all base and Geographically Separated Unit (GSU) organizations in the development and management of their COMPUSEC programs. Also provides Certification & Accreditation (C&A) guidance and assistance to wing and GSU units and ensures information system requirements documents include appropriate COMPUSEC requirements.

Network Control Center (NCC) – The 159th Fighter Wing NCC manages the local infrastructure that provides customers the communications and information resources needed to achieve operational objectives.

Unit COMPUSEC Manager - Unit commanders designate a unit COMPUSEC Manager to oversee the overall unit program. The COMPUSEC Manager is the single liaison between the IA office for COMPUSEC matters. They ensure all users receive computer security training and guidance. They provide direction and assistance to the personnel within their assigned units. COMPUSEC Managers also monitor compliance to ensure measures are taken to protect all Air Force information system resources and information effectively. They also provide C&A information to the wing office for appropriate tracking.

Users – The user is anyone with access to an Air Force AIS and information. They are the most important people in computer security and represent the eyes and ears of COMPUSEC. Users are responsible for complying with computer security policies and procedures. They must also protect system information and resources according to established security policies and procedures and report system security incidents, vulnerabilities, and virus attacks.

Policies & Procedures

Information protection requirements are defined in terms of the perceived threats, risks, and goals of an organization. This is often stated in terms of a security policy as written instructions, rules and regulations. The development of a security policy is necessary to ensure each AIS complies with AF instructions and remains reasonably secure from attack. A security policy is also required as part of the Certification & Accreditation package. Air Force instructions provide a list of basic requirements that must be met and adhered to as users operate systems. By developing an effective security policy, it is ensured that these requirements are met and keep LA ANG systems safe.

HQ LAANGI 33-3, **159th Fighter Wing Network Security Policy**, is the instruction that establishes the guidelines and procedures for the proper use of the 159th Fighter Wing Wide Area Network. This instruction was created to ensure all network computer users have adequate guidance regarding the policies that govern connection to the network and safeguarding information processed on the network. All COMPUSEC Managers should have this document readily available for reference and guidance purposes.

Basic COMPUSEC Requirements

☐ All AISs must have a security policy. The security policy also identifies roles and responsibilities of management, system and security administrators and end users.

- ☐ AISs must be formally accredited by the DAA before being placed into operation. The accreditation validates the risk analysis and certification and documents the residual risk the DAA is willing to accept.
- ☐ Security must be implemented in an effective, efficient and integrated manner to find the most cost-effective solutions possible.
- ☐ All AISs must have an effective risk management program as part of a continuous process to manage risk. Threats must be monitored, vulnerabilities minimized, and system modifications made in a manner that is consistent with the security policy.
- ☐ Access control mechanisms must exist on each AIS to individually identify and validate (authenticate) each user.
- ☐ AIS users must prevent unauthorized access to the AIS and information, and prevent the introduction of malicious logic (viruses).
- ☐ All AIS users must be trained to protect the information and resources against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons.
- ☐ All personnel who operate and maintain AISs must protect them at a level commensurate with the risk and the magnitude of harm that could result from disclosure, loss, misuse, alteration, or destruction of the information or AIS.

Risk Management

Proper risk management (instead of complete risk avoidance) is the total process of identifying, measuring, and minimizing threats and vulnerabilities. While all risk cannot be eliminated, users can achieve a goal of providing an appropriate level of protection. Risk management involves much more than just identifying threats and vulnerabilities, it focuses on specific areas where safeguards and controls can be implemented to minimize the risk of operating an AIS.

☐ **Risk Analysis** – Risk analysis is the process of determining the information’s sensitivity level, AIS and information mission criticality, and the risks associated with operating the AIS. It evaluates the AIS as a whole. The risk analysis process consists of sensitivity and criticality assessments; threat and vulnerability risk assessments; countermeasure economic assessments, and Security Testing & Evaluation.

☐ **Certification** – Certification defines the extent to which the implemented security meets specified requirements. The certifying official judges the AISs compliance with stated security requirements, requests approval to operate from the DAA, and certifies the AISs security measures perform technically as they were designed to perform.

☐ **Accreditation** - Accreditation is the DAAs formal written approval to operate the AIS and is given only after the DAA determines that the AIS has been provided the appropriate level of protection.

Threats

A threat can be defined as a current and/or perceived capability, intention, or attack directed to cause denial of service, corruption, compromise, or fraud, waste and abuse to a system. Listed below are three basic categories of threats to AISs and examples of each.

☐ Natural – Earthquakes, floods, hurricanes, snow/ice, tornadoes, windstorms, and other types of severe weather are examples of natural threats. Items in this category are commonly considered “Acts of God.”

☐ Environmental – These threats are man-made and are most often a result of flaws in building construction, improper implementation of utilities, faulty wiring, or poor housekeeping. The following situations would fall into this category: power disturbances/loss, utility failure, smoke damage, water damage, fires (major and minor), hardware/software failure, personnel injury or death, and explosions.

☐ Human – Human threats can either be intentional or unintentional.

Intentional – An intentional threat is a deliberate attack by a person(s) toward an information system, network resource, or information. The rationale for an intentional attack could include a desire to degrade the AIS integrity, revenge or personal gain. The following acts are considered intentional: bomb threat, compromise of classified information, disclosure of sensitive information, sabotage, misuse of AIS and network resource, theft, fraud, viruses/malicious logic and vandalism.

Unintentional – An unintentional threat is categorized as accidental or inadvertent damage to an AIS, network resources, or information. It is usually a result of carelessness, ignorance, or lack of training and includes, but is not limited to the following: hardware failure, software failure, communications failure and software alterations. An unintentional threat is the most common type of threat

Vulnerabilities

Every AIS has vulnerabilities, whether large or small. Vulnerability is a weakness that allows misuse or exploitation of an AIS or its data. Weaknesses can be found in information systems, cryptologic systems, or components. System vulnerabilities fall into the following categories.

☐ Physical – Physical vulnerabilities are weaknesses or deficiencies in the control and accountability of physical access to controlled areas. The controls can be technical (automated), non-technical (manual), or both. Deficiencies noted in this area can lead to sabotage, vandalism, asset theft and unauthorized disclosure.

☐ Environmental – Environmental vulnerabilities involve weaknesses or deficiencies in maintaining the environmental stability, control, and safety of the computer area. This includes housekeeping, fire detection and suppression, temperature and humidity control, and structural soundness. Deficiencies in this area can lead to minor/major fires, hardware failure or damage, media damage, or software failure.

☐ Personnel – Personnel vulnerabilities involve deficiencies in the controls established to ensure all personnel who have access to sensitive information have the required authorization (need to know) as well as appropriate clearances. Deficiencies in this area can lead to sabotage, fraud, unauthorized system use, data modification and inadvertent disclosure.

☐ Hardware – Hardware vulnerabilities involve deficiencies in installing, operating, and maintaining the AISs and network hardware. Deficiencies in this area can lead to major/minor fire, and hardware or software failure.

☐ Software - Software vulnerabilities involve deficiencies in the control of network and PC operating systems, system and application software versions, data, and related software security features. Deficiencies in this area can lead to procedural error, disclosure, software modification, data modification, data/software loss and unauthorized system use.

☐ Network/Communications – Network vulnerabilities involve deficiencies in the security and controls of the various communications media used to transmit data between the servers and network users. Deficiencies in this area can lead to sabotage, fraud, unauthorized system use, denial of service, data modification, software, and unauthorized disclosure.

☐ Procedural – Procedural vulnerabilities involve deficiencies in the development and maintenance of procedures, rosters, and forms that provide guidance, definition of responsibilities and identification of responsible personnel.

Threat Advisories

The Air Force Computer Emergency Response Team (AFCERT) is responsible for disseminating computer threat advisories Air Force wide. The AFCERT provides information protection assistance to all Air Force units. It conducts operations involving intrusion detection, incident response, computer security information assistance, and vulnerability assessment of Air Force automated information systems. Some of the duties of the AFCERT are as follows:

☐ Process and coordinate countermeasure development and disseminate countermeasures for all reported IA vulnerabilities.

☐ Establish and maintain IA vulnerabilities.

☐ Establish and maintain Internet Protocol (IP) databases.

☐ Assist unit commanders with computer attack damage control and recovery procedures.

☐ Distribute AFCERT Advisories, AFCERT IP Bulletins, and ASSIST Bulletins.

Advisory Compliance

AFCERT Advisory compliance is **MANDATORY**. The Information Assurance (IA) office receives the advisory via e-mail. Before compliance is reported to the MAJCOM, the actions required must be completed and documented for **ALL** affected systems.

It is extremely important to keep abreast of the current threats to AF systems. With more intrusion attempts being conducted everyday, users must organize efforts to protect DOD computers. By maintaining an active reporting system and taking prompt action on Air Force threat advisories, LA ANG members can stay ahead of the threat.

Marking & Labeling

COMPUSEC Managers must periodically review all paper products and storage media to ensure they are marked IAW AFI 31-401, *Information Security Program Management*. Appropriate marking and labels must be applied to all printed listings, display terminals, diskettes/jackets, and storage devices. Label all storage media with SF 711, **ADP Media Data Descriptor Label**, and the appropriate classification. Storage media may include floppy disks, removable hard drives, permanent hard drives, disks, CDs and tape drives.

Warning banners are another form of labeling and are required on all AF computer systems. These banners identify the system as a DOD resource and inform the user that unauthorized access is prohibited.

Warning banners will be clearly visible by all personnel logging onto the network and be unable to bypass during the login process.

Declassification and Destruction

Declassification is an administrative procedure wherein media is sanitized of the classification information and the sanitation is verified. Since the highest level of information on the 159th Fighter Wing Wide Area Network is sensitive but unclassified, declassification will only be necessary when classified information inadvertently contaminates the network.

Sanitize network or desktop systems inadvertently contaminated with classified information using an approved deguasser. COMPUSEC Managers will work with the 159CF/SCM branch when situations requiring sanitation arise.

Physical Security

The Security Forces Squadron is the primary source of information on physical security protection methods and procedures. Access to AIS resources is initially controlled by physical security controls. Procedures must be in place to restrict access to the AIS and media, not only to prevent unauthorized access, but also to guard against theft and tampering. Some ways to control access include the following:

- ☐ Key controls
- ☐ Alarms, intrusion detection or sensor systems
- ☐ Surveillance equipment
- ☐ Physical barriers
- ☐ Establishment of a controlled area
- ☐ Lock doors when unattended

Information Security

The Security Forces Squadron is the primary source of information on the information security program. The program provides for the protection of classified information from compromise by using proper classification and safeguarding. Another aspect of the Information Security program is the identification and control of special access categories of information. These categories are groupings of classified or sensitive unclassified information to which an additional restrictive label is applied to signify that personnel are granted access to the information only if they have access approval. Examples of these categories are For Official Use Only, Privacy Act, North Atlantic Treaty Organization and Secret Compartmentalized Information.

Operations Security (OPSEC)

The OPSEC program is an operation management program – not a traditional security program. Its objective is mission effectiveness. The primary purpose of the OPSEC program is to ensure the Air Force actively practices OPSEC to deny critical information to adversaries. It also strives to promote an understanding and an awareness of the benefits of OPSEC among all Air Force members. The OPSEC program includes the activities and infrastructure required to identify and control critical information, threats, sources of information, and OPSEC indicators.

Communications Security (COMSEC)

Communications Security is defined as measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC countermeasures stem from encryption, security of transmission lines and physical controls for the associated equipment.

Emission Security (EMSEC)

Air Force organizations acquiring or using AISs to process classified information must apply EMSEC proportionally to the threat of exploitation and the potential damage to national security if classified information is compromised. National policy requirements dictate that compromising emanations must be contained within an inspectable space. Inspectable space is the three-dimensional space surrounding equipment that processes classified or sensitive information. Within this space EMSEC exploitation may occur when equipment or hazard removal is considered impractical, or where legal authority to identify or remove a potential EMSEC exploitation exists. EMSEC inspections and evaluations are currently being accomplished by the 159CF/SCM branch.

Information Assurance (IA) Awareness Program

Proper training and education can greatly reduce the number of security incidents encountered and provide the most effective form of countermeasures. Users receive COMPUSEC training continually throughout their career. The program that ensured this training was Security, Awareness, Training and Education (SATE). The SATE Program was renamed to the Information Assurance (IA) Awareness Program. The objectives of the program remain the same. It ensures users receive training on the many disciplines associated with Information Assurance. The training consists of but is not limited to the following:

- ☐ Common threats and vulnerabilities of AISs and how they impact the AIS operation.
- ☐ Security policies and procedures for the protection of the AIS operating environment and its information.
- ☐ Users role in maintaining AIS security.
- ☐ Basic risk management concepts and the importance and effectiveness of the controls established for their AIS.
- ☐ Administrative procedures for the protection of sensitive information.
- ☐ Physical security procedures employed to protect the AIS and its information.
- ☐ Contingency procedures and operating instructions.

Certification & Accreditation (C&A)

Certification validates the security assurance for a system associated with an environment. Accreditation evaluates whether the operational impacts associated with any residual system weaknesses are tolerable or unacceptable. The degree of assurance assumed by the DAA ensures the system is able to enforce its security policy.

The C&A process allows the DAA and other key personnel to tailor the certification efforts to the particular system mission, threats, environment, degrees of assurance, and criticality of the system, as necessary as long as they apply with network connection rules.

Information systems must be recertified and reaccredited every three (3) years unless changes to the information system or environment baseline impact security, thereby necessitating earlier recertification or reaccreditation.

Type Accreditation

Type accreditation is a full technical assessment of one information system configuration operating in a stated environment for the purpose of applying the assessment to multiple copies of the system operating in similar environments. The suitability of the system to operate with an acceptable level of risk is evidenced by the DAAs approval to operate.

Contingency Planning

COMPUSEC Managers are responsible for assuring the adequacy of contingency plans for AISs in their area of responsibility. Although you may not actually write the plans, you may be called upon for guidance. The contingency planning process develops plans for disaster recovery to provide reasonable assurance that critical mission support can continue or resume within a specified time frame if normal system operations are interrupted. These plans outline the procedures to follow in the event of a catastrophic occurrence and how to reduce the impact to the information system from such occurrences.

These plans identify which AISs are most vital and the level of protection necessary to ensure mission accomplishment. Manual procedures must be developed to ensure mission requirements are met during periods when AIS support is not available.

No AIS is exempt from potential failure. Contingency plans provide safeguards and controls that ensure continuity of operations in the event of a disaster or restore operations in the event of an AIS failure. Contingency plans have three phases: backup/preparation, emergency response, and recovery. The scope and contents of the plans will vary depending on the criticality of the AIS. The plans should be revised as needed.

Types of Contingency Plans

☐ Emergency Plans – An emergency plan is the response phase of contingency plans, things to do while the emergency is in progress. The plans must address unique deployed operating conditions, such as temperature and humidity variations, power fluctuations, and dust if appropriate. Depending on your location, facilities, and other variables, the emergency plans should contain both a continuity of operations plan and responses to take while the emergency is in progress.

☐ Backup Procedures – Of primary consideration for continuity of operations is the existence of backup procedures for AISs. These procedures include provisions made for the recovery of information and for the restart or replacement of AIS equipment after a failure.

☐ Disaster Recovery Plan – A disaster recovery plan involves those actions necessary to recover from a contingency. It includes a specific recovery response before operations can continue. The steps you take to recover from a disaster depend on the type of disaster incurred.

Summary

While the information in this handbook is primarily directed at the Unit COMPUSEC Manager, it applies to everyone in today's Air Force. The Wing IA office is tasked with providing the necessary guidance.

The sections of this handbook also follow the guidelines established by Public Law 100-235, The Computer Security Act of 1987. It is applicable to all departments and agencies of the U.S. Government, their employees, and contractors.

Your job as a COMPUSEC Manager is often time-consuming and detailed oriented. It is not always an easy task. However, you can seek assistance from personnel in the Wing Information Assurance Office. Please do not hesitate to call with any questions regarding this handbook or other computer security related questions. You may contact MSgt Tiffanni Beckham or SSgt Ashley Despanza at 391-8311. CF/SCBS is located in Bldg. 149, Rm. 124.

Attachment 1

Glossary of References and Supporting Information

AFI 10-1101, *Operations Security*
AFI 31-401, *Information Security Program Management*
AFI 31-501, *Personnel Security Program Management*
AFI 33-115 V1, *Network Management*
AFI 33-119, *Electronic Mail (E-Mail) Management and Use*
AFI 33-202, *Computer Security*
AFI 33-203, *Emission Security*
AFI 33-204, *Information Assurance (IA) Awareness Program*
AFI 33-211, *Communications Security (COMSEC) User Requirements*
AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*
AFMAN 33-223, *Identification and Authentication*
AFSSI 5020, *Remanence Security*
AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*
AFSSI 5023, *Viruses and Other Forms of Malicious Logic*
AFSSI 5027, *Network Security Policy*
DOD 5200.1-R, *Information Security Program*
DOD 5200.8-R, *Physical Security Program*
159FWI 33-1, *Intranet/Internet Policy*
HQ LAANGI 33-1, *Network Management*
HQ LAANGI 33-3, *159th Fighter Wing Network Security Policy*
AFJQS 3C0X1-211RA, *Computer Security Managers Handbook*

Abbreviations and Acronyms

AFCERT	<i>Air Force Computer Emergency Response Team</i>
AIS	<i>Automated Information Systems</i>
C&A	<i>Certification & Accreditation</i>
CAMS	<i>Core Automated Maintenance System</i>
CF	<i>Communications Flight</i>
COMPUSEC	<i>Computer Security</i>
COMSEC	<i>Communications Security</i>
DAA	<i>Designated Approving Authority</i>
DBM	<i>Database Manager</i>
EMSEC	<i>Emission Security</i>
FOIA	<i>Freedom of Information Act</i>
GSU	<i>Geographically Separated Unit</i>
HD	<i>Help Desk</i>
HQ AFCA	<i>Headquarters Air Force Communications Agency</i>
I&A	<i>Identification & Authentication</i>
IA	<i>Information Assurance</i>
INFOSEC	<i>Information Security</i>
IP	<i>Internet Protocol</i>

NAC	<i>National Agency Check</i>
NCC	<i>Network Control Center</i>
OPSEC	<i>Operations Security</i>
OPR	<i>Office of Primary Responsibility</i>
SA	<i>System Administrator</i>
SATE	<i>Security, Awareness, Training, and Education</i>
SBU	<i>Sensitive But Classified</i>
SSAA	<i>System Security Accreditation Agreement</i>
WGM	<i>Workgroup Manager</i>
WIAO	<i>Wing Information Assurance Office</i>