

**BY THE ORDER OF  
THE INSTALLATION COMMANDER**

**CHARLESTON AFB INSTRUCTION 33-601**

**1 March 2000**

**Security**

**BASE METROPOLITAN AREA NETWORK  
SECURITY POLICY**



**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO/PP WWW site at:  
<http://afpubs.hq.af.mil>.

---

OPR: 437 CS/SCBS/CSSO (Mr. Jeffrey Morey)

Certified by: (Major Douglas J. Taylor)

Pages: 25

Distribution: F

---

**TABLE OF CONTENTS**

1. Introduction. ....	2
2. Concept of Operations. ....	5
3. System Security Policy.....	8
<b>Attachment 1—GLOSSARY OF REFERENCES, AND SUPPORTING INFORMATION</b>	<b>20</b>

**1. Introduction.** The United States Air Force has long been among the leaders in applying the latest technology to everyday problems. As a result, the Air Force has been at the forefront in employing computer systems to support its mission. The use of computer technology centers on the automation of information flow; that is, getting the right information to the right person at the right time. As beneficial as the use of computer technology can be, there are hazards inherent in automating the creation and flow of information. These hazards include the possibility of disclosure or misuse of information (a threat to confidentiality); the corruption of information or damaged storage media (a threat to integrity); and the denied access to data as a result of malicious computer attacks, improper use of a system, or deletion of data (a threat to availability). This security directive is part of the effort to accredit the 437 Air Wing Base Metropolitan Area Network (BMAN) and to ensure the confidentiality, integrity, and availability of the system and information it contains.

**1.1. Purpose.** The purpose of this document is to establish operational security requirements for the BMAN. Specifically, this security instruction implements network and computer security measures to ensure data confidentiality, data integrity, and assurance of service availability. It also addresses the minimum security measures for systems interfacing with the BMAN.

**1.2. Mission.** The mission of the BMAN is to support the electronic creation, transfer, sharing, and presentation of information by using networked personal computers and commercial off-the-shelf software. The BMAN is a general purpose, multi-user system used throughout the 315th and 437th Air Wings. It provides a myriad of electronic services (such as, electronic mail, word processing, spreadsheets, electronic forms, databases, etc.) and provides a gateway to the Internet. More importantly, the BMAN provides the staff with the tools to improve business processes. The result is increased efficiency and effectiveness. The BMAN also provides the data path for other command and control (C2) systems on Charleston AFB.

**1.3. Applicability and Scope.** This security directive establishes the minimum BMAN computer security requirements. It provides a set of rules and practices that regulate management, protection, and distribution of data entrusted to the network. The policies stated in this directive are mandatory for everyone administering and using the BMAN.

#### **1.4. Specific Roles**

**1.4.1. Designated Approval Authority (DAA):** 437 AW/CC is appointed as DAA for all Automated Information Systems (AIS) used on Charleston AFB. The AW/CC has delegated those duties and responsibilities, in writing, down to Squadron Commanders. The DAA for the BMAN is 437 CS/CC with DAA responsibilities for subordinate networks delegated to the responsible squadron commander. The DAA is the official who assumes responsibility for operating the BMAN. The DAA determines the acceptable level of risk at which the system will operate, and has the authority to allocate resources to achieve an acceptable level of security. It is the DAA's responsibility to provide authorization for connection of systems and networks to the BMAN. The DAA is the only person who has the authority to accredit a system.

**1.4.2. Certification Official:** The Certification Official is responsible for making the technical judgement of BMAN compliance with stated security requirements, and identifying and assessing the risks associated with operating the BMAN. The Certification Official will provide the DAA with an accreditation recommendation. The Certification Official for the BMAN is 437 CS/SCB.

**1.4.3. Program Manager (PM):** The Program Manager, as it pertains to the BMAN, assumes ultimate responsibility for implementation of security activities. The PM ensures modifications

and upgrades are acquired, designed, developed and maintained to fulfill fundamental security concepts. The PM will approve the accreditation plan prior to submission to the DAA. The PM for the BMAN is 437 CS/SCBN.

**1.4.4. Computer Systems Manager (CSM):** The Computer Systems Manager is responsible for operation of Automated Information Systems (AIS) and has supervisory or management responsibility of the functional area that operates the system. The CSM will plan and program budget, manpower, and training support for the implementation of the BMAN Computer Security (COMPUSEC) program. For office automation systems, the Office Chief or manager is normally the CSM. For the BMAN, the CSM is 437 CS/SCBN.

**1.4.5. Wing Information Assurance (IA) Office (WIAO):** The WIAO is responsible for managing and implementing COMPUSEC on Charleston AFB. This includes: Conducting initial/annual COMPUSEC training; establishing procedures for units to request DAA approval for new systems; establishing local COMPUSEC policy; conducting visits to all 315th, 437th and tenant units to ensure COMPUSEC compliance; and oversees inquiry computer intrusion and malicious logic incidents. The WIAO also ensures the provisions of all applicable security directives are implemented throughout the life cycle of the system. The WIAO works with management, other security personnel, and users to administer an effective security program.

**1.4.6. Information Protect Operations (IPO):** The IPO for the BMAN is 437 CS/SCBNS. The BMAN IPO is responsible for conducting daily security operations for the network. The IPO works with users, other security personnel, and management to administer an effective BMAN COMPUSEC program.

**1.4.7. Unit COMPUSEC Manager (UCM):** The UCM conducts daily security operations for their unit. This individual disseminates, applies, and enforces COMPUSEC policies and procedures. The UCM will: Certify and endorse all unit computers related AF Form 3215's (to verify the system is accredited), maintain a copy of applicable policies, ensures all copyright laws are adhered to, and obtains and disseminates the latest AF approved virus detection software. The unit commander will appoint in writing a primary and alternate UCM. Submit appointment letters to the WIAO, 437 CS/SCBS. Appoint replacement 30 days prior to the departure of the incumbent.

**1.4.8. Network System Administrator (SA):** Network SA ensures servers, workstations, peripherals, communication devices, and software are on-line and available to support customers. System administration's area of responsibility is from the user's terminal to the server, but does not include the network backbone infrastructure components. System administrators may be assigned outside the Network Control Center (NCC); however, they take direction from the NCC and must thoroughly understand the customer's mission and be completely knowledgeable of the hardware and software capabilities/limitations.

**1.4.8.1. Functional System Administrator (FSA):** The Functional System Administrator is assigned at the group level. There will be one FSA for every 250 users on the network. They provide oversight and management of specific resource servers to which they are assigned. They receive overall guidance from the network administrators. FSAs validate authorization to computer systems and networks IAW defined security directives and procedures. They work directly with Work Group Managers and individual users from initial set up through final disposition of each account.

**1.4.9. Work Group Manager (WGM):** The Work Group Manager provides initial problem resolution to users. They are assigned a small group of users usually in a building or a unit, and are primarily responsible for all support activities pertaining to single client workstations. Their duties may also include delegated responsibilities from the FSA. They receive guidance from FSA and Network SAs. If problems occur beyond the scope of their responsibility or training they will contact their assigned FSA or the NCC help desk (ext. 3-3511) for assistance and will work with them to resolve the problem. They have the responsibility of adding workstations to their local hub or switch when needed and forwarding requests for new accounts to the NCC. For security incidents, the WGM will notify the NCC help desk (ext. 3-3511) for guidance and resolution.

**1.4.10. Computer Systems Security Officer (CSSO):** The Computer Systems Security Officer is responsible for the security of terminals or small systems that interface directly (by dedicated access circuits) to the BMAN. They will monitor activities at the terminal areas to ensure compliance with BMAN Computer Security (COMPUSEC) procedures.

**1.4.11. Unit Commanders:** Each unit commander has overall responsibility for proper management of BMAN resources under their control. Commanders will validate all requests for access to the network. Commanders will also appoint, in writing, all system and security personnel for systems under his/her control.

**1.4.12. User (Customer):** To perform their mission, authorized users employ, but do not own, the BMAN. Each customer of the BMAN is responsible for following established security directives and procedures. Customers must safeguard sensitive data and critical resources, and mark output products appropriately (i.e., For Official Use Only (FOUO), Privacy Act, etc.). Users will report security problems or incidents through their WGM or FSA to the NCC Help Desk (ext. 3-3511) as soon as possible after detection.

**1.5. Network Control Center.** The NCC is composed of four interdependent workcenters.

**1.5.1. Network Administration Workcenter:** Provides oversight and management of the BMAN. Duties focus on configuration and user management of Charleston Domain servers. Network SAs are responsible for operational policy and guidance to the Functional System Administrators and also responsible for implementing security procedures on all network servers. They will perform, upon notification from the Wing Information Assurance Office, an initial evaluation of each security incident and begin corrective or protective measures.

**1.5.2. Network Management Workcenter:** Responsible for the infrastructure of the BMAN from the interface of the user's terminal to the interface(s) of the base-level host, base-level server, or transmission system providing connectivity to off-base assets and includes all the base network backbone infrastructure components. They manage and configure all hardware on the backbone including routers, switches, hubs, multiplexers, serial link modems, media converters, circuits, repeaters, bridges, routers, gateways, software, etc.

**1.5.3. Information Protection Operations Workcenter:** Responsible for overall security of the network through implementation and enforcement of DoD, and Air Force security policies and directives. They configure, manage, and monitor security tools implemented on the BMAN, validate security problems, and route them to the proper office for correction. They assist Air Force organizations in deterring, detecting, isolating, containing, and recovering from information system (IS) and network security intrusions. They work closely with network SAs and FSAs to ensure proper security measures are taken to protect the information on the network.

**1.5.4. Help Desk:** Receives trouble calls, opens trouble tickets, assesses and resolves problems, records fault-isolation procedures, closes trouble tickets within defined response times, and reports the status of problems and resolution actions to the affected customer(s). Provides a central repository for technical advice and solutions for network systems. Problems which Help Desk technicians are not trained or equipped to handle are routed to the appropriate office for resolution. The Help Desk is the central hub for all base network problems. There will be an up-channel to the AMC-level help desk for information sharing and problem resolution assistance.

**1.6. Terms.** The terms used in this instruction are defined in Glossary.

**1.7. References.** The references used to develop this instruction are listed under References.

**1.8. Relationship to Other Publications.** This instruction implements applicable requirements contained in high level policy documents, including the National Computer Security Center (NCSC) Standards and Guides (Rainbow Series), Department of Defense (DoD) Directives, Air Force Instructions (AFIs), Air Force Systems Security Instructions (AFSSIs), Memorandums (AFSSMs), AMC Instructions (AMCIs) and Charleston AFB Instructions (CAFBIIs). These documents govern the operation and management of AISs.

**2. Concept of Operations.** The purpose of the BMAN is to enable 437 Air Wing personnel to improve business processes and work efficiently. It allows organizational local area networks (LANs) and other systems on Charleston AFB to interconnect and provides the ability to connect to networks and systems external to the base.

**2.1. Operating Environment.** The BMAN is a collection of physical media and devices which provide the means to transmit information between one component on Charleston AFB to another component, possibly external to CAFB. The network consists of numerous routers, hubs, and Ethernet switches, domain name server, remote access server (RAS), network monitoring devices, and mail transfer agents using software programs like Windows NT, Microsoft Exchange, base supported anti-virus, Novell Netware, HP Openview, CA Unicenter, and UNIX operating systems.

**2.1.1. System Location:** The BMAN is located in many buildings throughout Charleston AFB. Configuration and infrastructure documentation is maintained in the NCC.

**2.1.2. Hours of Normal Operation:** The BMAN operates 24 hours a day, seven days a week. Heavy usage operating hours are from 0730 to 1630, Monday through Friday. During normal working hours, users will contact their WGMs and, if necessary, their FSAs for assistance. Users will attempt to contact their WGM or on-call FSA during non-duty hours. Users may contact the NCC Help Desk (ext. 3-3511) if other avenues of assistance are unavailable.

**2.1.3. Sensitivity and Criticality:** The highest sensitivity level of information authorized for processing on the BMAN is sensitive information. Extended periods of downtime would cause mission degradation and extreme inconvenience to the users. Increased interface with HQ AMC command and control systems increase the system's criticality.

**2.1.4. Operating System:** Windows NT is the network operating system authorized for use on the master domain (Charleston) for the BMAN. Systems currently running operating systems other than Windows NT will be allowed to continue to operate until they are obsolete; however, it will not be supported by the NCC. AF Form 3215s requesting the purchase of other operating systems will be returned for modification.

## 2.2. Employment

**2.2.1. Notice and Consent for Telecommunications Monitoring.** All systems connected to the BMAN are subject to monitoring. Network management or security personnel reserve the right to monitor a user's account. This warning is displayed upon logon. Warning banners are required by AFI 33-219, Telecommunications Monitoring and Assessment Program (TMAP), on all AISs. All workstations connected to the BMAN will have a login consent to monitoring warning banner. Additionally, each stand-a-lone or workstation will have a Consent to Monitoring Label prominently displayed on the front of the monitor.

**2.2.2. Using Government Owned Software For Personal Projects.** The unit commander or equivalent must approve use of government owned software for personal projects. Licensing regulations must be complied with when using software on personal projects and computers.

**2.2.3. Personally Owned Computers.** Computers personally owned by Air Force members, government employees, or contractor personnel will not be used to process classified or sensitive information. However, their use may be approved for remote dial-in modem connection to the BMAN for processing sensitive information, provided all security conditions for modem connections are met. Personally owned computers will not be directly connected to the BMAN.

## 2.3. Security

**2.3.1. Personnel Security:** Access to the BMAN is based on the key concepts of "authorization" and "need-to-know."

**2.3.1.1. Authorization:** Authorization is validated when a WGM or FSA notifies a NCC NA that an individual requires BMAN access to perform their official duties. Notification may be by e-mail or letter.

**2.3.1.2. Need-To-Know:** Each user is responsible for determining a person's need-to-know before disclosing information under his or her control.

**2.3.2. Security Clearances:** Access to the BMAN does not require a security clearance. However, the DAA reviews anyone who has his or her security clearance suspended or revoked for cause, or receives administrative punishment (such as an Article 15), for access eligibility. The authority that suspended or revoked a security clearance or imposed administrative punishment will make the determination to grant or deny access to the BMAN. If a user's continued access to the network is denied, withdraw access within one workday.

**2.3.3. Government Contractors:** Do not give government contractors access to any information accessible on the BMAN unless first approved through proper channels. Request approval for contractor access through the appropriate contracting officer only when required to satisfy the terms of the contract. The contracting office is responsible for obtaining appropriate nondisclosure agreements and ensuring requirements of the Privacy Act of 1974 are enforced.

## 2.4. Physical Security

**2.4.1. Resource Protection.** The first line of defense for protecting valuable assets is resource protection. All base personnel are responsible for positive identification of persons attempting to access BMAN assets in their area of control. They will verify the status of the individual and challenge any individuals they cannot positively identify.

**2.4.2. Network Infrastructure Access.** Restrict physical access to network infrastructure

components (servers, hubs, routers, and wiring) by locating them in a climate controlled lockable enclosure such as a room, closet, or cabinet. Limit access to authorized personnel only, such as the FSA, WGM, or network administrator. Technicians from the NCC must have 24 hour, 7 day a week access to all areas with networking equipment; the preferred method is to give them keys. If that is not practical, someone must be available to grant them access.

**2.4.3. Unattended Terminals.** Do not leave terminals logged into the BMAN when unattended. Users will either logout (the preferred method) or use a password protected screen saver when the terminal is left unattended. The user will log out of the BMAN prior to leaving at the end of his or her work shift.

**2.4.4. Hardware Inventory.** The unit Automated Data Processing Equipment (ADPE) Custodian will ensure all BMAN hardware assets (i.e., workstations, printers, etc.) under their span of control are listed in the ADPE Information Processing Management System (IPMS). In order to accomplish this, the unit ADPE Custodian must ensure that any unit purchased equipment is routed through the NCC ADPE section before placing it into the workplace, IAW AFI 33-112, para 10.2.1. The NCC will accomplish this task for network wide assets. ADPE Custodian and WIAO personnel will ensure the BMAN accreditation control number is associated with each IPMS BMAN equipment record.

**2.5. Software Security.** Users are to follow guidelines for software security as dictated in AFI 33-112, Automated Data Processing Equipment. Additionally, access to programs and utilities that perform maintenance of the network and security-related software will be restricted to use by authorized network management personnel.

**2.5.1. Network Software approval.** Network SAs will test all operating systems and application software considered for installation on BMAN equipment. When necessary they will conduct testing to ensure the new software does not circumvent existing BMAN security features. The Certification Official must certify and approve the software prior to installation on the network.

**2.5.2. Security Software.** Use security software products evaluated by the Air Force Information Warfare Center (AFIWC) Product Assessment and Certification Center to implement security safeguards, unless specifically waived. The Air Force Assessed Product List (APL) lists the available products. The WIAO, 437 CS/SCBS (ext. 3-2983) has a copy.

**2.5.3. Intrusive Software.** Do not install intrusive software on any BMAN file server or workstation without prior approval from the BMAN DAA. Intrusive software includes software that is specifically designed as packet analyzers with the purpose of capturing system passwords. Examples of intrusive software programs include, but are not limited to, Microsoft Network Monitor, RAPPER, SPY, CRACK, SATAN, and SNIFFER.

**2.5.4. Unauthorized Software.** Only government-approved software is authorized on the BMAN. All other software, including game and pornographic software, is unauthorized and will not be installed on either the BMAN file servers or workstations. Shareware and Freeware are only authorized when purchased or specifically approved by the DAA.

**2.5.5. Virus Scanning.** The NCC will run a continuous virus scanning program to check for known viruses on each system file server and on all files sent to its file servers via outside network connections. FSAs and WGMs are responsible for virus scanning on file servers and workstations under their control. Daily, BMAN users will run a virus detection program on workstation local drives, random access memory locations, and removal media diskettes prior to use on any work-

station. This includes workstations remotely connected to the BMAN via modem. The NCC provides a virus scanning program to support this function. Contact the WIAO for further guidance.

**2.6. Remanence Security.** Remanence security is the control of residual information that remains on magnetic computer storage media after erasure by standard program utilities such as the DOS delete operation.

**2.6.1. Remanence Security Philosophy.** All users will protect sensitive data from unauthorized recovery of previously deleted data. This is accomplished by using the remanence security process of clearing or purging. Processes that only remove pointers and leave data intact are not acceptable methods of either clearing or purging storage devices.

**2.6.2. Purging.** Purging is associated with classified data and is required when classified data is inadvertently entered into the BMAN. Users, WGMs, and FSAs will clear magnetic storage media under their control that contains sensitive information before reutilization or release from AMC control. Information owners will review files for record management disposition requirements prior to clearing the files from the magnetic storage media.

**2.7. Reporting Vulnerabilities or Incidents.** Suspicious activities include: browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to system hardware, firmware, or software characteristics without the owner's knowledge. BMAN users will immediately report vulnerabilities, security incidents, or unauthorized entry of the computer system to their FSA or WGM. The FSA or WGM will contact the NCC Help Desk (ext. 3-3511).

**2.7.1. Incident Reporting.** The WGM or FSA will perform an initial evaluation of each security problem or incident, document the circumstances, begin corrective or protective measures, and accomplish follow-on reporting as required. The WIAO, UCM, FSA or SAs are responsible for additional reporting requirements. Formal reporting of security incidents is accomplished IAW AFSSI 5021, Vulnerability and Incident Reporting. Functional OPRs may also require notification of a specific security incident. For example, notify the Command Privacy Act Officer (HQ AMC/SCMNA(R)) when Privacy Act incidents occur.

**2.7.2. In-Progress Attacks.** In the case of an in-progress intrusion or suspicious activity, the WGM or FSA will immediately contact the NCC Help Desk (ext. 3-3511). They will in turn immediately contact the WIAO (ext. 3-2983) or the Air Force Computer Emergency Response Team (AFCERT) at DSN 969-3157, toll free 1-800-854-0187, or commercial (210) 977-3157.

**3. System Security Policy.** The security policies stated in this instruction are to balance the Air Force computer security objectives of confidentiality, availability, and integrity while satisfying mission requirements.

**3.1. Security Requirements.** Commanders, functional managers, and supervisors are responsible for ensuring personnel under their control are knowledgeable on security requirements described in this instruction. It is the responsibility of each user to use all resources available, to include technical and administrative resources, to enforce this policy at their level.

**3.2. Assurance.** Assurance is the measure of confidence the security features and architecture of the BMAN accurately mediate and enforce security directives. Assurance is established by certification and accreditation of the BMAN and is maintained through compliance with this instruction and all applicable directives.

**3.3. Accountability.** The BMAN operating system software will maintain an automated audit trail to report security-related activities. The audit trail will be of sufficient detail to reconstruct events to determine the cause or magnitude of compromise should a security violation or malfunction occur. Each person with access to the BMAN will be held accountable for his or her actions. Because the BMAN is primarily an administrative system, only a subset of all available audit events will be activated for full time auditing. The system will abort/suspend and record unauthorized user activity through the use of Intruder Detection/Lockout security features.

**3.3.1. Auditing.** Audit events are selected to ensure the confidentiality, integrity, and availability of data placed on the BMAN. These events are primarily directed at the assignment and modification of a user's security rights and security attributes. All users will be audited to some degree, to include events such as logging in and logging out.

**3.3.2. Audit Events.** The following comprise audit events:

Use of account login and logout.

Actions to create, modify, copy, execute, or delete programs, directories, or files.

Actions taken by network administrators, Unit COMPUSEC Managers, and Functional System Administrators. Examples include adding a user, changing user rights, or performing file server restarts.

Any event that attempts to change the security profile of the system. Examples include changing access controls (rights or attributes) to files, directories, and user discretionary access, or changing a user password.

Any event that attempts to violate the security of the system. Examples include too many attempts to login or attempts to violate the access control limits of a device.

Passwords, or character strings incorrectly given as passwords that might possibly expose the password, shall not be recorded in the audit trail.

**3.3.3. Specific Audit Information.** The audit trail will record the following minimum information for each audit event:

Date and time of the event.

Unique identifier of the user or device generating the event.

Type of event.

Success or failure of the event.

Origin (terminal ID) of the request for identification and authentication events.

Name of the program or file introduced, addressed, or deleted.

Description of actions taken by the network administrators, Functional System Administrators and Unit COMPUSEC Managers.

**3.3.4. Audit Review.** The UCM will review audit data. The UCM will retain the audit trail data for a minimum period of six months. Discrepancies noted during the review shall be acted upon immediately. Retain audit records that cover periods involving a security incident in accordance with appropriate disposition record requirements.

**3.3.5. Protection of Audit Files.** Only the UCM is authorized to enable auditing, disable auditing, or configure the audit mechanism. Access to audit information shall be limited to those authorized by the UCM. Protect audit data files and products as sensitive information.

**3.3.6. Requesting an Audit.** Unit commanders or equivalent may submit requests for special audits in writing to the CSM. Written requests will be forwarded to the 437th AW Judge Advocate for review and approval. An example of a reason for requesting a special audit would be to support the investigation of suspected fraud, waste, or abuse of system resources. The only exemption to this written requirement is given to personnel who are authorized to immediately begin the auditing of suspected BMAN intrusion activity, such as AFOSI or Security Forces.

### 3.4. Access Control

**3.4.1. Discretionary Access Control (DAC).** Discretionary Access Control is the capability to restrict system user access to specific directories and files. This implements the principle that a user should be given only those privileges or access that enables the individual to do his or her job. DAC guards against "need-to-know" violations. Network SAs and FSAs will implement DAC by using the "rights and attributes" features of the operating system.

**3.4.2. Method of Access Control.** A combination of physical security, personnel security, and system security mechanisms is used to control access to the BMAN. Users must be properly identified and authenticated before accessing the system. The method of access control is a combination of a personal user login ID (identification) and a unique password (authentication).

**3.4.3. Identification.** The BMAN must accurately, consistently, and positively identify each user, and maintain that positive identification throughout the user's login session. Only network SAs have the authority to issue user login IDs.

**3.4.4. Closing User ID Accounts.** Delete user ID accounts and passwords within one workday of the user's departure from the organization, or when a user no longer requires access to perform official duties. This will allow personnel access to information in their accounts they need to take with them. All users must out-process through the ADPE section at which time they will leave a copy of their orders with the network SAs.

**3.4.5. Group IDs.** The use of group login IDs does not meet the security requirement for positive identification to the granularity of a single system user. Therefore, group login IDs are not authorized.

**3.4.6. User Authorization Revalidation.** The FSA will revalidate BMAN user authorization (user IDs) under their control annually to ensure individuals who no longer require access to the BMAN are deleted from the database of authorized users.

### 3.5. Authentication.

**3.5.1. Password Protection.** The use of a password is required to authenticate all BMAN user login attempts. Passwords are sensitive information and it is each user's responsibility to protect their password. This protects the user from having other people assume the user's identity on the system. Do not use current BMAN account passwords, to include dial-up modem account passwords, as a password to access unofficial or commercial systems or networks (i.e., America Online, CompuServe, or bulletin board systems). DO NOT WRITE YOUR PASSWORD DOWN. If it becomes necessary to write down a password, store the password in a manner that greatly reduces the risk of exposure. Do not disclose passwords or share with other personnel. If a pass-

word is disclosed to an unauthorized person, report the disclosure to the SAs, FSAs or UCMs and then change the password immediately.

**3.5.2. Password Length.** Passwords must be at least eight characters in length and must contain at least one of each of the following: upper-case letter, lower-case letter, special character, and numeric character.

**3.5.3. Password Generation.** The network SA will generate the initial password for a new user. Users will generate their own passwords after initial password assignment. CAFBI 33-501 covers the generation of passwords.

**3.5.4. Changing Passwords.** As a minimum, users are responsible to change their password every 90 days or when compromised. Using an expired password is not authorized. Users have a grace period of two logins following the expiration of their password. During this period, users are prompted to establish a new password. A user will be locked out after three unsuccessful password authentication attempts. All users, including personnel who are TDY, will contact their WGM when they are locked out from their account. WGMs must verify that the request is from an authorized BMAN account user.

**3.5.5. Dial-in/Remote Access Server (RAS) Accounts.** The dial-in modem accounts are additional capabilities to the user's BMAN account and requires the Network SA to grant user permissions. Use AF Form 3215, C4 Systems Requirements Document, to request a RAS account.

**3.5.6. Other Modem Connections.** Other modem connections to the BMAN are prohibited. Some legacy systems under extreme circumstances may require modem connections while connected to the BMAN until they are completely upgraded to new technology. These connections must be evaluated for security purposes and be approved by the BMAN DAA.

**3.5.6.1. Requests for Modem Connections.** The flight chief, branch chief, or higher level authority must submit requests for dial-out or dial-in modem connections on a AF Form 3215, C4 Systems Requirements Document, to the 437th Communications Squadron for approval. 437 CS/SCBN will implement and provide guidance on the appropriate procedures to follow. Dial-in remote connections must comply with all BMAN user identification and authentication requirements. Do not publicize modem telephone numbers to anyone other than those with a need-to-know. Protect these numbers as FOUO. Call forwarding is prohibited when callback or dial-back technology is used. The FSA will revalidate dial-in remote requirements annually.

**3.6. Network Connections.** Any connection to outside networks (i.e. NIPRNET and the Internet for TCP/IP networks) potentially introduces additional risks to the security of the BMAN. In order to provide the highest degree of protection to the BMAN, external connections to the network will only be accomplished within the immediate control of the NCC. This will ensure that all external connections are appropriately controlled and monitored for intrusion. Organizations that do not comply with this policy may be disconnected from the base infrastructure.

**3.6.1. New Network Connections.** The Certifying Official must confirm, prior to connecting a new network to the BMAN, that the new equipment satisfies the security requirements established by this Instruction. The confirmation process includes obtaining BMAN DAA approval to connect to the network. The DAA of the network requesting connection to the BMAN must submit an AF Form 3215 with an attached Memorandum of Agreement (MOA) which provides the following: data description and classification, name of the DAA who will resolve conflicts, intended recipi-

ents of transmitted data, accreditation status of the new equipment, and security mechanisms to be implemented prior to connection to the BMAN.

**3.6.2. Internet Protocol (IP) Addresses.** The 437th Communications Squadron will control and issue all IP addresses for the BMAN. Users are not allowed to assign an IP address to any computer system without the coordination and approval of 437 CS/SCBN. Unauthorized or duplicate IP addresses may compromise the security of the BMAN. Violators of this policy are subject to administrative, non-judicial, or judicial punishment. IP addresses in the range 1-20 on each subnet are reserved for NCC use (i.e., 137.4.XXX.1-20).

**3.6.3. Access by External Customers.** Outside agencies may require access to Charleston AFB resources in order to conduct their mission. Send all requests for access to the BMAN by external customers to 437 CS/SCBN (ext. 3-3491). The following information is required:

Local Information: System Administrator's name, organization, bldg. number, phone number, host name (machine name), and IP address of the host.

Distant-end Information: Customer name, organization, location, phone number, host or PC name, IP address, type of service required (TCP/UDP), and socket/port number and service (Telnet, FTP, printing, etc.)

**3.6.4. Internet Policy.** BMAN users are permitted access to the Internet in performance of official duties. Using the Internet for non-official purposes is unauthorized and may result in administrative, non-judicial, or judicial punishment. Commanders and supervisors are responsible for ensuring that assigned personnel use government equipment and services for official or authorized purposes only. Follow provisions outlined in AFI 33-129, Transmission of Information via the Internet. Many military sites are restricted to the ".mil" or ".gov" domain require Domain Name Service (DNS) entries for access. Send requests for DNS entries to 437 CS/SCBN with the following information: name, organization, building number, phone number, host name, and IP address.

### **3.7. World Wide Web (WWW) Server**

**3.7.1. WWW Internet Server:** The Charleston AFB WWW Internet Server is managed by the 437 AW/PA (Public Affairs) with guidance from the NCC. All requests to operate a Web page on the WWW server(s) must be coordinated with and approved by the Communications Squadron via an AF Form 3215. NCC personnel ensure that WWW servers obtain DAA approval before being connected to the BMAN. Refer to AFI 33-129 for further information. Accounts and hard disk space (within reason) for WWW directories can be provided to each functional area. All information must be cleared before being placed on the Web server in a manner consistent with procedures already in place for clearing hard copy information. The Web page maintainer must coordinate the release of information with the Public Affairs office. The following types of information can't be placed on a system with uncontrolled Internet access:

Unencrypted classified information.

FOUO information, including, but not limited to: Privacy Act; unclassified requiring special handling (Encrypt for Transmission Only, Limited Distribution, Scientific and Technical Information, etc.).

Scientific or Research and Development Information covered by AFI 61-204, distribution statements B through F.

Freedom of Information Act (FOIA)-exempt information not cleared for public release (AFI 37-131, para. 10).

**3.7.2. Restricted WWW Internet Server.** The Charleston Restricted Internet Server will be managed by the NCC with guidance for the 437AW/PA and will be restricted to ".mil" domains. This server allows the sharing of base specific information with other military bases and is not intended for public access. Access by domains other than ".mil" must be approved by the DAA. All provisions and restrictions of para **3.7.1.** apply.

**3.7.3. Intranet Web Server.** The Intranet Web Server is managed and controlled by the NCC. All changes and additions must go through the NCC Chief to the Network SAs. Information on the Intranet Web Server is for use by users of the BMAN and is not accessible from the internet.

**3.8. Converting a Workstation into a Web Server.** Some programs (i.e., Super TCP/IP and Windows 95) delivered as part of a standard workstation software package have the ability to convert a workstation into a Web Server. Workstations configured as Web Servers may create additional vulnerabilities to a user's personal data and the BMAN. Do not convert BMAN workstations into Web Servers. Web Servers must meet HQ AMC/IM Internet requirements prescribed in AMCI 37-106, Internet Information Management, and be approved by the BMAN DAA.

**3.9. Configuration Management and Documentation.** Ensures the integrity and security of critical functions. The NCC Chief maintains all documentation and at least two configuration management files: one for the infrastructure, and the other for authorized traffic that rides the infrastructure.

**3.9.1. Infrastructure File.** The infrastructure file shall contain the following information:

**Points of Contact:** Personnel who provide support for hardware, software, and recovery support (vendors, long-haul network support).

**Internal User Identification:** A list of internal users, their office symbol and phone number, and IP address.

**Hardware configuration:** A schematic of the current location of hardware.

**Software configuration:** A listing of software used on each infrastructure component, identified by vendor, application type, version/release number.

**Agreements and Warrantees:** Maintenance agreements and warranty documents for hardware and software.

**3.9.2. File of Authorized Traffic.** The Binder of Authorized Traffic (BAT) is the technical implementation of the base network security policy for the network. This is a dynamic repository of information to document mission critical and authorized traffic. The BAT will contain the following information:

**Community Information:** Listed by organization, their DAA, points of contact, and telephone number.

**Network:** Subnet address, subnet mask, building number.

**Types of services required:** TELNET, FTP, SMTP, etc.

**Network protocol type:** TCP/IP, UDP, etc.

**Security requirements:** Implemented security mechanisms, and desired security mechanisms.

**Mission criticality:** Required network protocols will be listed with the criticality of the connectivity.

**3.9.3. Major Additions/Modifications to Network Hardware.** The CSM will assess all additions and modifications to major hardware and software components before installation on

the BMAN. The CSM will coordinate changes with the network management personnel, and the FSA. After the assessment is complete, the Certification Official will either certify or not certify the recommended addition or modification when submitting the package to the DAA for approval. This requirement does not apply to the connection of user terminals or peripheral devices.

**3.9.4. Review of BMAN CSRDs for Security Impacts.** The CSM will review the technical solution for each major BMAN Communications-Computer Systems Requirement (CSRD) submission for possible impact on the BMAN security capabilities. The review is required prior to submission of the CSRD for final approval.

**3.9.5. Hardware and Software Configuration Control.** The NCC Chief ensures network hardware and software configuration control is in place and maintained. At a minimum, the network SAs maintain a current inventory of all software loaded on BMAN equipment and its approved implementation configuration.

**3.9.6. Windows NT and Windows for Workgroups Configuration Requirement.** Each BMAN account user who also uses either the Windows NT, Windows 95, or Windows for Workgroups (WFW) programs will properly configure their installed program to prevent unauthorized access to their files by other Windows NT, Windows 95, or WFW users. Guidance can be received from the NCC via the WGMs and FSAs.

**3.10. Charleston AFB Network Architecture.** The Single Master Domain model is the preferred architecture. This model limits trust relationships which greatly simplifies operations and positions the system to capitalize on future Windows NT directory capabilities. The Single Master Domain model provides centralized account and resource management. The master domain contains all user account data and groups. Base entities will create resource domains to contain the various resources of the entities. In this model, there is only a need for a one-way trust from the resource domain to the master domain.

**3.10.1. Secure Architecture Migration.** The basic plan is to stick with low risk, low maintenance intensive bulk point to point encryption (KIV 7s). Network SAs will incorporate both classified and unclassified networks into one backbone. The goal of this architecture is to provide a common set of NCC and base infrastructure equipment configurations to service all users while providing the framework for downward directed program support.

**3.11. Catastrophic Event Recovery Plan (CERP).** The CSSO, network managers, and users must develop a CERP to ensure the survival and timely recovery of their computer systems. These plans should describe the actions necessary to ensure continuity of operations in the event of a disaster, cyber attack, or to restore operation during a system failure. Managers must prioritize critical systems according to mission requirements in the plan. See AFSSM 5018, *Risk Analysis Guide*, or AFSSM 5022, *Network Risk Analysis Guide*, for guidance. These contingency plans should be reviewed at least annually and updated as necessary. They should also be tested to ensure they're adequate and the results should be documented.

### 3.12. Sensitive Unclassified Information

**3.12.1. User Responsibility:** It is the responsibility of each user to properly protect and safeguard all sensitive information under their control. Privacy Act records will not be sent to anyone outside of the DoD except when required under the FOIA, authorized by a Privacy Act exemption, or a "published" routine use. See AFI 37-132, Air Force Privacy Act Program, for guidance. For those occasions when more guidance is needed to determine whether specific information is sensitive or not, contact the WIAO, 437 CS/SCBS, (ext. 3-2903).

**3.12.2. Categories of Sensitive Information.** Sensitive information is the highest data sensitivity level authorized for processing on the BMAN. As defined by AF Manual 33-270, Command, Control, Communications, and Computer (C4) Systems Security Glossary, sensitive information is information that "the loss, misuse, unauthorized access to, or modification of could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S. Code, Section 552a (the Privacy Act), but has not been specifically authorized under the criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

**3.12.2.1. Privacy Act Data:** Examples of Privacy Act Data are medical records, individual financial information, recall rosters, manpower and personnel records, training records, marital status, number and sex of dependents, gross salary of military personnel, civilian educational degrees and major areas of study, school and year of graduation, home of record, home address, home phone number, age and date of birth, present or future assignments for overseas or for routinely deployable or sensitive units, and office and unit address and duty phone for overseas or for routinely deployable or sensitive units.

**3.12.2.2. Privileged Data:** Examples of Privileged Data are chaplain records, staff judge advocate records, safety records, and internal organizational management records (such as quality assurance data or credential's committee records).

**3.12.2.3. Proprietary Data:** Examples of Proprietary Data are copyright material and patented material and information.

**3.12.2.4. Other Types of Sensitive Information:** Other types of sensitive information are logistics records, procurement data, financial data, source selection sensitive data, investigative data, automated decision-making aids, maintenance records, audit records, essential elements of friendly information, FOUO data, critical technology data, scientific and technical data (which has national security related implications), unit mobility or deployment information, and war reserve materiel data.

**3.12.2.5. Aggregated Data:** Information that would individually be unclassified may require protection as sensitive information when combined or associated with other unclassified information. Users of the BMAN are cautioned and required to take appropriate steps to minimize the potential for aggregated information. The FSA will determine when aggregated data exists in or is being processed by the BMAN. The potential for creating classified information from aggregated data stored within the network is low. In no case will aggregated data in excess of sensitive information be authorized on the BMAN.

**3.12.3. Storing.** The preferred method of storing sensitive information is to use removable storage media, such as floppy diskettes. Users may store sensitive information on a network file server personal drive, such as a "U" drive. Users may also store sensitive information on a network file

server logical drive specifically assigned only to those users requiring access to the information as part of their official duties.

**3.12.4. Transmitting over e-mail.** When transmitting sensitive data over e-mail, the sender must ensure the receiver is authorized to receive the data. The e-mail message must conspicuously state that sensitive data is being transmitted.

**3.12.5. Disposition:** Dispose of computer products that contain sensitive information in accordance with AFI 37-138, "Records Disposition--Procedures and Responsibilities".

### **3.13. Classified Information. *DO NOT USE the BMAN to process classified information.***

**3.13.1. Computers Used to Process Classified Information.** Computers used to process classified information are prohibited from being connected to the BMAN or any other unclassified computer systems. A computer must be physically disconnected from the network prior to processing classified information. Contact the WIAO, 437 CS/SCBS, (ext. 3-2903) for specific security measures for processing classified information.

**3.13.2. Inadvertent Entry of Classified Information.** Classified information accidentally introduced into the BMAN requires immediate reporting to the NCC Help Desk, (ext.3-3511) and will require intervention by a network administrator.

### **3.14. Marking/Labeling**

**3.14.1. Labeling Removable Storage Media.** Apply labels to all removable storage media (floppy diskettes, tapes, and hard drives). The labels will indicate the storage media's owner, use, and description of contents. Use the Standard Form 711, Data Descriptor, or a commercial equivalent label, for this purpose. Additionally, removable magnetic storage media containing sensitive information must indicate that fact on the label. Personnel may use Air Force Visual Aid 205-15, Privacy Act Label, to indicate the storage media contains personal data.

**3.14.2. Marking/Labeling Sensitive Unclassified Information.** Mark/Label sensitive information output products (such as FOUO, Privacy Act Information, or Source Selection Sensitive Information) IAW the appropriate prescribing directives.

### **3.15. Maintenance**

**3.15.1. Hardware Maintenance.** Individual users will NOT perform hardware maintenance or modifications. Hardware maintenance in some cases will be performed by WGMs or FSAs, if work required is beyond their experience the system will be repaired by a qualified vendor. Although, users must ensure they do not give vendor maintenance personnel unrestricted access to sensitive information storage media or products during the repair or testing of system components.

#### **3.15.2. Software Maintenance**

**3.15.2.1. Backup Copies/Archiving Software and Files.** Network SAs will make backup copies of all original network software installed as "standard" on all system file servers. FSAs will make backup copies of all original software installed as a "unique" requirement on the file servers they maintain. Store backup copies separately from master copies whenever possible. Any duplication of commercially licensed software, except for backup purposes, is a violation of Federal copyright laws. At a minimum, network SAs will make a daily incremental tape backup and weekly full backup of the files on each BMAN file server. Users should periodi-

cally backup their personal files, especially files located on the workstation hard drive (i.e., C: drive). The BMAN file server backup process does not back up workstation files.

**3.15.3. System Maintenance.** User workstations and BMAN file servers do not require clearing of sensitive information when 437th Communications Squadron NCC personnel perform equipment maintenance. If 437 CS maintenance personnel cannot repair the equipment, they will notify the equipment user that vendor maintenance is required. The user will review the hard drive files to determine if sensitive information has been inadvertently stored on the hard drive before sending a workstation to vendor maintenance. If sensitive information is found, either remove the hard drive or use clearing procedures on those files containing sensitive information. In order to prevent the inadvertent release of sensitive information on file servers, network or functional SAs will remove the hard drive or clear all data files from the drive before sending a file server to vendor maintenance (Reference paragraph **3.12.5.**).

**3.15.3.1. Maintenance Fix Actions.** The NCC maintenance section will repair, or contract for repair, the network infrastructure components (i.e. hubs, routers) and common-user file servers that fail because of normal wear and tear. The NCC maintenance section should provide end-user organizations with an outage job number for tracking purposes only. This job number will be assigned through the initial trouble call to the Help Desk. The NCC maintenance section will maintain an outage log on components being repaired. Outages that affect single devices should be considered routine. Response to outages affecting an entire building or major directorates should be according to the priority identified on the matrix below:

CLASSIFICATION	DUTY HOURS	OFF DUTY HOURS
P1 (Critical)	1 Hour	On-call technicians
P2 (Priority)	4 Hours	1st thing next duty day
P3 (Routine)	24 Hours	Next duty day

**3.15.3.2. Maintenance Contracts.** The NCC maintenance section must be provided copies of any commercial maintenance contracts that affect network components. Normally, commercial maintenance contracts are maintained by the equipment control officer (ECO) in the NCC. When the need arises for outside support, proper coordination with the vendors will take place through the NCC help desk (ext. 3-3511) and NCC maintenance section.

**3.15.3.3. Hard Drives and Floppy Diskettes.** Clear magnetic storage media (hard disks and floppy diskettes) whenever the media is reallocated to another work center or is no longer needed in the performance of official duties. Clearing is not required when an employee leaves an office and the workstation remains under the control of the functional organization.

**3.15.3.4. File Server Directories.** Administrators will clear file server directories and associated files assigned to individual users when the user departs the organization, or when the user no longer requires access to the file server to perform official duties.

**3.16. Training**

**3.16.1. NCC-Provided.** The NCC will provide training for the standard suite of base applications and systems. The NCC will ensure that operators, workgroup managers, and functional systems

administrators each receive a level of instruction commensurate with their duties and responsibilities.

**3.16.2. Customer Core Systems Training.** The NCC will provide education and training to base computer users. In addition, the NCC will draft and forward a customer education letter or handbook, conduct a customer training survey, advertise training availability, prepare training outlines and course material, and train instructors. The NCC is responsible for preparing class schedules, scheduling customers for training, configuring computers for specific courses, conducting customer training classes and evaluations to see if training meets the customers' needs, and developing and maintaining a base reference library for hardware and software applications. The NCC will train FSAs and WGMs on the interim information protection operation (IPO) tools (Anti-Virus, Crack, MD5, and Security Profile Inspector for UNIX, Security Profile Inspector for VMS, TCP Wrappers, Tripwire, and Wuarchive ftpd). Security training is done on both classified and unclassified systems. Initial training will be conducted during newcomer in-processing. It will be followed by completion of AF Communications Agency's (AFCA) Information Assurance (IA) computer based training (CBT). Using this training will meet the SATE and COMPUSEC requirements for all classified and unclassified systems.

**3.16.3. Initial and Follow-On User Security Training.** All new users will receive initial training on the BMAN security features prior to being authorized access. The UCM, CSSO, if assigned, or FSA will provide the training prior to establishing a new account. At a minimum, it will cover the requirements addressed in this security instruction. Follow-on security training will be conducted annually by the CSSO or FSA. CSSOs or FSAs will document each user's name and date trained.

**3.16.4. Specialized Security Training.** All network SAs, FSAs, WGMs, and CSSOs will receive initial training that covers, as a minimum, the requirements addressed in this security instruction. The availability of specialized training is constantly changing. Therefore, individuals should check with the CSM for appropriate courses that cover additional specialized security training. The CSM will document all specialized training by name, assigned position, training subject, and date received.

**3.17. Accreditation.** Accreditation provides users with an assurance the system possesses adequate computer security. The objective of computer security is to protect information and resources so the organization can effectively accomplish its goals.

**3.17.1. Accreditation and Documentation Policy.** Protect certification and accreditation information from disclosure to unauthorized persons. Disclosure could cause the information to be exploited and may impact the function of the system or allow security features to be bypassed. Certification and accreditation information must be marked, handled, and controlled consistent with the sensitivity of the information it contains.

**3.17.2. Accreditation Control Number.** The WIAO assigns Accreditation Control Numbers (ACN) to systems during the certification and accreditation process. The ECO links that single ACN to all equipment components that comprise the system and is responsible for inputting this information into the Information Processing Management System (IPMS). The WIAO provides C&A information to the Base ECO for entry into IPMS.

**3.17.3. Re-accreditation Policy.** Evaluate changes to system architecture on a continuing basis to maintain system accreditation and ensure system modifications do not create new vulnerabili-

ties to existing threats that would create more risk. The UCM will reinstate the accreditation process whenever system modification warrants re-accreditation or when three years have past since the last accreditation.

**3.18. Information Operations Conditions (INFOCON):** INFOCON levels identify criteria for posturing forces to combat attacks against our information infrastructure. They address protection of AF assets against electronic offensive actions and defensive countermeasures, jamming, and denial of service. The goals of increased INFOCON levels are to provide enough security and protection for the systems and services to be useful and to provide sufficient restoral and backup capability to continue to operate in the event of an attack.

**3.18.1. INFOCON Levels.** Downward-directed at all levels of command, but can be set at the base level if the situation requires a change in condition. Each level establishes specific alert states and defines graduated response NCCs must take. INFOCON levels may be adjusted for 2 reasons: (1) to improve AF capability to detect and counter adverse network activity, (2) to reflect change priorities in information services needed to generate forces. When an INFOCON level is established, the NCC will take appropriate actions as defined in NCC INFOCON checklists. FSAs/WGMs will be notified of the implementation of increased INFOCON levels. If the required actions adversely impact a Group's mission, the FSAs will highlight that fact and the NCC Chief will research possible work-arounds and/or waiver requests.

**3.19. Documentation.** Other documents that relate specifically to the BMAN are:

**3.19.1. Security Awareness Tri-fold.** The Charleston Security Awareness Tri-fold is written for all users of the BMAN. The Guide uses terminology a user, unfamiliar with the BMAN operating system, would find easy to understand.

**3.19.2. Base Network and Computer Rules of the Road.** The Base Network and Computer Rules of the Road is written for all users of the BMAN. Included in this publication is guidance on the proper use of government computers, e-mail, internet access, and computer security. Any user who requires a copy of this document should contact their WGM.

**3.20. Conflicting Guidance.** The provisions of this security instruction do not replace requirements contained in Air Force and Department of Defense level documents. If there is a conflict, the higher level document takes precedence. Report the conflict to your UCM, CSSO, if assigned, or your FSA/WGM for resolution.

DENNIS M. KAAAN, Colonel, USAF  
Commander, 437th Support Group

**Attachment 1****GLOSSARY OF REFERENCES, AND SUPPORTING INFORMATION*****References*****Federal Standards**

FIPS PUB 102 Guideline for Computer Security Certification and  
Accreditation

OMB Circular 130, 12 Dec 85 Management of Federal Information Resources

**National Computer Security Center Standards and Guides**

NCSC-TG-001, 1 Jul 88 A Guide to Understanding Audit in Trusted Systems

NCSC-TG-016, Version 1, Oct 92 Guidelines for Writing Trusted Facility Manuals

NCSC-TG-026, Version 1, Sep 91 A Guide to Writing the Security Features User's  
Guide for Trusted Systems

NCSC-TG-029, Version 1, Jan 94 Introduction to Certification and Accreditation

NCSC-TG-031, Version 1, Feb 94 Certification and Accreditation Process Handbook (draft)

**Department of Defense Standards**

DoDD 5200.28, Mar 88 Security Requirements for Automated Information  
Systems (AIS)

DoD 5200.28 STD, Dec 85 Department of Defense Trusted Computer System  
Evaluation Criteria

**Air Force Directives**

AFI 33-103, 1 Jul 96 Requirements Development and Procedures

AFI 33-112, 6 May 94 Automated Data Processing Equipment (ADPE)  
Management

AFI 33-115, 1 Apr 96 Networks Management

AFI 33-129, 1 Jan 97 Transmission of Information via the Internet

AFI 33-202 Vol I, 19 Aug 98 Communications and Information—  
Information Assurance

AFI 37-131, 16 Feb 95 Freedom of Information Act Program

AFI 37-132, 11 Mar 94 Air Force Privacy Act Program

AFI 37-138, 31 Mar 94 Records Disposition - Procedures and  
Responsibilities

AFI 33-219, 12 Jun 95 Telecommunications Monitoring and Assessment

Program (TMAP)

### **Air Force System Security Directives**

AFSSM 5003, 29 Jan 93	Designated Approving Authority Guide
AFSSM 5006, 2 Aug 93	Computer System Security Officer's (CSSO)/ Network Security Officer's (NSO) Guide
AFSSM 5013, 1 Jul 96	Identification and Authentication
AFSSI 5020, 20 Aug 96	Remanence Security
AFSSI 5021, 15 Aug 96	Vulnerability and Incident Reporting
AFSSM 5023, 1 Aug 96	Viruses and Other Forms of Malicious Logic
AFSSI 5024 Vol. I, 1 Apr 97	Certification and Accreditation (C&A)
AFSSI 5024 Vol. II, 1 Apr 97	The Certifying Official's Handbook
AFSSM 5102, 23 Sep 96	The Computer Security (COMPUSEC) Program

### **Air Mobility Command Directives**

AMCI 33-202, Vol. I, 23 Dec 94	Computer Security (COMPUSEC) Automated Information System Certification and Accreditation Policy
AMCI 33-202, Vol. II	
AMCI 37-106, 1 Jun 96	Internet Information Management

### **Charleston Air Force Base Instructions**

CAFBI 33-501, 2 Jan 2000	Computer Security (COMPUSEC) Management
--------------------------	---

### **Terms**

**Access.**—1. (COMSEC) Capability and opportunity to gain knowledge or alter information or material. 2. (AIS) Ability and means to communicate with (input to or receive output from), or otherwise make use of any information, resource, or component in an Automated Information System (AIS). NOTE: An individual does not have “access” if the proper authority or a physical, technical, or procedural measure prevents them from obtaining knowledge or having an opportunity to alter information, material, resources, or components.

**Access Control.**—Process of limiting access to the resources of an AIS only to authorized users, programs, processes, or other systems.

**Accreditation.**—Formal declaration by a DAA that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards. See “Approval to Operate” and “Interim Approval to Operate.”

**Application Software.**—Mission support or mission-specific software programs designed by, or for, system users and customers. By using available computer system equipment and operating system software, application software completes specific, mission-oriented tasks, jobs, or functions. It can be either general-purpose packages, such as demand deposit accounting, payroll, machine tool control, or specific application programs tailored to complete a single or limited number of user functions.

**Assurance.**—Measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

**Audit.**—Independent review and examination of records and activities to assess the adequacy of system controls to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

**Authentication.**—Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

**Automated Information System (AIS).**—Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes software, firmware, and hardware. NOTE: Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment. See "Network."

**Availability.** —The property of being accessible and usable upon demand by an authorized entity.

**Base Metropolitan Area Network (BMAN).**—A computer network that services a large area. BMANs typically span large areas (states, countries, and continents) and are owned by multiple organizations. See "Local Area Network" and "Network."

**Certification.**—Comprehensive evaluation of the technical and non-technical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

**Certification and Accreditation (C&A) Program.**—Program designed to ensure critical decisions regarding the adequacy of AIS security safeguards are made by authorized managers using reliable technical information.

**Classified Information.** —National security information that has been classified pursuant to Executive Order 12356.

**Component.** —Hardware device, with its required firmware or software, that performs a specific AIS function. Components include modems, printers, communications controllers, tape drives, message switches, computers, gateways, peripheral controllers, etc.

**Computer.** —See "Automated Information System."

**Computer Network.** —See "Network."

**Computer Security (COMPUSEC).**—Measures and controls that ensure confidentiality, integrity, and availability of the information processed and sorted by a computer. See "Information Systems Security (INFOSEC)" and "Network Security."

**Computer System.** —See "Automated Information System (AIS)."

**Computer Systems Manager (CSM).** —The individual responsible for the overall operation of a network.

**Computer Systems Security Officer (CSSO).**—Individual responsible for security-related issues for terminals at a remote terminal area. The CSSO receives guidance from the Unit COMPUSEC Manager (UCM) and provides status and other reports to the UCM.

**Configuration Control.**—Process of controlling modifications to a telecommunications or AIS's

hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation. See “Configuration Management.”

**Configuration Management.**—Management of features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation of an AIS, throughout the development and operational life of a system.

**Data.**—Representation of facts, concepts, or instructions in a manner suitable for communication and interpretation. Data provides the building blocks for information processing. See “Information.”

**Denial of Service.**—Result of any action or series of actions that prevent any part of a telecommunications or AIS from functioning.

**Designated Approving Authority (DAA).**—Official with the authority to formally assume responsibility for operating an AIS or network at an acceptable level of risk.

**Discretionary Access Control (DAC).**—Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. NOTE: Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) on to any other subject. See “Mandatory Access Control.”

**Domain.**—Unique context (access control parameters) in which a program is operating; in effect, the set of objects that a subject has the ability to access. See “Object” and “Subject.”

**EMSEC.**—Short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

**File Security.**—Means by which access to computer files is limited to authorized users only.

**Hardware.**—Electric, electronic, and mechanical devices that make up a computer system.

**Identification.**—Process that enables recognition of an entity by an AIS. NOTE: This is generally accomplished by the use of unique machine-readable user names.

**Information.**—Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in media. See “Data.”

**Integrity.**—Computer security characteristic ensuring computer resources operate correctly and data in the system is accurate. This characteristic is applicable to hardware, software, firmware, and the databases used by the computer system. See also “Integrity” and “System Integrity.”

**Internet.**—An informal collection of government, military, commercial, and educational computer networks using the transmission control protocol/internet protocol (TCP/IP) to transmit information. The global collection of interconnected local, mid-level and wide-area networks that use IP as the network layer protocol.

**Local Area Network (LAN).**—A computer network that services a small area. LANs typically have a diameter of not more than a few miles and are owned by a single organization. See “Network” and “Metropolitan Area Network.”

**Logoff/Log Off.**—Procedure used to terminate connections.

**Logon/Log On or Login/Log in.**—Procedure used to establish the identity of the user and the levels of authorization and access permitted and establish connections.

**MAJCOM Information Assurance (IA) Office.**—Office charged with the responsibility for managing and executing the information protection security program for a MAJCOM, field operating agency, or direct reporting unit. The office reports to the MAJCOM DAA and provides security guidance to the Wing Information Assurance (IA) Offices.

**MODEM (Modulator/Demodulator).**—In the computer world, modems are primarily used for converting digital signals into quasi-analog signals for transmission and reconvertng back to digital signals at the destination.

**National Computer Security Center (NCSC).**—Organization responsible for encouraging the widespread availability of trusted computer systems throughout the Federal Government by creating national policy, performing software and hardware evaluations, writing standards, et cetera.

**Network.**—An interconnected collection of autonomous computers.

**Network Management Personnel.**—Personnel responsible for overall management of the network. Includes: Network administrators, Functional System Administrators, Computer Systems Manager, and Computer System Security Officer.

**Network Security.**—Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects. NOTE: Network security includes providing for data integrity.

**Password.**—Protected or private character string used to authenticate an identity or to authorize access to data.

**Personnel Security.**—Procedures established to ensure all personnel who have access to sensitive information have the required authority, as well as appropriate clearances, and the need-to-know for the information.

**Physical Security.**—1. (COMSEC) Component of COMSEC that results from all physical measures necessary to safeguard classified equipment, material, and information from access or observation by unauthorized persons. 2. (AIS) Use of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

**Residual Risk.**—Portion of risk that remains after security measures have been applied.

**Risk.**—Probability that a particular threat will exploit a particular vulnerability of the system.

**Risk Assessment.**—Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures.

**Security Directive.**—Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

**Security Features.**—Security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards.

**Security Requirements.**—Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

**System.**—See “Automated Information System.”

**Telecommunications.**—Preparation, transmission, communications, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro optical, or electronic means.

**Threat.**—Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or an information system.

**Trusted Facility Manual (TFM).**—Manual that documents the operational requirement; security environment; hardware and software configurations and interfaces; all security procedures, measures, and features; and the contingency plans for continued operations in case of a local disaster.

**Unclassified.** —Information that has not been determined, pursuant to Executive Order 12356 or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified.

**Unit COMPUSEC Manager (UCM).**—Individual formally appointed by a designated approving authority to ensure the provisions of all applicable instructions are implemented throughout the life cycle of an AIS network.

**User.**—Person accessing an AIS by direct connections (via terminals) or indirect connections. NOTE: “Indirect connection” relates to persons who prepare input data or receive output data that is not reviewed for content or classification by a responsible individual.

**User Identification (User ID).**—Unique symbol or character string that is used by an AIS to uniquely identify a specific user.

**Vulnerability.**—A weakness in an information system, or cryptographic system, or components (system security procedures, hardware design, internal controls) that can be exploited.

**Wing Information Assurance Office (WIAO).**—Office charged with the responsibility for managing and executing the Information Assurance (IA) security program for a base or wing. The office reports to the MAJCOM Information Assurance Office and provides security guidance to organization IA security offices or appropriate unit officials (COMSEC managers; Computer Systems Security Officers (CSSO); Security Awareness, Training, and Education (SATE) managers; EMSEC users).