

15 OCTOBER 1998



Communications and Information

**MCCHORD AFB METROPOLITAN AREA
NETWORK SYSTEMS SECURITY**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: 62 CS/SCBS (Mr. Baluyot)

Certified by: 62 CS/CC (Lt Col Ursheler)

Pages: 26

Distribution: F

This instruction applies to all users of the Metropolitan Area Network (MAN) on McChord AFB. This instruction implements Air Force Policy Directive 33-2, *Information Protection*; Air Force Systems Security Instruction (AFSSI) 5102, *The Computer Security (COMPUSEC) Program*; and AFSSI 5024, Volume 1, *The Certification and Accreditation (C&A) Process*.

1. General Information.	2
2. Operational Security Directives.	3
Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	16
Attachment 2— PERSONAL USER ID (PUID)/GROUP USER ID (GUID) RECEIPT	19
Attachment 3— LOGIN BANNER	21
Attachment 4— VIRUS INCIDENT REPORT	22
Attachment 5— INITIAL INTRUDER REPORT	23
Attachment 6— VULNERABILITY REPORT	25

1. General Information.

1.1. Introduction. Computer Security (COMPUSEC) protects your computer and everything associated with it. Most importantly, COMPUSEC protects the information you've stored in your system. All users of the systems and information contained therein must share the responsibility for the security, integrity, and confidentiality of the systems and the information. COMPUSEC is achieved by complying with this instruction.

1.2. Purpose. This document establishes system security for the base MAN, defines network security directives, and specifies required security countermeasures. This instruction also addresses the minimum security measures for systems interfacing with the MAN. Specifically, this document defines the network security measures to ensure security, confidentiality, and integrity of information obtained, created, or maintained by the MAN, and assures its service availability. Information includes all electronically stored and printed files contained on servers, micro- and minicomputers, and mainframes. Failure to observe the prohibitions and mandatory provisions in this publication, whether they apply to McChord AFB specifically or are dictated by higher directives, is a violation of Article 92, UCMJ, and noncompliance may result in punishment under Article 92, UCMJ.

1.3. Mission. The mission of the MAN is to support the electronic creation, transfer, sharing, and presentation of information by using networked personal computers and commercial off-the-shelf software. The MAN is a general purpose, multi-user system used by the 62d Airlift Wing (62 AW), its groups and squadrons, all wing agencies, and tenant units. It provides access to a myriad of electronic services (such as electronic mail [e-mail], word processing, spreadsheets, electronic forms, and databases) and a gateway to the Internet. As a result, the MAN provides users with the tools to improve business processes, resulting in increased efficiency and effectiveness. Therefore, this document was developed to provide MAN users and administrators with a pragmatic security directive, realistic guidelines, and the tools necessary to accomplish their mission.

1.4. Applicability and Scope. This security directive provides the minimum MAN computer security requirements and establishes the set of rules and practices to regulate management, protection, and distribution of data entrusted to the network. The policies stated in this instruction apply to everyone administering and using the MAN.

1.5. Relationship to Other Publications. The National Computer Security Center (NCSC) Standards and Guides (Rainbow-series), Department of Defense (DoD) Directives, Air Force Systems Security Instructions (AFSSIs), and Air Force Systems Security Memorandums (AFSSMs) govern the operation and management of information systems. Other documents that relate specifically to the MAN are as follows:

1.5.1. User Security Operating Instructions (OIs). Security OIs are written for everyday users of the MAN. They use generic terminology that users, unfamiliar with the MAN operating system, can understand. The unit computer systems security officer (CSSO) develops this document (see AFSSI 5102 para 2.8.3.3.). If a unit has no formal CSSO, then the computer systems manager (CSM) or the unit COMPUSEC manager (UCM) will develop the OI. Each organization on McChord AFB may use this instruction as a foundation to create their own unit OI specific to their mission and environment. If an organization decides not to use 62 AWI 33-7 as a basis for a unit OI, then AFSSI 5001, *Security Policy Development Guide*, must be followed to establish the required system security instruction.

1.5.2. **Conflicting Guidance.** The provisions of this security instruction and the user OIs do not replace the requirements contained in Air Force and DoD-level documents. If there is a conflict, the requirements in higher-level regulations govern. Report the conflict to your UCM or Terminal Area Security Officer (TASO).

1.6. **Basic System Facts.** The following basic system information describes the MAN.

1.6.1. **Authorized Data on the MAN.** The MAN *will not* be used to process *classified information*. Sensitive information is the highest level of data authorized on the MAN. In essence, sensitive information is that information which does not rise to the level for which it requires protection as classified information. However, it generally is that type of information that can impact the national interest, conduct of Federal programs, or individual privacy entitlements. Typically, sensitive information includes, but is not limited to, that protected by the Privacy Act of 1974, privileged data, proprietary data, and For Official Use Only (FOUO) data. See AFM 33-270, *Command, Control, Communications, and Computers (C4) Systems Security Glossary*, for a detailed definition of sensitive information.

1.6.2. **Minimum User Clearances.** Access to the MAN does not require a security clearance. MAN access is based on the key concepts of “authorization” and “need-to-know.” Authorization is validated when a unit security manager notifies the Network Control Center (NCC) that an individual requires MAN access to perform official duties and that a personal user ID (PUID) should be issued. Notification must be in person or by telephone and information about the user will be taken at that time. Need-to-know access to unclassified or sensitive information must be based on either an explicit written authorization or implicit authorization derived from the individual’s official duty assignment. Additionally, government contractors will not be given access to any information accessible on the MAN unless first approved through proper channels. Approval for contractor access will be worked through the appropriate contracting officer and approved only when required to satisfy the terms of the contract. The contracting office is responsible for obtaining appropriate nondisclosure agreements and for ensuring the requirements of the Privacy Act of 1974 and other laws protecting various information are enforced when it is necessary for contractors to have access to sensitive information on the MAN. All system administrators (SAs) working with contractors should maximize use of discretionary access controls described in para 2.3.4.

2. **Operational Security Directives.**

2.1. **Assurance.** Assurance is the measure of confidence that the security features and architecture of the MAN accurately mediate and enforce the security directives. Assurance is established by the certification and accreditation (C&A) of the MAN and is maintained through compliance with this document; AFSSI 5102, *The Computer Security (COMPUSEC) Program*; AFSSI 5024, Volume I, *The Certification and Accreditation Process*; and AFSSI 5024, Volume II, *The Certifying Official's Handbook*.

2.2. **Accountability.** IAW AFSSI 5027, *Network Security Policy*, the MAN operating system software will maintain an automated audit trail that can be used to report COMPUSEC-related activities. This will ensure people with access to the MAN can be held accountable for their actions. Only a subset of all available MAN auditable events will be activated for full-time auditing. The focus used to select the auditable events is based on providing the ability to monitor specific security features and is primarily directed at auditing the granting and modification of user security rights and security attributes. Although UCMs and SAs will be audited in greater detail due to their supervisory privileges, all MAN

users will be audited to some degree to include events such as logging in and out of the MAN. Additionally, the SA will terminate access when unauthorized user activity is detected. 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. The Wing Information Assurance (IA) office will review the audit trail data. Retention of audit records that cover periods involving a security incident will be in accordance with appropriate disposition record requirements.

2.2.1. Auditable Events. The following comprise auditable events:

2.2.1.1. Use of account login and logout.

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

2.2.1.3. Actions taken by SAs, UCMs, and work group managers (WGMs). Examples include adding a user, changing user rights, or performing file server restarts.

2.2.1.4. 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.

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

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

2.2.2. Specific Audit Information. The audit trail will record the following minimum information for each auditable event. Only the Wing IA office can grant authorization for SAs to disable auditing or change their configured audit mechanisms.

2.2.2.1. Date and time of the event.

2.2.2.2. Unique identifier of the user or device generating the event.

2.2.2.3. Type of event.

2.2.2.4. Success or failure of the event.

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

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

2.2.2.7. Description of actions taken by the SAs and computer system security officers.

2.2.3. Audit Review. The Wing IA office will randomly review audit data. They will review the following: patterns of access to individual objects, access histories of specific processes and users, use of various protection mechanisms and effectiveness, repeated attempts to bypass protection mechanisms, and monitor use of privileges. Upon request, each SA will temporarily configure their audit files to be viewed remotely by the Wing IA office.

2.2.4. Protection of Audit Files. Audit data files and products will be protected as sensitive information.

2.2.5. Events Selected for Audit. A subset of all available MAN events subject to auditing will be selected for auditing. These events are primarily directed at the assignment and modification of a user's rights and attributes.

2.3. Access Control.

2.3.1. Method of Access Control. A combination of physical security, personnel security, and system security mechanisms will be used to control access to the MAN. Users must properly identify and authenticate before accessing the MAN. The method of access control for the MAN is a combination of a personal user login ID (identification) and a unique password (authentication).

2.3.2. Identification.

2.3.2.1. Personal Accounts. MAN users must complete a Personal User ID (PUID)/Group User ID (GUID) Receipt when they receive their personal user ID and initial account password. By completing the PUID/GUID Receipt, the user agrees to comply with all MAN security requirements. See the NCC for additional guidance on establishing a personal account. Use the approved McChord AFB PUID/GUID Receipt in Attachment 2.

2.3.2.2. Group Accounts. The use of group user ID (GUID) does not meet the security requirement for positive identification of a single MAN user. Therefore, GUIDs will be authorized only on a case-by-case basis to meet unique necessary requirements. Fully justified requests for a GUID must be submitted in writing by the wing, group, or staff agency chief to the 62d Communications Squadron (62 CS) commander. On those rare occasions when a GUID is authorized, manual or automated procedures must be implemented to identify which member of the group actually performed the login function. Each member of a GUID account must sign a PUID/GUID Receipt prior to initially logging into the account. The following minimum security requirements apply to all group login accounts.

2.3.2.2.1. All members of a GUID account will track each "login" and "logout" as follows:

2.3.2.2.2. The member who performs the login function will make a log book entry identifying, as a minimum, his or her name, date, and time the GUID account is opened. The member who performs the logout function will perform, as a minimum, the same functions as login.

2.3.2.2.3. If the local GUID account policy allows an individual to use a workstation that has already been logged on by another group member, a separate log book entry is required by that individual. As a minimum, the name, date, and time this individual used the GUID account is required information.

2.3.2.2.4. End of shift procedures must include the logging out of the GUID account and the logging in by the next shift personnel.

2.3.2.2.5. Members of the group will not reveal the GUID account password to anyone except other authorized members of the GUID account or other authorized personnel such as their DAA, unit commander, or staff agency chief.

2.3.2.2.6. The GUID account password will be changed whenever any member of the group no longer requires access to the GUID account.

2.3.3. Authentication. All user login attempts must be authenticated by use of a password.

2.3.3.1. Password Length. Passwords must be at least eight alphanumeric characters (upper and lower case) with at least one special character (@, &, +, #, etc.) in length. Password composition is described in AFMAN 33-223, *Identification and Authentication*, paragraph 2.4.

2.3.3.2. Password Generation. A SA generates the initial password for a new user. Users will generate their own passwords after the initial password assignment.

2.3.3.3. Changing Passwords. The life cycle of passwords will be limited to a maximum of 90 days for users and 60 days for SAs. Passwords will be immediately changed upon the departure of a member of a group ID or if compromised.

2.3.3.4. Limiting Grace Logins. The unlimited use of an expired password is not authorized. Users will be restricted to three grace logins following the expiration of their password. During the grace login, users will be prompted to select a new password.

2.3.3.5. Unique Passwords. Passwords will not be reused on the same user ID account. All MAN file servers automatically store the last eight passwords used for authentication. This security feature delays reusing a password on the same account.

2.3.3.6. Password Lock-Outs. Users will be allowed three attempts to properly enter their password. A user ID will be locked-out after three unsuccessful password authentication attempts. All MAN users, to include personnel who are on TDY status, will contact their UCM or WGM when they are locked-out from their account. The UCM or WGM will in turn contact the 62 CS Help Desk (4-2563) to unlock the user account. UCM and WGM involvement is necessary to verify the request is coming from an authorized MAN account user.

2.3.3.7. Password Protection. MAN passwords are considered sensitive information. As such, it is each user's responsibility to protect his or her password. This protects the user from having another person assume his or her identity on the MAN without proper authorization or permission. Paragraphs 2.3.3.7.1 through 2.3.3.7.4 stipulate mandatory password protection requirements.

2.3.3.7.1. Passwords should not be written down. However, if it becomes necessary to write down a password, the password should be stored in a manner that minimizes disclosure. If a password is disclosed to an unauthorized person, the disclosure should be reported to the TASO or UCM, and the password should be changed immediately.

2.3.3.7.2. Password entry will not be automated. For example, do not place your password in a login script or batch file. If you use a program that caches or automatically stores passwords, such as Microsoft Windows 95, the Password Caching feature must be disabled.

2.3.3.7.3. Passwords should not be disclosed or shared with other personnel unless they have proper authorization or permission.

2.3.3.7.4. Current MAN account passwords, to include dial-up modem account passwords, will not be used as a password to access unofficial or commercial systems or networks (e.g., commercial internet access providers or bulletin board systems).

2.3.3.8. Login Banner. The network or information system must display, to each user attempting use or access, a warning about unauthorized use of DoD computer systems and a consent to monitoring statement. See Attachment 3 for the mandatory banner statement. The banner's language should not be expected to change often, but only when deemed necessary by DoD or the Defense Information Systems Agency (DISA). Wing IA will notify the appropriate personnel (i.e., NCC, SAs and UCMs) when login banner changes are made.

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

2.3.5. Closing User ID Accounts. MAN user ID accounts and passwords will be deleted within one duty day of the user's departure from an organization, or when a user no longer requires access to perform official duties. The TASO will notify the UCM when an account requires deletion. Make notifications in writing or by e-mail. This will ensure appropriate documentation for all user ID files.

2.3.6. Inactive User Accounts. Unit SAs, in coordination with the UCM, will validate user accounts under their control with the appropriate TASO and will remove any accounts that are no longer valid. The SA or UCM will contact the NCC to remove these accounts.

2.3.7. Simultaneous User ID Logins. MAN users will limit logging in to only one workstation at a time. There are very few instances where simultaneous logins are necessary. Individuals who have a valid duty requirement (e.g., SA, NCC personnel, UCM, TASO, Wing IA personnel) will be authorized to simultaneously login from multiple workstations. Fully justified requests for a single MAN user to simultaneously login from multiple workstations must be in writing and approved by the unit DAA. Contact Wing IA office for guidance on the appropriate procedures to be followed.

2.3.8. Network Connections.

2.3.8.1. Modem Connections. Use of modems is not allowed to connect to the base MAN. Users will access the MAN primarily through on-base terminals or through the NCC Remote Access Server. Users wishing to access the MAN through the use of modems must meet specific mission requirements. Mission needs will be dictated by the unit DAA and ultimately approved by the 62 CS. Users must submit such requests in writing through their flight chief, branch chief, or higher level authority and then coordinate the request through their SA, commander or staff agency chief, and finally to 62 CS/SCBN. If approved, 62 CS/SCBN will issue a separate login ID and password for modem users, distinct from their on-base MAN account. All such connections must comply with all MAN user identification and authentication requirements and AFMAN 33-223. Annually, UCMs will reevaluate the need for modem access that is granted.

2.3.8.2. New Network Connections. The Wing IA office must confirm, prior to connecting a new network to the MAN, that the new network satisfies the security requirements established by this instruction. The confirmation process will include obtaining 62 CS Designated Approving Authority (DAA) approval to connect to the new network. A Memorandum of Agreement (MOA) will be developed between the UCM of the requesting organization and 62 CS NCC. The MOA will include the following minimum information: C&A of the new server, data description and classification, user clearance levels, name of the DAA, group or unit commander, or staff agency chief who shall resolve conflicts, and intended recipients of transmitted data.

2.3.8.3. Internet Protocol (IP) Addresses. Each authorized user will have an established IP address. The unauthorized use or change of an IP address is prohibited without prior coordina-

tion with the NCC (4-2563). Violations will result in termination of the offending user's access to the MAN with reinstatement only by written request of the user's unit commander or staff agency chief.

2.4. Personnel Security.

2.4.1. Security Clearances. As stated in para 1.7.3, access to the MAN does not require a security clearance. However, personnel who have their security clearance suspended or revoked for cause, or receive administrative punishment (e.g., Article 15) will have their access eligibility to the MAN reviewed by the unit security manager and commander or staff agency chief. Once a determination has been made to deny access to the MAN, the UCM will be notified and, in turn, he or she will notify the NCC, ensuring MAN access is revoked.

2.4.2. Need-To-Know. Authorized access to the MAN occurs when a TASO notifies a UCM that an individual requires MAN access to perform official duties and that a PUID should be established. Each user is responsible for determining a person's need-to-know before disclosing information under their control.

2.5. Hardware.

2.5.1. File Server Access. Physical access to MAN file servers will be restricted by locating them in a climate-controlled, lockable enclosure such as a room, closet or cabinet. Access will be limited to authorized personnel only, such as SAs and authorized maintenance personnel.

2.5.2. Resource Protection. The first line of defense for protecting valuable assets is resource protection. To prevent misuse, abuse, or theft, system hardware will be located in facilities which can be physically secured or locked.

2.5.3. Major Additions/Modifications to Network Hardware. The NCC will assess all additions and modifications to major MAN hardware components. After the assessment is complete, the NCC will either recertify or not certify the recommended addition or modification when the package is submitted to the DAA for approval. This requirement does not apply to the connection of user terminals or peripheral devices.

2.5.4. Hardware Inventory. Organizational equipment control officers (ECOs) will ensure that all MAN hardware assets (e.g., workstations and printers) under their control are listed in the automated data processing equipment Information Processing Management System (IPMS). The NCC will accomplish this task for MAN-wide assets. Organizational ECOs and NCC personnel will ensure the MAN accreditation control number is associated with each IPMS MAN equipment record.

2.5.5. Hardware Maintenance. Only authorized maintenance personnel (e.g., NCC personnel, WGMs, and government-approved vendors) who are dispatched by the NCC will perform hardware maintenance on MAN equipment and workstations. Individual MAN users will not perform hardware maintenance or modifications without the express approval of the NCC. Additionally, vendor maintenance personnel will not be given unescorted access to sensitive information storage media or products during the repair or testing of system components.

2.5.6. Hardware Configuration Control. The MAN Computer System Manager (CSM) is responsible for ensuring network hardware configuration control is in place and maintained.

2.6. Software.

2.6.1. Making Backup Copies of Original Network Software. SAs will make backup copies of all original network software that is installed as “standard” on all MAN file servers. WGMs will make backup copies of all original network software that is installed as a “unique” requirement on the file servers they maintain. Backup copies will be stored separately (preferably off-site) from the master copies whenever possible. They should be stored under lock and key due to the high pilferability of the software. Any duplication of commercially licensed software, except for backup purposes, is a violation of Federal copyright laws.

2.6.2. Archiving (Backup) of MAN File Server Files. At a minimum, a daily incremental backup will be made for data files on each MAN file server or LAN file server connected to the MAN.

2.6.3. Archiving (Backup) of User Files. Users are encouraged to periodically backup their personal files. This is especially true for data files which are located on their workstation hard drive (i.e., C drive), since workstation files are not backed up in any way by the MAN file server backup process.

2.6.4. Software Certification. All network operating system and application software that specifically interacts with the MAN, but is not provided to units by official Air Force channels, must be tested Air Force level prior to its implementation. Network and application software testing will be accomplished to ensure the new software does not circumvent existing MAN security features.

2.6.5. Software Configuration Control. The MAN CSM is responsible for ensuring network software configuration control is in place and maintained. At a minimum, the SA will maintain for each file server a current inventory of all software loaded and their approved implementation configuration.

2.6.6. Security Software. When possible, security software products evaluated by the Air Force Information Warfare Center’s Product Assessment and Certification Center should be used to implement security safeguards. The Air Force Assessed Product List (APL) lists the available products.

2.6.7. Malicious Software. Malicious software will not be installed on any MAN file server or workstation. Except for written approval from 62 CS/CC, this prohibition includes software that is specifically designed as packet analyzers with the purpose of capturing system passwords.

2.6.8. Unauthorized Software. Only government approved software is authorized on the MAN. Games and pornographic software is unauthorized and will not be installed on any computer or file server. Unless approved by the DAA, group or unit commander or staff agency chief, freeware or shareware will not be authorized on the MAN file servers or workstations. Before installing any privately owned commercial software, freeware, or shareware, the DAA, group or unit commander or staff agency chief will verify a true need to do so and to ensure compliance with all applicable regulations.

2.6.9. Using Government Owned Software for Personal Projects. DAAs, group or unit commanders, or staff agency chiefs must approve any use of government computer equipment for personal educational projects, job hunting, or similar uses. All such approvals must set out the limitations found in DoD Directive 5500.7-R, *Joint Ethics Regulation*.

2.6.10. Virus-Scanning.

2.6.10.1. Scanning of Workstations and Servers. IAW with AFSSI 5102, the use of antiviral software is mandatory. Units will ensure that each server and workstation will have antiviral

software to provide virus protection for MAN users. The UCM will ensure the antiviral software is kept up to date. At a minimum, the UCM or TASO will configure the program to automatically run when each machine initially boots up. SAs are responsible for loading antiviral software on each server on the MAN.

2.6.10.2. Scanning Individual Workstation Storage Media. MAN users will perform a virus scan of floppy diskettes prior to any follow-on use of the diskettes on a MAN workstation. This includes workstations remotely connected to the MAN via a modem. The Wing IA office will provide the virus-scanning program to support this function. The unit OI will include guidance on how to use the virus scanning capability.

2.6.11. File Encryption. Individuals are encouraged to encrypt their files for an added degree of security protection. The unit OI will include how to use file encryption, if applicable.

2.7. Marking/Labeling.

2.7.1. Labeling Removable Storage Media. Labels will be applied to all removable storage media (floppy diskettes, tapes, and hard drives) IAW AFSSI 5027, paragraph 5.6. Standard Form 711, **Data Descriptor**, will be used whenever possible. If SF 711 is not available for use, the original labels that came with the media may be used. Either label will indicate the storage media's owner (by name or office symbol), use, and description of contents. Additionally, appropriate markings must be indicated on the label of all removable magnetic storage media that contains sensitive information. Air Force Visual Aid 205-15, **Privacy Act Label**, may be used to indicate the storage media containing personal data. All removable media will have one of the following classification labels: SF 706-TOP SECRET, SF 707-SECRET, SF 708-CONFIDENTIAL, or SF 710-UNCLASSIFIED.

2.7.2. Marking/Labeling Controlled Unclassified Information. "FOUO," "Sensitive But Unclassified" information, and "Sensitive Information," as defined by the Computer Security Act of 1987, fall into the category of "unclassified controlled information." These types of information will be marked/labeled IAW DoD 5200.1-R, *Information Security Program*, Appendix C, paragraphs 2-201.b.(3), 3-301, and 6-601.

2.8. Processing Classified Information. Currently, the MAN is not authorized to process classified information.

2.9. Inadvertent Entry of Classified Information in the MAN. Classified information accidentally introduced into the MAN requires immediate reporting and intervention by key personnel. Procedures set forth in DoD 5200.1-R will be strictly adhered to. As a minimum, the following personnel will be notified: the SA, UCM, unit security manager, unit DAA, base NCC, Wing Information Assurance office, 62 CS/CC, and higher headquarters. NCC personnel will follow locally established procedures for purging classified information from the MAN.

2.10. Computers Used to Process Classified Information. Systems accredited to process classified information in a stand-alone configuration must be physically disconnected from the MAN or unit local area network (LAN) when processing classified information. The specific security measures used must be included in the unit security OI, as required by paragraph 1.6.1.

2.11. Sensitive Information.

2.11.1. User Responsibility. It is the responsibility of each user to properly protect and safeguard all sensitive information under his or her control. Sensitive information is discussed in paragraph

1.7.1, and defined in AFM 33-270. Please note that the aggregation of information can result in the creation of sensitive data. For those occasions when guidance is needed to determine if specific information is sensitive or not, contact 62 CS/SCBR (Records Management, 4-2888).

2.11.2. Storage. The preferred method of storing sensitive information is to use removable storage media, such as floppy diskettes. However, sensitive information may be stored on the "C" drive. If you choose to store sensitive information on the "C" drive, the user must take the appropriate security measure to protect that information. See AFSSI 5102 for further guidance.

2.11.3. Aggregating Data. When storing data on the MAN, each user must be careful to avoid collecting or grouping independent information where the sensitivity of the whole is greater than the sensitivity of the parts, potentially creating data not authorized for use on the MAN. In no case will users aggregate data for placement on the MAN when any portion of the data taken individually, or taken as a whole, would be considered "classified." Users should also limit use of sensitive information on e-mail systems accessed through the MAN. Individual users should consult with their functional managers to determine when issues regarding aggregated data arise.

2.11.4. Transmitting Over E-Mail. When transmitting sensitive information over e-mail, the sender must ensure that the receiver is authorized to receive the data and has an official need to know. The e-mail message must conspicuously state that sensitive information is being transmitted. Further, if the message is transmitted to an off-site location, users are strongly encouraged to encrypt the message and all attachments. Use appropriate levels of protection to prevent unauthorized disclosure of sensitive information. See AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, for further information on this subject.

2.11.5. Disposition. Computer products that contain sensitive information will be disposed of IAW AFI 37-138, *Records Disposition-Procedures and Responsibilities*, paragraph 3.10.

2.11.6. Categories of Sensitive Information.

2.11.6.1. Privacy Act Data. Privacy is a personal and fundamental right protected by the Constitution of the United States. Protecting individuals from unwarranted invasion of their personal privacy is the overriding purpose of Privacy Act of 1974. Some common examples of non-releasable data to a third party (without the concerned individual's consent) are medical records, recall rosters, manpower and personnel records, training records, individual financial information, information regarding marital status and dependents, ethnic background, religious preference, and information of a personal nature. See AFI 33-132, *Air Force Privacy Act Program*, for detailed information.

2.11.6.2. Privileged Data. This category is defined as data that is not subject to usual rules because of confidentiality imposed by law, such as certain chaplain, legal, and medical, safety, and internal organizational management records (i.e., quality assurance data or credentials committee records).

2.11.6.3. Proprietary Data. Proprietary information is material and information relating to or associated with a company's products, business, or activities. Examples of proprietary data are copyrighted material and patented material/information.

2.11.6.4. 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, auditor records, critical informa-

tion, For Official Use Only (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.

2.12. 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.

2.12.1. Remanence Security Philosophy. Sensitive information must be protected from unauthorized recovery of previously deleted data. This is accomplished by using either the remanence security process of clearing or purging. By definition, clearing removes sensitive information from computer storage devices (hard disks and floppy disks) in a manner that renders the data unrecoverable by normal system utilities or non-technical means. Clearing will not purge information from storage. Additionally, routines that only remove pointers and leave data intact are not acceptable methods of either clearing or purging storage devices. There are three authorized methods of clearing magnetic computer storage media: (1) Overwrite all locations with any single character. The Air Force APL identifies several commercial products that are available to overwrite all locations on MS-DOS formatted magnetic storage media (e.g., local hard drives and floppy diskettes). (2) Use a Type I degausser. (3) Destroy the magnetic storage media. Either method two or three must be used whenever the use of method one is not possible, such as when a hard drive is not operational. In contrast to clearing, purging is defined as the removal of sensitive information from computer storage devices in a manner that gives assurance, proportional to the sensitivity of the data, that the information is unrecoverable by technical means. Purging is associated with classified data and will only be required when classified data is inadvertently entered into the MAN. See AFSSI 5020, *Remanence Security*, for additional information on clearing and purging magnetic storage media.

2.12.2. When to Clear Computer Magnetic Storage Media. Users and UCMs will clear magnetic storage media under their control that contain unclassified or sensitive information before reutilization or release from user control. Information owners will review files for record management disposition requirements prior to clearing the files from the magnetic storage media.

2.12.2.1. Users and UCMs will 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.

2.12.2.2. User workstations and MAN file servers do not require clearing of sensitive information when NCC personnel perform equipment maintenance. If NCC personnel cannot repair the equipment, the NCC will notify the equipment user that vendor maintenance is required. Prior to sending a workstation to vendor maintenance, the hard drive files will be reviewed by the user to determine if sensitive information has been stored on the hard drive. If sensitive information is found, either the hard drive must be removed or those files containing sensitive information must be cleared. Prior to sending file servers to vendor maintenance, the file server hard drive will either be removed or all data files must be cleared to prevent the inadvertent release of sensitive information.

2.12.2.3. UCMs or SAs will clear file server directories and the 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. UCMs or SAs will use the NetWare purge utility to remove any residual data stored on the MAN file servers.

2.13. Security Training.

2.13.1. Initial and Follow-Up User Security Training. All new users will receive initial training on the MAN security features prior to being authorized access to the MAN. The TASO and UCM will provide the training prior to establishing a new account. At a minimum, it will cover the requirements addressed in this instruction and the organizational OI. Follow-up security training using the SAFEWARE computer program will be conducted annually by the TASO and UCM. TASOs and UCMs will document each user's name and date trained.

2.13.2. Specialized Security Training. UCM and TASO responsibilities are outlined in AFSSI 5102. Wing IA will conduct some training during the required annual UCM meeting. Additionally, training aids received from HQ AMC will be provided to all base UCMs by the Wing IA office. The SAs should request training from the vendor of the specific operating system they are using.

2.14. Reporting Vulnerabilities or Incidents. MAN users will immediately report vulnerabilities, security incidents, or unauthorized entry into the computer system to their UCM. UCMs 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. In the case of an in-progress intrusion or suspicious activity, the UCM will immediately contact the Air Force Computer Emergency Response Team (AFCERT) at DSN 969-3157, toll free 1-800-854-0187, or commercial (210) 977-3157, and the Wing IA office. 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. Formal reporting of COMPUSEC incidents is accomplished IAW AFSSI 5021, *Vulnerability and Incident Reporting*. See Attachments 5 and 6 for reporting formats.

2.15. Malicious Logic Incidents. AFSSI 5021 provides instructions for reporting viruses detected in a government-owned information system. The user, upon detecting a suspected or actual malicious logic infection, must notify the UCM. If able, the user will remove the virus using approved antiviral software. The UCM will remove the virus if the user is incapable of doing so. Wing IA personnel can also assist the UCM or TASO in removing the virus. Upon discovery of a virus, a formal virus incident report (see Attachment 4) will be sent immediately to the Wing IA office. Therefore, pertinent viral information should be recorded at the time the virus is detected and removed. The Wing IA office will forward the report to HQ AMC and AFCERT along with the action taken by the user, UCM or Wing IA personnel.

2.16. Internet Fraud, Waste, and Abuse (FWA) Reporting Procedures. All users must report potential security violations or other incidents directly to their TASO and UCM. UCMs will determine the appropriate level of notification IAW AFSSI 5021, Table 1, for individual incidents. Non-COMPUSEC incidents may fall under the jurisdiction of other programs for investigation and reporting purposes. Examples include inadvertent disclosure of classified information (may or may not involve compromise); theft of information or information systems resources; Internet fraud, waste, and abuse (FWA), and copyright violations. You may use AF Form 102, **Inspector General Complaint Data Collection**, for reporting to the IG, or you may call the hotline at DSN 223-5030, toll free 1-800-424-9098. You may also use AF Form 635, **USAF Fraud, Waste, and Abuse Disclosure**, for

reporting FWA incidents to the AFOSI. Unit commanders will be notified of any FWA incidents. Keep in mind the UCM may play an active role in the investigation and correction after the fact.

2.17. Unattended Terminals. A terminal in a public access, unsecured location that is logged onto the MAN will not be left unattended unless the user either logs out of the MAN (the preferred method), uses a password-protected screen saver, and/or employs physical measures (i.e., keyboard locks). A terminal will be logged out of the MAN prior to the user leaving at the end of their work shift.

2.18. Personally Owned Computers. Personal computers owned by Air Force members, government employees, or contractor personnel will not be used to process classified information. Personally owned computers will not be connected to the MAN. The use of personally owned computers at work is strongly discouraged, however, it may be used for processing unclassified and SBU information with DAA approval. IAW AFSSI 5102, para 3.9.4, written DAA approval will specify the conditions under which the computer will operate and the duration of the approval. If the personally owned computer is used outside of the work area, government-owned SBU information must remain on removable media and be marked and protected accordingly. Using personally owned computer hardware and software for official business should be a last resort and actions should be taken to preclude their use.

2.19. Review of MAN Communications-Computer Systems Requirement Document (CSRD) for Security Impact. The Wing IA office will review the technical solution for each major MAN CSRD submission for possible impact on the MAN security capabilities. The review is required prior to submission of the CSRD for final approval.

2.20. Configuring a Workstation as 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 MAN system. MAN workstations will not be converted into a Web Server unless it meets the requirement in AFI 33-129, *Transmission of Information via the Internet*, and be approved by the DAA in writing.

2.21. Two Accounts for Persons with MAN Supervisor Privileges. Personnel who have a MAN account with supervisor privileges (including SAs, UCMs, and Wing IA personnel) will have a second account with user-only privileges established. Personnel will login with supervisor privileges only when performing supervisor tasks. At all other times, they will login via the second account as a regular MAN user.

2.22. Air Force Computer Emergency Response Team (AFCERT) Advisories. These advisories identify specific software and operating system vulnerabilities. By naming affected platforms and making recommendations for corrections, patches, or workarounds, the vulnerability of applicable named systems is minimized to an acceptable level. SAs and UCMs will receipt for each advisory and ensure the corrective actions to each vulnerability, as recommended in the AFCERT advisory, is immediately implemented. Furthermore, the SA and UCM will receipt for every AFCERT advisory within 24 hours of receipt, by e-mail, to the Wing IA office. Upon implementation of the recommended solution, the SA and/or the UCM will immediately inform the IA office of what action was taken. If immediate implementation of the corrective action is not possible, provide Wing IA with a weekly status report on what action is being taken to comply with the advisory. SAs and UCMs will send a courtesy copy of all outgoing reports to their unit commander. The Wing IA office will consolidate all unit responses and forward a summary report to HQ AMC IPC. The IA office will also file unit responses and update

its AFCERT database with actions taken. See AMCI 33-202, Volume 1, *Information Assurance*, paragraph 6.2, for information on security advisory registration, implementation, and tracking.

RAYMOND E. JOHNS, JR., Colonel, USAF
Commander, 62d Airlift Wing

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 90-301, *Inspector General Complaints*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-129, *Transmission of Information via the Internet*

AFI 33-132, *Air Force Privacy Act Program*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFM 33-270, *Command, Control, Communications, and Computers (C4) Systems Security Glossary*

AFMAN 33-223, *Identification and Authentication*

AFSSI 5001, *Security Policy Development Guide*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Vulnerability and Incident Reporting*

AFSSI 5024, Volume I, *The Certification and Accreditation Process*

AFSSI 5024, Volume II, *The Certifying Official's Instruction*

AFSSI 5027, *Network Security Policy*

AFSSI 5102, *The Computer Security (COMPUSEC) Program*

AFSSM 5023, *Viruses and Other Form of Malicious Logic*

AMCI 33-202, Volume 1, *Information Assurance*

DoD 5200.1-R, *Information Security Program*

DoDD 5500.7-R, *Joint Ethics Regulation*

HQ AMC Wing LAN Security Directive

Abbreviations and Acronyms

ADPE—Automated Data Processing Equipment

AFCERT—Air Force Computer Emergency Response Team

AFI—Air Force Instructions

AFSSI—Air Force Systems Security Instructions

AFSSM—Air Force Systems Security Memorandum

APL—Assessed Product Listing

C&A—Certification and Accreditation

COMPUSEC—Computer Security

CSM—Computer Security Manager
CSRD—Communications-Computer Requirements Document
CSSO—Computer Systems Security Officer
DAA—Designated Approving Authority
DAC—Discretionary Access Control
ECO—Equipment Control Officer
E-MAIL—Electronic Mail
FWA—Fraud, Waste, and Abuse
GUID—Group User Identification
IA—Information Assurance
IPMS—Information Processing Management System
MAN—Metropolitan Area Network
MOA—Memorandum of Agreement
NCC—Network Control Center
NCSC—National Computer Security Center
PUID—Personal User Identification
SA—System Administrator
TASO—Terminal Area Security Officer
UCM—Unit COMPUSEC Manager
WGM—Work Group Manager

Terms

Accreditation —Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls.

Information System—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, hardware and firmware.

Certification—Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system to establish the extent to which a particular design and implementation meet a set of specific security requirements.

Computer Security Manager (CSM)—Official with supervisory or management responsibility for an organization, activity, or functional area that owns or operates an information system.

Countermeasure—The sum of a safeguard and its associated controls.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an information system or network within specified environment.

Information—Data derived from observing phenomena and the instructions required to convert that data into meaningful information. *NOTE*: Includes operating system information such as system parameter settings, password files, audit data, etc.

Safeguards—Protective measures and control prescribed to meet the security requirements of an information system.

Attachment 2**PERSONAL USER ID (PUID)/GROUP USER ID (GUID) RECEIPT**

The following is the Personal User ID (PUID)/Group User ID (GUID) Receipt worksheet. This receipt will be used to formally acknowledge proper password accountability and network use.

Personal User ID (PUID)/Group User ID (GUID) Receipt

I declare an official duty requirement for an account on the McChord Metropolitan Area Network (MAN). I understand I am responsible for the protection of the password for my account. I will comply with these instructions. I will not divulge the password to any other individual. I will report to the Unit COMPUSEC Manager (UCM) or Wing Information Assurance (4-2945/5726) any problem(s) I encounter in the use of the password or any misuse of passwords by other personnel which may occur in my presence. I will abide by these rules for all government systems to which I have access.

 LOGON (User ID)

 Office Symbol

 Last, First, Middle Initial

 Rank/Grade

 Organization

 Phone
Unclassified User Agreement

CONSENT TO MONITORING: Official U.S. Government Systems are for authorized use only. Do not discuss, enter, transfer, process, or transmit classified/sensitive national security information of greater sensitivity than that for which this system is authorized. Use of this official U.S. Government System constitutes consent to security testing and monitoring.

1. I am responsible for all activity that occurs under my PUID. (This does not include those actions resulting from unauthorized intrusions that are beyond the user's control.) I will protect the password that authenticates the identifier, using the security classification of For Official Use Only (FOUO).
2. I will not permit anyone else to use the PUID given to me, and I will change my password at least every *90 days*.
3. I will not automate the entry of my password, and I will store it in a manner that minimizes its exposure to disclosure.

4. I will comply with AFI 33-119, *Electronic Mail (E-Mail) Management and Use*; AFI 33-129, *Transmission of Information via the Internet*; and any other related Air Force Instructions. I will also comply with any Air Mobility Command and 62d Air Wing Instructions and policy on Internet use, e-mail use, and other related topics. Some of the following specific prohibitions are identified in these AFI's:

- a. I will not add any software or hardware to the system without authorization from my Designated Approving Authority (DAA) who is _____.
 - b. I understand that I am not allowed to view/place computer games or pornography on official government systems, or to use official government systems for personal financial gain.
 - c. I will not install any freeware or shareware on my computer without the written permission of the DAA and the Wing Information Assurance office.
 - d. If I have an Internet Protocol (IP) address, which allows access to the Internet, I will not change it, nor will I attempt to enter any sites using any form of Web Protocol that are in violation of AFI 33-129.
 - e. I know it is a security violation for any user to mask their identity or use the identity of another user.
 - f. I know this system is for unclassified and sensitive unclassified information (Privacy Act and FOUO).
 - (1) I will not enter data into the system if the data is of a higher classification level than the system. I will not enter data that is proprietary, contractor excluded, or otherwise needs special protection, unless approved by the host UCM.
 - (2) Only authorized personnel are authorized access to my microcomputer.
 - (3) I will not release government information to the public unless authorized.
 - (4) I will transfer sensitive information on the base MAN only to those authorized to receive such information and will store it only on a server, workstation, or stand-alone computer that utilizes the proper access/security controls (passwords and authorized login ID) IAW current directives.
5. If I observe anything that indicates inadequate security for this system, I will immediately notify the local TASO and UCM.
6. I will report any suspected instances of fraudulent or unauthorized practices or use immediately to my immediate supervisor or through the procedures stated in AFI 90-301, *Inspector General Complaints*.
7. I agree to follow my office security procedures, official regulations, and policies applicable to information system operations. This certificate is only a short summary to stress these key points.

I understand this agreement, acknowledge receipt of the unclassified PUID, and will keep the system secure. I also understand that use of this system constitutes consent to security testing and monitoring. Unauthorized use could result in disciplinary action or criminal prosecution.

Date

Signature

Date

UCM Verification of Training

Attachment 3

LOGIN BANNER

“This is a Department of Defense computer system for authorized use only. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate against unauthorized access, and to verify security procedures, survivability, and operational security. Using this system constitutes consent to monitoring. All information, including personal information, placed on or sent over this system may be obtained during monitoring. Unauthorized use could result in criminal prosecution.”

The McChord AFB MAN and each information system will display the following login banner. [Source: AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, para A2.3.5, dated 1 June 1998.]

Attachment 4

VIRUS INCIDENT REPORT

The following is the format to be used when reporting malicious logic incidents. Requests for assistance in filling out this form should be directed to the unit UCM. If necessary, contact the Wing Information Assurance Office (DSN 984-5726/3809) for further assistance.

1. Date Reported: _____

2. Report Individual Information:

a. Rank/Name _____

b. Organization _____

c. DSN Phone _____

d. E-mail Address _____

3. Date of Incident: _____

4. Virus Name: _____

5. Operating System: _____

Version #: _____

6. Antiviral Tool/Software Used: _____

7. Is the Information System Mission Critical?

Yes No

12. Mission of Computer/Impact of Virus on Mission: _____

13. Damage Observation: _____

14. Source of Infection: _____

8. Impact (Choose all that apply):

a. Data Alteration

b. Denial of Service

c. Data Integrity

d. None

9. Number of Systems Infected: _____

Number of Floppies Infected: _____

Network/IP: _____

10. Work-Hours Lost: _____

11. Fix Action:

a. Rebuilt System

b. Eradicated Virus

c. Destroyed Floppy

Attachment 5

INITIAL INTRUDER REPORT

The following is the format to be used when reporting intrusion incidents. Requests for assistance in filling out this form should be directed to the unit UCM or SA. If necessary, contact the Wing Information Assurance Office (DSN 984-5726/3809) for further assistance.

1. Report Date: _____
 2. Report Originator Information:

a. Rank/Name _____	f. E-mail Address _____
b. Unit/Base _____	g. Message Address _____
c. DSN Phone _____	h. Mailing Address _____
d. Position _____	_____
e. MAJCOM _____	_____
 3. Target Information (*Additional targets need separate sheet*):
 - a. Network Domain Name _____
 - b. IP Address _____
 - c. Computer Model (i.e., Sparc 5) _____
 - d. Operating System/Version _____
 - e. Security Mode of Operation _____
 - f. Network/System Mission _____
 - g. Security Classification _____
 - h. Network Structure/Type _____
 - i. How Detected _____
 - j. Impact on Mission _____
 - k. Information System Auditing _____
 4. Attack Session Information (*Correlates with the target information*):
 - a. Date(s) of Session _____
 - b. Time _____
 - c. Attack Method _____
 - d. Success _____
 - e. Account (*Include host name if available*) _____
 - f. First Layer Point of Origin _____
 5. Brief Scenario (*Description of incident*): _____
-

6. Countermeasure(s) Installed: _____

Name and Date Installed: _____

7. Notifications (*Indicate name, date, and time notified*):

a. UCM _____

b. Wing Information Assurance Office _____

c. MAJCOM Information Assurance Office _____

d. AFCERT _____

Attachment 6

VULNERABILITY REPORT

The following is the format to be used when reporting vulnerabilities. Requests for assistance in filling out this form should be directed to the unit UCM or SA. If necessary, contact the Wing Information Assurance Office (DSN 984-5726/3809) for further assistance.

1. Report Date: _____

2. Report Originator Information:

a. Rank/Name _____

f. E-mail Address _____

b. Unit/Base _____

g. Message Address _____

c. DSN Phone _____

h. Mailing Address _____

d. Position _____

e. MAJCOM _____

3. Description of Technical/Administrative Vulnerability:

(Describe the nature and effect of the vulnerability. The description should sufficiently reconstruct the computing environment so you can repeat the flaw without further information. Describe codes or procedures discovered that might reduce the impact of the vulnerability.)

4. Impact (Choose one):

a. Denial of Service b. Integrity c. Compromise

d. Others (Fully explain) _____

5. Hardware and Software Information:

a. CPU Model _____

b. Configuration (Indicate if the Information System is a workstation or stand alone) _____

c. Name and Version Number of Affected Software _____

d. Security Classification _____

6. Connectivity:

a. LAN Name, MAJCOM, Unit _____

b. WAN Name, MAJCOM, Unit _____

c. Attack Method _____

7. Work-Hours Lost: _____

8. Notifications (Identify vendors, developers, and COMPUSEC
Individuals _____

