BY ORDER OF THE
SECRETARY OF THE AIR FORCE

341 SPACE WING INSTRUCTION 33-202

1 JULY 2001

Communications and Information

INFORMATION SYSTEMS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: (Capt George B. Kinney)

Certified by: (Lt Col Steven J. Hennessy)
Pages: 16
Distribution: F

This publication implements the Computer Security Act of 1987 (Public Law 100-235); Department of Defense (DoD) Directive 5200.28, Air Force olicy Directive (AFPD) 33-2, Air Force Instruction (AFI) 33-115, Volume 1 and Volume II, Air Force Instruction (AFI) 33-112, Air Force Systems Security Instruction (AFSSI) 5027, Air Force Instruction 33-202, and AFSSI 5024, Volume 1. It applies to all personnel assigned to the 341st Space Wing and subordinate units, and personnel assigned or attached to, or supported by, Malmstrom AFB, Montana.

1. Introduction. Mission success increasingly depends on information systems, which makes it necessary to treat our networks like weapon systems.

1.1. Purpose. This document establishes wing guidance for computer operations for 341st Space Wing units and tenant organizations. It specifies policies and procedures that are required to ensure reliability and availability of computer systems. This instruction will be the primary source when wing users need to reference policy.

1.2. Applicability. This instruction applies to all Air Force military and civilian personnel and to Air Force contractors who develop, acquire, deliver, use, operate, or manage Air Force information systems. This includes systems not connected to the base network.

2. Roles and Responsibilities.

2.1. General. The base network processes sensitive but unclassified information used to meet the office automation requirements at Malmstrom AFB. Primarily, these requirements consist of electronic mail; word processing, scheduling, spreadsheet, database, and Internet access applications. This chapter will clarify the duties and functions within Malmstrom AFB and the 341st Communications Squadron. The 341st Communications Squadron is responsible for providing various types of computer related service from the following workcenters: Automated Data Processing Equipment (ADPE), Plans and Programs, Network Control Center (NCC), and Wing Information Assurance (IA). ADPE handles the purchasing and receiving of computer equipment. Plans and Programs receives, coordinates, and implements new communication-computer system requirements. The NCC is responsible for the management and operation of the base network. Wing IA develops, disseminates, and implements policies to ensure all base computers, computer networks, and communications devices are secured.

2.2. Wing Information Assurance Office (Wing IA). Assists all wing and tenant organizations in the development and management of their IA programs. Acts as the single focal point for Certification & Accreditation requirements for all information systems and provides accreditation guidance to Designated Approving Authorities (DAA). Wing IA also ensures compliance with vulnerability and incident reporting.

2.3. Network Control Center (NCC). The NCC provides responsive mission support by managing the local infrastructure that provides customers the communications and information resources needed to achieve their operational objectives. The NCC team consists of Network Management, Network Security, Network Administration, and NCC Customer Service.

2.4. Network Management (NM). NM provides proactive and reactive network management by monitoring and controlling the network, available bandwidth, hardware, and distributed software resources. They respond to detected network faults (errors) and user reported outages at the time of NCC Customer Service referral. Their area of responsibility is the base backbone infrastructure components (i.e., switches, routers, etc.).

2.5. Network Security (NS). NS employs hardware and software tools to enhance the security of the base network. They provide proactive security functions to assist organizations in deterring, detecting, isolating, containing, and recovering from information system and network security intrusions. They also install, monitor, and direct proactive and reactive network information protection. These defensive measures ensure the availability, integrity, accountability and confidentiality of base network information resources. NS also assists Wing IA in developing local security polices, strategies, and plans to counter identified network security threats.

2.6. Network Administration (NA). NA centrally manages various functional area networks from the network servers and software operating systems level. Tasks include all core services provided by the NCC to the base populace. NA is responsible for all NCC owned servers, e-mail, data, and user accounts. They are the base experts in system administration and also provide technical assistance to the Functional System Administrators (FSA) and Workgroup Managers (WM). In addition, NA is responsible for managing the base Intranet and Internet Web servers. NA also assists the Public Affairs office with Web page content management.

2.7. NCC Customer Service (CS). CS is the WMs' and FSAs' primary point of contact (POC) for problems that they cannot resolve. CS acts as the interface between the customer and the other NCC functional areas such as NM, NS, and NA. CS also provides a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, and repair service support. It also routes problems it cannot handle to other NCC functional areas, to the Defense Mega Center (DMC) or, if necessary, to other technical support agencies such as Defense Information Systems Agency and Air Force Space Command Network Operations and Security Center (AFSPC NOSC). CS determines the type of reported system problem, reports the status of problem resolution to the affected customer's WM or FSA, and maintains a historical database of problem resolution.

2.8. Plans and Programs. The Plans and Programs office is responsible for managing new communications requirements and service requests for the 341st Communications Squadron. All communications service actions, no matter how small, should be requested through the use of an AF Form 3215. Common service requests are new Local Area Network (LAN) drops, telephone installations, and communications technical solutions. Each AF Form 3215 will contain an accurate description of the work desired, mission essential justification and signature. Drawings or floor plans should be included as attachments to ensure effective processing of your requirement. The appropriate personnel must sign all AF Forms 3215. All 3215s will be returned if there is not a proper signature.

2.9. Automated Data Processing Equipment (ADPE). ADPE is responsible for the management of the base's computer systems and equipment. This management involves accountability, issuing, transferring, and processing equipment for DRMO or donation to schools. The ADPE section receives assistance in this area from Equipment Custodians. Equipment Custodians are appointed to manage their units' assigned equipment. In addition, the ADPE section is responsible for the training of all appointed Equipment Custodians.

2.10. Commanders. The commander is ultimately responsible for the management of their computer support program within their unit. Other wing personnel pertinent to ensuring quality computer support are the Group Computer Managers (GCM), Organizational Computer Managers (OCM), FSAs, WMs, and the computer users. The GCM, OCM, FSA, and WM positions must be appointed in writing with a primary and alternate indicated; at least one of these individuals must be available at all times. If one of these individuals separates, PCAs, or PCSs, a new appointment letter must be submitted indicating the replacement.

2.11. Group Computer Manager (GCM). The GCM is appointed by the group commander to assist in the performance of the commander's computer support program. The GCM is the group-level POC for the NCC and Wing IA. As a minimum, the GCM is responsible for the implementation and dissemination of computer related issues. The GCM is responsible for retaining a list of the OCM, FSA, and WM appointees within their group. The GCM is responsible for ensuring all unit-level OCM, FSA, and WM appointment letters are current. In addition, the GCM will provide a copy of the appointment letters to both Wing IA and the NCC.

2.12. Organizational Computer Manager (OCM). The squadron or unit level commander appoints the OCM in writing. OCMs take policy, guidance, and implementation direction from the GCM. OCMs coordinate all computer and associated equipment purchases for their unit and submits the required documentation to the Communications Squadron for approval. OCMs are responsible for ensuring system accreditations are accomplished for their units systems (i.e., laptops, standalones, unique systems, etc.). The OCM is responsible for ensuring its organization's FSA and WM appointment letters are current and are forwarded to the associated GCM. We don't recommend appointing a WM as an OCM due to a WM's typical workload (which typically includes Information Manager functions).

2.13. Computer Systems Security Officer (CSSO). The CSSO manages the COMPUSEC Program for an information system. CSSOs monitor information system activities to ensure system integrity; establish reaction and maintenance controls for the facility; and perform system access or revocation tasks. CSSOs continually identify threats, deficiencies, and associated countermeasures. CSSOs measure and report incidents. CSSOs ensure that the information system is operated, maintained, and disposed of according to security policies and practices.

2.14. Functional System Administrator (FSA). The squadron or unit-level commander appoints the FSA in writing. The FSA is responsible for a specific system (e.g., PC3, CMOS, SBSS, CAMs, etc.). FSAs are the focal point for the Certification and Accreditation (C&A) of their system and are also responsible for the security and support of that system. FSAs take direction from the OCM and/or NCC. They must thoroughly understand the customer's mission, and stay completely knowledgeable of the hardware and software capabilities and limitations. FSAs ensure the servers, workstations, peripherals, communication devices, and software are on-line and available to support the customers of their system. FSAs contact CS as necessary if they cannot resolve a problem. The FSA assumes the responsibilities of the CSSO for the applicable system. If the FSA cannot perform the CSSO duties, an alternate FSA can be appointed to fulfill this responsibility. Consult 33-202 for CSSO responsibilities. FSAs are required to complete training as required by AFI 33-115, Vol 2.

2.15. Workgroup Manager (WM). The squadron or unit level commander appoints the WM in writing. It is the responsibility of WMs to resolve day-to-day administrative and technical system problems that computer users experience. For this reason, WMs should possess knowledge of hardware, software, and communications principles, such as the installation, configuration, and operation of client/server devices. In the event they cannot resolve a problem, they should contact CS for assistance. The WM should be a 3A0X1 (Information Manager). When an Information Manager is not assigned, any AFSC or occupational series can perform the duties of a WM, once trained and certified. In order to provide quality support for the unit, it is recommended that a WM not be responsible for more than 30 to 40 workstations. WMs are required to complete training as required by AFI 33-115, Vol 2. For additional information about WM responsibilities, consult AFI 33-115, Vol 2, Licensing Network Users and Certifying Network Professionals.

2.16. Computer User. Computer users must comply with all computer policies in the course of their duties. Prior to receiving network access each user must be trained in proper security procedures IAW AFI 33-204, Information Protection Security Awareness, Training and Education (SATE) and AFI 33-115v2, Licensing Network Users and Certifying Network Professionals. For assistance with computer-related issues or problems, the computer user must contact their unit's WM or FSA. Computer users will not contact the NCC for assistance.

3. Computer Security (COMPUSEC).

3.1. Computer Compliance Messages.

3.1.1. The NCC will post computer compliance messages in the GCM/OCM/FSA/WM public e-mail folder along with required fix actions, suspense, and compliance/non-compliance reporting instructions (see **Attachment 2** for sample e-mail). The NCC will also send applicable GCMs an e-mail notifying them of the compliance message. GCMs will send an e-mail back to the NCC acknowledging they received notification of the compliance message. The GCM will e-mail the NCC when their group or unit is compliant. If the GCM's group or unit can't complete compliance actions by the suspense date, they will e-mail the NCC stating their non-compliance.

3.1.2. Computer security advisory messages will be posted in the GCM/OCM/FSA/WM public e-mail folder. GCMs, FSAs and WMs will ensure compliance and stay apprised of all new advisories.

3.1.3. Local administrators for remotely controlled systems, not part of the base network, should contact the remote administrators of these systems to obtain compliance status. Systems under the jurisdiction of the NCC will comply as directed.

3.1.4. All changes to information systems, including security patches, must be approved by the DAA before implementation. The NCC and/or Wing IA may implement AFCERT directed security patches without prior DAA approval if both offices concur.

3.1.5. Wing IA will obtain and disseminate anti-virus software and updates. Wing IA will centrally manage automatic updating of all LAN workstations. FSAs and WMs will ensure systems not automatically updated are updated manually. Additionally, FSAs and WMs will ensure that those machines that should be updated automatically are being updated properly.

3.1.6. Users will report all virus activity to WMs who will in turn report to Wing IA.

3.1.7. Unit commanders are the Designated Approving Authority (DAA) for non-Top Secret systems in their unit. It is the duty of the DAA to approve or disapprove the use of a particular system on Malmstrom AFB.

3.1.7.1. Air Force policy dictates that all Air Force systems must be accredited before put into use. The system may be "turned on" for testing purposes only before acquiring an accreditation approval.

3.1.7.2. Unit CC's will ensure all systems are accredited before going operational. Unit CC's will appoint in writing a certifying official to create the C&A package. Wing IA is the central POC for accreditations. Wing IA will assist the certifying official and make recommendations to the DAAs.

3.1.7.3. OCMs will review accreditation packages annually and recertify every 3 years for systems such as laptops, standalones, unique systems, etc.

3.1.7.4. No system will be connected to the base network without an approved accreditation and written approval from the DAA. If an unaccredited system is found connected to the base network it will be disconnected immediately.

3.1.7.5. OCMs will create a list of all systems in their unit annually. One copy will be kept with the OCM and a copy will be forwarded to and kept by Wing IA.

3.1.7.6. No changes to the system will be made without approval of the DAA and appropriate updates to the affected accreditations.

3.1.7.7. When a new system requirement is identified, the certifying official will contact Wing IA for direction on creating a package for the new system.

3.1.7.8. C&A packages will be submitted to Wing IA for review before being sent to the DAA for approval. Wing IA will advise DAAs in all C&A matters.

3.1.8. All hardware and/or software that allow user access or affects security features of a system must be approved in writing before installation.

3.1.8.1. Personally owned hardware and/or software may not be used on any government-owned system without written consent from the DAA. Contact Wing IA for assistance.

3.1.8.2. Government-owned hardware and/or software may not be used on any privately owned system without written consent from the DAA. Exceptions to this are Norton Anti-virus, McAffee Virus Shield, and JetForm FormFlow. Contact Wing IA for assistance.

3.1.9. Data Contamination:

UNCLASSIFIED SYSTEM + CLASSIFIED DISK = CLASSIFIED SYSTEM & CLASSIFIED DISK

CLASSIFIED SYSTEM + UNCLASSIFIED DISK = CLASSIFIED SYSTEM & CLASSIFIED DISK

3.1.9.1. All DoD computer systems and networks are approved to process at a specified level of sensitivity. If information at a higher level of sensitivity is introduced, the system becomes contaminated.

3.1.9.2. All removable media must be marked with the appropriate classification level, to include unclassified (i.e., unclassified, Confidential, Secret, Top Secret.).

3.1.9.3. All classified systems must be marked with the appropriate classification level.

3.1.9.4. Any media introduced into a classified system with a higher classification level than the media automatically becomes classified at that system's level and must be treated as such.

3.1.9.5. Classified media introduced into any system with a lower classification level will classify that system to the same level as the classified media.

3.1.9.6. In the event of data contamination, stop work immediately and safeguard system appropriately. If possible, physically isolate the contaminated systems to prevent further contamination and report immediately to Wing IA and the Unit Security Manager. The system must be disconnected from all external connections (LAN drops, etc.). Wing IA and NCC will assist in the declassification of all affected systems.

3.1.9.7. File deletion and/or disk formatting are not approved methods of declassification. Contact Wing IA for assistance. Wing IA and NCC will ensure procedures and appropriate software exist to declassify systems in the event of data contamination.

3.1.9.8. Auto-forwarding of e-mail messages to off base commercial accounts (non-DoD accounts) is prohibited to all Malmstrom AFB network users. This policy is in effect in accordance with AFI 33-119, Electronic Mail (e-mail) Management, which defines the need to safeguard the information maintained in e-mail. There are no mechanisms to stop potentially sensitive or classified information from leaving controlled DoD networks when auto-forwarding e-mail to commercial accounts.

3.1.10. Wing IA will maintain declassification procedures and software to assist the user in classified media destruction.

3.1.11. WMs/FSAs will ensure systems are appropriately declassified before turn-in for reuse or deposition.

3.1.12. Password authorization is the first line of defense against unauthorized access to the network. The Computer Emergency Response Team estimates that 80% of all network security problems are created by bad passwords. Users must take their responsibility to provide secure, unique passwords seriously. IAW AFM 33-223, Identification and Authentication, passwords must remain in the sole possession of the user, and must not be shared with any other users. Passwords must be at least eight characters long, consist of at least one number, one capital letter, one lowercase letter, and one special character. Passwords will not be easy to guess. Do not use names, places, dates, any word from a dictionary, foreign words or words spelled in reverse. Per AFSSI 5027, programs will periodically be run to check the strength of user passwords. The network administrator will assign an initial password, which the user must change on the first use. Network administrators will not issue passwords without positive identification of the authorized user. User passwords will be protected as sensitive (FOUO) and will expire every 90 days. User accounts will be disabled after three consecutive failed logon attempts. Users must memorize their password. Do not place passwords on desks, walls, sides of terminals, or store them in a function key, login script, or the communications software. If documentation is necessary for mission accomplishment (i.e., pre-established accounts for contingency or exercise), place the password in a safe. If an authorized user suspects their password has been compromised, notify the CSSO and change the password immediately. Failure to comply with this password policy will result in the following:

3.1.12.1. The first time a user's password is cracked the NCC will modify the user's network account to require a password change at the next logon.

3.1.12.2. The second time a user's password is cracked the NCC will lock the user's network account. The user's account will remain locked until the NCC receives a letter signed by the user's unit commander. The letter must state the user's unit commander authorizes them access to the base network and the offender has re-accomplished SATE training.

3.1.12.3. The third time a user's password is cracked the NCC will lock the user's network account. The user's account will remain locked until the NCC receives a letter signed by the user's group commander. The letter must state the user's group commander authorizes them access to the base network and the offender has re-accomplished SATE training.

3.1.12.4. The fourth time a password is cracked the NCC will lock the user's network account. The user's account will remain locked until the NCC receives a letter signed by the wing commander. The letter must state the wing commander authorizes them access to the base network and the offender has re-accomplished SATE training.

3.2. Emissions Security (EMSEC).

3.2.1. Unit commanders will identify all electronic devices and systems processing classified information and provide a list to Wing IA each April.

3.2.2. Unit commanders will ensure that all electronic devices and systems processing classified information are identified to Wing IA for an EMSEC assessment before made operational.

3.2.3. The Wing EMSEC Manager will then conduct a hands-on inspection of the classified equipment and the area surrounding the classified equipment for compliance with AFI 33-203, AFSSM 7011, and AFSSI 7010.

3.2.4. Facility changes will be identified to Wing IA before implemented to ensure EMSEC requirements continue to be met.

3.2.5. FSAs for classified system will ensure that no modifications to system equipment or physical location are made without prior approval from Wing IA.

3.3. Security Awareness Training and Education (SATE).

3.3.1. All users of government-owned telecommunications systems, i.e. radios, pagers, cell phones, computers, fax machines, etc., will receive security training to ensure data integrity, confidentiality, and availability.

3.3.2. Wing IA will conduct all initial training.

3.3.3. FSAs will ensure users of their systems have received SATE training before granting users access.

3.3.4. All users will receive annual recurring training.

3.3.5. WMs will ensure all users have completed required SATE training for network access.

3.3.6. WMs will track, by month, total number of users receiving recurring SATE training. OCMs will consolidate their unit's SATE training status and provide a monthly report to Wing IA.

3.4. Certification and Accreditation.

3.4.1. The base network is accredited IAW AFPD 33-2, Information Protection. Accreditation is the formal written declaration by the Designated Approving Authority (DAA) that a particular system is approved to operate in a given mode, against stated residual risks, with stated countermeasures. The DAA formally accepts responsibility for the operation of the system and personal liability and accountability. Due to the size of the base network, organizational LANs are accredited individually. Consult AFSSI 5024, Volumes I and II, The Certification and Accreditation (C&A) Process and The Certifying Official's Handbook, for more information on the accreditation process.

3.4.2. Documentation consists of a completed System Security Authorization Agreement (SSAA). The SSAA is maintained by the CSSO and stays with the system. Forward a copy of all SSAAs to the Wing IA office.

3.4.3. Reaccredit every 3 years or upon significant changes to hardware, software, or environment. The SSAA is a living document where changes and updates are constantly occurring. An accreditation package is not to be left in a file and completely re-accomplished every 3 years. Most changes to the system will only require an update of a page within the SSAA. If a major change occurs, the bulk of the agreement is re-usable in a reaccredidation.

4. Network Control Center (NCC).

4.1. Customer Service Procedures.

4.1.1. All computer network users' requests for support or assistance will be directed to their respective WM, FSA or OCM. If the WM, FSA or OCM is unable to resolve the problem, the NCC will be contacted for assistance. Only WMs, FSAs, OCMs, or GCMs may contact the NCC directly for assistance. The only exception to this is NCC customer walk-in service.

4.1.2. The NCC Customer Service office is open for walk-in service daily, except weekends and holidays, during posted walk-in service hours. Walk-in service is defined as customers dropping off network access request forms, picking up completed network access request forms and establishing new network passwords. All other customer needs will be handled by his or her respective WM, FSA or OCM.

4.1.3. All computer network users' requests for after duty hours support or assistance will be directed to their respective WM or FSA. NCC personnel provide after-duty hour emergency support on a stand-by basis. If a WM or FSA contacts the NCC for after-duty hour emergency support, NCC stand-by personnel will be notified in accordance with local policy.

4.2. User Network Account Management.

4.2.1. Users who have locked out their network account due to entering their password incorrectly three consecutive times will contact their WM or FSA to have it reset. In turn, if the WM or FSA can't reset the user's network account they will contact the NCC for assistance.

4.2.2. Users who need to change their password because they've forgotten it or it isn't working need to contact their WM or FSA for assistance. Users may also come to the NCC Customer Service office during walk-in hours with their military identification card. Customer service personnel will verify your identification and will assist you with changing your password.

4.3. Preventive Maintenance (PM).

4.3.1. PM will be performed on an as needed basis. PM will be scheduled after duty hours, when feasible. The NCC will schedule PM at least 5 duty days prior to PM to be conducted.

4.3.2. The day, hours, and type of preventative maintenance to be conducted will be in the PM notification, which will be posted in the Distro F, Distro G, and GCM/OCM/FSA/WM public e-mail folders.

4.3.3. Preventative maintenance will cause some or all network services to be unavailable during the maintenance period, depending on the type of PM being performed.

4.4. System Management Server (SMS).

4.4.1. SMS is a software application the NCC uses to remotely distribute software updates and provide remote client workstation troubleshooting. The NCC will not support a client workstation that doesn't have the SMS client software loaded.

4.4.2. All WMs will ensure their users' Windows NT client workstations have Domain Administration in the local administrator's group. This will allow SMS to automatically detect if the SMS client software is present or not. If SMS detects the SMS client software isn't installed, it will automatically install the necessary software.

4.5. Wing Share Drive.

4.5.1. The wing share drive, named SHARE-10DAYS, is for temporary sharing of files. No files are allowed to remain in the SHARE-10DAYS folder for more than 10 days. NA will delete files older than 10 days.

4.5.2. If you require long term file sharing, please contact your WM with a written request. Your WM will submit an AF Form 3215 to the NCC. The 3215 will include the rank/name of individuals requiring access, type of access needed (read, read/write, etc.), and length of time the share will be needed. The NCC can then create a shared folder for the requesting user.

4.6. Network Shares.

4.6.1. File sharing on computer systems other than network servers is strictly prohibited. Users requesting to share files on the network must send the request through their WM. WMs will submit an AF Form 3215 to the NCC. The 3215 will include the rank/name of individuals requiring access, type of access needed (read, read/write, etc), and length of time the share will be needed. The NCC can then create a shared folder for the requesting user.

4.6.2. If printers are shared on the network they must be shared on a Windows NT/2000 computer system. Printer sharing on a Windows 95 computer system is prohibited. A Windows NT/2000 computer system must be accredited as a print server before the computer can be setup to share a printer. The Wing Information Assurance Office can help users with print server accreditations.

4.7. Network Printing.

4.7.1. Currently, the only NCC supported printer network card is the HP JetDirect card. This card comes standard with HP network capable printers. After the printer is connected to the network, do not use the share option when setting up the printer on a workstation.

4.7.2. If you are having a problem with the installation of a JetDirect card or network printer, please contact your WM.

4.8. E-mail Public Folders.

4.8.1. Requests for e-mail public folder requirements must be in writing. Forward the requests for e-mail public folders to your WM. WMs will submit an AF Form 3215 to the NCC.

4.8.2. E-mail public folders are For Official Use Only and may not be used to share personal or privacy act information.

4.9. Network User Policy.

4.9.1. All network users must comply with network policies. Failure to comply with network policies will result in the following actions:

4.9.2. The first time a user fails to comply with network policies, the NCC will lock the user's network account. The user's account will remain locked until the NCC receives a letter signed by the user's unit commander. The letter must state the user's unit commander authorizes them access to the base network and the offender has re-accomplished SATE training.

4.9.3. The second time a user fails to comply with network policies, the NCC will lock the user's network account. The user's account will remain locked until the NCC receives a letter signed by the user's group commander. The letter must state the user's group commander authorizes them access to the base network and the offender has re-accomplished SATE training.

4.9.4. The third time a user fails to comply with network policies, the NCC will lock the user's network account. The user's account will remain locked until the NCC receives a letter signed by the wing commander. The letter must state the wing commander authorizes them access to the base network and the offender has re-accomplished SATE training.

4.10. Web Administration.

4.10.1. All units are encouraged to develop a web page. Units are responsible for developing and maintaining their web page. A unit Webmaster will be appointed, in writing, by their unit commander. All unit Webmasters will be a 3A0X1 because this function is an official part of their career field. A copy of the appointment letter will be forwarded to the Wing Information Manager's Program Management Office.

4.10.2. All new Internet (external) pages must be accompanied by a Space Command Form 12 and approved by Public Affairs prior to being submitted to the Base Webmaster for posting. Submit an AF Form 3215 to the Base Webmaster for all requests to post a new Internet page or pre-authorized updates to existing Internet pages.

4.10.3. All new Intranet (internal) pages require approval by the Base Webmaster. To request approval from the Base Webmaster, submit an AF Form 3215 to the Base Webmaster. The unit Webmaster may post updates to Intranet pages, if security permissions have been granted. If not, submit an AF Form 3215 to the Base Webmaster.

4.11. Network Security.

4.11.1. Use only AF/SC approved IP tools. These tools are operated by the NCC and in some cases, WMs and FSAs. These tools perform numerous security functions including boundary protection, viral detection, configuration inspection, network mapping, remote patching, vulnerability testing, etc. They are used to protect information systems and to measure the security posture of information systems.

4.11.2. Because of the intrusiveness of some IP tools and the sensitivity of the information that may be observed during IP operations, only MAJCOM, IWS, NCC, Commanders, AFIWC and AFOSI designated personnel are authorized to use intrusive IP tools. The procedures and guidelines for using and interpreting the IP tools are outlined in AFSSI 5009, Information Protection Interim Toolset. The tools will be used periodically to scan all information systems connected to the base network. If a system is found to be vulnerable it must be fixed and then rescanned. If the system is still vulnerable after another scan it will be disconnected from the base network, and the controlling commander will be notified of the discrepancy. Only after coordination with the NCC will the system be reconnected to the network for another scan.

4.11.3. Standard Air Force systems (i.e., SBSS, DEERS/RAPIDS, Sentinel Key, etc.) usually require outside connectivity to other systems on other bases. This cannot happen unless the firewall is configured to allow the appropriate protocols, ports, and IP addresses. See MAFBI 33-203, Network Security Policy, for an explanation of protocols, ports, and IP addresses.

4.11.4. A memorandum must be created and signed by the WM and unit commander before performing changes to the firewall. In addition, a complete accreditation package must be on file with Wing IA before configuring the firewall. Contact Network Security for the current format, or go to the Intranet web page and download it.

4.12. Automated Data Processing Equipment (ADPE).

4.12.1. The appropriate Equipment Custodian (EC) will handle all Automated Data Processing Equipment (ADPE) requirements. This includes the transfer, inventory, turn-in, excess equipment, and receipt of ADP equipment. All other computer related requirements (i.e. picking up software or other computer items) will be handled by the unit's OCM. These requirements will be handled during the ADPE section walk-in customer service hours.

4.12.2. All small computer purchases must be coordinated through your OCM and approved by the 341CS Small Computer Manager. Small computer purchases include all peripheral equipment (i.e. zip drives, printers, CD-ROM drives, scanners, etc.), storage media (i.e. diskettes, zip disks, CD-ROMs, etc.), and software. Blank media does not require prior approval to purchase. OCMs will submit an AF Form 3215, or local form, for all small computer purchases to the Small Computer Manager for a technical solution and/or approval. No small computer purchase may take place until formally approved by the 341CS Small Computer Manager. In addition, all IMPAC purchases of computer equipment and software must use the 341CS Small Computer IMPAC Form.

4.12.3. Processing of excess equipment will follow the guidelines in AFI 33-112, Computer System Management and AFSPC SUP 1 to AFI 33-112. The following are additions to the process.

4.12.3.1. An excess equipment letter must be generated and forwarded to the ADPE section for processing. See ADPE Handbook for sample letter. The EC needs to follow up with the ECO to determine if the excess equipment has been granted a release date. Once the equipment has a release date it is the ECs responsibility to make arrangements for delivery to DRMO. The EC will then notify the ECO to ensure turn-in paperwork (1348-1) is generated.

4.12.3.2. Copies of the signed paperwork by DRMO must be returned to the ADPE section so the equipment can be removed from the ECs account.

4.12.4. Duties and responsibilities will follow the ones stated in AFI 33-112 and AFSPC SUP 1 and the Equipment Custodian Handbook.

4.12.5. When new equipment is received the appropriate EC will be contacted. The EC will then come to the ADPE section during customer service hours and sign for the equipment. The EC then maintains copy of the signed receipt with their inventory until a new inventory is requested and the new equipment is on it.

4.12.6. New computer systems must meet accreditation guidelines IAW Air Force Instructions before being issued. Contact Wing IA for assistance.

4.12.7. The following are the requirements to ensure ADPE accounts are in good standing:

4.12.7.1. ADPE inventory must be accomplished on an annual basis or more frequently.

4.12.7.2. Update ADPE Appointment letter annually or as needed.

4.12.7.3. Complete ADPE training annually.

4.12.7.4. These requirements are identified in an ADPE policy letter signed by the 341 CS/CC and are located in the Equipment Custodian Handbook.

4.12.8. Accounts not in good standing may become frozen. This means the account will not be able to process any ADPE requirement i.e. transfer, turn-in, purchase or sign for any equipment. Once an account becomes frozen it will remain frozen until all delinquent items are updated.

THOMAS F. DEPPE, Col, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 31-101, *The Air Force Installation Security Program*, 1 Dec 99

AFI 31-401, *Information Security Program Management*, 1 Jan 99

AFI 33-112, *Computer Systems Management*, 1 Dec 97

AFI 33-114, *Software Management*, 1 Jul 00

AFI 33-115v1, *Network Management*, 2 Jul 99

AFI 33-115v2, *Licensing Network Users and Certifying Network Professionals*, 1 Nov 99

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, 1 Mar 99

AFI 33-129, *Transmission of Information Via the Internet*, 1 Aug 99

AFI 33-202, *Computer Security*, 1 Feb 99

AFI 33-204, *Information Protection Security Awareness, Education and Training Program*, 26 Apr 99

AFI 33-208 (Draft), *Information Protection Operations*, 1 May 97

AFMAN 10-401v1, *Operation Plan and Concept Plan Development and Implementation*, 1 May 98

AFMAN 33-223, *Identification and Authentication*, 1 Jul 98

AFMAN 33-229, *Controlled Access Protection*, 1 Nov 97

AFPD 33-2, *Information Protection*, 1 Dec 96

AFSSI 4100v1, *The Air Force Communications Security (COMSEC) Program* (future AFI 33-201), 1 Aug 98

AFSSI 5009, *Information Protection Interim Toolset,* 30 Jan 98

AFSSI 5020, *Remanence Security*, 20 Aug 96 (future AFMAN 33-224)

AFSSI 5021, *Vulnerability and Incident Reporting*, 15 Aug 96

AFSSI 5024v1, *The Certification and Accreditation (C&A) Process*, 1 Sep 97

AFSSI 5024v2, *The Certifying Official's Handbook*, 1 Sep 97

AFSSI 5027, *Network Security Policy*, 27 Feb 98

Abbreviations and Acronyms

ACL—Access Control List

ADPE—Automated Data Processing Equipment

AFIWC—Air Force Information Warfare Center

AFOSI-—Air Force Office of Special Investigations

ASCAS-—Automated Security Clearance Approval System

BGP-—Border Gateway Protocol

CAP-—Controlled Access Protection

CCB-—Configuration Control Board

CSSO-—Computer System Security Officer

DAA-—Designated Approving Authority

DAC-—Discretionary Access Control

DNS-—Domain Name System

FSA-—Functional System Administrator

FTP-—File Transfer Protocol

GCM-—Group Computer Manager

GPS-—Global Position System

HTTP-—HyperText Transfer Protocol

I & A-—Identification & Authentication

ICMP-—Internet Control Message Protocol

IGRP-—Internet Gateway Routing Protocol

IPO-—Information Protection Operator

IRC-—Internet Relay Chat

ISO-—International Standards Organization

IWS-—Information Warfare Squadron

LAN-—Local Area Network

MBONE-—Multicast Backbone

MTA-—Message Transfer Agent

NAC-—National Agency Check

NCC—Network Control Center

NFS-—Network File System

NIS/YP-—Network Information System/Yellow Pages

NNTP-—Network News Transport Protocol

NOSC-—Network Operations and Security Center

NTP-—Network Time Protocol

OCM-—Organizational Computer Manager

OSI-—Open Systems Interconnection

OSPF-—Open Shortest Path First

RIP-—Routing Information Protocol

SMTP-—Simple Mail Transfer Protocol

SNMP-—Simple Network Management Protocol

SSAA-—System Security Authorization Agreement

SunRPC-—Sun Remote Procedure Call

TFTP—Trivial File Transfer Protocol

WAIS-—Wide Area Information Servers

WM-—Workgroup Manager

WWW-—World Wide Web

Y2K-—Year 2000

Attachment 2

AFCERT COMPLIANCE MESSAGE (ACM) ALERT

SUSPENSE DATE:

NOSC NOTAM XX-XX

Advisory Message

Fix Action

Compliance Criteria

To report compliance within your group, send an e-mail message to the "CS Help" mailbox containing the following information:

Your name, e-mail address, and phone number
Your group
The following statement:

I acknowledge that all systems within the XXX Group have been fixed in compliance with NOSC NOTAM XX-XX. All systems within the XXX Group have been checked individually to ensure compliance.

To report non-compliance within your group, send an e-mail message to "CS Help" indicating the number or percentage of systems completed and not completed. Indicate the reason for non-compliance as well as an estimated time and date of completion.