



**COMMUNICATIONS SYSTEM
SECURITY POLICY AND
OPERATING GUIDELINES**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the internet at the following location
<http://www.4asog.usafe.af.mil/publications.htm>

OPR: 4 ASOG/LG (MSgt Franklin J. Valerio)

Certified by: 4 ASOG /CC (Col Curry)

Pages: 15

Distribution: F

This instruction establishes operational system security policy for the 4th Air Support Operations Group (4 ASOG) processing of unclassified, sensitive, or classified information and requirements for functional local area networks (LANs), telephones, personal wireless communications and security containers. Unclassified and sensitive information will be processed on the portion of the ARMY Unclassified-LAN and or Air Force Unclassified-LAN, which throughout this document will be addressed as the NIPRNET (Non-secure Internet Protocol Network), as applicable. Sensitive information is defined as any information, which the loss, misuse, unauthorized access to or modification of, could adversely affect the national interest or conduct of Federal programs. This information could also affect the privacy individuals are entitled to under the Privacy Act but has not been specifically authorized to be secret by an Executive Order or Act of Congress. Information classified up to the SECRET level may be processed on that portion of the ARMY Secret-LAN or Air Force Secret-LAN, addressed throughout this document as SIPRNET (Secure Internet Protocol Network), as applicable. It specifies the minimum-security measures required to ensure availability, integrity, confidentiality, and accountability of information and resources directly connected to or remotely accessed on the network. (NOTE: The term LAN will be used throughout this document when addressing both NIPRNET & SIPRNET systems.)

References: AFSSI 5027, The Air Force Network Security Policy, and AFI 33-202, Computer Security and USAFESUP1, AFI 33-112, AFI 33-115V2, AFI 33-115V1 Communications and Information, Computer Security, AFI 33-106, AFI 33-106 USAFE Supp 1, Army Manual 25-1, 380-19, 380-53, USAREUR Pamphlet 25-25.

Chapter 1 Duty Titles and Responsibilities

Applicability and Scope.....	3
Communication Operations Organizational Structure.....	3
Roles and Responsibilities.....	3
Designated Approval Authority.....	3
Squadron Commanders.....	3
DAA Representative.....	4

Certifying Official.....	4
Unit Information Assurance Manager.....	4
Wing Information Assurance Office.....	4
System Administrator.....	4
Work Group Managers and Information Management Officers	5
Granting Access to Network.....	5
Network Users	6

Chapter 2 Network Policies and Procedure

Modems.....	7
Malicious Logic.....	7
Unauthorized Software.....	7
Use of Government Software.....	7
File Server Back-up.....	7
Permissible Internet and E-mail Actions.....	7
Prohibited Internet and E-mail Actions.....	8
Suspension of Network Privileges.....	10
Anti-Virus Software.....	10
Automated Data Processing Equipment and Property Book Inventory.....	10
Personally Owned Computers.....	11
Personal Digital Assistants (PDA)	11
Prohibited PDA Actions.....	11
Personally Owned PDA.....	12
Replacement of Automated Data Processing Equipment	12
Physical Security.....	12
Entry Controls to Computer Facilities.....	12
Entry to Controls to Remote Terminals.....	12
Physical Resource Protection.....	13
Non-removable Magnetic Media.....	13
Operating Systems.....	13
Emission Security.....	13
DAA Accreditation Requirements.....	13
Reaccreditation.....	13
Conclusion.....	13
Appendix A Glossary of Abbreviations and Acronyms.....	15

Chapter 1

DUTIES AND RESPONSIBILITIES

1.1 Applicability and Scope.

1.1.1 The policy applies to all 4 ASOG computer users, organizations and subordinate units that utilize Army or Air Force computer systems. This policy also applies to all Work Group Managers (WGM), Information Management Officers (IMO) and System Administrators (SA). This is a group-specific document to meet the 4 ASOG's network security requirements. This security policy will not be changed without the approval of the designated approval authority (DAA). Conflict between requirements interpretation in this policy and higher-level requirements will be brought to the attention of the 4 ASOG DAA and Unit Information Assurance Manager (UIAM). When a conflict exists, the UIAM will notify the DAA and enforce the more stringent interpretation until the area of conflict is resolved and recommended action is documented.

1.1.2 Communication Operations Organizational Structure

1.1.2.1 The structure is designed to align squadron detachment WGMs or IMOs under the squadron WGMs or IMOs and to align group detachment IMOs under 4ASOG/LG.

1.1.2.2 SAs exist where computer systems connect to Air Force domain. In those cases the SAs receive technical guidance from 86 Airlift Information Assurance Office (786 CS/SCBI) located at Ramstein AFB.

1.1.2.3 4 ASOG/LG will work communication policies and processes for the group and act as the liaison between 4ASOG, 3AF, and USAFE.

1.2 Roles and Responsibilities.

1.2.1 Designated Approval Authority (DAA). IAW AFI 33-202 and USAFESUP1, Computer Security, the DAA for the 4 ASOG is the 4 ASOG/CC. This applies to units which connect to Air Force systems. The DAA is responsible for reviewing the results of the risk analysis and certification documents presented by the certification official and determining whether the residual risk is sufficiently low to accredit the system/network for operational use. The DAA is responsible for the Air Force network infrastructure, including all workstations and network devices owned by tenant and subordinate units that are geographically separated (GSU). The DAA ensures that the systems meet Department of Defense (DoD), Air Force, and HQ USAFE/SC security requirements. The DAA certifies that configuration and installed applications are in compliance with the USAFE network type accreditation and Certificates to Operate.

1.3 Squadron Commanders will:

1.3.1 Appoint a primary and alternate WGM or IMO.

1.3.2 Appoint a primary and alternate Unit Information Assurance Manager (UIAM). For units connected to Army systems the primary UIAM will be the group UIAM.

1.3.3 Appoint a primary and alternate Computer Equipment Custodian (EC) and Property Book (Pbook) Custodian for Army property. This position requires appointment no later than 45 days before the departure of the present EC. Alternates can serve as primary during overlap period.

1.3.4 Appoint a primary and alternate Telephone Control Officer (TCO). Squadron TCOs can be assigned to manage their detachments.

1.3.5 Ensure newly assigned personnel complete appropriate training before granting access to Army or Air Force systems see para 1.10.1 and 1.10.2 for details.

1.4 DAA Representative. The DAA representative is responsible for the day-to-day network operations. He should remain active in all communications planning and approval process. The 4 ASOG/CD will serve as the DAA representative.

1.5 Certifying Official. The certifying official works on behalf of the DAA and develops the System Level Security Authorization Agreement (SSAA) or network system accreditation. The certification official will provide the DAA with a recommendation for or against accreditation and operational limitations. The certification official documents any security deficiencies in the SSAA submitted to the DAA. The 4 ASOG/LG serves as the Certifying Official.

1.6 Unit Information Assurance Manager (UIAM). UIAMs administer unit-level Information Assurance (IA) programs in Computer Security (COMPUSEC), Emission Security (EMSEC), Telecommunications Monitoring and Assessment Program (TMAP), Certification and Accreditation (C&A), and Information Assurance Awareness Program (IAAP). UIAMs serve as liaisons between the unit and the Wing IA office for the IA programs listed above. An appointment letter will be submitted to 86 Wing IA office for this duty. Each Squadron will appoint personnel in the Air Force Specialty Codes 3AXXX or 3CXXX for this position when available.

1.7 Wing Information Assurance (IA) Office. The 86 Wing IA office personnel oversee the implementation of information protection policy and guidance. They establish, review, and coordinate security requirements for the 4 ASOG. They also serve as the local expert and advisor to the DAA, DAA representative, certifying officials, UIAMs, and others involved in the 4 ASOG system security policy formulation.

1.8 System Administrators (SA). Currently units that have SAs are 4 ASOS, 2 ASOS and 2 ASOS Det 2. SAs are responsible for maintaining the primary domain controller (PDC). SAs are responsible for proper PDC configuration and back-up of operating system and data. SAs are responsible for reviewing audit trails on PDC. The audit trails will be reviewed and documented daily for the following areas security, systems, and applications. SAs must subscribe to Time Compliance Network Orders (TCNO). Compliance must be accomplished by the SA IAW the suspense date. To subscribe for TCNO SA must request UIAM training from Wing IA Office at:

wingia@ramstein.af.mil. SA's will report completion of TCNO to their Network Control Center. SAs will adhere only to technical guidance from 86 Airlift Information Assurance Office. Depending on unit manning level SAs may also be tasked with Work Group Mangers duties.

1.9 Work Group Managers & Information Management Officers (WGM & IMO) Responsibilities.

1.9.1 WGMs and IMOs perform similar duties. WGM is the Air Force term and IMO is the Army term this position. When possible WGM or IMO duties and responsibilities should be assigned to personnel with the 3AOX1 AFSC. WGMs or IMOs assist in directing the security program for terminal areas and remote terminals that are part of or access the system. Each WGM or IMO will ensure established security procedures are followed; report security vulnerabilities, incidents, and problems to the UIAM, CSSO, NCC or NOC; and ensure all users in their terminal area receive initial and recurring computer security training. WGMs or IMO's will also serve as the liaison for the following:

1.9.1.1 WGM's will be the liaison between Air Force Network Control Centers (NCCs), and the end users for technical assistance.

1.9.1.2 IMO's will be the liaison between Army Network Operation Center (NOC), and the end users for technical assistance.

1.9.2 The WGMs or IMOs are responsible for making sure each computer within their area of responsibility is configured properly. This includes all of section 2.1.9 Anti-Virus Software.

1.9.3 The WGM or IMO is responsible for making sure user's SIPR and NIPR accounts are deleted or disabled once the user PCS's, PCAs, retires, or is discharged. If a user loses his security clearance, the WGM or IMO will ensure the user's SIPRNET account is disabled until the security clearance security clearance is reinstated.

1.10 Granting Access to Local Area Network.

1.10.1 WGMs ensure users of Air Force systems complete Information Assurance Awareness Program (IAAP) Computer-Based Training (CBT) before granting access to Air Force systems. (NOTE: The IAAP CBT is available at <https://wwwmil.usafe.af.mil/ramstein-ia/> then click on the IAAP link on the left side of the page. You will also need to download the CBT player.)

1.10.2 IMOs ensure users of United States Army, Europe (USAREUR) systems receive USAREUR Computer Training and License before granting access to USAREUR systems. Users will receive a copy of USAREUR Pamphlet 25-25 to study and test at <https://www.uatp.hqusareur.army.mil/>

1.10.3 WGMs and IMOs should add the above training requirements to the unit's in-processing checklist.

1.10.4 Maintain a hard copy record of IAAP or USAREUR Computer License completion for all users in the unit.

1.10.5 WGMs and IMOs ensure users complete annual Air Force IAAP training if connected to Air Force systems or USAREUR Computer Training and License if connected to Army systems. (see para 1.10.1 or 1.10.2 for details)

1.10.6 WGMs or IMOs must verify a user's security clearance with the unit's Security Manager before granting access to SIPRNET. Further, user's must read and sign an agreement form acknowledging access to a classified systems before the access is granted.

1.10.6 All users connected to SIPRNET must have a minimum U.S. Secret security clearance.

1.11 Network User.

1.11.1 All users connected to Army systems will follow local Army password policies. Users connected to Air Force systems will follow password polices in AFSSI 50-27 para 5.2.2 thru 5.29.

1.11.2 All 4 ASOG personnel will protect NIPRNET passwords as "For Official Use Only (FOUO)" and SIPRNET passwords as "SECRET".

Chapter 2

NETWORK POLICIES

2.1 Network Policies and Procedures

2.1.1 Modems. Modems may not be purchased for servers or desktops without completion of a certification and accreditation package and approval of the DAA. Strict controls must be adhered to so that established security controls are not by-passed, which can result in a successful network intrusion by our adversaries. Internal organizations will not connect external access devices (e.g., modems, fax/modems, scanner/fax/modems, etc.) to their local networks.

2.1.2 Malicious Software. Malicious software will not be installed on any file server or workstation. Malicious software includes, but is not limited to, software that is specifically designed as packet analyzers for the purpose of capturing system passwords. The only exception to this policy is for Information Protection Operations personnel in the performance of their official duties.

2.1.3 Unauthorized Software and Data. Only government-approved software is authorized on automated processing equipment. Software, including games, peer to peer software, freeware software, and shareware software are unauthorized and will not be installed on government-owned automated data processing equipment. Downloading or opening pornographic files are also strictly prohibited.

2.1.4 Use of Government Owned Software For Personal Reasons. The use of government owned software or hardware for personal projects (e.g., academic projects, professional military education (PME), Career Development Course (CDC), etc.) must be approved by a unit commander or designee. The use of commercial study materials developed for promotion testing, regardless of whether it is for Weighted Airman Promotion System (WAPS) or non-WAPS training is strictly prohibited.

2.1.5 File Server Back-ups. WGMs or IMOs are responsible for ensuring validated backups are accomplished on all managed servers on a routine basis. WGMs and IMOs are accountable for ensuring all unit maintained servers have regular and reliable system backups of the data.

2.1.6 Permissible Internet and E-mail Actions. All government communication systems and equipment (including government-owned telephones, facsimile machines, e-mail, Internet systems, and commercial systems when use is paid for by the Federal government) will be for official use and authorized purposes only. Permissible uses are defined to include all uses not prohibited by law, regulation, instruction, command, or local policy. Internet and e-mail use must not adversely affect the performance of official duties, be of reasonable duration and frequency, serve a legitimate public interest, not create any additional expense to the Air Force or Army, and does not violate any security directives.

Authorized users may use the government Internet services and e-mail for:

- Emergency communications and communications that are necessary in the interest of the Federal government.
- Morale and welfare communications while deployed for extended periods away from home on official DoD business.
- Brief communications while traveling on government business to notify family members of official transportation or schedule changes.
- Personal communications from the work center that are most reasonably made while at the work center (e.g., checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief Internet searches; E-mailing directions to visiting relatives).
- Educational work while pursuing collegiate degrees or self-improvement in the best interest of the DoD. Limited access is approved after duty hours when it does not conflict with organizational activities, and is coordinated with commander.
- Professional military education (e.g., Squadron Officer School, Senior NCO Academy) is approved after duties hours when it does not conflict with organizational activities. This does not include the Weighted Airmen Promotion System (WAPS), which is not authorized.

2.1.7 Prohibited Internet and E-mail Actions. Use of government information systems, including use of the e-mail and Internet services, is subject to monitoring, interception, accessing and recording, and may be passed to law enforcement. Any violation of this policy can result in disciplinary or administrative action. The following list is NOT inclusive but provides guidance about prohibited e-mail and Internet actions. These actions are prohibited because they increase vulnerabilities or limit the network capability provided to the war fighter. Abuse of network resources is categorized as intentional or unintentional (person did not understand consequences of their actions). NOTE: This list is not prioritized.

- Creating/sending or “auto forwarding” official E-mails from a computer connected to the base network to a commercial Internet or Internet Service Provider (ISP) E-mail account.
- Auto forwarding official e-mail messages to off-base commercial accounts (non-DoD accounts).
- Forwarding unofficial E-mails to *.ALL extensions. This action usually results in a denial of service and limits the capability of personnel to accomplish the mission.
- Sending messages with attachments larger than 10 megabytes. Special exceptions to this limitation can be made for commanders, group accounts, and mission critical requirements with written approval to the controlling NCC or NOC.
- Sending E-mail to more than 249 addresses. Users who need to send to more than 249 addresses require appropriate approval from either SAs, WGMs or IMOs.
- Accessing, sensitive, For Official Use Only (FOUO), Freedom of Information Act (FOIA), or Privacy Act protected information in violation of established security and information release policies.
- Accessing, storing, processing, displaying, distributing, transmitting, or viewing inappropriate material such as pornography, racist material, material promoting hate crimes, or material which may have adverse effect on good order and discipline.
- Visiting, participating in, or downloading files from gaming, chat or hacker sites.

- Obtaining, installing, copying, pasting, transferring or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret or license agreement.
- Obtaining, installing, copying, posting, transferring or using software obtained through other than official means.
- Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms and macro viruses.
- Promoting partisan political activity.
- Disseminating religious materials outside an established command religious program.
- The use of commercial web-based e-mail (e.g., Hotmail, AOL, COMPUSERVE, YAHOO, etc) is not authorized for official correspondence. Deployed 4 ASOG users should utilize an approved government-controlled web e-mail service (e.g., Web mail or GI-MAIL, Air Mobility Command (AMC) tool or Army Knowledge Online.).
- Data streaming applications (e.g., Real Player audio/video, PointCast, and Media Player, etc.) will be used only for official business.
- The use of chat programs (e.g., AOL Instant Messenger, ICQ, MSN Messenger, Yahoo Messenger, and Internet Relay Chat, etc.).
- The use of unofficial peer to peer network software (e.g., Napster, KazAA, Aimster, Bearshare, Morpheus, File Navigator, LimeWire, Gnutella, etc.).
- Accessing Internet data storage and/or transfer services for storage, back-ups, or to share data.
- Attempting to circumvent or defeat security or auditing systems without prior authorization or permission.
- Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.
- Modifying or altering the network operating system or system configuration without first obtaining permission from the administrator of that system.
- Using someone else's identity (user id) and password.
- Physical tampering of building communication closets or network equipment.
- Installing and using a modem in a server, computer, or laptop that is also connected to the network.
- Permitting any unauthorized individual access to the network.
- Connecting or installing a non-approved system or software package to the network.
- Any use of government-provided computer hardware or software for other than official or authorized government use.
- Sending harassing, intimidating, abusive, or offensive material that violates AF standards of behavior.
- Sending and receiving e-mail, or conducting an Internet transaction for commercial or personal financial gain (e.g. buying/trading stocks, advertising or soliciting services, sale of personal property.).
- Gambling, wagering or placing of any bets.
- Subscribing to unofficial mailing lists without commander approval.
- Downloading freeware, shareware, or beta software programs without prior approval of the DAA, DAA representative, NOC or NCC Chief.
- Violating remote access (dial-in) security procedures.
- Writing, forwarding, or participating in further propagation of chain or hoax E-mails.
- Posting personal home pages.

2.1.8 Suspension of Network Privileges. In the event a 4 ASOG user (identified by their user-id) is suspected of abusing network resources, the SA, UIAM, WGM, or IMO will validate the user-id and provide supporting documentation to the Wing IA office or Local Army NOC. Once it has been determined that the individual undeniably violated the 4 ASOG System Security Policy, access to the system will be suspended immediately.

Furthermore, SAs, WGMs, or IMOs with assistance from the NCC or Army NOC are authorized to suspend network privileges or delete accounts as required to protect the performance and integrity of the system. Once a user's access is disabled, a letter or e-mail must be forwarded from the SA, WGM, IMO, or UIAM and coordinated by the unit commander outlining actions taken to prevent recurrence and stating that IA or applicable training has been reaccomplished. This letter or e-mail must be submitted to the Wing IA or Army NOC office to reestablish access.

Failure to comply with the above policies will result in the below listed sanctions. These are the minimum actions; the scope and maliciousness of the offense could result in more severe actions. These actions can be changed by the unit commander at any time.

2.1.8.1 First Time Offender. The user's account will be locked for no less than 5 duty days.

2.1.8.2 Second Time Offender. The user's account will be locked for no less than 30 days.

2.1.8.3 Third Time Offender. The user's account will be locked/deleted for no less than 60 days. The DAA, in consultation with the unit commander, will determine if network access will be permanently revoked.

2.1.9 Anti-Virus Software (AVS).

2.1.9.1 For the purpose of standardization, Norton AVS will be the standard for all laptops, workstations and servers on Air Force and Army systems.

2.1.9.2 WGMs or IMOs are responsible for ensuring networked servers, workstations, stand-alone computers and laptops are properly configured with the AF's approved anti-virus program(s). A continuous virus scanning program is required on each system file server to check for known viruses.

2.1.9.3 WGMs or IMOs are responsible for ensuring that all users are receiving their AVS signature file update via auto push method, except on areas where it is not technically possible. For areas where it is not possible to implement the auto update solution, WGMs or IMOs must contact the Wing IA office or Army NOC and obtain the AVS updates through other methods.

2.1.9.4 Norton AVS will be configured to run automatic weekly scan of all files on user workstation local drives. Norton AVS must be running in the background at all times.

2.1.10 Automated Data Processing Equipment Inventory. Organizational equipment custodians (ECs) will ensure that all Air Force ADPE assets (e.g., workstations, printers, personal digital assistants, etc.) under their span of control are listed in the Automated Data Processing Equipment (ADPE) Information Processing Management System (IPMS). 4 ASOG

ADPE account managers and Property Book account managers will accomplish inventories of their assets at least annually and as otherwise required by the applicable program. Any system without an IPMS label could be confiscated until the customer properly enters that system into IPMS. Army ADPE listed in the Army Property Book will be managed separate from Air Force property. Army equipment will be identified with a self-made label with the proper Army Property Book Account Number. Inventory of Army Property Book equipment will be done at least annually and at the Army's request. The Army can request return of any Property Book item at any time.

2.1.11 Personally Owned Computers. Personally-owned desktop or notebook computers owned by DoD members, government employees, or contractor personnel will not be used to process classified information. Personally owned computers (desktops, notebook or Personal Digital Assistant) will not be physically connected to the DoD systems without DAA approval. Users may access Air Force or Army systems via their personally-owned computers if they use an approved remote access method. Access is limited to sensitive but unclassified information.

2.1.12 Personal Wireless Communication System (PWCS). PWCS consist of cellular phones, beepers and land mobile radios. 4 ASOG personnel will use AFI 33-106 and AFI 33-106 USAFE Supp-1 for guidance on PWCS.

2.1.13 Personal Digital Assistants (PDA). The interest in using PDAs and Handheld Terminals (HHTs) within the Air Force has increased significantly. This family of devices offers personal productivity enhancements, particularly by making certain features of your Microsoft Outlook portable, including contacts, notes, appointments, and e-mail. However, depending on the product and features, these devices introduce potential risks to our networks. A PDA is an automated information system (AIS) and therefore is subject to Air Force directives governing the security, connectivity, and use of a desktop or notebook computer. PDA's must have an IPMS sticker, and consent to monitoring decal.

2.1.14 Prohibited PDA Actions.

- Do not process or maintain classified information. There are currently no approved methods for sanitizing or clearing classified from these devices. If a PDA receives any classified information, security personnel must protect, confiscate, and possibly destroy the affected PDA.
- Do not connect to commercial Internet Service Providers (ISP). The use of commercial ISPs for official business is not allowed.
- Do not synchronize the PDA across the networks or remotely by direct dial-in access to desktops. The only authorized connection through a PDA modem is to an official Air Force remote access server (RAS) account or TSACS for Army accounts.
- Do not download or load freeware or shareware software enhancements for the PDA or for the desktop.
- Afford the same physical protection as any laptop or device containing SBU and FOUO data.
- PDAs purchased with unit funds must remain the property of the unit when the member departs and must be accounted for by the unit ADPE custodian. Use an AF Form 1257 to document issue to members.

- Do not use wireless (infrared capable) PDA within controlled areas.
- Desktops will not be configured to permit dial-in access for the purpose of synchronizing the PDA remotely

2.1.15 Personally Owned PDA. Users using personally owned PDAs on government owned computers will adhere to all the policies outlined in this system security policy regarding the use of PDAs and require DAA approval.

2.1.16 Replacement of ADPE. Replacement of ADPE should occur on an annual basis. Currently the life cycle for desktops and laptops is approximately 4 years. Each work center should budget to replace 25% of assigned computers. When possible replace desktop computers with laptops/docking stations. This should provide greater flexibility for deployments. All other ADPE should be budgeted for replacement on a 5 year cycle or 20% of that type of equipment currently on hand. All purchasing of computer equipment will be centralized for the entire group. Units are responsible for including the appropriate replacements requests in their annual budgets. 4 ASOG/LG will centrally purchase ADPE to minimize compatibility issues, yield better price per unit, simplify maintenance, and reduce spare parts requirements..

2.1.17 Physical Security. Physical Security is used to prevent unauthorized access to equipment, facilities, materials, and information. It includes the application of physical barriers and control procedures as countermeasures against threats to resources, system resources (hardware, software, network media, etc.), and information. Systems will be protected from natural threats (e.g., heat, weather, floods, etc.), physical disasters (e.g., fire, building collapse, etc.), human threats (intentional and unintentional), and any other identified physical threats. Additional physical security mechanisms to prevent or limit damage will be proposed, evaluated, and implemented where deemed feasible and cost effective.

2.1.18 Entry Controls to Computer Facilities. Entry to all SIPRNET resources will be controlled. All authorized users will be responsible for positive identification (by personal recognition) of persons attempting to gain access to SIPRNET assets. Personnel will challenge any individual they cannot positively identify. If in doubt, they will verify the status of the unknown individual. Status implies not only the appropriate clearance and need to access SIPRNET resources, but that the individual is authorized to perform the function for which access is requested and the function constitutes official business.

2.1.19 Entry Controls to Remote Terminals. Only authorized personnel will be granted access to user workstations. WGMs or IMOs will ensure that these devices are secure from any unauthorized access and challenge any unknown individual attempting access. Unclassified workstations will be monitored during duty hours and kept in locked areas during non-duty hours. Classified workstation areas will be secured IAW procedures defined for classified Controlled Areas. Users must maintain security over classified workstations and controlled areas. Users are at all times responsible for maintaining area and workstation security until the Security Manager can be notified of a problem affecting the security posture. If a workstation is to be left unattended for more than 30 minutes, it must be logged off from the network.

2.1.20 Physical Resource Protection. System assets will be installed in areas that afford maximum physical protection or continuous observation. System installation plans must consider the potential for physical damage, information exposure, malicious tampering, and theft. All office areas containing safes with classified information or SIPRNET connectivity will require an Standard Form 701 Activity Security.

2.1.21 Non-removable Magnetic Media. All non-volatile storage media (tapes, disks, battery powered RAM, etc.) used on network components will be controlled to insure personnel privacy act and FOUO information is not disclosed to unauthorized personnel. No ADPE will be released to outside agencies (e.g., DRMO, other bases, etc) until the storage media has been purged or removed.

2.1.22 Office Automation Workstation Operating System. All office automation workstations connected to DoD systems must use Microsoft Windows NT or Window 2000 operating system with the latest service pack authorized by the AF Wing IA office or Army RCERT as appropriate. This is due to the inadequate security features of the Windows 9x and older operating systems. Any waivers require a justification letter approved by the DAA. 86 AW/CC has directed that the wing migrate to the NT / Windows 2000 file system. This policy also applies to all Army computers. The purchase of Novell products or enhancements is not authorized. Software baseline will consist of Microsoft Office Suite, Form Flow, Winzip, Adobe Acrobat Reader, Norton AVS and Internet Explorer at a minimum.

2.1.23 Emission Security (EMSEC). Cellular phones, two-way radios, two-way beepers and any other electronic equipment that can receive and transmit a signal are prohibited in all staff offices or areas where sensitive or classified information may be discussed.

2.2 DAA Accreditation Requirements. All systems must be accredited IAW AFD 33-2, Information Protection or equivalent Army guidance. Accreditation is the formal written declaration by the DAA that a particular system is approved to operate in a given mode, against stated residual risks, and with stated countermeasures. The DAA formally accepts responsibility for the operation of the system as well as personal liability and accountability. Use DITSCAP and/or AFSSI 5024 Volume I, The Certification & Accreditation Process to complete an accreditation package for Air Force systems. The Army performs their own accreditation process for their systems. Units connected to an Army network must locally maintain a copy of the Army accreditation package or a memorandum stating the accreditation process has been accomplished on the their system.

2.2.1 Reaccreditation. Reaccredit systems every three years or upon significant change to hardware, software, or environment. The System-level Security Authorization Agreement (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 three years. Most changes to the system will only require an update of a page within the SSAA. Should a major change occur, the bulk of the agreement is reusable in a re-accreditation.

The Air Force and Army have invested a significant amount to establish the network infrastructure to ensure communication requirements are met. This investment can only be recouped with the full cooperation of every organization to properly communicate and

coordinate any actions that may alter the security posture of our network. This operating instruction has been developed with a clear understanding of the mission, operational impact these policies impose, and first hand knowledge what will result if an adversary penetrates our defenses. No organization can stand alone to counter the daily probes from unknown sources, but must rely on the professionalism and integrity of those charged with enforcing network security regulations to minimize the associated risks. A risk accepted by one, is a risk that is shared by all connected to our wide area network.

Appendix A

4.1 GLOSSARY OF ABBREVIATIONS AND ACRONYMS*Abbreviations
and Acronyms**Definitions*

ADPE	Automated Data Processing Equipment
AF	Air Force
AFCERT	Air Force Computer Emergency Response Team
AFI	Air Force Instruction
AFSSI	Air Force System Security Instruction
AIS	Automated Information Systems
ASCAS	Automated Security Clearance Approval System
AVS	Anti-Virus Software
C2	Command and Control
C&A	Certification and Accreditation
CAP	Controlled Access Protection
CBT	Computer-Based Training
CD	Compact Disk
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CSM	Computer Systems Manager
CSRD	C4 Systems Requirements Document
CSSO	Computer System Security Officer
CTO	Certificate to Operate
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DGSA	DoD Goal Security Architecture
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMS	Defense Messaging System
DOD	Department of Defense
EC	Equipment Custodian
E-mail	Electronic Mail
EMSEC	Emission Security
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSA	Functional System Administrator
GSU	Geographically Separated Unit
HHT	International Standards Organization
IA	Information Assurance
IAAP	Information Assurance Awareness Program
IATO	Interim Approval to Operate
IAW	In Accordance With
ID	Identification
IMO	Information Management Officer (Army)

LAN	Local Area Network
LFC	Local Files Check
NAC	National Agency Check
NCC	Network Control Center
NOC	Network Operations Center (Army)
NOSC	Network Operations and Security Center
NOTAM	Notice to Airmen
OPSEC	Operation Security
PC	Personal Computer
PBOOK	Property Book (Army)
PCS	Permanent Change of Station
PDA	Personal Digital Assistant
PPE	Password Policy Enforcer
RAS	Remote Access Server
SA	System Administrator
SSAA	System-level Security Authorization Agreement
SBU	Sensitive But Unclassified
SLA	Service Level Agreement
SSAA	System Security Authorization Agreement
TCNO	Time Compliance Network Order
TSAC	Terminal Server Access Card
UIAM	Unit Information Assurance Manager
UPS	Uninterrupted Power Supply
USAFE	United States Air Forces in Europe
USAREUR	United States Army Europe (Army)
USM	Unit Security Manager
WAN	Wide Area Network
WGM	Work Group Manager
WM	Workgroup Manager