

**1 AUGUST 2003**



***Communications and Information***

**NETWORK SYSTEM SECURITY PROCEDURES**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: 913 CF/SCBN (Mr. Larry Antonio)  
Supersedes 913 AWI 33-201, 1 August 2000

Certified by: 913 MSG/CC (Lt Col V. Ray Kicker)  
Pages: 14  
Distribution: F

---

This instruction implements Air Force Policy Directive 33-2, *Information Protection*. It establishes the Information Security Policy for the 913 AW Local Area Network (LAN). The Sensitive But Unclassified LAN is the Non-secured Internet Protocol Routing Network (NIPRNET). The classified LAN is the Secured Internet Protocol Routing Network (SIPRNET). This instruction establishes the minimum-security requirements needed to protect the sensitive unclassified and classified information on the networks. The Security requirements identified are intended to prevent or minimize the unauthorized modification, removal or destruction of the information processed and to control access to the information on a need-to-know basis. This instruction applies to all military members and civilian employees assigned to the 913th Airlift Wing, Willow Grove Air Reserve Station (WGARS), Pennsylvania and the assigned Geographically Separated Units (GSUs). Violations of these provisions by civilian employees may result in adverse administrative action. Violations of these provisions by military personnel may result in prosecution under the Uniform Code of Military Justice (UCMJ).

**1. Introduction.** Since the Department of the Air Force has classified network systems as weapons, security measures must be implemented to protect these resources. Computer Security (COMPUSEC) protects computers and everything associated with it. Most importantly, COMPUSEC protects the information stored in the 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.

**2. Mission.** The mission of the WGARS LAN is to support the electronic creation, transfer, sharing, and presentation of information by ensuring the confidentiality and integrity of data processed, handled, and stored by the system, using networked personal computers. The WGARS LAN is a general purpose, multi-user system used by the 913 AW staff agencies, its squadrons, and tenant organizations. 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 WGARS LAN provides users with the tools to improve business processes, resulting in increased efficiency and effectiveness.

Therefore, this instruction was developed to provide LAN users, Workgroup Managers (WM), and administrators with a pragmatic security directive, realistic guidelines, and the tools necessary to accomplish their mission.

**3. Applicability and Scope.** This instruction provides the minimum WGARS LAN 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/or using the LAN.

**4. Relationship to Other Publications.** The National Computer Security Center standards and guides (Rainbow-series), Department of Defense (DoD) directives, Air Force Systems Security Instructions (AFSSI), and Air Force Systems Security Memorandums (AFSSM) govern the operation and management of information systems. The provisions of this security instruction and any user-developed operating instructions do not replace the requirements contained in Air Force and DoD-level documents. If there is a conflict, the requirements in higher-level publications govern. Report the conflict to your unit Information Systems Security Officer (ISSO) or Organizational Computer Manager (OCM).

**5. Appointments.** It takes personnel assigned specific duties to maintain proper security to the WGARS LAN. The following describes key assignments

**Table 1. Key Assignments**

| <i>Appointment</i>                                | <i>Who/What Appoints</i>   |
|---|--|
| Designated Approval Authority (DAA)               | AFI 33-202 paragraph 3.2.  |
| Certifier   | DAA – AFI 33-202 paragraph 2.7.5.  |
| Wing Information Assurance (IA) Awareness Officer | 913 CF/SC AFI 33-204, paragraph 13   |
| Unit IA Awareness Manager                         | Unit Commander 33-204, paragraph 15  |
| Unit COMPSEC Manager (UCM)                        | Organizational Commanders - AFI 33-202 paragraph 2.11.                             |
| ISSO  | UCM, [UCM will perform ISSO duties if none appointed] - AFI 33-202 paragraph 2.11. |
| OCM   | Organizational Commander – AFI 33-112 paragraph 8.                                 |

**6. Basic System Facts.** The following basic system information describes the WGARS LAN.

6.1. Authorized Data on the LAN. The WGARS LAN will not be used to process classified information. Sensitive information is the highest level of data authorized on the LAN. 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 AFI 33-303, *Compendium of Communications and Information Terminology*, for a detailed definition of sensitive information.

6.2. Minimum User Clearances. WGARS LAN access is based on the key concepts of “authorization” and “need-to-know.” Users must have a completed National Agency Check (NAC) or equivalent prior to requesting access to the WGARS LAN. See AFSSI 5027, *Network Security Policy*, paragraph 5.3.1 for additional information. Authorization is validated when a WM notifies the Network Control Center (NCC) that an individual requires WGARS LAN access to perform official duties, has a NAC on file, has been licensed as a network user by completing two Computer Based Training (CBT), Network User License and INFOCON submitting a properly completed 913th Airlift Wing Form 1, **913<sup>th</sup> Airlift Wing Local Area Network (LAN) User Agreement**, to the NCC. Completion of the form is self-explanatory. After processing the request, the NCC keeps the completed form in accordance with AFMAN 37-139. Workgroup Managers (WMs) will license network users, using the training requirements in AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*. 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 WGARS LAN. All WMs, OCMs, System Administrators (SA), and NCC personnel working with contractors should maximize use of discretionary access controls.

**7. Assurance.** Assurance is the measure of confidence that the security features and architecture of the WGARS LAN accurately mediate and enforce the security directives. Assurance is established by the certification and accreditation (C&A) of the WGARS LAN and is maintained through compliance with AFI 33-202, *Computer Security*.

**8. Accountability.** In accordance with AFSSI 5027, *Network Security Policy*, the LAN 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 LAN can be held accountable for their actions. Only a subset of all available WGARS LAN 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 WMs, OCMs, SAs, and NCC personnel will be audited in greater detail due to their LAN privileges, all WGARS LAN users will be audited to some degree to include events such as logging in and out of the LAN. Additionally, the SA and/or NCC personnel 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 the compromise should a security violation or malfunction occur.

8.1. Auditable Events. The following comprise auditable events:

8.1.1. Use of account login and logout.

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

8.1.3. Actions taken by SAs, OCMs, WMs and NCC personnel. Examples include adding a user, changing user rights, or performing file server restarts.

8.1.4. 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. 8.1.5. 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.

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

8.2. Specific Audit Information. The audit trail will record the following minimum information for each auditable event. Only the DAA can grant authorization for anyone to disable auditing or change their configured audit mechanisms.

8.2.1. Date and time of the event.

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

8.2.3. Type of event.

8.2.4. Success or failure of the event.

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

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

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

8.3. Audit Review. The SAs, WMs, OCMs and NCC personnel will randomly review audit data. They will review the following: patterns of access to individual objects, access histories of attempts to bypass protection mechanisms, and monitor use of privileges.

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

## 9. Access Control.

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

9.2. Identification. All users on the WGARS LAN will have a unique user name.

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

9.3.1. Password Generation. The NCC generates the initial password for a new network user and functional system SAs generates the initial password for users of a functional system. Users will generate their own passwords after the initial password assignment.

9.3.2. Password Composition. Passwords must be at least eight characters and contain at least one uppercase character, one lowercase character, one number, and one special character (@&+, etc.).

9.3.3. 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.

9.3.4. Password Security. The life cycle, lockouts, and protection of passwords will be set according to AFMAN 33-223, *Identification and Authentication*.

9.3.4.1. Account lock out. If an account is locked out, it will only be unlocked by NCC personnel through, Voice recognition or the presentation of proper ID (I.E. Military, Civilian or

Contractor ID)

9.4. 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 AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, paragraph A2.3.5 for the mandatory statement.

9.5. All workstations connected to the WGARS LAN will have, at a minimum, the Willow Grove Domain Managers group, PC Technicians group, and the organizations OCM group placed in the administrator group.

9.5.1. All servers connected to the WGARS LAN will have, at a minimum, the Willow Grove Domain Managers group placed in the administrators group.

9.6. Closing User ID Accounts. LAN user ID accounts and passwords will be deleted when the user out processes from WGARS, or when a user no longer requires access to perform official duties. Supervisors of organizations not required to out process through the NCC (contractors, NAFs, and tenant organizations) must send an email to <mailto:helpdesk@willowgrove.af.mil> identifying the user for deletion.

9.7. Inactive User Accounts. The NCC will disable any user accounts inactive for 60 days. Any account that is still inactive for another 30 days will be deleted.

9.8. Network Connections.

9.8.1. General Information.

9.8.1.1. Screen Savers. All workstations connecting to the WGARS LAN will have an active password protected screen saver. The screen saver must be configured to activate after five minutes of inactivity. Any workstation connecting to the WGARS LAN without an active password protected screen saver will be force installed during the login.

9.8.1.2. Anti-Virus. All workstations and servers connecting to the WGARS LAN will have the current, prescribed anti-virus software installed and managed. Any workstation or server connecting to the WGARS LAN without the current prescribed anti-virus software installed and managed will be automatically updated during the login.

9.8.2. Modem Connections. The use of modems to connect to workstations or servers directly connected to the WGARS LAN is not permitted. Users will access the LAN primarily through on-base terminals or through the NCC Remote Access Server (RAS). Users wishing to access systems connected to the WGARS LAN through the use of modems must meet specific mission requirements. If mission needs or systems with requirements for direct modem access, SAs or OCMs will prepare a C&A package for each system for the DAA to issue an approval to operate.

9.8.2.1. At no time will a server, workstation, or laptop use a modem to connect to systems outside the WGARS LAN while the system is physically connected to the WGARS LAN. For example, a laptop connected to the WGARS LAN via a LAN cable cannot connect to an Internet Service Provider or another base using the modem as long as the LAN cable is connected.

9.8.2.2. Procedure to request WGARS LAN RAS should state the following: Request that I (state your name) be provide dial-in access to the Willow Grove ARS base LANS. Dial-in access is required for the following purposes: Send a request to <mailto:helpdesk@willowgrove.af.mil> for review. During increased INFOCON levels, RAS

services will be restricted or even terminated. When RAS services are restricted, access will be limited to GSUs, remote recruiters, and group/unit commanders. Other users requiring access due to mission essentialness must submit their request to <mailto:helpdesk@willowgrove.af.mil> where the request will be reviewed for approval.

9.8.3. Internet Protocol (IP) Addresses. The unauthorized use or change of an IP address is prohibited without prior coordination with the NCC. Violations will result in termination of the offending user's access to the WGARS LAN with reinstatement only by written request of the user's organizational commander.

9.8.4. Internet Access. All Internet traffic accessing sites will go through the WGARS proxy server, proxy use is forced by the NCC. All Internet usage will be in accordance with AFI 33-119, *Transmission of Information VIA the Internet*.

## 10. Personnel Security.

10.1. Security Clearances. Access to the LAN 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 WGARS LAN reviewed by either the unit security manager, commander and/or staff agency chief. Once a determination has been made to deny access to the LAN, the WM and NCC will be notified, ensuring LAN access is revoked.

10.2. Need-To-Know. Authorized access to the WGARS LAN occurs when the WM notifies the NCC that an individual requires WGARS LAN access to perform official duties, is licensed as a network user 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.

## 11. Hardware.

11.1. File Server Access. Physical access to servers is limited to authorized personnel only, such as functional SAs, NCC personnel and authorized maintenance personnel. Servers are accessible only to authorized personnel; physical access is restricted by lock and Alarm.

11.2. 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.

11.3. Major Additions/Modifications to Network Hardware. The NCC will assess all additions and modifications to major WGARS LAN 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.

11.4. Hardware Inventory. Organizational Equipment Custodians (EC) will ensure that an AF 3215 is submitted for all hardware (e.g., workstations, printers, and personal digital assistants (PDA)) over \$500 original purchase price and all Software. These assets will be purchased on the IT account card. All other standalone peripherals under \$500 (e.g., external CD ROM, printer) identified to the Equipment Control Officer (ECO) by submitting a AF 3215. The ECO will update the ECs account to reflect current inventory using the Information Processing Management System. See AFI 33-112, Computer Systems Management, for additional inventory requirements.

11.5. Hardware Maintenance. Only authorized maintenance personnel, (e.g., OCMs, SAs, NCC personnel, WMs, and government-approved vendors) will perform hardware maintenance on WGARS servers, workstations and peripherals. No individuals other than NCC personnel or government-approved vendors, accompanied by NCC personnel, will perform hardware maintenance on any WGARS LAN backbone or infrastructure hardware (e.g., hubs, switches, modems, LAN drops). Individual LAN users will not perform hardware maintenance or modifications without the express approval of the WM, OCM or 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.

11.6. Hardware Configuration Control. The LAN Manager is responsible for ensuring network hardware configuration control is in place and maintained.

## 12. Software.

12.1. Making Backup Copies of Original Network Software. Any duplication of commercially licensed software, except for backup purposes, is a violation of Federal copyright laws.

12.2. Archiving (Backup) of NCC Servers. At a minimum, a daily incremental backup will be made for data files on each WGARS LAN server maintained at the NCC, with full backups done once a week.

12.3. 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 (e.g., C:\ drive), since workstation files are not backed up in any way by the WGARS LAN file server backup process.

12.4. Software Certification. All network operating system and application software that specifically interacts with the WGARS LAN, but is not accredited by higher-level Air Force channels, must be accredited through the DAA prior to its installation on systems connected to the WGARS LAN. Network and application software testing will be accomplished by the NCC to ensure the new software does not circumvent existing WGARS LAN security features or adversely affect the operation of the WGARS LAN.

12.5. Software Configuration Control. The NCC is responsible for ensuring network software configuration control is in place and maintained. At the direction of the DAA, NCC personnel will perform periodic inspections to ensure compliance with all advisories, bulletins and other compliance messages.

12.6. Unauthorized Software. Only government approved software is authorized on the WGARS LAN. Games, music, video (i.e. movies) and pornographic software are unauthorized and will not be installed on any computer or file server. Unless approved by the NCC and the DAA, freeware, personal software, or shareware will not be authorized on the WGARS LAN file servers or workstations.

12.7. Using Government Owned Software for Personal Projects. The DAA, 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*.

12.8. Commercial Off-The-Shelf Software (COTS). All COTS installed on WGARS computer systems will be in compliance with the software license and maintained in accordance with AFI 33-114, *Software Management*.

12.9. Virus-Scanning. Scanning of Workstations and Servers. In accordance with AFI 33-202 the use of antiviral software is mandatory. OCMs, SAs, UCMs and ISSOs will ensure that each server and workstation will have antiviral software to provide virus protection for WGARS LAN users. They will ensure the antiviral software is kept up-to-date, managed and configured to NCC specifications. Antivirus updates are located on the Y Drive – Norton- Updates. SAs are responsible for loading antiviral software on each server under their control on the WGARS LAN. The latest updates will be pushed out by the NCC and loaded to the workstation at login.

### **13. Marking/Labeling.**

13.1. Labeling Removable Storage Media. Mark all removable storage media (floppy diskettes, tapes, and hard drives) in accordance with AFI 31-401, *Information Security Program Management*.

13.2. 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 in accordance with DoD 5200.1-R, *Information Security Program*, Appendix C, paragraphs 2-201.b.(3), 3-301, and 6-601.

**14. Processing Classified Information.** Currently, the WGARS LAN is not authorized to process classified information.

**15. Inadvertent Entry of Classified Information in the LAN.** Classified information accidentally introduced into the LAN requires immediate reporting and intervention by key personnel. Procedures set forth in DoD 5200.1-R and AFSSI 5020, *Remanence Security*, will be strictly adhered to. As a minimum, the following personnel will be notified: the DAA, SC, Wing IA Awareness Manager, and the AFRC NOSC. The DAA will instruct the WMs, SAs and/or NCC personnel, based on AFSSI 5020, paragraph A5, as to what level of sanitation to conduct.

**16. Computers Used to Process Classified Information.** Systems accredited to process classified information in a stand-alone configuration must be physically disconnected from the WGARS LAN when processing classified information.

### **17. Sensitive Information.**

17.1. User Responsibility. It is the responsibility of each user to properly protect and safeguard all sensitive information under their control. Sensitive information is defined in AFMAN 33-270, *Command, Control, Communications, and Computers (C4) Systems Security Glossary*. 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 913 CF/SCB Office.

17.2. 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 AFI 33-202 for further guidance.

17.3. **Aggregating Data.** When storing data on the LAN, 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 WGARS LAN. In no case will users aggregate data for placement on the LAN 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 LAN. Individual users should consult with their functional managers to determine when issues regarding aggregated data arise.

17.4. **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.

17.5. **Disposition.** Computer products that contain sensitive information will be disposed of in accordance with AFI 37-138, *Records Disposition—Procedures and Responsibilities*, paragraph 3.10.

**18. 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 or deleting a file using Windows Explorer. 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.

18.1. **Clearing.** 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 removes 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, wipe disk is the only product approve at Willow Grove ARS. This product will be controlled by the ECO (Equipment Control Officer) and issued to WGM upon request for approved use.

18.2. **Purging** is 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 WGARS LAN. (See AFSSI 5020 for additional information on clearing and purging magnetic storage media.)

18.3. Users, OCMs, ECs and SAs will clear magnetic storage media under their control that contain unclassified or sensitive information before reutilization, whenever the media is reallocated to another work center, or is no longer needed in the performance of official duties. Forward all documentation on systems cleared to the responsible ISSO, who is responsible for maintaining records on the clearing (See AFSSI 5020 for responsibility information). Information owners will review files for record management disposition requirements prior to clearing the files from the magnetic storage media.

18.3.1. Clearing is not required when an employee leaves an office and the workstation remains under the control of the functional organization.

18.3.2. User workstations and WGARS LAN file servers do not require clearing of sensitive information when NCC personnel or WMs perform equipment maintenance. If NCC personnel or WMs cannot repair the equipment, they 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.

18.3.3. The AFRC NOSC has purchased for each AFRC base a licensed and Air Force approved overwrite program. Contact the ECO for the signing out of this program.

## 19. Security Training.

19.1. Initial and Follow-Up User Security Training. All new users will be licensed network users prior to being authorized to access the WGARS LAN. Instructions for necessary Information Assurance Awareness Training can be found on the Computer Based Training web site .

19.2. Specialized Security Training. OCM, SA, UCM and ISSO responsibilities are outlined in AFI 33-112 and WM responsibilities in AFI 33-202. Specific training requirements can be found on the WGARS Intranet site. The SAs should request training from the vendor of the specific system they are administrating.

**20. Reporting Vulnerabilities or Incidents.** LAN users will immediately report vulnerabilities, security incidents, or unauthorized entry into the computer system to their ISSO or WM and the Network Protection Office. The ISSO or WM and the Network Protection Office (NPO) 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, contact the Network Protection Office and NCC who will immediately contact the Air Force Computer Emergency Response Team (AFCERT) at DSN 969-3157, toll free (800) 854-0187 or commercial (210) 977-3157. 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 in accordance with AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*.

**21. 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 ISSO and NPO. If able, the user will remove the virus using approved antiviral software. The OCM or WM will remove the virus if the user is incapable of doing so. NCC personnel can also assist the OCM or WM in removing the virus. Upon discovery of a virus, a formal virus incident report will be sent immediately to the Wing IA office via hardcopy or emailed to <mailto:913CF.SCB@willowgrove.af.mil>, using the reporting format located at [http://afcert.kelly.af.mil/virus\\_report.txt](http://afcert.kelly.af.mil/virus_report.txt). Therefore, pertinent viral information should be recorded at the time the virus is detected and removed. The NCC will forward the report to HQ AFRC and AFCERT along with the action taken by the user, OCM, WM or NCC personnel.

**22. Internet Fraud, Waste, and Abuse (FWA) Reporting Procedures.** All users must report potential security violations or other incidents directly to their OCM or ISSO. OCMs will determine the appropriate level of notification in accordance with AFSSI 5021 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 FWA, and copyright violations. You may use the Willow Grove ARS FWA program to report violation; use AF Form 102, **IG Personal and Fraud, Waste and Abuse Complaint Registration**, for reporting to the IG; or you may call the hotline at DSN 991-1989. Unit commanders will be notified of any FWA incidents. Keep in mind the OCM and WM may play an active role in the investigation and correction after the fact.

**23. Unattended Terminals.** All workstations that are logged onto the LAN will not be left unattended unless the user either logs off the LAN (the preferred method), uses a password-protected screen saver, and/or employs physical measures (e.g., keyboard locks). All terminals will be logged out of the WGARS LAN prior to the user leaving at the end of their work shift.

**24. Personally Owned Computers and PDA.** Personal computers owned by Air Force members, government employees, or contractor personnel will not be used to process classified information. Personally owned computers and Personal Digital Assistants (PDAs) will not be connected to the WGARS LAN. The use of personally owned computers at work is strongly discouraged, however, it may be used for processing unclassified and non-secure information with DAA approval. AFI 33-202, paragraph 3.10.4 and written DAA approval will specify the conditions under which the computer will operate and the duration of the approval. Using personally owned computer hardware and software for official business should be a last resort and actions should be taken to preclude their use. Per AFRC guidance letter, *AFRC Guidance on Purchase and Use of Personal Digital Assistants (PDAs)*, personally or contractor owned PDAs will not transfer data to or from any government computer.

**25. Review of LAN Communications-Computer Systems Requirement Document (CSRD) for Security Impact .** The Network Manager will review the technical solution for each major WGARS LAN submission for possible impact on the WGARS LAN security capabilities. The review is required prior to submission of the CSRD for final approval.

**26. Configuring Web Server.** Some programs (e.g., Super TCP/IP and Windows 95) delivered as part of a standard workstation software package has 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 WGARS LAN system. WGARS LAN workstations or servers will not be converted into a Web Server under any circumstances. The only authorized web server that will be connected to the WGARS LAN is contained and maintained in the NCC.

**27. AFCERT Advisories and Notices to Airmen.** 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. The AFCERT and NOTAM will be tracked at the NCC by Network Protection Personnel. Upon implementation of the solution, the Network Protection Personnel will immediately update the HQ AFRC NOCS web page.

**28. Computer Shares.** A share gives the ability to allow remote users at other workstations access to a drive, folder, or application on another workstation.

28.1. The only shares allowed and required on workstations are shares designed to administer or security scan the workstation. These shares must be hidden and only allow access to personnel contained in the administrator group.

28.2. Information shared data will be maintained on network drives maintained in the NCC so that share access is controlled by the network domain controller user-identification/password system.

28.3. Functional application servers can share folders used directly in support of the server's applications and for software distribution for the application. The C&A package for the server must identify these shares and the protection used to secure the shares. These shares will not be used to share out other organizational information. This information will be shared out on network drives maintained in the NCC.

**29. Prescribing Directive.** This instructive is the prescribing directive for 913 AW Form 1, **913<sup>th</sup> Airlift Wing Local Area Network User Agreement**. The form is available on the server under the 913 Forms folder.

TIMOTHY J. THOMSON, Col, USAFR  
Commander

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

AFI 31-401, *Information Security Program Management*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-115 V2, *Licensing Network Users and Certifying Network Professionals*

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

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

AFI 33-202, *Computer Security*

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

AFMAN 33-223, *Identification and Authentication*

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

***Glossary***

AFI 33-303, *Compendium of Communications and Information Terminology*

AFI 33-332, *Air Force Privacy Act Program*

AFI 37-138, *Records Disposition—Procedures and Responsibilities*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting*

AFSSI 5027, *Network Security Policy*

DoD 5200.1-R, *Information Security Program*

DoDD 5500.7-R, *Joint Ethics Regulation*

***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.

**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 33-332, *Air Force Privacy Act Program*, for detailed information.

**Privileged Data**—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 (e.g., quality assurance data or credentials committee records).

**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 and/or information.

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