



***Communications and Information***

***NETWORK SECURITY POLICY***

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

This publication implements the Computer Security Act of 1987 (Public Law 100-235); Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; OMB Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems Containing Sensitive Information*; Department of Defense (DoD) Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988; Air Force Policy Directive (AFPD) 33-2, *Information Protection*; Air Force Instruction (AFI) 33-115, *Network Management*; Air Force Systems Security Instruction (AFSSI) 5102, *The Computer Security (COMPUSEC) Program*; and AFSSI 5024, Volume 1, *The Certification and Accreditation Process*. Use of extracts is encouraged. Direct questions, comments, and recommended changes through appropriate command channels to Headquarters, Air Force Communications Agency, Information Protection Division (HQ AFCA/GCI), 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234.

***SUMMARY OF REVISIONS***

This is the initial publication of AFSSI 5027.

<b>CHAPTER 1-- OVERVIEW.....</b>	<b>4</b>
1. Introduction.....	4
1.1. Purpose.....	4
1.2. Applicability.....	4
<b>CHAPTER 2 -- ROLES AND RESPONSIBILITIES.....</b>	<b>5</b>
2. General.....	5
2.1. DAA.....	5
2.2. Certifying Official.....	5

2.3 Network Manager .....	5
2.4. Information Protection Operator.....	5
2.5. System Administrators.....	5
2.6. Help Desk Technicians.....	6
2.7. Workgroup Managers.....	6
2.8. Wing Information Protection Office.....	6
2.9. Computer System Security Officers (CSSO).....	6
2.10. Users.....	6
<b>CHAPTER 3 -- SYSTEM DEFINITION.....</b>	<b>7</b>
3. Description.....	7
3.1. System and Data Criticality.....	7
<b>CHAPTER 4 -- SECURITY REQUIREMENTS .....</b>	<b>8</b>
4. General.....	8
4.1. Confidentiality.....	8
4.2. Availability.....	8
4.3. Integrity.....	8
4.4. Accountability.....	8
<b>CHAPTER 5 -- SECURITY PRINCIPLES .....</b>	<b>9</b>
5. General.....	9
5.1. Auditing.....	9
5.2. Identification and Authentication.....	9
5.3. Personnel Security.....	10
5.4. Network Sustainment.....	10
5.5. Hardware/Software.....	11
5.6. Marking and Labeling.....	12
5.7. Maintenance .....	12
5.8. Declassification and Destruction.....	12
5.9. Vulnerabilities and Incidents.....	12
5.10. Encryption.....	13
5.11. Information Protection Tools .....	13
5.12. Barrier Reef.....	13
<b>CHAPTER 6 -- NETWORK INFRASTRUCTURE SERVICES AND PROTOCOLS POLICY.....</b>	<b>15</b>
6. General.....	15
6.1. Simple Network Management Protocol (SNMP).....	15
6.2. Domain Name System (DNS).....	15
6.3. Network Time Protocol (NTP).....	16

6.4. Syslog.....	16
6.5. Finger.....	16
6.6. Network Information System/Yellow Pages (NIS/YP).....	17
6.7. Internet Control Message Protocol (ICMP) and TCP/UDP ECHO Services.....	17
6.8. Routing Services.....	18
6.9. Simple Mail Transport Protocol (SMTP).....	18
6.10. X.400 Electronic Mail.....	18
6.11. X.500 Directory Services.....	19
6.12. Post Office Protocol (POP).....	19
6.13. Network News Transport Protocol (NNTP).....	19
6.14. UNIX 'r' Commands.....	20
6.15. TELNET.....	20
6.16. X Window System (X).....	21
6.17. Sun Remote Procedure Call (Sun RPC).....	21
6.18. HyperText Transfer Protocol (HTTP).....	22
6.19. Gopher.....	22
6.20. Wide Area Information Servers (WAIS).....	22
6.21. Archie.....	23
6.22. File Transfer Protocol (FTP).....	23
6.23. Trivial File Transfer Protocol (TFTP).....	23
6.24. Network File System (NFS).....	24
6.25. Printing (lpd).....	24
6.26. SQL*Net.....	24
6.27. Talk.....	24
6.28. Internet Relay Chat (IRC).....	25
6.29. Multicast Backbone (MBONE).....	25
6.30. RealAudio.....	25
6.31. Lotus Notes.....	25
6.32. Intrusion Detection Tools Registered on DARPA Internet Domain Name Servers.....	26
6.33. NetBIOS.....	26
<b>CHAPTER 7 -- NETWORK USE.....</b>	<b>27</b>
<b>CHAPTER 8 -- ACCREDITATION.....</b>	<b>28</b>
8. General.....	28
8.1. Accreditation Documentation Policy.....	28
8.2. Reaccreditation Policy.....	28
<b>CHAPTER 9 -- SECURITY, AWARENESS, TRAINING AND EDUCATION.....</b>	<b>29</b>

## Attachments

1.- Glossary of References, Abbreviations, and Acronyms ..... 30



## CHAPTER 1

### OVERVIEW

**1. Introduction.** The Air Force core competencies of Precision Engagement and Information Superiority are information technology driven and information dependent. Increasingly, mission success depends on information systems, which makes the protection of our mission critical networks an absolute priority. Protection of our networks and the information contained within them is the central focus of the certification and accreditation process. The key element to network certification is the establishment of a security policy. The security policy is the expressed set of laws, rules, and procedures that govern how the system will be operated and the resources (information and equipment) protected. It informs the people who manage and use the network about their obligations for protecting information assets. All certification efforts are predicated on the creation, implementation, and testing of the network's security policy.

**1.1. Purpose.** This document establishes the baseline security policy for Air Force base-level networks processing sensitive information. 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, or the privacy to which individuals are entitled to under the Privacy Act but which has not been specifically authorized to be secret by an Executive Order or Act of Congress. It specifies the minimum security measures required to ensure availability, integrity, confidentiality, and accountability of Air Force networks and the sensitive information contained within.

**1.2. Applicability.** This document is to be used by certifying officials as the foundation for establishing base-level network security policy. Ultimately, the base network security policy is developed after incorporating this document with site-specific security concerns and approved by the Designated Approving Authority (DAA). Policy contained in this document that is not implemented due to technical, fiscal, or mission requirement constraints must be documented in the network's accreditation documentation and approved by the DAA. This document can also be incorporated when establishing security policy for higher echelon and classified networks.

## CHAPTER 2

### ROLES AND RESPONSIBILITIES

**2. General.** Base-level networks processing sensitive information are used primarily to meet the office automation requirements at an installation, including electronic mail, word processing, scheduling, spreadsheet, data base, and Internet access applications. DAAs, certifying officials, network managers, information protection operators, system administrators, workgroup managers, help desk technicians, wing information protection office personnel, Computer System Security Officers, and users all have roles in the development and implementation of network security policy.

**2.1. DAA.** The DAA formally accepts security responsibility for the systems operation and officially declares the system will provide an appropriate level of protection against compromise, destruction, or unauthorized modification. The DAA gives the “thumbs up” to operate a network and also has the authority to “pull the plug” should conditions dictate. The DAA approves the network security policy. Additional information about DAA responsibilities can be found in AFSSI 5024, Volume I, *The Certification and Accreditation Process*.

**2.2. Certifying Official.** The certifying official works on behalf of the DAA and develops the security policy. The certifying official oversees each task associated with network certification, compiles all related documentation, and recommends an accreditation decision to the DAA. Additional information about certifying official responsibilities can be found in AFSSI 5024, Volume I, *The Certification and Accreditation Process*.

**2.3. Network Manager.** Network managers provide proactive and reactive network management by monitoring and controlling the network, available bandwidth, hardware, and distributed software resources. Network managers respond to detected security incidents, network faults (errors), and user reported outages at the time of help desk referral. Their area of responsibility is from the base service delivery point to the server and includes the base backbone infrastructure components.

**2.4. Information Protection Operator.** IP Operators work in the NCC and employ hardware and software tools to enhance the security of the base network. They provide proactive security functions to assist AF 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 defensive measures to ensure the availability, integrity, and confidentiality of base networked information resources. IP Operators also assist the Wing’s Information Protection Office in developing local security policy, strategies, and plans to counter identified network security threats.

**2.5. System Administrators.** System administrators ensure servers, workstations, peripherals, communication devices, and software are on-line and available to support customers. They install and configure software and hardware. They add, delete, or modify user accounts. They enforce password control, set permissions, perform security management functions, and coordinate maintenance call-out with the Network Control Center (NCC) help desk. System administrators must thoroughly understand the customer’s mission, and be completely knowledgeable of the network capabilities/limitations and the

network security policy. The system administrator's area of responsibility is from the user's terminal to the server, but does not include the network backbone infrastructure components.

**2.6. Help Desk Technicians.** Help Desk technicians are assigned to the NCC and determine the type of reported systems problems within defined response times, report the status of problem resolution to the affected customer, and maintain a historical database associated with problem resolution. They also use a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, hardware exchange, and repair service support. Since they work closely with users and workgroup managers, Help desk technicians must be familiar with the contents of this publication for early detection of new vulnerabilities and incidents.

**2.7. Workgroup Managers.** Workgroup managers typically perform duties at the component (workstation) level. Personnel possess specific, focused subject knowledge; are able to identify nomenclature; can state facts and principles; and perform basic installation, configuration, operation, and problem resolution. Workgroup managers must be familiar with their network's security policy due to their close relationship with Computer System Security Officers (CSSOs) in providing customer service. Consult AFI 33-115, *Network Management*, for additional information on network manager, information protection operator, system administrator, help desk technician, and workgroup manager responsibilities.

**2.8. Wing Information Protection Office.** Information Protection Office personnel oversee the implementation of information protection policy and guidance at their installation. They serve as the local expert on this publication and serve as an advisor to DAAs, certifying officials, and others involved in network security policy formulation. Consult AFPD 33-2, *Information Protection*, and AFSSI 5102, *The Computer Security Program*, for additional information on wing information protection office responsibilities.

**2.9. Computer System Security Officers (CSSO).** CSSOs work at the unit level and assist system administrators in the security aspects associated with network operations. They make sure users operate, maintain, and dispose of information systems according to the established security policy. CSSOs perform an initial evaluation of each vulnerability or incident occurring at the user level, begin corrective or protective measures, and report according to AFSSI 5021, *Vulnerability and Incident Reporting*. CSSOs work with workgroup managers to determine if user workstation problems are security related. Consult AFSSI 5102, *The Computer Security Program*, for additional information on CSSO responsibilities.

**2.10. Users.** The end user complies with the network security policy in the course of their duties. Each user must be trained in proper security procedures IAW AFI 33-204, *Security Awareness, Training and Education*.

## CHAPTER 3

### SYSTEM DEFINITION

**3. Description.** The typical base network consists of the base backbone and organizational local area networks (LANs). The backbone, managed by the NCC, provides customers the information resources needed to achieve their operational objectives. This backbone normally consists of communications media, routers, gateways, and other types of communications equipment. Through the use of network management systems, firewalls, and intrusion detection and vulnerability assessment tools, the NCC performs network management and problem resolution for the backbone. Communications and information services entering and exiting the base or site fall under the operational control of the NCC. Organizational LANs connect to the base backbone for intranet and internet connectivity. These LANs provide office automation services for the unit and are frequently managed by system administrators assigned to that unit. NCCs, in accordance with a Service Level Agreement, may assume responsibility for system administration services to a unit should mission requirements dictate. Organizational LANs normally consist of servers (file, mail, and web), networking devices (routers, bridges, etc.), media, user workstations, and printers.

**3.1. System and Data Criticality.** System criticality is based on AFMAN 10-401, *Operational Plan and Concept Plan Development and Implementation*. Categories include:

- Group I – *Mission Critical*. System loss would cause immediate stoppage of direct mission support of wartime or contingency operations.
- Group II – *Mission Essential*. System loss would cause an eventual stoppage of direct mission support of wartime or contingency operations.
- Group III – *Mission Impaired*. System loss would have an effect on (but would not stop) direct mission support of wartime or contingency operations.
- Group IV – *Nonmission Essential*. System loss would have no effect on direct mission support of wartime or contingency operations.

Based on these categories, the typical base network would be Group II – Mission Essential. This will vary depending on the mission that the network supports.

The highest classification of information processed on the base network is sensitive. NOTE: The term “Sensitive But Unclassified (SBU)” is no longer recognized as an AF term - it is a Department of State term.

## CHAPTER 4

### SECURITY REQUIREMENTS

**4. General.** The security requirements for base networks are listed below not necessarily in order of importance.

**4.1. Confidentiality.** Confidentiality is preventing inadvertent disclosure of information. The information processed, stored, and transiting the base network must have strict enforcement of confidentiality. The information will be at the sensitive and unclassified levels. Classified information must not be stored or processed. No information can be made available to those without a valid need-to-know.

**4.2. Availability.** The base network and the information processed, stored, or transiting the system must be protected from loss or destruction and available whenever needed. The base network will be available 24 hours a day, 7 days a week, excluding preventive/remedial maintenance downtimes.

**4.3. Integrity.** There are two distinct aspects of integrity:

**4.3.1. Data Integrity.** The information itself must be accurate and complete. It must be plausible and users must trust the information as a true representation as it was entered, stored, or processed. Information has data integrity if there is assurance it has not been tampered with.

**4.3.2. System Integrity.** The network itself (hardware and software) must operate correctly and not corrupt the information within it.

**4.4. Accountability.** All security relevant actions on the base network must be traceable to a single user who is accountable for those actions. Accountability includes authentication and non-repudiation.

**4.4.1. Authentication.** To the maximum extent possible, the base network must ensure the originator of a file, message, or process can be proven and not “spoofed.” The use of audit trails, date-time stamps, and future digital signature technology assists in this goal.

**4.4.2. Non-repudiation.** Non-repudiation is undeniable proof of involvement (i.e., the recipient cannot deny receipt and the sender can prove delivery). To the maximum extent possible, the base network will employ non-repudiation features.

## CHAPTER 5

### SECURITY PRINCIPLES

**5. General.** This section implements the requirements in section 4 by providing specific instructions.

#### **5.1. Auditing.**

**5.1.1. Events and Information to be Audited.** As a minimum the use of identification and authentication (I&A) is to be tracked and retained. Audit both successful and unsuccessful logons and logouts. Track all system restarts, unsuccessful attempts to alter file permissions, unsuccessful access attempts to the audit or password files, and remote system accesses.

**5.1.2. Automated or Manual Audit Policy.** Use an automated audit log.

**5.1.3. Time-out Policy.** Protect normal connections by a password protected screen saver when the workstation is left unattended. Terminate inactive sessions after 8 hours.

**5.1.4. Retention of Audit Records.** Maintain audit records for 90 days. This includes both audit records generated by network servers and workstations.

**5.1.5. Audit Review.** Review audit logs daily.

**5.1.6. Protection of Audit Files.** Protect audit files through file permissions. The system administrator and CSSO will have read privileges to the audit file. Write and delete privileges to the audit file are restricted to the system administrator.

**5.2. Identification and Authentication.** This section provides the necessary instructions for implementing a robust identification and authentication mechanism on the base network. Additional information can be found in AFSSI 5013, *Identification and Authentication* (future AFMAN 33-223).

**5.2.1. Method of Access Control.** Employ discretionary access control (DAC). DAC provides the ability to control a user's access to information according to the authorization granted the user. It provides the data owner (individual user or groups) a capability to specify permissions (read, write, delete, or execute) to information for each of their files and programs contained in the network. Files do not require internal classification labels.

**5.2.2. Password Length.** Passwords must be at least eight characters long and consist of alphanumeric characters with at least one special character.

**5.2.3. Password Generation.** Use machine or user generated passwords. Usually, the base network employs user generated passwords. The system administrator will assign an initial password which the user must change on the first use. Check the strength of passwords by running an approved password cracking program at least monthly.

**5.2.4. Password Protection.** Protect passwords as sensitive (FOUO).

**5.2.5. Changing Passwords.** Change passwords every 90 days. The minimum time for password change is 2 days. Former passwords will not be used for 6 months.

**5.2.6. Password Lock-outs.** Lock out accounts after three consecutive failed logon attempts. System administrators must not reinstate passwords without positive identification of the authorized user.

5.2.7. **Password Disclosure.** Users must memorize their password. Do not place passwords on desks, walls, sides of terminals, or store them in a function key, log-in 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.

5.2.8. **System Administrator and User Privileges.** Limit system administrator (root) privileges to the least possible number of users. System administrators will log onto the system under their individual user-id and password and then switch to the root account. Do not log on as "root" unless required for system initialization or rebuild.

5.2.9. **Password Manager.** The CSSO is the password manager and performs duties as outlined in AFSSI 5013, *Identification and Authentication*.

5.2.10. **Dial-in Access.** The NCC will concentrate and manage all dial-in access. Use of dial-in services must be logged and authenticated by the NCC. The NCC will process all requests for dial-in access and brief users on the risks associated with dial-in access. The users will sign a statement acknowledging they have been briefed and they understand and accept the responsibility for enforcing security procedures and requirements. The NCC will maintain a list of personnel having dial-in access. Dial-in hardware or software will disconnect sessions after 15 minutes of inactivity. The hardware or software may warn the user five minutes prior to disconnection. The host organization will permit access only to those services and data required by the remote users to perform their functions. Do not publicize modem telephone numbers to anyone other than those with a need-to-know and treat them as sensitive information.

5.2.11. **Remote Login.** Allow remote software diagnostics or maintenance only if the system audits such activities or if an appropriately cleared individual (capable of identifying unauthorized activity) observes such activities. The system being remotely maintained will authenticate the identity of the maintenance personnel. When maintenance activities are suspended or completed, disconnect or disable maintenance access to the system.

**5.3. Personnel Security.** The system administrator, in conjunction with the unit security monitor, oversees the personnel security program for the base network.

5.3.1. **Security Clearances.** All persons accessing the base network must, at minimum, have a completed National Agency Check (NAC, ENTNAC, or equivalent) verified through the automated security clearance approval system (ASCAS) roster.

5.3.2. **Need to Know.** All users have clearance and access approval for all information within the system but not all users have a need to know all of the information within the network. The CSSO will brief users on protection requirements for the various categories (e.g., Privacy Act, FOUO, proprietary) within the network.

#### **5.4. Network Sustainment.**

5.4.1. **Entry Control.** The NCC is to be located in an area to which access is restricted. Entry to the NCC must be controlled by the facility manager and all tenants. Base network users are responsible for the positive identification (by personal recognition) of individuals attempting to access network assets.

5.4.2. **Resource Protection.** The base network is made up of high value items (both physically and logically) which are subject to pilferage. Physical resources are the network equipment, physical storage media, and the physical environment (site). Logical resources encompass data and software.

5.4.2.1. **Physical Resource Protection.** Protect base network resources from natural threats, physical disasters, human threats, and any other identified physical threat using existing mechanisms. Consult AFI 31-209, *The Air Force Resource Protection Program*, and AFI 31-101v1, *The Air Force Physical Security Program*, for further information.

5.4.2.2. **Logical Resource Protection.** Perform server backups daily and retain for a minimum of 1 month. Store all removable media, do not leave on desktops or in the workstation. An additional removable hard drive may be used as the backup. Mark, store, and handle the backups as Sensitive.

5.4.3. **Contingency Planning.** The base network is essential to the wing's operation. Develop continuity of operations plans or emergency action plans to enhance system survivability. These plans must be consistent and integrated with disaster recovery plans maintained by the Wing and organization. Test contingency plans periodically to ensure currency. AFMAN 10-401 provides further guidelines in contingency planning.

5.5. **Hardware/Software.** Make sure the available hardware and software security features which provide controlled access protection (i.e., DAC, I&A, Audit, and Object reuse) are not by-passed or disabled.

5.5.1. **Configuration Management.** The base network is a relatively complex network with connectivity through the NCC. The network manager conducts configuration management for the base backbone. Network managers and/or system administrators conduct configuration management for organizational LANs. Significant changes (e.g. additional servers, new operating system) to the network configuration must be coordinated with the NCC and the local configuration control board (CCB), and subsequently documented in the system architecture section of the network's accreditation package. Any configuration changes that affect AF or DOD level systems must be approved by the appropriate CCB.

5.5.2. **Software Use.** Users must follow the guidelines for software security as dictated in AFI 33-112, *Automated Data Processing Equipment (ADPE) Management* and AFI 33-114, *Software Management*. In addition, access to diagnostic programs and security-critical software shall be restricted to use by authorized personnel. Shareware or public domain software must be required for mission accomplishment and authorized by the DAA on a case-by-case basis in order to be placed on an operational system.

5.5.3. **Controlled Access Protection (CAP) Products.** Use products listed in the National Security Agency's Evaluated Products List, the Air Force Assessed Products List, or an approved locally developed solution. Ensure local solutions that provide controlled access protection (i.e., DAC, I&A, Audit, and Object reuse) meet Air Force requirements IAW AFMAN 33-229, *Controlled Access Protection*. Evaluate, assess, or locally test and approve all hardware, software, and firmware products that provide security features prior to use on the network.

5.5.4. **Y2K Compliance.** Base networks whose lifespan extends beyond 1999 must have countermeasures in place to correct the Year 2000 vulnerability. Test for this vulnerability on all

network components. For Y2K vulnerabilities not countered, determine corrective measures, seek approval from the network DAA, and document them in the network's accreditation documentation.

**5.6. Marking and Labeling.** Mark all products and media IAW AFI 31-401, *Managing the Information Security Program*. Appropriate marking/labeling applies to printed listings, display terminals, diskettes/jackets, and storage devices. Appropriate, pre-printed, Air Force labels will be used whenever possible for standardization.

5.6.1. **Output Products.** Print appropriate markings on all applicable pages for output products printed from sensitive documents or segments of documents.

5.6.2. **Internal Files.** Markings on sensitive information within a paragraph, illustration, table, figure, or other internal document will be applied by the user upon creation of the file.

5.6.3. **Storage Media.** Label storage media using standard forms (SF) 710. Storage media includes floppy disks, removable hard disks, permanent hard disks, CD-ROMs, and tape disk drives.

5.6.4. **Peripheral Devices.** Label peripheral devices (e.g., printers, printer ribbons, card readers, CD ROMs, CD ROM Reader) using an SF 710.

**5.7. Maintenance.** In-house maintenance on the base network is preferred.

5.7.1. **Maintenance on Hardware Devices.** Workgroup managers and system administrators perform initial troubleshooting and component replacement. Purge all sensitive information before releasing equipment for contract maintenance. The CSSO conducts, verifies, and documents sanitization of any media (hard drive or memory) that requires vendor/contract maintenance or replacement. Sanitization procedures are listed in AFSSI 5020, *Remanence Security*.

5.7.2. **Software Maintenance.** Remote diagnostics must be restricted (e.g., length of remote session, authorized personnel) and approved by the network DAA. The system administrator conducts software maintenance and installs vendor patches.

**5.8. Declassification and Destruction.** Since the highest level of information on the base network is sensitive, declassification will only be necessary when classified information inadvertently contaminates the network. Declassification is an administrative procedure wherein media is sanitized of the classified information and the sanitization is verified. In this context, it should not be confused with declassifying information in accordance with AFI 31-401. Destruction is done with approved devices in accordance with AFSSI 5020 for magnetic media and AFI 31-401 for paper.

5.8.1. **Sanitizing Storage Media.** Sanitize network or desktop systems that are inadvertently contaminated with classified information using an approved degausser. If degaussing is not practical, the DAA may approve the use of an assessed overwrite routine (Norton Utilities Wipe, Unishred Pro, etc.). CSSOs, workgroup managers, and system administrators work together with consultation provided by the Wing IP Office to develop and perform sanitization procedures. Remember these procedures must be approved by the DAA after consultation with the information owner.

5.8.2. **Output Products Destruction.** Make sure an approved shredder is available for destruction of documents containing sensitive information.

**5.9. Vulnerabilities and Incidents.**

5.9.1. **Reporting.** Proper reporting of newly discovered vulnerabilities and incidents ensures containment of impact, recovery of network availability, identification of breach and perpetrator, and

countermeasure implementation. CSSOs train users on vulnerability and incident reporting procedures. CSSOs, workgroup managers, system administrators, and network managers must comply with the procedures found in AFSSI 5021, *Vulnerability and Incident Reporting*.

5.9.2. **Protecting.** All IP operators, system administrators, CSSOs, and Wing IP Office personnel must subscribe to AFCERT and ASSIST advisory distribution lists and implement patches as appropriate.

**5.10. Encryption.** Use National Security Agency Type I or II endorsed products or National Institutes of Standards and Technology Federal Information Processing Standard 140-1 validated products when transmitting sensitive information IAW AFSSI 4100.

**5.11. Information Protection Tools.** Use only AF/SC approved IP tools. These tools are operated by the NCC and in some cases, system administrators. 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.

5.11.1. **Use.** 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. Guidance will be further expounded upon in the forthcoming 33-208, Information Protection Operations.

5.11.2. **Training on IP Tools.** All personnel (to include contractors) required to use IP tools will be trained on the use of the tools and the rules of engagement, either through Air Force approved courses, or through on-the-job training conducted by personnel who received their training from Air Force approved courses.

**5.12. Barrier Reef.** AF/SC has endorsed the Air Force Barrier Reef Process as the official concept for boundary protection of Air Force networks. NCCs are to incorporate the barrier reef process in preparation for Combat Information Transfer System/Base Information Protection (CITS/BIP) implementation. Barrier Reef is the electronic equivalent of the physical perimeter defense provided on our AF bases by our security forces. Proxies and firewalls act as electronic “gate guards,” inspecting traffic and allowing only the traffic that is authorized to traverse the network. The Barrier Reef policy stance is “Allow authorized traffic and Deny all else.” The Barrier Reef process was operationally validated at Barksdale AFB by a team of AFCA engineers. The Barksdale AFB Case Study may be downloaded from the Barrier Reef Homepage. The Barrier Reef process consists of 12 steps.

5.12.1. **Know Thyself.** Identify and reduce exterior network access points to a manageable number, all under NCC control. Conduct traffic analysis to determine the protocols and throughput that currently exist.

5.12.2. **Requirements Determination.** Validate the traffic identified in Step 1 is mission required.

5.12.3. **Policy Formation.** Create a base-level network security policy, involving all tenants and functional areas (the policy contained in this publication is a good place to start). “Deny all that is not specifically allowed”--enumerate all allowable services.

- 5.12.4. **Filter Packets.** Take advantage of existing router Access Control List (ACL) capabilities. Block as many unsafe services as possible based on Transmission Control Protocol/Internet Protocol (TCP/IP) headers.
- 5.12.5. **Monitor Network.** Integrate network monitoring device(s) such as the Automated Security Incident Monitor (ASIM). Place outside the boundary protection mechanism to monitor all attempted attacks.
- 5.12.6. **Integrate Time Server.** Integrate GPS receiver to provide a reliable, accurate time source for base systems. Protect base from introduction of false time.
- 5.12.7. **Centralize Dial-in Access.** Aggregate multiple dial-in solutions into one centralized service. Protect access through this service via strong authentication of users.
- 5.12.8. **Proxy World-Wide Web Requests.** Direct all outgoing WWW requests through a WWW proxy device to hide users' identities from Internet eavesdroppers, reduce wide-area network utilization and improve user response time. Provide positive control over web access to unauthorized sites.
- 5.12.9. **Internet and Intranet Services.** Place the Web servers in demilitarized zone to reduce internal network access. Establish a system to keep public data updated and separate from internal web servers. Provide a public "lobby" for e-mail entry and access to data for wide distribution.
- 5.12.10. **Proxy Common and Special Services.** Authenticate outside users before granting access for "dangerous" services (TELNET, ftp). Implement controlled access for specialized AF services (e.g., Info Connect).
- 5.12.11. **Conceal Network.** Hide internal network address space from public domain. Separate public and private domain name servers (DNS).
- 5.12.12. **Train, Maintain, and Certify.** Establish continuity for training, system changes, and upgrades. Certify and accredit boundary protection system and the base network.

## CHAPTER 6

### NETWORK INFRASTRUCTURE SERVICES AND PROTOCOLS POLICY

**6. General.** This section defines common infrastructure services and policies, their vulnerabilities, and states the policy for usage. For the purposes of this document, inbound is defined as coming from outside the base network boundary (i.e., from the internet). Outbound is defined as originating within the base network and leaving the base network boundary (to the internet). NOTE: In this chapter, the acronym IP stands for Internet Protocol vice Information Protection.

#### **6.1. Simple Network Management Protocol (SNMP).**

**6.1.1. Description.** SNMP is used for remote management of networks and network devices. SNMP uses TCP and User Datagram Protocol (UDP) ports 161 and 162.

**6.1.2. Vulnerabilities.** Risks include the disclosure and modification of settings on managed objects via spoofing and sniffing attacks, allowing an attacker the opportunity to change the network configuration or to shut down the network. Additionally, an attacker could obtain a complete mapping of a network via SNMP. The enhanced security features in the latest version of SNMP have not been accepted by the industry and are generally not implemented.

**6.1.3. Policy.** Prohibit inbound and outbound SNMP traffic across the security perimeter. However, if required, outbound SNMP traffic from a specified (internal) management system to a specified list of (external) systems being managed can be permitted. IP address-based packet filtering can be used to restrict outbound traffic.

#### **6.2. Domain Name System (DNS).**

**6.2.1. Description.** DNS provides a mechanism for translating host names to IP addresses and vice-versa. DNS also provides translations for mail host addressing. DNS operates on TCP/UDP port 53.

**6.2.2. Vulnerabilities.** Allowing inbound access to an internal DNS server may provide an attacker with access (via DNS zone transfer) to a complete list of internal hosts. Additional information such as host information and mail routes might be compromised. This might enable an attacker to determine employee-specific information such as movement between projects. Additionally, an attacker may cause false information to be loaded into the name server's cache if the name server is configured incorrectly. If a remote connection to a host is based on an access control list that relies on the name of the remote host, DNS spoofing could allow an intruder to gain unchallenged access.

**6.2.3. Policy.** The authoritative source for reverse address resolution must be the NCC DNS. Where possible, use a split server configuration using two DNS servers, one inside and one outside the security perimeter. Some firewalls provide this split DNS function. The internal server provides the names and addresses of all internal hosts. Any internally generated unresolved queries are passed through the internal DNS server to the external DNS server which resolves the query. Externally generated queries merely resolve to the name of the gateway host. DNS traffic is only permitted across the security perimeter between the two DNS servers; all other traffic is disallowed by blocking TCP/UDP port 53. In either case, the latest version of software should be used on all internal workstations.

#### **6.3. Network Time Protocol (NTP).**

6.3.1. **Description.** NTP provides a means for host time synchronization across a network regardless of system clock speed or network throughput. NTP uses UDP port 123.

6.3.2. **Vulnerabilities:** An intruder could use a time replay attack to alter system clocks. This could subvert time-based processing. Time stamps would be inaccurate. Time-based authentication mechanisms such as Kerberos would be affected. Other attacks could include the manipulation of system logs such that attack attempts appear to happen at incorrect times.

6.3.3. **Policy.** Do not allow NTP traffic to flow across the security perimeter. This can be accomplished by filtering out packets to UDP port 123. Establish an NTP server within the enterprise obtaining the correct time locally from other sources such as Global Positioning Satellites. (If there is no local source, use multiple external sources and restrict NTP across the security perimeter to traffic between the designated internal NTP server to the designated remote NTP servers.)

#### 6.4. Syslog.

6.4.1. **Description.** The syslog service is a general-purpose logging facility for system events such as hardware and software errors. The facility is controlled by the syslogd program which reads messages from the special file `/dev/log` (on some systems another file, `/dev/klog`, is used for kernel messages) and a UDP port specified in `/etc/services`, typically 514. When a message is received, syslogd stores the message in a file, or submits it to another host's syslogd, based on facility and level flags associated with the message. Programs submit messages to syslogd via the syslog function. A command line interface to the syslog function, `logger`, is available, typically used for shell scripts.

6.4.2. **Vulnerabilities.** Bogus messages may be submitted by users to cause false alarms. The files that syslogd stores messages in can be written to until the file system is full, preventing subsequent messages from being logged. This could be used by a successful attacker to hide from auditing. On some systems, the syslog function does not perform appropriate bounds checking on the message submitted to it, which is copied to a static buffer. An attacker could use this vulnerability to run arbitrary code by doing something that causes the program to generate a log message large enough to overflow the buffer and push arbitrary machine-executable code onto the stack. Note that this is not a problem with the syslogd program but rather with all programs that call the syslog function.

6.4.3. **Policy.** Do not allow Syslog messages to pass inbound or outbound across the security perimeter. Ensure that at least all systems that might be accessible from the Internet have either been patched or are running OS versions that do not have the syslog vulnerability.

#### 6.5. Finger.

6.5.1. **Description.** The finger service is used to look up information about users logged into a particular host. This information can include a user name, the user's real name, and possibly other information such as office location or phone number (at the discretion of the target host's administrator). The finger service uses TCP port 79.

6.5.2. **Vulnerabilities.** An attacker can obtain a list of valid user names currently logged into a host and those that are not logged into the host. From this, an attacker could determine when the users are likely to be logged in and therefore the best time to attack a particular account. Finger is subject to data-driven attacks. Terminals that allow for keys programmable via sequences of control characters

could suffer attacks. One such attack might program the string “rm -rf \*” into a key and cause it to be executed.

6.5.3. **Policy.** Do not allow incoming finger requests to pass across the perimeter. This is accomplished by IP port filtering TCP port 79. Outbound finger requests can be safely handled by the *safe\_finger* program that comes with the TCP Wrappers suite, which limits finger output to printable characters.

## 6.6. Network Information System/Yellow Pages (NIS/YP).

6.6.1. **Description.** NIS/YP provides distributed access to centralized databases. These databases, known as *maps*, can contain anything the administrator wishes but are commonly used to provide password, host, services, and mail alias data. The centralized database provides this information on and for hosts and users in its NIS/YP domain. This NIS/YP domain is separate and distinct from an enclave’s Internet domain. NIS/YP uses the Sun RPC service. Sun RPC is discussed later in this section.

6.6.2. **Vulnerabilities.** Attackers can attack NIS in two ways: attacking the NIS protocols or attacking the underlying Sun RPC services. Attackers who are able to obtain the NIS domain name of a host may be able to direct NIS to deliver the entire contents of the *passwd* map suitable for cracking. NIS domain names can be obtained by the *domainname* command or they can be guessed. (A user must be logged into a host to be able to execute the *domainname* command.) Some early versions of NIS allow attackers to substitute their own NIS servers for the real server and to provide their own *passwd* maps. This can be accomplished by creating a program that emulates the NIS server process *ypserv* by answering queries from the client program *ypbind*. Should an attacker be able to create a counterfeit *ypserv* process and supply a counterfeit *passwd* map, unrestricted access to the host could be gained.

6.6.3. **Policy.** Do not allow NIS to travel inbound or outbound across the perimeter. This is done by disallowing Sun RPC *portmap* traffic by filtering access to TCP/UDP port 111. This prohibits access to the *portmapper* and therefore effectively shuts off easy access to most RPC-based services. In this security policy, however, no RPC-based services are permitted to traverse the security perimeter, so access to the *portmapper* should be denied. Consistent with the basic security policy, *all* UDP ports should be blocked unless required for a specific service. This prevents the direct access to NIS via port guessing.

## 6.7. Internet Control Message Protocol (ICMP) and TCP/UDP ECHO Services.

6.7.1. **Description.** ICMP provides a number of diagnostic and error notification facilities for the Internet Protocol (IP). ICMP is implemented as an unreliable protocol over IP, as specified in RFC 792. ICMP is integral to the efficient operation of the IP network. Because many of the ICMP messages are generated during times of network stress, and may be subject to high loss rates, IP operation will continue without ICMP messages, although less efficiently.

6.7.2. **Vulnerabilities.** ICMP can be used to map a network via “ping,” “traceroute,” or packet probing looking for host or network unreachable messages. Service can be denied by sending bogus ICMP unreachables or source quench messages. Traffic can be misdirected using ICMP redirects.

6.7.3. **Policy.** Do not allow inbound “echo request,” “time to live exceeded,” and “redirect” packets (to block inbound ping, traceroute, and direct attacks, respectively). All other ICMP messages should be allowed in both directions.

## 6.8. Routing Services.

6.8.1. **Description.** Routing Information Protocol (RIP), Border Gateway Protocol (BGP), Internet Gateway Routing Protocol (IGRP), and Open Shortest Path First (OSPF) are used for managing the routing of packets through the network.

6.8.2. **Vulnerabilities.** Routing protocols can be exploited by a malicious user to redirect packets in an attempt to capture information or to disrupt services.

6.8.3. **Policy.** Do not allow inbound or outbound routing protocols across the security perimeter. This prevents Internet routing attacks from corrupting the internal sites. Routing protocols are permitted to run internally and externally provided they do not traverse the perimeter.

## 6.9. Simple Mail Transport Protocol (SMTP).

6.9.1. **Description.** SMTP is a common means of sending and receiving electronic mail throughout the Internet. SMTP servers use TCP port 25 and are found on all UNIX variants and on many other platforms. Newer electronic mail application systems support SMTP in addition to their own proprietary formats.

6.9.2. **Vulnerabilities.** SMTP is text-based, i.e., the synchronization of mail agents and the addressing of mail messages are accomplished via a two-way communication using clear text messages in lieu of specific binary representations of commands. Electronic mail messages can be intercepted by network sniffing. An SMTP server is unable to distinguish between a server providing data and data entered by a malicious user at a keyboard. Other than the possibility of data-driven attacks and the ease of mail forgery, SMTP has no inherent vulnerabilities. However, many SMTP-based servers, *sendmail* in particular, are prone to attack. Because of their complexity, these servers contain many bugs and features that can be exploited to cause damage to a network. For example, *sendmail* functions such as sending mail to a program or the debug feature, left many systems open to attack.

6.9.3. **Policy.** Permit inbound SMTP traffic across the security perimeter using a centralized secured mail forwarder as the mail agent for the protected domain. If using Sendmail, use privacy options to disable the use of *expn* and *vrify* commands. Some bases may wish to use multiple forwarders for redundancy or performance reasons (this protects against flawed SMTP-based servers). As an added precaution, hosts requiring the *sendmail* agent must run the most up-to-date version of *sendmail*. Allow outbound SMTP to traverse the perimeter unimpeded; however, for operational and management reasons, it may be easier to direct outgoing SMTP traffic through the centralized mail forwarders also.

## 6.10. X.400 Electronic Mail.

6.10.1. **Description.** The X.400 Electronic Mail messaging protocol was developed as part of the Open Systems Interconnection (OSI) protocols by the International Standards Organization (ISO). X.400 uses TCP ports 103 and 104.

6.10.2. **Vulnerabilities.** There is little information on the security implications of X.400 as there are only a few X.400 mail networks available or in use. The advent of the Defense Message System will significantly increase usage of X.400 protocol. Vulnerabilities such as data-driven attacks and mail

forgery that exist in other types of electronic mail systems also exist in X.400-based electronic mail. Electronic mail messages can be intercepted by network sniffing.

**6.10.3. Policy.** X.400 is similar to SMTP and should be treated accordingly. Specifically, route inbound X.400 traffic through a central Message Transfer Agent (MTA). Outbound traffic can be directly routed; however, for operational and management reasons, it too should be routed through the central MTA. A proxy-based solution is not recommended since there are currently neither widely known X.400-based attacks that could be easily detected using a proxy nor in fact do any X.400 proxies exist.

### **6.11. X.500 Directory Services.**

**6.11.1. Description.** The X.500 Directory Services provide a user's distinguished name and encryption keys. X.500 is generally employed in concert with the X.400 mail services. X.500 uses TCP port 102.

**6.11.2. Vulnerabilities.** The X.500 directory service features of greatest concern are the distribution of encryption keys that pertain to a given user and the distribution of host names, account names, and the possible disclosure of an internal organizational structure.

**6.11.3. Policy.** Due to the sensitivity of X.500 data, support X.500 directory services using a split server approach. An intermediate Directory Server Agent (DSA) outside the perimeter with *minimal* X.500 directory services (distinguished names, O/R addresses, and Fortezza certificates) responds to external X.500 queries. Another master database—larger and more complete—should be located inside the security perimeter and used to respond to internal X.500 queries. If necessary, internal queries should be “chained” across the perimeter to the outside DSA. Therefore, restrict inbound and outbound X.500 to the designated internal and external DSAs only.

### **6.12. Post Office Protocol (POP).**

**6.12.1. Description.** The POP allows a user to read mail messages that are stored on a central server. POP3, the latest version, uses TCP port 110, while POP2 and older versions use TCP port 109.

**6.12.2. Vulnerabilities.** Passwords and electronic mail messages are sent across the network in the clear and therefore can be intercepted by network sniffing.

**6.12.3. Policy.** Do not allow inbound or outbound POP traffic across the security perimeter without enforcing strong authentication.

### **6.13. Network News Transport Protocol (NNTP).**

**6.13.1. Description.** NNTP is used for the transportation of USENET articles. NNTP runs on TCP port 119.

**6.13.2. Vulnerabilities.** NNTP security is controlled by an Access Control List (ACL) that determines which systems can use the different features of NNTP. The ACL can be based on a host name, rendering it vulnerable to DNS spoofing attacks, or by IP address. The NNTP protocol is similar to the SMTP protocol in that the synchronization and delivery of messages is text-based and vulnerable to forgery. A successful attack against an NNTP server may allow an unauthorized user to read or post articles or obtain access to a shell. If an organization has specific groups for discussion of internal and sensitive topics, an intruder may be able to read confidential information. Offensive

messages could also be posted via a compromised server. Since program source code can be distributed via USENET, there is the risk of data-driven attacks.

**6.13.3. Policy.** Allow inbound and outbound NNTP traffic to traverse the security perimeter. However, permissible connections should be limited to internal and external NNTP servers specifically designated by IP address. Multiple internal or external servers may be designated for redundancy.

#### **6.14. UNIX ‘r’ Commands.**

**6.14.1. Description.** The UNIX ‘r’ commands (*rlogin*, *rsh*, *rexec*) are commands that use the remote access protocols. They provide methods of performing functions on remote hosts without having to explicitly log in to those hosts with an account name and password. The *rexec* command (TCP port 512) allows users on one host to execute commands on a remote host without logging in. The *rlogin* command (TCP port 513) allows a user to log in to a remote host without typing a user name. If the connection comes from a trusted host (as defined by the content of the files */etc/hosts.equiv* and *~/.rhosts*), the user need not enter a password. The *rsh* command (TCP port 514) provides similar functionality but for the purpose of executing one command only. Authentication is accomplished at the server by examining the source port to see if it is less than 1024 and by examining two null-terminated strings for the local user name and the remote user name. A host is defined as trusted if there is an appropriate entry in the server’s */etc/hosts.equiv* or user’s *~/.rhosts* file on the server. If a plus sign (+) appears in either of these two files, attackers using an identical user name will be able to access the host from any host on the network.

**6.14.2. Vulnerabilities.** The *rexec* authentication is accomplished by sending the command, user name, and password in clear text to the server *rexecd*. The server does not authenticate based on IP address. The *rexecd* differentiates between invalid user names and passwords by returning the messages “Login incorrect” for invalid user names and “Password incorrect” for invalid passwords. Thus, it is possible to determine a valid user name by repeatedly executing a simple command providing different user names and waiting until the “Password incorrect” message is displayed. The *rlogin* authentication is derived from the user name as it is passed from the client to the *rlogind* server running on the remote host. The user name is passed through the network in clear text, rendering it vulnerable to sniffing attacks. Connection hijacking of established connections is also feasible. However, *rlogin* is less risky to network sniffing than is TELNET, as the user’s password is not necessarily transmitted across the network. The *rsh* vulnerabilities are similar to those for *rlogin*.

**6.14.3. Policy.** Do not allow ‘r’ commands across the security perimeter.

#### **6.15. TELNET.**

**6.15.1. Description.** TELNET (TCP port 23) is a remote access protocol that allows one to have a “virtual terminal” connected to any host on the Internet possessing a TELNET server. Once a TELNET session is established and a valid user name and password are entered, keystrokes entered at the user’s keyboard are effected on the remote host, and output from the remote host is displayed on the user’s screen.

**6.15.2. Vulnerabilities.** The vulnerabilities intrinsic to TELNET include the interception of keystrokes, including a user name and password via sniffing. Additionally, there is the risk of having an established connection “hijacked,” where an attacker assumes control of an active session.

6.15.3. **Policy.** Permit outbound TELNET connections across the security perimeter. Inbound TELNET connections are only permitted when used with strong authentication. When possible, use proxies that encrypt TELNET traffic in order to protect against session hijacking.

### 6.16. X Window System (X).

6.16.1. **Description.** The X protocol allows a user to run a variety of applications in a client/server environment. The X protocol uses TCP ports 6000 through 6063. X allows multiple virtual user windows on a single display screen and provides a rich graphics environment. There are two basic protection mechanisms: *xhost* allows activities only from specified hosts based on IP address, and *xauth* provides a similar protection by way of a “magic cookie” complex text string.

6.16.2. **Vulnerabilities.** There are numerous methods of attacking systems that use the X protocol. One method is for an attacker to create an invisible window that encompasses all the windows on the screen, the keyboard, and the mouse. All window displays are directed to the attacker’s host without the knowledge of the victim. Keyboard and mouse entries are directed to the victim host, allowing the attacker to execute commands on the victim host. Another method takes advantage of lax *xhost*/*xauth* configurations. Without access controls enabled, an attacker would be able to start a window session remotely and execute commands on the victim host.

6.16.3. **Policy.** Because of the current state of X Window System proxies, do not allow inbound and outbound X connection requests.

### 6.17. Sun Remote Procedure Call (Sun RPC).

6.17.1. **Description.** The Sun RPC facility is used by many client/server applications. Sun RPC supports both UDP and TCP, but the majority of applications use the UDP implementation. Sun RPC applications can exist at a fixed port or at random ports, making it difficult to support via a proxy or packet filter. Sun RPC-based server applications may use different port numbers on different invocations. By registering with the *portmap* (SunOS) or *rpcbind* (Solaris) process, an application is assigned a port number. Client applications connect to TCP/UDP port 111 on a remote host and query the portmap process for the server’s port number by providing a unique Sun RPC identifier. It is not necessary to use the portmap process to use the Sun RPC facilities.

6.17.2. **Vulnerabilities.** Network port numbers belonging to Sun RPC-based applications can be determined via the *rpcinfo* command. A user need not be logged into a specific host to determine the port numbers in use on that host. Once new port numbers are known, new services can be discovered and may be attacked. Early versions of the portmap process allowed any application to register itself as a Sun RPC server. This allowed an attacker the opportunity to register a clandestine NIS server and provide phony user names and passwords.

6.17.3. **Policy.** Do not allow inbound and outbound Sun RPC traffic. Blocking Sun RPC-based applications is accomplished by disallowing UDP packets for UDP port 111 and all other UDP ports that are not needed by a required service.

### 6.18. HyperText Transfer Protocol (HTTP).

6.18.1. **Description.** HTTP is a recent protocol and is the basis for the World Wide Web (WWW), providing the most user-friendly interface to the Internet. HTTP servers use TCP port 80 as the default, but are configurable to allow other ports as well.

6.18.2. **Vulnerabilities.** Risks inherent in HTTP include the disclosure of information such as a credit card number and the discovery of Web pages through the use of link pointers. As the protocol and the types of services grow, more vulnerabilities are being discovered. These include the ability of malicious programs written in mobile code such as Java or Visual Basic languages to download malicious code or to mail sensitive files to the attacker without the consent or knowledge of the user. HTTP servers allow unchecked information, documents, and programs to be retrieved, allowing for the possibility of the introduction of a virus or Trojan Horse, many of which can be discovered via antivirus tools. Finally, HTTP Server may be configured to run on nonstandard ports. There is a risk of having a server run on a port that is allowed across the perimeter.

6.18.3. **Policy.** Use dual servers with one server outside the perimeter containing documents for public access and another protected server inside the perimeter containing documents for internal use only. Do not allow inbound connections requests across the security perimeter; they are only permitted to the external server. Outbound connections to the internal server do not traverse the security perimeter and are permitted. Use an HTTP proxy for outbound connections traversing the security perimeter to external web servers (to support nonstandard port usage, caching, URL access restrictions, logging, etc.).

## 6.19. Gopher.

6.19.1. **Description.** Gopher is a menu-driven, text-based means for browsing, organizing and publishing information on the Internet. Gopher servers usually run on TCP port 70. Gopher can be configured to automatically run applications associated with a document. For instance, if a document is a GIF file, Gopher may automatically run a GIF viewer.

6.19.2. **Vulnerabilities.** Gopher access control is based on IP addresses, rendering it vulnerable to DNS attacks. Gopher allows unchecked information, documents, and programs to be retrieved, allowing for the possibility of the introduction of a virus or Trojan horse, many of which can be discovered via antivirus tools. A partially implemented “put” command may be present in some Gopher servers which could be used to write files to the server’s disk.

6.19.3. **Policy.** Use dual servers with one server outside the perimeter containing documents for public access and another protected server inside the perimeter containing documents for internal use only. Do not allow inbound connections requests across the security perimeter; they are only permitted to the external server. Outbound connections to the internal server do not traverse the security perimeter and are permitted. Outbound connections traversing the security perimeter to external gopher servers are to be via a gopher proxy (to support nonstandard port usage, caching, logging, etc.).

## 6.20. Wide Area Information Servers (WAIS).

6.20.1. **Description.** WAIS is a database indexing and searching tool. WAIS generally uses TCP port 210.

6.20.2. **Vulnerabilities.** WAIS access control is based on IP addresses, rendering it vulnerable to IP spoofing and DNS attacks. WAIS will allow unchecked information, documents, and programs to be retrieved, allowing for the possibility of the introduction of a virus or Trojan horse, many of which can be discovered via antivirus tools.

6.20.3. **Policy.** Use dual servers with a server outside the perimeter containing documents for public access and a protected server inside the perimeter containing documents for internal use only. Do not allow inbound connection requests across the security perimeter; they are only permitted to the external server. Outbound connections to the internal server do not traverse the security perimeter and are permitted. Outbound connections traversing the security perimeter to external WAIS servers is to be via a WAIS proxy (to support nonstandard port usage, caching, logging, etc.).

#### 6.21. Archie.

6.21.1. **Description.** Archie is a mechanism for searching anonymous FTP archives. It uses UDP port 1525. Archie servers are becoming less populated with the advent of Web browsing software.

6.21.2. **Vulnerabilities.** The risks involved with using Archie are identical to those in any UDP-based service. Data-driven attacks are possible.

6.21.3. **Policy.** Disallow inbound Archie by filtering out packets destined for UDP port 1525. Run Archie servers outside the perimeter. Users requiring access to Archie client services use TELNET to contact the server with the user name *archie*, or Email using the address format *archie@some.host.domain*, or access the Archie WWW interfaces.

#### 6.22. File Transfer Protocol (FTP).

6.22.1. **Description.** FTP operates on TCP ports 20 and 21. FTP provides the capability to transfer files between hosts. User authentication is handled via a user name and a corresponding password. There is an optional facility to relax user authentication by way of the user name “anonymous” and an arbitrary password (usually the user’s email address). An example of a service involving anonymous FTP would be the providing of information to the general public with no provision for the public to deliver files to your host.

6.22.2. **Vulnerabilities.** The risks inherent with FTP include misconfigured software that allows an intruder to deliver unwanted files containing malicious software or contraband, the possibility of denial of service because of a full disk, or the interception of valid user names and passwords via network sniffing. An attacker could observe a valid user name and password via a sniffing attack and use the information for subsequent accesses. Data obtained via FTP poses the same risks as any data transferred via the Internet, particularly data-driven attacks.

6.22.3. **Policy.** Allow inbound FTP to traverse the security perimeter using strong user authentication. Should there be a requirement for anonymous FTP service, implement on a host outside the security perimeter. Permit unrestricted outbound FTP.

#### 6.23. Trivial File Transfer Protocol (TFTP).

6.23.1. **Description.** TFTP is a UDP-based file transfer mechanism using port 69.

6.23.2. **Vulnerabilities.** TFTP has no security. If not properly configured, TFTP will allow a user (or attacker) to download or upload any host file.

6.23.3. **Policy.** Do not allow inbound and outbound TFTP traffic across the security perimeter.

#### 6.24. Network File System (NFS).

6.24.1. **Description.** NFS is a method of sharing entire file systems between hosts. NFS is an RPC-based application using UDP that shares many of the RPC vulnerabilities listed in prior sections.

6.24.2. **Vulnerabilities.** NFS provides an access control list based on IP address and is thus vulnerable. Improperly configured NFS allows attackers to plant Trojan Horse or other types of malicious programs. Some versions of NFS software limit the access control list (ACL) to 10 hosts or 255 characters. Lists that exceed this limit are ignored without warning, disabling access controls entirely and allowing for mounting of an NFS-shared file system to any host on the Internet. Attackers need merely create a user name whose User-ID (UID) maps to an identical UID on the NFS host to manipulate files on an NFS-shared file system. Finally, if the local host exports its file system to itself, external mount requests sent to the portmapper and forwarded to the NFS server are treated as local requests, thus potentially granting access to a remote host despite any ACL.

6.24.3. **Policy.** Do not allow inbound and outbound NFS traffic across the security perimeter.

### 6.25. Printing (lpd).

6.25.1. **Description.** Printing protocols have simple IP address-based access control built in. The protocols use TCP port 515.

6.25.2. **Vulnerabilities.** The address-based access control is subject to IP spoofing and DNS attacks. A denial-of-service attack can be mounted by filling a target disk.

6.25.3. **Policy.** Do not allow inbound printing traffic across the security perimeter. Allow outbound printing.

### 6.26. SQL\*Net.

6.26.1. **Description.** SQL\*Net is Oracle's network interface that allows communications to Oracle products over the network. SQL\*Net uses TCP port 1525 as the default.

6.26.2. **Vulnerabilities.** SQL\*Net provides little authentication on its own, although the Oracle C2 product offers password encryption. Authentication may be based on an Oracle user name and password combination or based on a UNIX user name and password combination, depending on the Oracle configuration. There is a possibility of unauthorized retrieval or overwriting of data.

6.26.3. **Policy.** Allow inbound SQL\*Net traffic to pass across the security perimeter only if the Oracle Secure Network Services (SNSs) are implemented. Allow outbound SQL\*Net traffic.

### 6.27. Talk.

6.27.1. **Description.** Talk (UDP port 517 or 518) is a text-based method of chatting between two users. Talk uses a complex multiple connection method between clients and servers. Talk sets up connections via UDP ports 517 or 518 while data flows across arbitrary TCP ports greater than 1023. This leads to the virtual impossibility of being able to filter or proxy this protocol. Note that similar functionality is offered via Web servers that support Web Chat.

6.27.2. **Vulnerabilities.** Talk does not filter data to permit text-only messages. This allows an attacker to include a Trojan Horse in a message. Examples include *block send* or *answer back* sequences that cause a terminal to execute an arbitrary command or change terminal settings.

6.27.3. **Policy.** Do not allow inbound and outbound Talk connections across the security perimeter (by blocking access to UDP ports 517 and 518).

### 6.28. Internet Relay Chat (IRC).

6.28.1. **Description.** Internet Relay Chat (IRC) generally uses TCP port 6667. IRC provides a method for multiple users to form virtual rooms in order to communicate with one another. Some enhanced Web browser plug-ins support IRC, but if IRC is blocked, the full functionality of the Web browser is restricted.

6.28.2. **Vulnerabilities.** If the IRC requires a user name and password to be accessed, naive users may use the same user name and password used on their internal hosts. New users may be coerced into exploring a “feature” that is in reality a harmful device. Determining whether an IRC contains a back door can be difficult.

6.28.3. **Policy.** Do not allow inbound and outbound IRC connections across the security perimeter.

### **6.29. Multicast Backbone (MBONE).**

6.29.1. **Description.** The MBONE provides a method for transmitting real-time audio and video to the Internet. The protocol uses Multicast which is difficult to proxy.

6.29.2. **Vulnerabilities.** The MBONE is a high-volume service and is prone to causing denial of services by flooding a network.

6.29.3. **Policy.** Do not allow inbound and outbound MBONE connections across the security perimeter.

### **6.30. RealAudio.**

6.30.1. **Description.** RealAudio provides for streaming sound over the Internet using TCP port 7070 and UDP ports 6970 through 7170. This means a user need not download an entire file before playing the sound. Real Audio uses a large number of UDP ports to transmit the sound data.

6.30.2. **Vulnerabilities.** Newer versions of RealAudio have the capability to control multimedia applications and possibly other programs on a workstation.

6.30.3. **Policy.** Allow inbound and outbound RealAudio connections across the security perimeter only with the use of proper proxies.

### **6.31. Lotus Notes.**

6.31.1. **Description.** Lotus Notes has a wide range of functionality built in. It is possible to provide server-to-server connectivity across the security perimeter. Lotus Notes uses TCP port 1352.

6.31.2. **Vulnerabilities.** Risks include the possibility of data disclosure and electronic mail forgery. Lotus Notes also provides mail macro capabilities that can be exploited to deposit letter bombs, Trojan horses, viruses, etc.

6.31.3. **Policy.** Allow inbound and outbound server-to-server connectivity to pass across the security boundary. (A one-to-many server communications can be accomplished by means of a star server. Each Lotus Notes server communicates with a hub server one-to-one. The latest versions of Lotus Notes provide encryption to deter sniffing and IP spoofing attacks. At least one third-party product—from Sybari software—can protect against the application layer macro-based attacks alluded to above).

### **6.32. Intrusion Detection Tools Registered on DARPA Internet Domain Name Servers.**

6.32.1. **Description.** These tools (such as ASIM) frequently are found registered on the Defense Advanced Research Products Agency Internet domain name servers.

6.32.2. **Vulnerabilities.** Misnamed IP addresses can give potential intruders information about network security tools within the protected domain. This information could include the type of monitoring software used and its placement on the network. An example of misnaming is listing the ASIM host as asim.somebase.af.mil. By defeating the security tools ability to monitor a network, an intruder could gain access to the domain unnoticed.

6.32.3. **Policy.** Limit the ability of outside sources to do zone transfers. Use ambiguous names for IP addresses of network monitoring tools such as the hostname provided by the AFCERT for ASIM systems.

### 6.33. NetBIOS.

6.33.1. **Description.** There are two main ways to allow users to access servers. DNS can be used to resolve the correlation between a name and its IP address (the main way for the Internet). NetBIOS Name Resolution is an easier method usually used for intranets. Windows-based networks (Win95, WinNT) can use the NetBIOS naming scheme for systems in which name resolution is done by systems announcing their NetBIOS name across the network or by using a static mapping in the LMHOSTS file. This can be enhanced by using a centralized WINS server to resolve NetBIOS names.

6.33.2. **Vulnerabilities.** Using NetBIOS on the Internet can be dangerous, for all that a user needs to do is find the name (which is easy if it is broadcasting), type it in to locate the server, and exploit any shared entities. When installing WinNT, a NetBIOS share (file, directory, or resource) is created that by default has all access enabled (anyone with computer access have full access to the NetBIOS share). NetBIOS uses three ports: 137 (NetBIOS Name Service), 138 (NetBIOS Datagram Service), and 139 (NetBIOS Session Service). Port 139 gives a person with NT knowledge the ability to steal your username and password. This could be very damaging if the username they steal has Administrator rights. This also allows hacker programs such as Win-Nuke to wreak havoc on a system. Port 139 would be open due to the use of a TCP/IP WINS client (only Windows machines use this). If Port 139 is closed, someone trying to TELNET to your machine will not get a connection. Of course, this will also hinder any WINS DNS resolution. If the WINS client is disabled, file shares are not possible which renders your username and password unretrievable.

6.33.3. **Policy.** Block ports 137-139 at the router or firewall.

**CHAPTER 7**  
**NETWORK USE**

**7. General.** Use networked resources for official or authorized use only. Consult AFIs 33-112, *ADPE Management*, 33-119, *Electronic Mail Management and Use*, and 33-129, *Transmission of Information via the Internet* for specific policy.

## CHAPTER 8

### ACCREDITATION

**8. General.** Accredit the base network IAW AFD 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. Use AFSSI 5024, *Certification & Accreditation* to complete accreditation. Due to the size of the base network, it is advisable to accredit the base backbone and organizational LANs individually.

**8.1. Accreditation Documentation Policy.** 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 MAJCOM IP office.

**8.2. Reaccreditation Policy.** Reaccredit every three years or upon significant change 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 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 re-usable in a reaccreditation.

## **CHAPTER 9**

### **SECURITY, AWARENESS, TRAINING AND EDUCATION**

**9. General.** The CSSO conducts security training and awareness using AF training materials and software available from the Wing IP Office. HQ AFCA provides these materials to all MAJCOMs, FOAs, and DRUs. Training minimum is one hour of training on an annual basis.

**JOHN D. COLLIER, Lt Col, USAF**  
**Chief, Networks Division**

## GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

### *References*

NIST (National Institutes of Standards and Technology) FIPS (Federal Information Processing Standard) 140-1, 11 Jan 94

AFMAN 10-401, *Operational Plan and Concept Plan Development and Implementation*, 28 Oct 94

AFI 31-101v1, *The Air Force Physical Security Program*, 1 Dec 96

AFI 31-209, *The Air Force Resource Protection Program*, 10 Nov 94

AFI 31-401, *Managing the Information Security Program*, 22 Jul 94

AFI 33-112, *Automated Data Processing Equipment (ADPE) Management*, 1 Dec 97

AFI 33-114, *Software Management*, 30 Jun 94

AFI 33-115, *Network Management*, 1 Apr 96

AFI 33-119, *Electronic Mail Management and Use*, 1 Mar 97

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

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

AFI 33-204, *Security Awareness, Education and Training*, 1 Oct 97

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

AFSSI 5009, *Information Protection Interim Toolset*

AFSSI 5013, *Identification and Authentication* (future AFMAN 33-223), 1 Jul 96

AFSSI 5020, *Remanence Security*, 20 Aug 96

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

AFSSI 5024, *Volume I The Certification and Accreditation Process*, 1 Sep 97

AFSSI 5102, *The Computer Security Program*, 23 Sep 96

### *Acronyms and*

#### *Abbreviations*

#### *Definition*

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
CITS/BIP	Combat Information Transfer System/Base Information Protection
CSSO	Computer System Security Officer
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DNS	Domain Name System
FTP	File Transfer Protocol
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
NTP	Network Time Protocol
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
WWW	World Wide Web

Y2K

Year 2000