

14 MARCH 2003

Communications and Information

NETWORK MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: 159 CF/SCB (CMSgt Elaine P. Vix)
Supersedes HQ LA ANGI 33-1, 2 Feb 2000

Certified by: HQ LA ANG/ESSO (Col John G. Robinson)
Pages: 11
Distribution: F

This instruction provides statewide direction and structure for the Louisiana Air National Guard (LA ANG) Wide Area and Local Area Networks (WAN/LAN). The purpose of this instruction is to ensure all network computer users understand Department of Defense (DoD), Air Force (AF), and Air National Guard (ANG) directives governing the management of government owned computer assets and to express local management requirements for the proper use of the network.

SUMMARY OF REVISION

This instruction replaces the term “Unit Communications-Computer Systems Manager (CSM)” with the more current title of “Unit Workgroup Manager (WGM)”, and lists duties and responsibilities of the position. A (★) indicates revisions from the previous edition.

1. **Glossary of References and Supporting Information.** See Attachment 1.
2. **Roles and Responsibilities** (ref: AFI 33-101, *Communications and Information Management Guidance and Responsibilities*): Below is a summation of duties directed in the reference publication.

2.1. **Commanders at all levels will:**

2.1.1. Plan for and manage communications and information (C&I) systems under their control.

★2.1.2. Ensure the host wing Computer and Information Systems Officer (CSO) reviews all plans (operational, contingency, support, facilities, and etc.) involving C&I resources or activities.

★2.1.3. Appoint a Unit Workgroup Manager (WGM) and alternate in writing. Responsibilities of the WGM are listed in paragraph 2.5 of this publication.

2.1.4. Enforce requirements of this policy and those of the AFI 33 series publications.

2.1.5. Commanders will not allow the implementation of a new communications system (hardware or software) without prior approval from the host wing Communications Systems Officer.

2.2. Wing Commander will:

2.2.1. Designate the host wing communications officer as the base CSO.

2.2.2. Designate a Command, Control, Communications, Computers, and Intelligence (C4I) architect to ensure compliance with requirements, plans, and architectures. The C4I architect is usually the base CSO.

2.2.3. Serve as the base-level approval authority for the base C&I systems blueprint. Ensure architectural compliance, proper classification, functional review (i.e. Base Civil Engineer) and support prior to blueprint approval.

★2.2.4. Serve as the base-level approval authority for requirements documents (AF Form 3215, **IT/NSS Requirements Document**) submitted for implementation of communications and information systems. This authority is delegated to the base CSO.

★2.2.5. Serve as the Designated Approving Authority (DAA) for the LA ANG network and request Approval to Operate.

★2.2.5.1. In accordance with provisions of AFI 33-202, *Computer Security*, the 159th Fighter Wing DAA has appointed the Base CSO as his representative to handle routine accreditation issues.

★2.2.5.2. The wing commander may delegate DAA authority to the ranking officer at each Geographical Separated Unit (GSU) for desktop computers, systems, and networks assigned to their respective units but not connected to the LAANG network. This appointment must be in writing - further delegation is prohibited.

2.2.6. Preside as chairman over a periodic planning forum (C4 Advisory Board), to include wing and GSU representation, to discuss current and future issues affecting C&I systems.

★2.2.7. Designate in writing a unit Computer Security (COMPUSEC) manager to oversee the Wing COMPUSEC program.

2.3. Commanders of GSUs will:

★2.3.1. All GSUs must coordinate with the Base CSO to ensure their systems will integrate and inter-operate, when necessary, with the DOD, AF, ANG and host base information infrastructure.

★2.3.2. Ensure documents are properly prepared to accredit networks and approved desktop systems at their installation.

★2.3.3. Ensure compliance with the Service Level Agreement between the GSUs and Network Services.

★2.3.4. Appoint in writing a unit COMPUSEC manager to oversee their local COMPUSEC program.

2.4. **Base CSO** will:

2.4.1. Organize, train, and lead all assigned communications and information personnel.

2.4.2. Be responsible for meeting the wing's and assigned GSUs' communications and information mission needs (home station and deployed).

2.4.3. Ensure network compatibility, system integration, and blueprint issues are fully coordinated and managed in accordance with the ANG defined infrastructure for the wing and GSUs.

2.4.4. Plan for the life-cycle management and evolution of systems supporting the units'/users' mission.

2.4.5. Coordinate plans and requirements with the base-level Systems Telecommunications Engineering Manager (STEM-B) to ensure incorporation into the base communications and information systems blueprint.

2.4.6. Establish a Network Control Center (NCC) for customer contact for automated systems and network problems, network systems administration, and system and network security protection requirements.

★2.4.7. Establish a periodic planning forum (C4 Advisory Board) comprised of wing and GSU representation, to discuss current and future issues affecting C&I systems and funding.

★2.5. **Unit Workgroup Manager (WGM).** The unit commander appoints a WGM and alternate in writing. The WGM assists in the performance of the commander's C&I responsibilities and is the focal point for computer operation (not accountability) issues. The WGM will:

★2.5.1. Serve as the primary point of contact to the NCC for C&I issues in their assigned unit:

2.5.1.1. Assist others within their organization in resolving computer systems problems.

★2.5.1.2. Respond to users' request for assistance by performing initial troubleshooting and minor repair within his or her capability and authority. The WGM is the only individual outside of Communications Flight that may be authorized to perform minor maintenance on desktop computers or peripherals.

2.5.1.3. Perform as the primary point of contact between users in their area of assignment and the Communications Flight for obtaining technical assistance with communications and information systems; ensure members of their organization adhere to local reporting procedures.

2.5.1.4. Provide advice to unit commander on the unit's need for computer hardware and software resources, training needs, and IT support.

2.5.1.5. Validate computer systems and equipment requirements submitted by a unit Equipment Custodian (EC).

2.5.1.6. Assist with installing, testing, and accepting computer systems in strict accordance with guidance from the NCC.

★2.5.1.7. Provide unit commanders with recommendations for the expenditure of Information Technology funds to the C4 Advisory Board with regard to their own unit needs.

2.5.1.8. Ensure all computer equipment and software within their organization, and the interfaces to systems and networks, is managed in accordance with applicable Air Force Instructions, HQ LA ANG directives, and local policy.

★2.5.1.9. Validate (through unit commander) and forward requests from users for remote access to the LA ANG network.

★2.5.1.10. Ensure appropriate approval from CSO is received for computers and networked systems in their area prior to operation.

★2.5.1.11. Ensure new users receive appropriate initial training prior to requesting network user accounts from the Communications Help Desk.

★2.5.1.12. Assist Information Technology (IT) equipment custodians in the IT inventory process.

★2.5.2. Serve as the Unit COMPUSEC managers and ensure program compliance.

2.6. NCC (Network Control Center) – The NCC will provide proactive and reactive management of resources by monitoring and controlling the network, available bandwidth, hardware, and distributed software. The NCC will consist of Communications Flight members from the following functional areas: SCBN (Network Administration), SCBS (Information Assurance), SCBI (Information Resource Management Help Desk), and SCM (Computer

Maintenance). The detailed list of responsibilities is contained in AFI 33-115V1, *Network Management*. The NCC will:

2.6.1. Respond to requests for assistance in accordance with the prioritization plan below:

TABLE 1		
159FW COMMUNICATIONS PRIORITIZATION PLAN		
ORDER	CATEGORY	ISSUE
Priority 1	Emergency	Safety, Compliance or Security
Priority 2	Immediate	Mission (communications security (COMSEC) and any other communications issue that directly impairs the flying mission).
Priority 3	High	Communications-Computer Systems Support - (WAN/LAN, state-wide issues or GSU connectivity, i.e., data circuits, major system outage, work stoppage in critical areas or where software is not duplicated on another computer).
Priority 4	Routine	Routine repairs and preventative maintenance.
Priority 5	Low	Routine installation of new communications requests, or changes/moves of a current system. These items should be scheduled in advance.

2.6.2. Assist the Wing Information Assurance (IA) office in establishing and maintaining currency of a written security policy for the network; assist wing IA office in collecting accreditation information for networks and systems.

2.6.3. Perform as Equipment Custodian for network equipment.

★2.6.4. Control all remote network communications services.

2.6.5. Control and provide all access to Non-Secure Internet Protocol Router Network (NIPRNET) and the Internet.

2.6.6. Control all service points to the base network.

2.6.7. Maintain, manage, control, and distribute the Internet Protocol (IP) address space allocated to the base internet.

2.6.8. Establish, maintain, control, and enforce the LA ANG email and internet use policies (reference AFI 33-119, *Electronic Mail (E-Mail) Management and Use* and AFI 33-129, *Transmission of Information VIA the Internet*, respectively).

2.6.9. Ensure security of data stored on network equipment in a variety of forms: backups, uninterruptable power source, intrusion deterrents, virus protection, and firewall.

2.6.10. Document repair actions in a common database and order, track, and receipt for parts required to facilitate those repairs.

2.6.11. Perform all other standard network management and administration functions associated with configuration management, fault management, performance management, and security management.

2.6.12. Maintain control over Domain Administrator permissions. Certain personnel (such as server or backup operators) may request and be granted this permission only after receiving a recommendation from Network Management (NM) personnel and approval by the 159th Communications Flight commander. Approval will be based on a combination of experience level, knowledge level, and proven trust level of the individual requesting permission.

★2.6.13. Perform network upgrades and/or patches upon notification from the Wing Information Assurance Office that a new security compliance issue has been directed. Corrective action will include the facilitation of desktop security compliance.

2.7. **Communications Help Desk** will:

★2.7.1. Serve as the initial point of contact for all communications services requests, to include computers (hardware and software), peripherals and network services, telephones, and land mobile radios. The Base Visual Information Manager has a separate job control system, but the Unit WGM submits all other requests regarding communications services to the Help Desk.

2.7.2. Order and track repair parts for desktop computers, peripherals, and network equipment for items under warranty.

2.7.3. Perform standard Help Desk (HD) functions, i.e., enter requests for service in the Help Desk job control database, issue Job Control Numbers, track job progress, issue job status information upon request, assign priority code in accordance with Table 1 of this publication.

2.7.4. Maintain control of all-inclusive member mail lists.

★2.7.5. Create LA ANG network user accounts upon request from WGM only after security clearance, proper approval, and initial training has been verified and documented.

★2.7.6. Create limited “guest” accounts when requested by WGM to facilitate email traffic and internet access only.

★ 2.7.7. Remove email and user accounts upon notification of a member’s separation.

★2.8. **Web Administrator.** The top-level home page for each web server will have a web server administrator identified by name, office symbol, phone number, and email address. This individual is the point of contact for customers having problems with web documents on that

server. The Web Administrator for the LA ANG network is the 159th FW Base Information Resource Manager. The Web Administrator will:

★2.8.1. Maintain the home page for the 159th Fighter Wing and LAANG.

2.8.2. Maintain access and security controls, grant and monitor write-access privileges.

2.8.3. Ensure all links from pages under their control are appropriate, legal, valid, and in compliance with AFI 33-129.

2.8.4. Encourage training and use of web technology to decrease the amount of data files stored on the public drive of the network.

★2.9. **The Wing Information Assurance Office** will:

2.9.1. Perform as the Office of Responsibility for insuring compliance with AFCERT security issues and Time Compliance Network Order (TCNO) compliance.

2.9.2. Receive, acknowledge, and report TCNO compliance.

2.9.3. Inform Network Administrators of new network/desktop security issues and set suspense dates for compliance and reporting based on the issuing agency's directives.

2.9.4. Develop and implement the wing COMPUSEC program.

★2.10. **Functional System Administrators.** A "Functional System Administrator" (FSA) will be appointed for each embedded network operating through the LAANG network. An FSA is not assigned to the NCC; however, they still take direction from the NCC. In the performance of their duties, FSAs will:

2.10.1. Ensure servers, workstations, peripherals, communication devices, and software are on-line and available to support customers using the functional system.

2.10.2. Ensure security compliance (upgrades, patches, virus protection) on servers and desktops processing the functional system.

2.10.3. Provide any unique user training required for the functional system.

2.10.4. Ensure compliance with any Memorandum of Understanding or Service Level Agreement established with the wing NCC.

2.10.5. Perform server or desktop actions directed and approved by the NCC.

★2.11. **Network Users' Responsibilities.** Any questions should be directed to the Communications Help Desk. Network users' responsibilities include but are not limited to the following:

★2.11.1. Users will comply with network security policy regarding passwords.

★ 2.11.1.1. Users will not share individual password with others.

★2.11.1.2. Users will comply with minimum password standards (length of 8 characters (mixed upper and lower case, numbers, special characters, no spaces).

★2.11.2. Users will not load application software on IT equipment or a network drive assigned to the wing or a GSU unless specifically authorized to do so by the NCC.

2.11.3. Users will not load executable files or perform any modification to configuration files on computers or a network drive (i.e., adding unauthorized screen savers, bios passwords, etc.). Such action will be considered abuse of government resources. The performing Communications Flight technician is authorized to take appropriate action (i.e., remove illegal software, reconfigure the system to regain compliance, or remove the server/desktop from operation).

★2.11.4. Users will ensure their computers have the latest anti-virus signature files and that data on storage disks is routinely scanned.

★2.11.5. Users will not use personal, shareware, or freeware software on government computers without the specific consent of the NCC.

2.11.6. Chain letters of any type are strictly prohibited. Members involved in the dissemination of a chain letter are subject to disciplinary action.

2.11.7. Any information on a suspected computer virus should be forwarded to the Communications Help Desk or Wing IA office only. Do not promulgate misinformation or cause undue concern by forwarding these types of messages to coworkers and friends.

3. General Guidance.

3.1. Obtaining Assistance.

3.1.1. The primary means of requesting Communications assistance for IT-related problems is to report it to the appropriate unit WGM. That individual will report the problem to the Communications Help Desk via email address HELPDESK@LANEWO.ANG.AF.MIL.

3.1.2. If the matter is a Priority 3 or higher and requires immediate attention, the WGM should place a call to the Help Desk, the Information Systems Branch Chief, or the Communications Flight Commander, in the stated order.

★3.2. **Maintenance of IT Equipment.** Only personnel assigned to the 159th Communications Flight or those authorized in writing will perform maintenance on IT equipment assigned to the wing or a GSU.

3.2.1. During the troubleshooting and/or repair process, the performing technician will remove any illegal software including freeware, shareware and application software. This action may be taken without prior consultation with the computer's user or WGM.

3.3. Email, Internet and Network Connectivity.

3.3.1. Email traffic destined for other military sites (within the “.mil” domain) will not be routed through a commercial Internet Service Provider (ISP), and traffic from a commercial ISP will not be routed through the receiving base network to other military networks. Other than the mail service provided by the LAANG (MS Exchange), no other commercial mail service (i.e., AOL, Hotmail, Yahoo, and etc.) is authorized. Access to these sites from the LAANG network will be blocked.

3.3.2. Computers that use a dial-up modem or process classified information will not be attached to the LA ANG network.

3.3.3. The following activities involving the use of government-provided computer hardware or software are specifically prohibited (Refer to AFI 33-129, paragraph 6.1 for a complete list):

3.3.3.1. Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, “hate literature,” such as racist literature, materials or symbols, and sexually harassing and/or obscene materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.

★3.3.3.2. Attempting to circumvent or defeat security or auditing systems without prior authorization or permission from the NCC.

3.3.3.3. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor’s software license or copyright agreement.

★3.3.3.4. Modifying or altering the network operating system or system configuration without first obtaining permission from the NCC.

★3.3.3.5. Activities for personal or commercial financial gain, which include, but are not limited to, chain letters, commercial solicitation, and sales of personal property (unless specifically authorized by the DAA through the use of an established bulletin board or web site).

3.3.3.6. Any use of government-provided computer hardware or software for other than official and authorized government business.

4. Non-Compliance.

4.1. For military members, failure to observe the provisions in paragraph 3.3. above constitutes a violation of Article 92, UCMJ. Civilian employees who fail to observe the provisions in paragraph 3.3. may face administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions. This disciplinary action will vary depending on the severity of the offense, and may include verbal counseling to removal of computer or network access.

★4.2. Personnel found to be abusing government IT resources will be reported to their unit commander for disciplinary action.

★4.3. The following incidents will require immediate action by the NCC, to include removal of user privileges, until the situation can be researched and resolved:

★4.3.1. Incidents that appear to jeopardize the security and/or operational integrity of the network and its data.

★4.3.2. Flagrant and obvious misuse of government resources.

5. Forms prescribed. AF Form 3215, IT/NSS Requirements Document

BY ORDER OF THE GOVERNOR

BENNETT C. LANDRENEAU
Major General, LAARNG
The Adjutant General

OFFICIAL

//Signed//

JOHN G. ROBINSON, Col, LA ANG
Executive Support Staff Officer

Attachment:
Glossary of References and Supporting Information

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

AFI 33-101, *Communications and Information Management Guidance and Responsibilities*

AFI 33-115V1, *Network Management*

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

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

AFI 33-202, *Computer Security*

Abbreviations and Acronyms

AF - Air Force

ANG - Air National Guard

C4I - Command, Control, Communications, Computers, and Intelligence

C&I - Communications and Information

COMPUSEC - Computer Security

COMSEC – Communications Security

CSO - Computer and Information Systems Officer

DAA - Designated Approving Authority

DoD - Department of Defense

EC - Equipment Custodian

FSA - Functional System Administrator

GSU - Geographical Separated Unit

HD - Help Desk

IA - Information Assurance

IP - Internet Protocol

ISP - Internet Service Provider

IT - Information Technology

LA ANG – Louisiana Air National Guard

NCC - Network Control Center

NIPRNET - Non-Secure Internet Protocol Router Network

NM - Network Management

STEM-B - Systems Telecommunications Engineering Manager

TCNO – Time Compliance Network Order

WAN/LAN - Wide Area and Local Area Networks

WGM - Workgroup Manager