

1 NOVEMBER 1999



Communications and Information

**LICENSING NETWORK USERS AND
CERTIFYING NETWORK PROFESSIONALS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: <http://afpubs.hq.af.mil>. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCLO (SMSgt Hill)

Certified by: HQ USAF/SCXX (Mr. Paul Armel)

Pages: 17

Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*; Office of Management and Budget (OMB) Circular Number A-130, *Management of Federal Information Resources*; and Department of Defense (DoD) Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988. It provides the policy and procedures for certifying network professionals who manage and operate government-provided information systems on Air Force networks and the training and licensing of Air Force network users. Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/XPPX), 203 West Losey Street, Room 1060, Scott AFB IL 62225-5222, through appropriate channels, using Air Force (AF) Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCLO, 203 West Losey Street, Room 3010, Scott AFB IL 62225-5222. A glossary of references and supporting information is at [Attachment 1](#).

1. Introduction . The Air Force network is similar to a weapon system in that it should be treated as a mission critical asset. Communications and information resources have become force multipliers, and Air Force information systems and networks must evolve to effectively implement the expeditionary aerospace force (EAF) vision. To achieve the light, lean, and lethal forces our national military strategy depends on, the DoD and United States Air Force (USAF) must ensure fully qualified personnel operate and maintain these systems and networks.

1.1. This instruction defines the policy and procedures for training and licensing all users and Air Force network professionals who access the Air Force network (af.mil) domain. Compliance with this AFI meets the DoD initiative to train and certify all computer users and to certify those network professionals who actively manage, configure, and control the network, to a consistent verifiable skill level ensuring the DoD information assurance (IA) posture is uncompromised.

Report Documentation Page		
Report Date 01 Nov 1999	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Air Force Instruction 33-115 Volume 2, Communications and Information, Licensing Network Users and Certifying Network Professionals	Contract Number	
	Grant Number	
	Program Element Number	
Author(s)	Project Number	
	Task Number	
	Work Unit Number	
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington, DC 20330-1250	Performing Organization Report Number AFI33-115,V2	
Sponsoring/Monitoring Agency Name(s) and Address(es)	Sponsor/Monitor's Acronym(s)	
	Sponsor/Monitor's Report Number(s)	
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes Volume 2 of 2 Volumes		
Abstract		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 17		

2. Background . The Air Force has initiated an aggressive drive to operationalize and professionalize its networks. Certification is now included in the operational Status of Resources and Training System (SORTS) described in AFI 10-201, *Status of Resources and Training System*. Certification and licensing will also be included in the Inspector General agenda. This instruction builds on the guidance provided in AFI 33-115V1, *Network Management*. Standard licensing criteria will ensure all personnel who access the Air Force network are knowledgeable of their roles and responsibilities for protecting information flow. Standard certification criteria will ensure network professionals maintain a demonstrable set of core skills and knowledge across the Air Force.

3. Applicability . This guidance and policy applies to:

3.1. All military, civilian, and local national employees using or providing professional network services in the Air Force network (af.mil) domain on any Air Force system, network, or Air Force-operated joint system as a part of their official duties.

3.2. All contractors using or providing professional network services in the Air Force network (af.mil) domain on any Air Force system, network, or Air Force-operated joint system as a part of their official duties. (**NOTE:** Contracts must include a requirement that contract employees providing professional network services meet the skill set and knowledge requirements consistent with the certification track for each position they perform.)

4. Licensing Network Users .

4.1. Introduction. Every individual who has access to the Air Force network (af.mil) domain, specialized systems, and mission systems is a network user. Before becoming an Air Force network user an individual must be trained and licensed. Details on the training and licensing requirements and guidance on access to the training will be provided to the users by workgroup managers (WM). Upon successfully completing training, the user is licensed to use the network and granted access to required network resources. This process of training and licensing ensures that every Air Force network user is trained and aware of the basic principles of network security and their role in IA.

4.2. Procedures. User IA training has been standardized in the IA Internet-based training (IBT) course (see AFI 33-204). Successful completion of this course satisfies DoD user certification, Air Force SATE training, and Air Force network users licensing. Records of user training is contained in the IA IBT data base. Additional user training may be developed locally to reflect local needs and concerns. WMs administer the locally developed training to their network users, track users' completion of this training, and maintain a record of the training program using locally developed procedures. WMs make training available to new or suspended users on an as-needed basis. When a user completes user license training, the WM ensures their network access is granted. At this point, a user is considered licensed and may access the Air Force network. Whenever a user requires a new user identification (userID)(due to permanent change of station, permanent change of assignment, temporary duty, etc.), the gaining WM must license the user before allowing the user access to the network. In emergency or deployment situations, the WM may rely on a record review to license a user.

4.3. License Suspension. If a user engages in conduct inconsistent with the licensing principles, the WM may, with the approval of the user's supervisor, recommend their access be suspended. Network access suspension is a non-punitive action and the suspension alone, as opposed to the underlying conduct, may not provide the basis for adverse action. The designated approval authority (DAA) or

designee may, based on the WM's recommendation, suspend a user's license when deemed necessary in the interest of information operations. Actions inconsistent with licensing principles include, but are not limited: failure to maintain an acceptable level of proficiency on a critical program; actions that threaten the security of a network or a governmental communications system; actions that may result in damage or harm to a network or governmental communications system; or actions that constitute unauthorized use under the provisions of AFI 33-119, *Electronic Mail (E-Mail) Management and Use*, or AFI 33-129, *Transmission of Information Via the Internet*.

4.3.1. Procedural Requirements - Minor Infraction. On discovery of an action inconsistent with the initial user license training provided by the WM, the WM will recommend to the user's supervisor that their access to a network be suspended. With supervisor concurrence, the WM will notify the user immediately, in writing, of the access suspension, including the specific reason for the suspension and the steps the user must take to have access reinstated.

4.3.1.1. The user may accept the suspension or dispute the grounds for the suspension by providing a written request, within three duty days, that the suspension be rescinded. If the user accepts the suspension, the WM has two duty days to make available to the user whatever appropriate remedial training necessary for the user to qualify for re-licensing.

4.3.1.2. If the user disputes the suspension, the WM has four duty days following receipt of the user's request to reconsider suspension. The WM, after consultation with the user's supervisor, will either notify the user in writing that the suspension was inappropriate and immediately reinstate the user's license or refer the matter to the DAA for final action by sending a copy of the case file. The DAA will consider the case file to determine if suspension was appropriate. The DAA may order reinstatement of the user's license, mandate remedial training, or take other necessary actions. After receiving the documentation, the DAA will notify the user in writing, within six duty days, of the final determination.

4.3.2. Procedural Requirements - Major Infraction. On discovery of a serious action inconsistent with the initial user license training provided by the WM, the WM will inform the user's supervisor and the NCC that access has been disabled. The WM will then inform the user in writing per guidance in the previous paragraph.

4.4. Reinstatement. Ordinarily, a suspended user will be required to participate in remedial training. Upon satisfactorily completing retraining, the WM reinstates the user's license. However, there may be situations that indicate to the WM and the user's supervisor that even with remedial training the user would pose a threat to the security of the system or operations. Under such circumstances, the DAA, following full review of the case file and all associated documents, may suspend a user's privileges indefinitely.

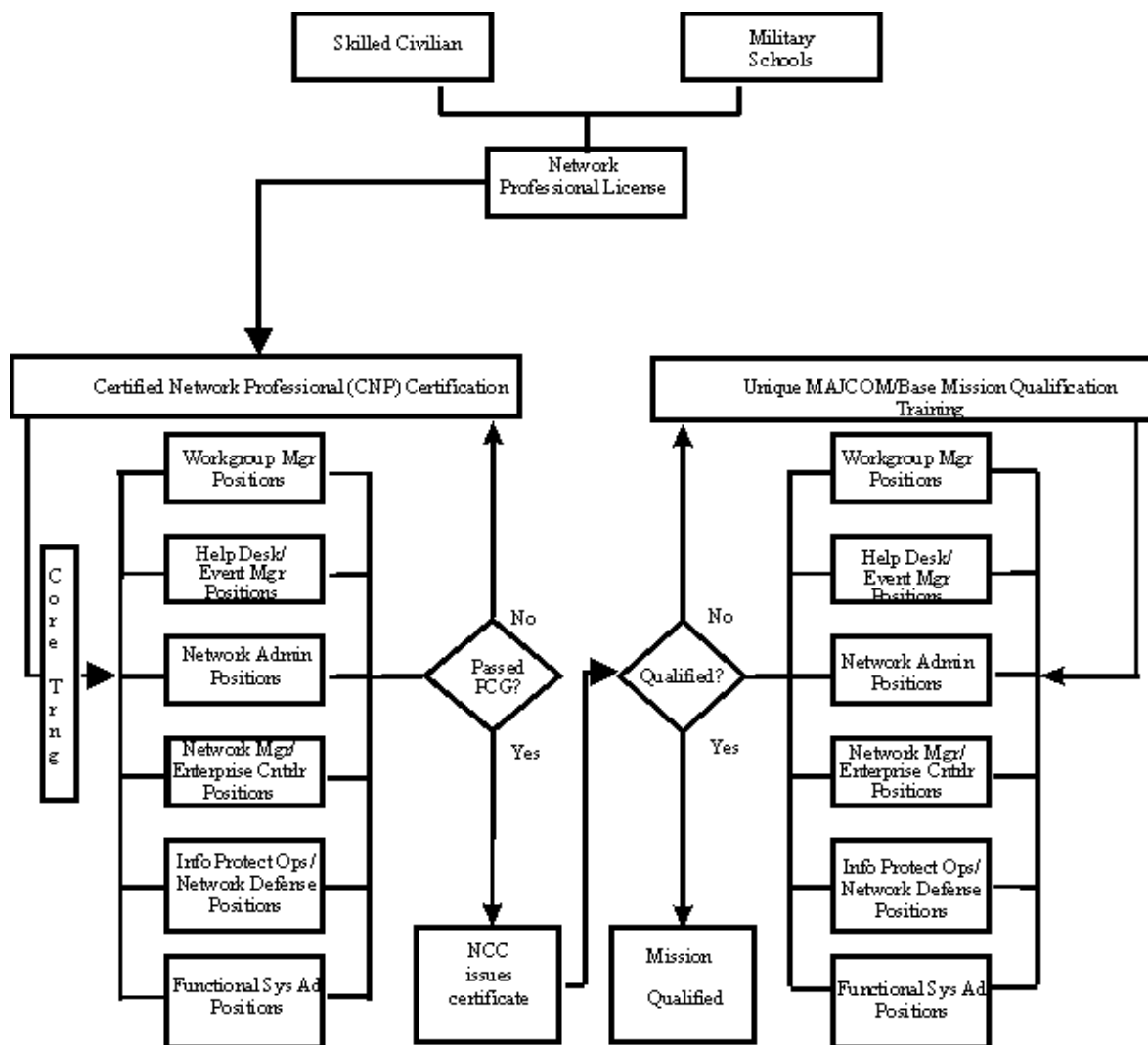
5. Certifying Network Professionals .

5.1. Introduction. The objective of the network certification program is to qualify network operators for position certification during peacetime and combat operations in support of the EAF. Network operators are those military and civilian professionals who perform daily network management (NM), control, and administration of information flow within the functional areas as well as within the NCC. Certification is achieved through a combination of in-residence courses, supervised hands-on on-the-job training (OJT) and Air Force-provided interactive computer based training (CBT). AFCA will develop and field position-specific Position Certification Guides (PCG) to standardize training

requirements and identify objectives and technical references. Upon successful completion of training and time requirements, the network operator is position-certified to perform network operations.

5.2. Procedures. Supervisors will use the appropriate PCG to train network operators on specific core-knowledge and task items required for position certification. A sample PCG is provided in [Attachment 2](#). A separate PCG is used for each network operations position and includes all applicable network operating systems. The PCG identifies general core requirements, the position-specific requirements, and the OJT and Master Training Task List (MTTL) to train network operators on specific knowledge and task items. However, major commands (MAJCOM)/bases may add locally unique training requirements to ensure position certification is comprehensive and meets mission needs. Due to the track-based nature of position certification, the procedures are identical for all positions. All network professionals must complete the network user's training and license requirements (see paragraph 4.) before beginning the appropriate certification curriculum. [Figure 1](#) depicts the certified network professional (CNP) certification process and the MAJCOM/base unique mission qualification process.

Figure 1. CNP Certification Process.



5.2.1. Supervisors of personnel who perform one of the network operations crew positions will determine the appropriate PCG based on the trainee's duties. They will ensure that new arrivals are certified in the required crew position and operating system used at the gaining location. If the individual is certified on a different position/operating system, the supervisor will begin required initial certification action for the new position.

5.2.1.1. Supervisors monitor the progress of the individual using established timelines as outlined in each PCG. The supervisor will submit a certification course completion document to the servicing NCC or unit training manager after an individual completes all training objectives.

5.2.1.2. Supervisors maintain training records on all individuals serving as network professionals, regardless of rank. Document the course completion progress for military on the AF Form 623A, **On-The-Job Training Record - Continuation Sheet**, locally developed training record, or AF Form 971, **Supervisor's Employee Brief**, for civilians.

5.2.2. The trainee will complete all required courses for the training assigned and notify the supervisor of conditions preventing certification completion.

5.2.2.1. Air Force civilians follow local Civilian Personnel Office (CPO) procedures, such as completing a Department of Defense (DD) Form 1556, **Request, Authorization, Agreement, Certification of Training, and Reimbursement**, prior to starting a certification track. The final certification certificate is submitted to the CPO for inclusion in the civilian's personnel record.

5.2.3. The NCC or communications training manager will publish a list of CNPs for each of the positions and will also verify certification transfer from the individual's supervisor for newly assigned personnel who were previously certified in the same operating system and crew position.

5.2.3.1. The training manager receives and reviews certification documentation package from the individual's supervisor, generates a certification certificate using AF Form 1256, **Certificate of Training**, and signs the left block authenticating certification completion. Certification transfers and certification certificates are sent to the DAA or their designee for approval with validation of curriculum completion.

5.2.4. Time Limits. The estimated time to complete the various curricula depends on the operating system selected and the crew position assigned. MAJCOMs determine the time limits for training based on mission requirements. If a trainee has the required skills (i.e., already performs the tasks, previous vendor certification) completion may be expedited.

5.2.5. Certification Suspension. The DAA, or designee, may suspend a network professional's network privileges when the network professional's actions are inconsistent with certification policies and procedures. Actions inconsistent with certification policy include, but are not limited to the following: loss of or failure to maintain an acceptable level of proficiency on a critical program, actions that threaten the security of a network or a governmental communications system, or actions that may result in damage or harm to a network or a governmental communications system.

5.2.5.1. The supervisor will inform the NCC Officer in Charge (OIC) immediately upon notification of any actions inconsistent with certification principles. These actions could also be inconsistent with licensing policies identified in paragraph 4.

5.2.6. Procedural Requirements. Upon discovery of any action inconsistent with the initial certification training provided by the NCC, the OIC directs the network professional's network privileges be suspended and notifies the network professional and his or her supervisor immediately, in writing, of this action, including the specific reason for the suspension and the steps necessary to lift the suspension. If the action was also a violation of user licensing policy, the users license could also be affected as specified in paragraph 4.

5.2.6.1. The notification provides the network professional with three duty days to respond. The network professional may accept the suspension or may dispute the grounds for the suspension by providing the NCC OIC with a written request that the suspension be rescinded. If the network professional accepts the suspension, the NCC OIC has two duty days to make available to the network professional whatever remedial training the NCC OIC determines necessary for the network professional to qualify for re-certification.

5.2.6.2. If the network professional disputes the suspension, the NCC OIC has four duty days

following receipt of a network professional's request to reconsider suspension. At that time, the NCC OIC either notifies the network professional in writing that the suspension was inappropriate and immediately reinstates the network professional's certification or refers the matter to the DAA for final action by sending a copy of the case file. Within six duty days, the DAA considers the case file to determine if suspension was appropriate and may order reinstatement of the network professional's certification, mandate remedial training, or take other necessary actions and notifies the network professional in writing.

5.2.7. Re-certification. Ordinarily, a suspended network professional is required to participate in remedial training. After satisfactorily completing retraining, the OIC may re-certify the network professional. However, there may be situations that indicate to the OIC, and the network professional's supervisor, that even with remedial training, the network professional would pose a threat to the security of the system. Under such circumstances, the DAA, following full review of the case file and all associated documents, may suspend a network professional's privileges indefinitely.

6. Responsibilities .

6.1. HQ Air Force Communications and Information Center (AFCIC) will:

6.1.1. Establish policy and guidance for the Certifying Network Professionals and Licensing Network Users Program.

6.1.2. Convene utilization and training workshops with HQ Air Education and Training Command (AETC), MAJCOM functional managers, and subject matter experts to inject certification criteria and the MTTL into formal technical training courses and the Career Field Education and Training Plan (CFETP).

6.1.3. Direct AETC in production of any required training documentation to aid operations.

6.1.4. Coordinate the Air Force certification and licensing program with DoD efforts to certify proficiency of computer system users and network professionals.

6.2. HQ AFCA:

6.2.1. Develop, maintain, and manage the Certifying Network Professionals and Licensing Network Users Program and control and promote program integrity.

6.2.2. Coordinate criteria and certification methodology with MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) to ensure standard program administration.

6.2.3. Develop PCGs and recommend certification policy, guidance, criteria, and training methodology to certify all personnel subject to this instruction.

6.2.4. Field PCGs and maintain a MTTL.

6.3. HQ AETC will work with career field managers to inject certification criteria in formal technical training courses during utilization and training workshops. HQ AETC will also provide and field training documents as directed by the career field manager.

6.4. MAJCOMs, FOAs, and DRUs will:

6.4.1. Implement the Network Professional Certification and Network Users Licensing Program.

6.4.2. Ensure subordinate units fulfill their responsibilities as outlined in these instructions.

6.4.3. Ensure contracted network professionals meet the same skill set and knowledge requirements as Air Force military and civilian network professionals.

6.4.4. Monitor the certification program and consolidate training data from their subordinate units as needed.

6.4.5. Supplement the PCGs to reflect MAJCOM specific mission needs.

6.4.6. Supplement this AFI as required.

6.5. Subordinate Units:

6.5.1. Administer the PCG curricula to Air Force military and civilian network professionals assigned to their installations, whether host or tenant.

6.5.2. Ensure contracted network professionals meet the skill set and knowledge requirements consistent with Air Force military and civilian network professionals.

6.5.3. Assist unit training managers, supervisors, trainers, and trainees in accomplishing their responsibilities.

6.5.4. NCCs determine which Joint Technical Architecture – Air Force operating systems apply.

6.5.5. The communications squadron commander should assign a primary and alternate NCC or unit training manager to administer the certification program. These trainers also assist WMs to implement the training and licensing program for their network users.

7. Program Guidance .

7.1. Certification Transfer. Certification is transferable between duty crew positions assuming the certified individual fulfills the same type of duties on the same operating system at the gaining location. The gaining supervisor determines if the certification is valid for the assigned duty crew position.

7.2. Certification and License Suspension and Reinstatement. The DAA retains sole responsibility and accountability for operations and security of the network; therefore, authority to suspend an individual's license or certification and reinstatement authority rests with the DAA. The DAA may delegate this authority to a senior manager of the network.

7.3. Integrity and Control. The DAA, supervisor, training manager, other CNPs and licensed network users team to maintain the integrity and control of the program. The DAA, or delegated senior network manager, approves/disapproves all access to the network. Supervisors determine whether individuals are eligible for certification based on completion of the appropriate PCG. The training manager validates all certifications and works closely with supervisors.

7.4. Training Data. Supervisors and training managers must maintain a record of all PCG training. Either paper documentation as outlined in paragraph [5.2.1.2](#). or MAJCOM-approved automated

records may be used for documentation. If automated records are kept, they must be readily available to the trainee, trainer, and supervisor.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

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

DoDD 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988

OMB Circular No. A-130, *Management of Federal Information Resources*

AFI 10-201, *Status of Resources and Training System*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

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*

AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*

Abbreviations and Acronyms

AETC—Air Education and Training Command

AF—Air Force (used for designated forms only)

AFCA—Air Force Communications Agency

AFCIC—Air Force Communications and Information Center

AFI—Air Force Instruction

AFNOC—Air Force Network Operations Center

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

AIS—Automated Information System

ATM—Asynchronous Transfer Mode

BGP—Border Gateway Protocol

CBT—Computer Based Training

CFEPT—Career Field Education and Training Plan

CNP—Certified Network Professional

CPO—Civilian Personnel Office

DAA—Designated Approval Authority

DD—Department of Defense (used for designated forms only)

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

EAF—Expeditionary Aerospace Force

FDDI—Fiber Distribution Data Interface

FOA—Field Operating Agency

FSA—Functional System Administrator

HD—Help Desk

IA—Information Assurance

IBT—Internet-Based Training

IGRP—Interior Gateway Routing Protocol

IOS—Internetwork Operating System

IPO—Information Protection Operations

ISDN—Integrated Services Digital Network

LAN—Local Area Network

MAJCOM—Major Command

MAN—Metropolitan Area Network

MTTL—Master Training Task List

NA—Network Administration

NCC—Network Control Center

NM—Network Management

NOSC—Network Operations and Security Center

OIC—Officer in Charge

OJT—On-the-Job Training

OMB—Office of Management and Budget

OSPF—Open Shortest Path First

PCG—Position Certification Guide

PPP—Point-to-Point Protocol

RIP—Routing Information Protocol

SATE—Security Awareness, Training, and Education

SORTS—Status of Resources and Training System

SMDS—Switched Multimegabit Data Service

TCP/IP—Transmission Control Protocol/Internet Protocol

USAF—United States Air Force

UserID—User Identification

WAN—Wide Area Network

WM—Workgroup Manager

Terms

Crew Commander - Base/MAJCOM and Above Level—The crew commander maintains tactical control and administrative control over their assigned crews. The crew commander is accountable for successful mission execution, maintaining crew integrity, and ensuring crewmembers are trained and certified as required. The crew commander analyzes, prioritizes, and if necessary, makes recommendations to the commander (or designated representative) to redirect network assets to ensure mission accomplishment.

Designated Approving Authority (DAA)—As identified in AFI 33-202, *Computer Security*, the MAJCOM commander is the DAA for automated information systems (AIS) within the command's jurisdiction that process information for the command. The commander may delegate this authority entirely or on a system-by-system basis. The DAA delegate should be in the operational chain of the organization for whom the AIS operates, has the authority to formally assume responsibility for operating an AIS or network at an acceptable level of risk, and is most affected by its failure (i.e., installation commander).

Enterprise Controller - MAJCOM and Above Level—Focal points for metrics collection in support of its enterprise infrastructure and information flow management. They provide proactive and reactive management of resources by monitoring and controlling their networks, available bandwidth, hardware, and distributed software resources. They respond to detected security incidents, network faults (errors), and user reported outages at the time of base NCC referral.

Event Managers - MAJCOM and Above Level—Operate the Event Management System which passes a consolidated view of all NCC fault, performance degradation, and corrective actions to the hierarchical command authority. This consolidated view of network events and responses is shared with the Air Force Network Operations Center (AFNOC), other network operations and security centers (NOSC/NOSC-D), and with all supported NCCs. Event managers are the single focal point for NCC access to NOSC/NOSC-D resources and services.

Functional System Administrator (FSA) - Unit/Base Level—FSAs are not assigned to the NCC; however, as part of the network team, they still take direction from the NCC, which has the lead. They must thoroughly understand the customer's mission and stay completely knowledgeable of the hardware and software capabilities and limitations. The FSA's area of responsibility is from the user's terminal to the system server, but does not include the network backbone infrastructure components or network core services. FSAs ensure servers, workstations, peripherals, communications devices, and software are on line and available to support customers.

Help Desk (HD) - Base Level—The HD is the base's focal point for problem resolution and is the primary point of contact for problems that WMs or FSAs cannot resolve. The HD provides a central repository for technical advice and solutions for network systems, software applications assistance, automatic data processing support, hardware exchange, and repair service support. The HD determines the type of reported system problem, reports the status of problem resolution to the affected customer, and

maintains a historical database of problem resolution.

Information Protection Operations (IPO) - Base Level—IPO is a critical subcomponent of the NM function that implements and enforces national, DoD, and Air Force security policies and directives. It provides proactive security functions established to assist Air Force organizations in deterring, detecting, isolating, containing, and recovering from information system and network security intrusions. The NCC conducts IPOs using hardware and software tools to enhance the security of their networks. It installs, monitors, and directs proactive and reactive computer network defense measures to ensure the availability, integrity, and reliability of base networked and stand-alone information resources. It coordinates implementation of these solutions with the HD, NM, and customer representatives.

Network Administration (NA) - Base Level—The network operator assigned to perform NA is assigned directly to the NCC and centrally manages various functional area local area networks (LAN) from the network hardware and software operating systems level. Tasks include all core services provided by the NCC to the base populace. These network operators are the base experts in systems administration and also provide technical assistance to FSAs and WMs who provide administration support from their servers to their end-user workstations.

Network Defense Controller - MAJCOM and Above Level—Responsible for execution of both passive and active network defense missions, in accordance with the command authority directives, and in reaction to their current network situation. Network defense controllers oversee the implementation of proactive and reactive security measures to ensure operational availability of the network and information flow of mission-critical applications.

Network Management (NM) - Base Level—Provides proactive and responsive management of resources by monitoring and controlling the network, available bandwidth, hardware, and distributed software resources. NM responds to detected security incidents, network faults (errors), and user reported outages at the time of HD referral. If NM personnel cannot resolve a customer complaint or query, the HD refers the problem to a systems specialist in the specific area support function.

Workgroup Manager (WM) - Unit Level—The WM is normally a duty supporting a functional community (e.g., workcenters, flights, squadrons, or organizations) and is the first line of help that customers contact to resolve problems. The WM should be a 3A0X1 (Information Manager). Information managers receive 3/7-level training on workgroup administration, a significant part of WM duties. When a 3A0X1 is not assigned, available Air Force specialty codes (AFSC) or civilian occupational series can perform WM duties once trained and certified. WMs are usually not assigned to the NCC, though are logically an extension of the Help Desk (HD) team. WMs possess developed knowledge of hardware, software, and communications principles, and install, configure, and operate client/server devices. They resolve the day-to-day administrative and technical system problems users experience and contact their functional system administrator (FSA) or HD if they cannot resolve their problem.

Attachment 2

SAMPLE -- POSITION CERTIFICATION GUIDE

A2.1. Infrastructure Technician .

A2.1.1. Network Function Description:

A2.1.1.1. Network Management (NM). Installs, configures, and maintains the base information transport (backbone). Provides proactive and reactive management of resources by monitoring and controlling the transport and associated components. Manages and controls Internet and remote dial-in network access. NM responds to detected security incidents, network faults and user reported outages at the time of Help Desk referral. Two positions that constitute this function are Internet Services and Infrastructure Technician.

A2.2. Network Crew Position Description .

A2.2.1. Infrastructure Technician:

A2.2.1.1. Transport Maintenance. Installs and maintains routers, switches, and hubs comprising the base backbone.

A2.2.1.2. Configuration Management. Maintains network files including system backups. Modifies switch, router, and hub configurations to ensure optimum network performance and configures access control lists to grant/restrict network access and use to authorized users and processes.

A2.3. Certification Process .

A2.3.1. Network User\Professional License:

A2.3.1.1. Every person who has access to the Air Force network (af.mil) domain, specialized systems, and mission systems is a network user and must be trained and licensed. Licensing ensures that every Air Force network user is trained and aware of the basic principles of network operations. User license training will be a standardized Air Force computer based training (CBT). Additionally, network professionals are required to successfully complete the network professional module of the Air Force CBT.

A2.3.2. Core Network Fundamentals Training:

A2.3.2.1. This PCG is used to certify the NM infrastructure technician position within the network control center (NCC) and the enterprise controller position at the network operations and security center (NOSC) or Air Force Network Operations Center (AFNOC). Document infrastructure technician training on the task list/Career Field Education and Training Plan (CFETP). The training is focused on NM for the base and enterprise network infrastructure. The emphasis of this guide is on understanding NM operations and how to manage the network to ensure optimal information flow. This track applies to 3C2X1, 3C0X1, 33S Air Force specialty codes (AFSC) and the appropriate Air Force occupational civilian series. Expeditionary units may additionally apply this certification guide to AFSC 2E2X1, 2E3X1, or 2E6X3 per operational commander's discretion. Required CBTs and completion time are greatly reduced for personnel who test out of any of the subject areas.

A2.3.2.2. Networking fundamentals are a required core competency for all Air Force network professionals. Air Force-provided CBTs required to achieve this core competency are as follows:

Table A2.1. Core Network Fundamental.

TRAINING SOURCES	PROJECTED HOURS
Core Network Fundamentals	Total: 81
<i>Information Assurance (IA):</i>	9
IA Certification IBT Volume 1 – System Administration	3
IA Certification IBT Volume 3 – Information Condition	3
IA Certification IBT Volume 4 – NOSC/NCC Crew Positions	3
<i>Internetworking Essentials:</i>	27
Internetworking Overview	6
Fundamentals of Internetworking	5
Internetworking: Essentials	4
Internetworking: Devices	4
Internetworking: Bridging Protocols	4
Internet Security: An Overview	4
<i>Local Area Network (LAN) Technologies:</i>	45
IEEE Eth Ethernet, Fast Ethernet, and Gigabit Ethernet	5
Fiber Distribution Data Interface (FDDI), Asynchronous Transfer Mode (ATM), and High Speed LANs	4
LAN Media and Components	4
LAN Topologies and Techniques	4
Transmission Control Protocol/Internet Protocol (TCP/IP) Architecture and Routing	6
Introduction to Common Networking Protocols	6
LAN Fundamentals	6
Network Types	3
Network Adapter Cards	3
Personal Computer (PC) Concepts in a Networking Environment	4

A2.3.3. Position Specific Training. Position specific training is the final step for certification of Air Force network professionals. Training required to achieve the infrastructure technician certification is as follows:

Table A2.2. Position Specific Training.

TRAINING SOURCES	PROJECTED HOURS
Network Management Infrastructure Technician:	Total: 475 CBT: 135 Course: 340
<i>Cisco Internetwork Operating System (IOS)(Introduction to Cisco Router Configuration):</i>	31
Cisco Router Configuration Basics	4
TCP/IP Addressing and Cisco Routers	4
Implementing Distance Vector Router Protocols	4
Wide Area Network (WAN) Connections on Cisco Routers	4
Transparent and Source Route Bridging for Cisco Routers	4
X.25 Configuration for Cisco Routers	4
Frame Relay Configuration for Cisco Routers	4
Integrated Services Digital Network (ISDN) Configuration for Cisco Routers	3
<i>Cisco IOS (Advanced Cisco Router Configuration):</i>	32
Router Configuration using TCP/IP	4
TCP/IP Routing Protocols and Cisco Routers	4
Implementing Open Shortest Path First (OSPF) on Cisco Routers	4
Implementing IP Enhanced Interior Gateway Routing Protocol (IGRP) on Cisco Routers	4
WAN Scalability and Cisco Routers	4
Concurrent Routing and Bridging and Advanced Bridging Options	4
Point-to-Point Protocol (PPP) Configuration for Cisco Routers	4
Switched Multimegabit Data Service (SMDS) and ATM Configuration for Cisco Routers	4
<i>WAN Technologies:</i>	28
SMDS, Metropolitan Area Networks (MAN), and Fiber Networks	4
ATM Principles	4
ATM Networking	4
ATM Architecture and Protocols	4
Fast Packet Technologies	4
Packet Switching WANs	4
PPP: The Point-to-Point Protocol	4
<i>Network Management and Security:</i>	20
NM and Operation Overview	4
Management and Security	4
Internet Security: An Overview	4
Managing LANs	4
Troubleshooting LANs	4
<i>Routing, Bridging, and Switching:</i>	24

Bridging Protocols	4
Virtual LANs	4
Routing Fundamentals	4
Netware Link Services Protocol	4
Routing Information Protocol (RIP) and Border Gateway Protocol (BGP)	4
OSPF	4
AETC Systems Network Support Course	Up to 280
Basic/Advanced Cisco Router Configuration	60
Operational Experience (Total required minimum time in crew position)	12 Months

A2.3.4. OJT Training. All network fundamentals and position specific training will be mapped to the CFEPT and training task table. Document completion and follow instructions as outlined in AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals*.

A2.3.5. Mission Qualification Training: All crew positions have mission specific associated training requirements. The certification received under this guide prepares personnel to accomplish specific MAJCOM/base mission qualification training.