BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-115, VOLUME 1

3 MAY 2004

Communications and Information

NETWORK OPERATIONS (NETOPS)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: HQ AFCA/GCLO (SMSgt Pickard)
Supersedes AFI 33-115, Volume 1, 15 November 2002.

Certified by: HQ USAF/ILC (Col Michael Sinisi)
Pages: 62
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems***.** Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/ITXD), 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication***,* with an information copy to HQ AFCA/GCLO, 203 West Losey Street, Room 2100, Scott AFB IL 62225-5222, and Headquarters United States Air Force (HQ USAF/ILC), 1030 Air Force Pentagon, Washington DC 20330-1030. Major command (MAJCOM) supplements to this AFI will not reduce stated requirements. The term Air Force Reserve forces includes reference to the Air National Guard. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force WEB-RIMS Records Disposition Schedule (RDS) located at **https://webrims.amc.af.mil/rds/index.cfm**. Public Law 104-13, *Paperwork Reduction Act of 1995*, and AFI 33-360, Volume 2, *Content Management Program—Information Management Tool (CMP-IMT)*, affect this publication. See Attachment 1 for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

Many concepts previously addressed in the *Joint* and *Air Force Network Operations Concept of Operations (CONOPS), Air Force Enterprise Network Operations Configuration Management, and Air Force Enterprise Management Capability CONOPS* documents were incorporated into this instruction. This revision incorporates the new Network Operations and Security Center (AFNOSC) reporting structure. The AFNOSC Command and Control (C2) Division at Barksdale AFB LA, has operational control over the AFNOSC Net Operations Division located at Maxwell Air Force Base, Gunter Annex, AL [formerly Air Force Network Operations Center (AFNOC)], and the AFNOSC Net Security Division located at Lackland AFB TX [formerly Air Force Computer Emergency Response Team (AFCERT)]. It addresses information flow among the various management tiers, and defines Air Force Network Operations Mis-

sion Areas and Core Services. It describes the Time Compliance Network Order (TCNO) and the Command, Control, Communications and Computers Notice to Airmen (C4 NOTAM). The reporting requirements in this directive (paragraph 4.6.3.) are exempt from licensing in accordance with AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*.

Chapter 1—GENERAL INFORMATION **4**

1.1. Background. 4

1.2. Air Force Network Operations (NETOPS) Scope. 4

Chapter 2—AIR FORCE NETWORK OPERATIONS HIERARCHY **6**

2.1. Overview. 6

Table 2.1. Air Force Hierarchy of NETOPS. 6

Figure 2.1. Air Force Network Operations Command Relationships. 8

2.2. Global (DISA/AFNOSC), Regional (NOSC) and Local (NCC) Organizations. 9

Chapter 3—ORGANIZATIONAL ROLES AND RESPONSIBILITIES **11**

3.1. Air Force Chief Information Officer (AF-CIO). 11

3.2. Deputy Chief of Staff/Warfighting Integration (HQ USAF/XI). 11

3.3. Deputy Chief of Staff/Installations and Logistics (HQ USAF/IL). 11

3.4. Air Force Communications Agency (AFCA). 12

3.5. Air Force Command and Control & Intelligence, Surveillance, and Reconnaissance... 12

3.6. 8th Air Force. 12

3.7. Major Commands (MAJCOM). 14

3.8. Air Education and Training Command (AETC). 14

3.9. Air Force Material Command (AFMC). 14

3.10. Wings and Air Base Host Units. 14

Chapter 4—OPERATIONAL ROLES AND RESPONSIBILITIES **16**

4.1. General. 16

4.2. Air Force Network Operations and Security Center (AFNOSC). 16

4.3. AFNOSC Net Operations Division. 17

4.4. AFNOSC Net Security Division. 18

4.5. Network Operations and Security Center (NOSC). 20

4.6. Network Control Center (NCC) (Air National Guard ROSC). 22

4.7. Functional Systems Administrator (FSA). 31

4.8. Workgroup Manager (WM). 32

Chapter 5—AIR FORCE ENTERPRISE NETWORK (AFEN) ACTIVE DIRECTORY MANAGEMENT 34

5.1. Overview. 34

5.2. Authority. 34

Chapter 6—MISSION AREAS, NOSC OPERATIONS, CREW POSITIONS AND CORE SERVICES 35

6.1. Mission Areas. 35

6.2. NOSC Organization. 36

Figure 6.1. NOSC Operations. 36

6.3. Crew Positions. 37

Figure 6.2. NOSC Crew Position Structure. 38

Figure 6.3. NCC Crew Position Structure. 38

6.4. Core Services. 39

Chapter 7—INFORMATION EXCHANGES, RELATIONSHIPS, AND REPORTING 40

7.1. General. 40

Figure 7.1. Information Exchanges. 41

7.2. Network Status and Management Reports. 41

Figure 7.2. Trouble Ticket Reporting and Tracking. 45

Chapter 8—AIR FORCE TECHNICAL ORDERS 46

8.1. General. 46

8.2. Maintaining Air Force TOs. 46

Chapter 9—SERVICE LEVEL AGREEMENTS (SLA) 47

9.1. Service Level Agreements (SLA). 47

9.2. Information Collections, Records, and Forms or Information Management Tools... 47

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 48

Attachment 2—SERVICE LEVEL AGREEMENT 54

Attachment 3—CREW POSITIONS 57

Chapter 1

GENERAL INFORMATION

1.1. Background.

1.1.1. This AFI provides the overarching policy, direction and structure for the Air Force Enterprise Network (AFEN). It is a key component in the efforts to Operationalize and Professionalize the Network (OPTN). The goal of Network Operations (NETOPS) is to provide effective, efficient, secure, and reliable information network services used in critical Department of Defense (DoD) and Air Force communications and information processes. This instruction provides the guidance necessary to manage the increasingly complex network environment and provide customers high quality services. Our networks have evolved into mission critical systems supporting Air Expeditionary Forces (AEF) and joint operations. Continued reliance on information-based weapons systems drive the need for a cohesive Air Force network.

1.1.2. Previously, management of the AFEN was centered around the base Network Control Centers (NCC). Today, our goal for managing the AFEN is to migrate to a hierarchical environment whereby management of the AFEN is distributed across three management tiers (see **Table 2.1.**). This operational concept has evolved over time with the explosive growth and increasing interconnectivity of the many networks and information services that make up the AFEN. What is needed is a new way to manage and control the AFEN so it can support the increasing demands placed on it by the warfighter.

1.2. Air Force Network Operations (NETOPS) Scope.

1.2.1. General.

1.2.1.1. The AFEN is a system that provides a set of value-added functions operating in a global context to provide processing, storage and transport of information, human interaction, systems and network management, information dissemination management, and information assurance. These functions must be fully integrated and interoperable with one another in order to achieve overall success across the AFEN. As a result, the AFEN is an information environment comprised of interoperable computing and communication components. The AFEN is part of the Global Information Grid (GIG). Therefore, AFEN is the interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The AFEN includes all owned and leased communications and computing systems and services, network operating systems, data, security services, and other associated services necessary to achieve information superiority.

1.2.2. Applicability.

1.2.2.1. This instruction applies to the Air Force Total Force which includes HQ USAF, functional communities, MAJCOMs, direct reporting units (DRU), field operating agencies (FOA), and Air Force Reserve.

1.2.2.2. This instruction also applies Air National Guard (ANG) Network Operations and Security Centers (NOSC) and Regional Operations Security Centers (ROSC). ANG Communications Flight NCCs are exempt from this instruction. However, ANG will develop applicable supple-

ments to this instruction. ANG personnel who deploy in support of active duty missions will comply with this instruction.

1.2.2.3. The AFEN includes any system, equipment, software, or service that meets one or more of the following criteria:

1.2.2.3.1. Transmits information to, receives information from, routes information among, or interchanges information with other equipment, software, and/or services.

1.2.2.3.2. Processes data or information for use by other equipment, software, and/or services.

Chapter 2

AIR FORCE NETWORK OPERATIONS HIERARCHY

2.1. Overview.

2.1.1. The Defense Information Infrastructure Control Concept (DIICC) and Air Force NETOPS Relationship.

2.1.1.1. The Air Force NETOPS hierarchy adheres to the DIICC. The DIICC consists of three areas of distributed responsibility at global, regional, and local levels. Internal to the Air Force, NETOPS relationships and responsibilities span all three levels. However, within the DoD hierarchy, the Air Force Network Operations and Security Center (AFNOSC), AFNOSC Net Operations Divisions (formerly known as Air Force Network Operations Center), AFNOSC Net Security Division (formerly known as Air Force Computer Emergency Response Team), and MAJCOM NOSC are all considered regional organizations in recognition of Defense Information Systems Agency's (DISA) overarching responsibility for other military services and other DoD agencies. The Air Force NETOPS organizations and their areas of responsibility (AOR) within the Air Force are depicted in **Table 2.1.**

Table 2.1. Air Force Hierarchy of NETOPS.

NETOPS Level	Responsible Air Force Organizations
Global (Tier 1)	AFNOSC C2 Division, AFNOSC Net Operations Division, AFNOSC Net Security Division
Regional (Tier 2)	MAJCOM NOSC, AFRC and ANG NOSC, Air Force Forces (AFFOR) NOSC-Deployed (NOSC-D), Mission Support Center (MSC), Functional Awareness Cell (FAC)
Local (Tier 3)	Active Duty NCC, AFRC and ANG ROSC, AFFOR NCC-Deployed (NCC-D)

2.1.1.2. **Table 2.1.** provides examples of major support activities aligned with each level of the Air Force NETOPS hierarchy. **Figure 2.1.** depicts the Air Force NETOPS command relationships between the global, regional, and local levels. The associated Joint, DISA, MAJCOM, and base-level elements are also shown. These relationships are the means for ensuring global systems interoperate without diminishing the authority of local commanders to direct and manage the information technology and communications assets under their control. Processes and procedures governing these relationships are meant to be complementary and minimize redundancy.

2.1.1.3. Air Force NETOPS Commander.

2.1.1.3.1. To create accountability for NETOPS, the Commander, Eighth Air Force (8 AF/CC) is designated as the Air Force Commander for NETOPS. The NETOPS/CC will exercise specific compliance enforcement and directive authorities over MAJCOM units/assets. The NETOPS/CC will also be authorized Direct Liaison Authority (DIRLAUTH) to MAJCOM SCs, System Control Centers, NOSCs and NOSC-Ds. The 8 AF/CC, as the NETOPS/CC, has delegated directive authority to the AFNOSC Director.

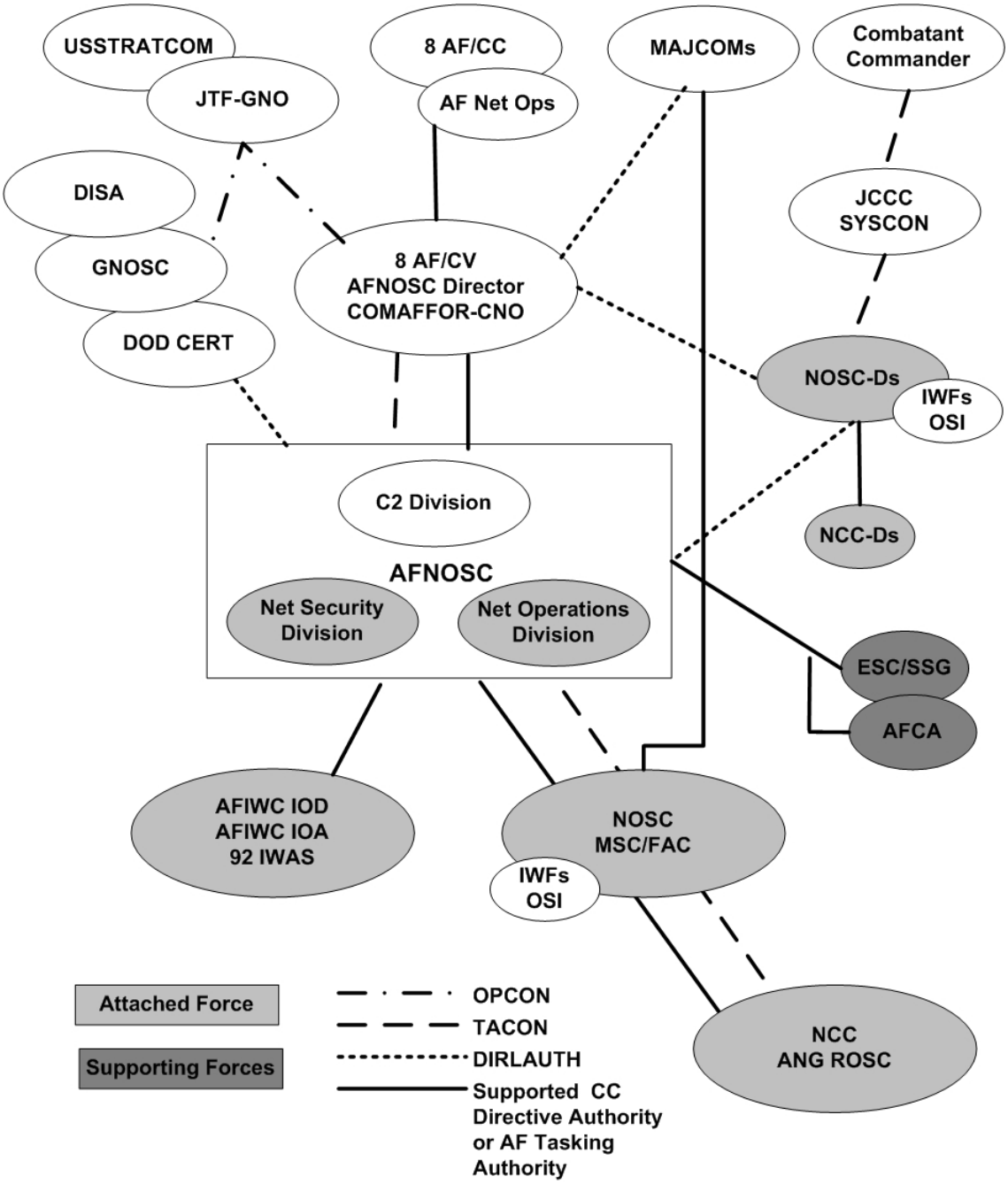
2.1.1.4. Commander, Air Force Forces-Computer Network Operations (COMAFFOR-CNO)/ AFNOSC Director.

2.1.1.4.1. The 8 AF/CV, as the COMAFFOR-CNO, serves as the Air Force component commander to the Commander Joint Task Force for Global Network Operations (JTF-GNO) and is responsible for ensuring Air Force Forces perform the missions and tasks assigned by the JTF-GNO. The COMAFFOR-CNO exercises Tactical Control (TACON) over attached units and supported commander directive authority or Air Force tasking authority over supporting forces to implement Computer Network Defense (CND) actions in support of joint objectives. The COMAFFOR-CNO will be dual-hatted as the AFNOSC Director and will be responsible for integrating NETOPS and CND functions across the AFEN.

2.1.1.4.2. Under the integrated NETOPS/CND Command and Control (C2) construct, the COMAFFOR-CNO will have the authority to task in response to events that cross MAJCOMs, affect the preponderance of the AFEN, or are time-critical to assure network availability and security. In general, this will include taskings to direct NOSCs' and NCCs' configuration changes, Information Operations Condition (INFOCON) changes, and changes to security postures. Supporting plans will define situations and objectives under which each supported/ supporting relationship occurs.

NOTE: ANG units remain under control of the their respective state unless activated by the President. Therefore, this must be taken into consideration when executing C2 of the AFEN.

Figure 2.1. Air Force Network Operations Command Relationships.



2.1.2. Deployed NETOPS Hierarchy.

2.1.2.1. The relationship between the fixed and equivalent deployed NETOPS hierarchy is also shown in **Figure 2.1.** The Combatant Command J-6 establishes the Joint Communications Control Center (JCCC) for the JTF AOR, and gives direction through the service's Systems Control (SYSCON). The JCCC does the planning and high-level management of the Joint network and provides specific guidance on Joint circuits.

2.1.2.2. DISA's span of control in the deployed environment extends to the JTF SYSCON. When deployed, Air Force component SYSCONs NOSC-Ds and NCC-Ds will use the approved joint

suite of NETOPS tools [e.g., Joint Network Management System (JNMS)] to execute their responsibilities and forward network status to the JTF SYSCON.

2.2. Global (DISA/AFNOSC), Regional (NOSC) and Local (NCC) Organizations.

2.2.1. Global.

2.2.1.1. DISA's Global NOSC (GNOSC) is responsible for the worldwide management and operational oversight of the Defense Information Infrastructure (DII). DII network and systems management policy and standards are developed jointly by DISA, the services, and agencies.

2.2.1.2. DISA's span of control ends at the Air Force base network Service Delivery Points (SDP) for fixed communications, and at the Joint SYSCON SDP for deployed operations.

2.2.1.3. All DoD organizations are responsible for complying with the published policies and standards. The NOSCs and NCCs are the primary Air Force organizations responsible for applying and enforcing these policies at the regional and local level.

2.2.1.4. The AFNOSC is comprised of the AFNOSC C2 Division, Net Operations Division, and Net Security Division. The Net Operations and Net Security Divisions execute Air Force NETOPS and CND through distributed operations. The Net Operations Division is the NETOPS execution arm of the AFNOSC, and the Net Security Division is the CND execution arm of the AFNOSC. Although elements of the AFNOSC may be physically separated, it will remain one staff under the command and direction of the AFNOSC Director/COMAFFOR-CNO.

2.2.2. Regional.

2.2.2.1. Regional operation centers depicted in **Table 2.1.** perform NETOPS to ensure operational control by implementing Systems and Network Management (S&NM), Information Assurance/Computer Network Defense (IA/CND), and Information Dissemination Management (IDM) within a specific AOR.

2.2.2.2. AFFOR NOSC-D is responsible for deployed Air Force NETOPS and reports to the JTF JCCC.

2.2.2.3. Mission Support Centers (MSC) and Functional Awareness Cells (FAC). These regional level entities exist at the same NETOPS management tier as the MAJCOM NOSC. They report to and take direction from the AFNOSC.

2.2.2.3.1. MSCs look, feel and act similar to a MAJCOM NOSC but are assigned to a FOA or DRU. They are responsible to a functional for monitoring network and application performance to ensure mission accomplishment over and above what is done by the local NCC.

2.2.2.3.2. FACs require only a small amount of the equipment and perform situational awareness for a functional system or mission. They act as the point of contact for all computer system trouble calls supporting a particular functional system or group of functional systems. FACs are typically owned and operated by the functional community that the computer system serves. The FAC evaluates problems and typically provides solutions for the application and data associated with that system(s).

2.2.2.3.3. To maintain base network integrity, MSCs and FACs will operate their networks in accordance with Service Level Agreements (SLA), Memorandums of Agreement (MOA), or Memorandum of Understanding (MOU) established with either the NCC, NOSC, or AFNOSC

as appropriate. The SLA, MOA, or MOU will include how core services (paragraph **6.3.**) are provided by the AFNOSC, NOSC, or NCC so not to jeopardize the integrity of the AFEN. See **Attachment 2** , Service Level Agreements, for policy and procedure guidance.

2.2.3. Local.

2.2.3.1. NCCs are the local network control elements through which NOSCs exercise management and operational direction over their MAJCOM network segments. NCCs also generate a situational awareness picture and partner with NOSCs to deliver S&NM, IA/CND, and IDM. They provide reliable, secure networks and network services for base-level customers.

Chapter 3

ORGANIZATIONAL ROLES AND RESPONSIBILITIES

3.1. Air Force Chief Information Officer (AF-CIO). The AF-CIO will:

3.1.1. Provide the overarching policy and oversight for all Air Force operational, system, and technical architectures, including establishing Information Technology (IT) standards and providing architectural support to the core Air Force processes.

3.1.2. Integrate Air Force planning, budget, financial, and program management processes for IT investments.

3.1.3. Review all 33-series and 37-series Air Force instructions for currency and relevance. The AF-CIO will ensure updates are made and published for all policy documents related to communications and information.

3.1.4. Develop and define the Air Force IT services for the AFEN.

3.1.4.1. Provide oversight of the implementation status of Air Force IT services on behalf of the Secretary of the Air Force (SECAF) and Chief of Staff of the Air Force (CSAF).

3.1.4.2. Ensure Air Force IT services are in-line with the DoD GIG enterprise services.

3.1.4.3. Provide oversight of the AFEN performance by measurement and analysis of Air Force-level metrics on behalf of the SECAF and CSAF.

3.2. Deputy Chief of Staff/Warfighting Integration (HQ USAF/XI). HQ USAF/XIC is the Director of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Infostructure. HQ USAF/XIC will:

3.2.1. Develop, validate, and monitor execution of plans, policies, and requirements for modernization of Air Force Communications and Information Infostructure. Provide overall integrated oversight of requirements, plans, schedules, budgets, and performance criteria for all modernization efforts associated with communications and information infostructure.

3.2.2. Lead the development and implementation of communications and information architectures for the Air Force and represent the Air Force position for joint architectures.

3.2.3. Provide policy and guidance for IT registration and administration of the Systems Compliance Database (SCD).

3.2.4. Work with program management offices to ensure all new community of interest systems/servers are developed and implemented with the intent of the CSAF server consolidation effort. Consolidation should start at the DISA Defense Enterprise Computer Center (DECC), however, consolidation to the AFNOSC Net Operations Division or NOSC is acceptable as well. Consolidation could include using remote management, co-location, or shared hosting consolidation as best fits the operational mission.

3.3. Deputy Chief of Staff/Installations and Logistics (HQ USAF/IL). The Directorate of Communications Operations (HQ USAF/ILC) will:

3.3.1. Oversee the day-to-day execution of Air Force communications and information programs and processes.

3.3.2. Develop and articulate positions for communications and information force structure and organizational issues. Analyze proposed MAJCOM force structure and organizational changes, and identify impacts on communications and information resources.

3.3.3. Establish course requirements and planning guidance for the professional development, advanced education, and technical training of the communications and information workforce through government and civilian institutions.

3.3.4. Lead career field managers for the communications, information, postal, visual information, and combat camera career fields.

3.3.5. Be the lead for communications and information readiness (Status of Readiness and Training Systems [SORTS], Air Expeditionary Forces [AEF], Unit Type Code [UTC] Functional Area Manager). Determine training requirements and ensure implementation of training programs for assigned Air Force specialties.

3.3.6. Be the lead for the establishing an Air Force policy on contingency of operations plans for the NOSC and NCC.

3.4. Air Force Communications Agency (AFCA). AFCA will:

3.4.1. Develop network enhancement initiatives. Act as the policy and standards adjunct of HQ USAF/XIC, HQ USAF/ILC, and AF-CIO. AFCA will administer the OPTN program.

3.4.2. Support the AF-CIO by managing and administering Command, Control, Communications, Computers and Intelligence Support Plan (C4ISP) which defines the Designated Approving Authority (DAA) functions and the process for certifying the network. (AFI 63-127, *Command, Control, Communications, Computers, and Intelligence Support Planning (C4ISP)*, will contain Air Force C4ISP guidance when published).

3.4.3. Address AFEN manpower issues. Identify future funding requirements and prepare Program Objective Memorandum (POM) submission in coordination with HQ USAF/XIC, HQ USAF/ILC and AF-CIO.

3.4.4. Develop, review, and update Air Force-level SLAs with external agencies as required.

3.4.5. Assist and advise NOSCs and NCCs on optimization of network infrastructures.

3.5. Air Force Command and Control & Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC). AFC2ISRC will:

3.5.1. Solicit requirements and develop guidance for Airborne, Air Operations Center (AOC), Intelligence, and Command and Control networks.

3.5.2. Review all policy and guidance to ensure network solutions meet warfighter requirements.

3.5.3. Support end-to-end interoperability of network solutions.

3.5.4. Advocate and support appropriate technology and platform implementations.

3.6. 8th Air Force.

3.6.1. AFNOSC C2 Division will:

3.6.1.1. Provide Air Force level C2 and situational awareness for the AFEN.

3.6.1.2. Enforce compliance with accreditation and other network policy.

3.6.1.3. Develop options and direct configuration changes, INFOCON changes, and changes to security postures in response to vulnerabilities and incidents, JTF-GNO direction, and outages that cross MAJCOMs, affect the preponderance of the AFEN, or are time critical in nature.

3.6.2. AFNOSC Net Security Division will:

3.6.2.1. Comply with TCNO and C4 Notice to Airmen (NOTAM) provisions of Air Force Systems Security Instruction (AFSSI) 5021, *Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting,* (will become AFI 33-138, *Enterprise Network Operations Notification and Tracking*).

3.6.2.2. Direct specific actions related to computer network defense.

3.6.2.3. Evaluate and respond to Air Force network intrusions and malicious logic events.

3.6.2.4. Develop countermeasures to network vulnerabilities and disseminate to applicable organization.

3.6.2.5. Assist AFNOSC/NOSCs/NCCs with computer attack damage control and recovery procedures.

3.6.3. AFNOSC Net Operations Division will:

3.6.3.1. Provide top-level tier of technical support for AFNOSC, NOSC, and NCC Wide Area Network (WAN) operations between SDPs. Technologies and programs to be supported include Domain Name Service (DNS), Air Force Virtual Private Network (VPN), and SDP technology insertion. Specific operational roles and responsibilities are listed in paragraph **4.2.**

3.6.3.2. Interface with the AFNOSC Net Security Division on information protection related incidents and provide network outage via Commander's Situation Report (SITREP) through operational reporting channels.

3.6.3.3. Collect and maintain a common view of MAJCOM's summary status of WAN resources and communications services within their AOR.

3.6.4. Air Force Information Warfare Center, Information Operations Directorate (AFIWC/IO), will:

3.6.4.1. Provide development and employment support for network sensors and CND weapon systems (AFIWC/IOD), as well as computer and network threat awareness, analysis, and intelligence support (AFIWC/IOA).

3.6.4.2. Report to MAJCOM NOSCs all backdoors and unauthorized connections to Air Force networks discovered during the course of operations. Reports will be made immediately upon discovery if associated with an on-going incident and within 48 hours from discovery if not associated with an incident response action.

3.6.4.3. Ensure the 23rd Information Operations Squadron develops Tactics, Techniques, and Procedures (TTP) for conducting Information Operations.

3.6.4.4. Ensure the 92nd Information Warfare Aggressor Squadron provides assistance to MAJCOMs by conducting computer and network vulnerability assessments and exercise red team support.

3.6.4.5. Ensure the 346th Test Squadron conducts formal testing and evaluation of CND weapon systems, as well as implementation assistance.

3.7. Major Commands (MAJCOM). Each MAJCOM will:

3.7.1. Establish and maintain a NOSC to provide command and control of the MAJCOM network (Specific NOSC roles and responsibilities are listed in paragraph **4.5.**).

3.7.2. Develop policies, procedures, and special instructions that pertain to the MAJCOM network.

3.7.3. Establish a Standardization/Evaluation (Stan/Eval) program to encompass the NOSC and NCC operations according to AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*.

3.7.4. Identify and submit network upgrade and operational requirements to Combat Information Transport System (CITS) Lead Command (HQ AFCA/GCLD.)

3.7.5. Provide network support such as engineering, strategic planning, risk management, developing SLAs, budgeting, inspecting, and contract management to subordinate units. Authorize adequate down time in order to support preventive maintenance inspections.

3.8. Air Education and Training Command (AETC). AETC will:

3.8.1. Manage and provide formal training in support of training, including initial, advanced, supplemental, and qualification training, delivered in-residence and through distance learning.

3.8.2. Identify and submit course resource estimate inputs to the 3C and 33S Career Field Managers for training. Provide oversight of Air Force supplemental technical training. To obtain formal training quotas, refer to Air Force Catalog (AFCAT) 36-2223, *USAF Formal Schools*, and AFI 36-2201, Volume 3, *Air Force Training Program, On the Job Training Administration*.

3.8.3. Identify all training resources required to Career Field Managers.

3.8.4. Plan and program classroom equipment for technology refresh.

3.9. Air Force Material Command (AFMC). AFMC will:

3.9.1. Provide POM inputs for technical solutions and life-cycle support to AFCA.

3.9.2. Review all TCNOs and C4 NOTAMs for applicability to all AFMC provided information systems.

3.10. Wings and Air Base Host Units. Hosting base units will:

3.10.1. Operate and manage NCCs to provide base level networking services. Specific NCC operational roles and responsibilities are listed in paragraph **4.6.**

3.10.2. Submit networking sustainment and upgrade requirements to their respective MAJCOM.

3.10.3. Ensure units coordinate with MAJCOMs for formal training requirements.

3.10.4. Ensure unit commanders establish an appropriate number of Workgroup Manager (WM) positions and fill with 3A0X1 personnel if assigned. WM appointment letters will be sent to the NCC.

Chapter 4

OPERATIONAL ROLES AND RESPONSIBILITIES

4.1. General. The AFNOSC, NOSC, and NCC are the tiered levels of AFEN operations working in concert to ensure networks are available to support mission demands. These centers perform the AFEN mission operation areas described in **Chapter 6** . Specific definitions of each tier, as well as roles and responsibilities, are discussed in this chapter.

4.2. Air Force Network Operations and Security Center (AFNOSC). The AFNOSC is the Air Force's top network operations tier. The AFNOSC develops options and directs configuration changes and changes to security postures in response to vulnerabilities and incidents, JTF-GNO direction, and outages that cross MAJCOMs, affect the preponderance of the network, or are time critical in nature. The AFNOSC provides Air Force-level metrics, situational awareness, and enforces compliance with accreditation and other network policy. Although the AFNOSC represents the top tier of the AFEN, it does not relieve MAJCOMs from managing, resourcing, and implementing the AFEN within their respective MAJCOMs. The AFNOSC has TACON over the MAJCOM NOSC, Base NCC and the MSC or FAC to direct configuration changes, INFOCON changes, and changes to the security posture of the AFEN. The AFNOSC will:

4.2.1. Operate 24 hours a day, 7 days a week.

4.2.2. Interact with the DISA, the JTF-GNO, MAJCOM NOSCs, and the commercial sector to identify and correct anomalies in Air Force networks, systems, and applications.

4.2.3. Have DIRLAUTH speak for the Air Force to MAJCOMs, other Air Force agencies, sister services, and other external agencies for network operations and network security issues.

4.2.4. Perform Information Dissemination Management.

4.2.4.1. Provide senior leaders with global visibility and situational awareness of AFEN resources and capabilities, including Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET).

4.2.4.2. Issue, track, document, and report compliance with TCNOs according to AFSSI 5021 (will become AFI 33-138), directing all AFEN operational, security, and configuration based changes. Issue Air Force-level C4 NOTAMs according to AFSSI 5021 (will become AFI 33-138).

4.2.4.3. Direct all AFEN operational, security, and configuration based changes.

4.2.5. Perform System and Network Management.

4.2.5.1. Perform continuous network monitoring and analysis of operations for identification of network availability or degradation events.

4.2.5.1.1. Monitor the Air Force IT services as defined by the AF-CIO.

4.2.5.2. Ensure situational awareness of CITS equipment is maintained and respond/report any system degradation events.

4.2.6. Perform Information Assurance/Computer Network Defense.

4.2.6.1. Perform continuous network monitoring operations for identification of on-going attacks against the network or interconnected systems.

4.2.6.2. Provide real-time analysis, response and reporting according to AFSSI 5021 (will become AFI 33-138) for network attacks and security incidents.

4.2.6.3. Correlate network events with supporting network data, threat data, and technical vulnerability information.

4.2.6.4. Maintain global situational awareness of events threatening Air Force networks.

4.3. AFNOSC Net Operations Division. The Net Operations Division of the AFNOSC provides senior leaders an Air Force-level view of the AFEN. One of its primary roles is to manage SDP network routers to produce global visibility of the AFEN and critical applications. The AFNOSC Net Operations Division monitors and responds to anomalies in communications and information networks, systems, and applications in coordination with DISA, MAJCOMs, and the commercial sector. It also operates in concert with AFNOSC Net Security Division to provide strong computer network defense capability to Air Force networks. The AFNOSC Net Operations Division will report to and take direction from the AFNOSC C2 Division for operational issues. AFNOSC Net Operations Division will:

4.3.1. Operate 24 hours a day, 7 days a week.

4.3.2. Coordinate with base NCC and MAJCOM NOSC to ensure presence of site personnel for troubleshooting operations when requested by DISA Network Operations Center.

4.3.3. Participate in Air Force Systems Network (AFSN)-led configuration control board to address AFEN requirements.

4.3.4. Perform Information Dissemination Management.

4.3.4.1. Implement TCNOs according to AFSSI 5021 (will become AFI 33-138), directing all Air Force-level operational, security, and configuration based changes. Utilize C4 NOTAMs according to AFSSI 5021 (will become AFI 33-138).

4.3.4.2. Draft SITREPs according to AFI 10-206, *Operational Reporting*. Draft Operational Event/Incident Reports (OPREP3) according to AFI 10-206 to document and report significant network events affecting Defense Information Systems Network (DISN) connections not previously reported in SITREPs.

4.3.4.3. Provide Help Desk services to MAJCOM NOSCs as a focal point for AFEN problem resolution.

4.3.4.4. Document and track trouble calls to final resolution.

4.3.4.5. Utilize Network Common Operating Picture (NETCOP) to consolidate NOSC up channeled metrics of C4 systems and report overall AFEN metrics to HQ USAF/ILC, HQ USAF/XIC, AF-CIO and other senior leaders as required.

4.3.4.6. Monitor and report status and critical metrics of Air Force IT services, as defined by the AF-CIO, NIPRNET, and SIPRNET connections to senior leaders and MAJCOM NOSC, MSC, FAC, and Base NCCs as needed or required.

4.3.5. Perform System and Network Management.

4.3.5.1. Manage Air Force level (af.mil and af.smil.mil) DNS.

4.3.5.1.1. Maintain and provide technical support for the af.mil and af.smil.mil domain and sub-domains.

4.3.5.2. Monitor Air Force-level Internet Protocol (IP) address space.

4.3.5.3. Manage the Tactical Internet Protocol (TAC-IP) Program to provide temporary IP address space for deployed units.

4.3.5.4. Administer and maintain Air Force-level system capabilities as negotiated in SLAs.

4.3.5.5. Manage the AFNOSC Net Operations Division's portion of the USAF Circuit Upgrade Program.

4.3.5.5.1. Identify and report circuits that exceed established thresholds to AFSN office.

4.3.6. Perform Information Assurance/Computer Network Defense.

4.3.6.1. Manage Air Force long-haul user VPN.

4.3.6.2. Maintain secure communications with NOSCs.

4.3.6.3. Update Access Control Lists on SDP routers per AFNOSC direction.

4.3.7. Develop and/or exercise contingency plans to continue operations in at least one location in the local area and one location outside the local area in the event of natural or unnatural disaster, utilities failure, and contractor issues.

4.3.8. Supply data to program offices, DISA, JTF-GNO, and other agencies, as required, to ensure systemic Air Force-level problem areas are tracked and fixed.

4.3.9. Provide situational awareness and status of the AFEN to HQ USAF/ILC, HQ USAF/XIC, AF-CIO, AFCA and to leaders at all levels based on their operational needs.

4.4. AFNOSC Net Security Division. The AFNOSC Net Security Division is the single point of contact in the Air Force for computer security incidents and vulnerabilities. This division of the AFNOSC assesses, analyzes, and provides countermeasures for computer security incidents and vulnerabilities reported by monitoring equipment, AFNOSC Net Operations Division, NOSCs, and other agencies. The AFNOSC Net Security Division is responsible for the defense of Air Force networks against computer network attack and exploitation. It serves as the Air Force OPR responsible for incident response and countermeasure generation for incidents that traverse multiple MAJCOMs or meet/exceed current Air Force incident thresholds. The AFNOSC Net Security Division also identifies vulnerabilities, validates and analyzes incidents, provides correlation services, generates risk reduction countermeasures, and collects, compiles, assesses, and reports unauthorized network activity and security incident statistics. The AFNOSC Net Security Division works with the AFNOSC Net Operations Division, MAJCOM NOSCs, and bases in eradicating malicious logic from a network and/or information system and assists in assessing the scope of unauthorized network activities and incidents. The AFNOSC Net Security Division is the Air Force OPR to register, acknowledge, and track implementation of DoD CERT Information Assurance Vulnerability Alerts as defined in DoD directives. The AFNOSC Net Security Division will report to and take direction from the AFNOSC C2 Division for security issues. AFNOSC Net Security Division will:

4.4.1. Operate 24 hours a day, 7 days a week.

4.4.2. Assist COMAFFOR-CNO in building upon current Air Force policies and programs to implement and maintain a network security posture that will defeat hostile Computer Network Attacks (CNA) and attempts to exploit Air Force network.

4.4.3. Serve as the Air Force single point-of-contact for receiving reports from and reporting computer security incidents and vulnerabilities to organizations external to the Air Force.

4.4.4. Perform Information Dissemination Management.

4.4.4.1. Implement TCNOs according to AFSSI 5021 (will become AFI 33-138), directing all security configuration based changes. Utilize C4 NOTAMs according to AFSSI 5021 (will become AFI 33-138).

4.4.4.2. Draft SITREPs according to AFI 10-206. Draft OPREP3s according to AFI 10-206 to document and report significant network events affecting the security of the AFEN not previously reported in SITREPs.

4.4.4.3. Supply data to program offices, DISA, JTF-GNO, and other agencies, as required, to ensure systemic Air Force-level problem areas are tracked and fixed.

4.4.4.4. Provide status of on-going law enforcement investigations related to computer security incidents to COMAFFOR-CNO.

4.4.4.5. Report COMAFFOR-CNO validated CNAs, suspicious activities, and security incidents to JTF-GNO, DoD CERT, GNOSC, Air Force Office of Special Investigations (AFOSI), Information Warfare Flights, MAJCOM NOSCs, NCCs, and other activities, in accordance with DoD and Air Force guidelines.

4.4.5. Perform System and Network Management on any AFNOSC Net Security Division owned systems needed to conduct IA/CND.

4.4.6. Perform IA/CND.

4.4.6.1. Analyze NETOPS security posture using security management software tools such as intrusion detection and vulnerability assessment.

4.4.6.2. Analyze customer impact of all network incidents, problems and alerts, and develop corrective actions or management changes.

4.4.6.3. Require network defense countermeasures and other defensive or corrective actions in response to command direction, INFOCONs, or vulnerability alerts.

4.4.6.4. Develop contingency plans to continue operations in at least one location in the local area and at least one location outside the local area in the event of natural or unnatural disaster, utilities failure, and contractor issues.

4.4.6.5. Conduct CNA assessments, correlate incidents, conduct spot check compliance, and conduct on-line surveys for suspicious activities (internal and external) across Air Force network domains. Notify COMAFFOR-CNO and the DISAGNOSC of attacks and suspicious activities. Conduct trend analysis to determine patterns of attack.

4.4.6.6. Conduct and manage Air Force vulnerability analysis and assistance functions in accordance with AFI 33-207, *Computer Security Assistance Program*. Notify COMAFFOR-CNO of technical vulnerabilities impacting Air Force computers and computer networks.

4.4.6.7. Assist the COMAFFOR-CNO in implementing the Air Force INFOCON program. AFI 10-2002, *Information Operations Conditions*, will contain Air Force INFOCON program guidance when published.

4.5. Network Operations and Security Center (NOSC). The mid-level (regional) MAJCOM NOSC is the mid-level organization in the three-tiered NETOPS structure. A MAJCOM NOSC provides commanders with real-time operational network intrusion detection and perimeter defense capabilities, as well as MAJCOM-level NETOPS and fault resolution activities. This dedicated first-line of defense is employed at the commander's direction to defend information networks both in-theater and in-garrison. NOSC personnel monitor and support the day-to-day operational issues associated with their subordinate bases and units. Their mission focus is to ensure their command's operational and support systems are fully capable. As appropriate, they support their commanders with information assurance capabilities, such as information systems security, decision analysis, and other technological capabilities. MAJCOM NOSCs will:

4.5.1. Operate 24 hours a day, 7 days a week.

4.5.2. Assist the AFNOSC (and DISA when requested through the AFNOSC) with ensuring presence of on-site personnel when requested by AFNOSC Net Operations Division to perform troubleshooting procedures to restore faulty, Air Force owned and operated, WAN transmission equipment and circuits.

4.5.3. Establish SLA, MOA, or MOU with Main Operating Bases (MOB), Geographically Separated Units (GSU), tenant units, Air Force and MAJCOM functional communities of interest defining agreed upon levels of support. Additionally, maintain SLA, MOA, or MOU with other MAJCOMs for providing back–up services as needed.

4.5.4. Perform Information Dissemination Management.

4.5.4.1. Implement, track, document and report compliance with TCNOs directed by the AFNOSC. Issue, implement, track, document and report compliance with MAJCOM-level TCNOs. Issue and review all C4 NOTAMs for applicability to all MAJCOM unique information systems according to AFSSI 5021 (will become AFI 33-138).

4.5.4.2. Draft SITREPs according to AFI 10-206. Draft OPREP3s according to AFI 10-206 to document and report significant network events affecting MAJCOM-level systems not previously reported in SITREPs.

4.5.4.3. Provide Help Desk services to NCCs and other NOSC customers for the MAJCOM; forward lessons learned and situations requiring additional assistance to next upper level tier Help Desk.

4.5.4.4. Provide situational awareness and visibility of the MAJCOM C4 systems as directed by the AFNOSC, but no less than every 12 hours, via NETCOP. As a minimum, NIPRNET, SIPRNET, Defense Switched Network (DSN), Air Traffic Control and Landing Systems (ATCALS), Automated Security Incident Measurement (ASIM), weather, Defense Message System (DMS) and Global Command and Control System (GCCS) will be monitored. Other systems may be added as requirements dictate.

4.5.5. Perform System and Network Management.

4.5.5.1. Provide and manage external DNS service to assigned bases, coordinate with AFNOSC Net Operations Division on Air Force-level DNS issues.

4.5.5.2. Manage MAJCOM-level (majcom.af.mil and majcom.af.smil.mil) DNS and assigned IP addresses. Those MAJCOM NOSCs that manage base-level IP addresses will follow guidance in paragraph **4.6.5.2.**

4.5.5.3. Perform distributed control of remote access services for the MAJCOM. Follow guidance in paragraph **4.6.5.3.**

4.5.5.4. Provide MAJCOM level Core Services (as defined in paragraph **6.3.**) to assigned bases.

4.5.5.5. Provide Network Time Protocol (NTP) management. NOSCs will use NTP on all systems within the CITS Network Operations and Information Assurance (NO/IA) boundary to synchronize system clocks with a local Global Positioning System (GPS) receiver. Additionally, ensure that as a minimum run NTP is enabled on all core servers and backbone equipment. Do not allow external NTP sources through the NO/IA boundary due to inherent security problems.

4.5.5.6. Detect, respond, and report network events affecting operational availability of MAJCOM network, user service levels, support to critical applications, and core services to the AFNOSC and others as appropriate.

4.5.5.7. Provide technical assistance to assigned NCCs.

4.5.5.8. Perform system backup and recover operations on NOSC managed servers.

4.5.5.9. Maintain capability to filter web sites to meet operational requirements e.g. MINIMIZE.

4.5.5.10. Monitor and manage Core Services via tools provided by the CITS Program Management Office.

4.5.6. Perform Information Assurance/Computer Network Defense (IA/CND).

4.5.6.1. Respond to and support the MAJCOM/Numbered Air Force (NAF) Information Warfare Flight.

4.5.6.2. Centrally operate and manage boundary protection and intrusion detection tools for all bases within their respective MAJCOM. This can be accomplished by either physically consolidating the servers at the NOSC or using remote management.

4.5.6.3. Protect against unauthorized intrusions and malicious activities; monitor and report intrusion detection activity in accordance with AFSSI 5021 (will become AFI 33-138).

4.5.6.4. Monitor, detect, and implement CND actions.

4.5.6.5. Maintain secure communications with AFNOSC Net Operations Division and NCCs.

4.5.6.6. Use vulnerability assessment software tools to analyze base networks under NOSC control for potential vulnerabilities and research/recommend appropriate protective measures; report suspected vulnerabilities and recommended protective measures to the AFNOSC Net Security Division. Ensure vulnerability scans are run monthly within MAJCOM.

4.5.6.7. Assist the MAJCOM IA office in developing a MAJCOM-level network security policy according to AFI 33-202, *Network and Computer Security*. Provide any network reports requested by the MAJCOM IA office required for Certification and Accreditation (C&A) of MAJCOM unique systems.

4.5.6.8. Analyze customer impact, within the MAJCOM, of all network incidents, problems and alerts, and develop corrective actions or management changes.

4.5.7. Take the following measures to meet the intent of the CSAF Server Consolidation effort:

4.5.7.1. Consolidate all MAJCOM external web servers (external web servers are those web servers that permit anyone access to from outside the .mil domain) to the NOSC. Use remote management, co-location or shared hosting consolidation as best fits the operational mission.

4.5.7.2. Assist in consolidating all functional community of interest servers. Preferred location is to the DISA DECC, however, consolidation to the NOSC is acceptable as well. Consolidation could include using remote management, co-location, or shared hosting consolidation as best fits the operational mission. In some instances, consolidation to the NCC is more appropriate to the operational mission in which case see paragraph **4.6.7.2.**

4.5.7.3. Manage desktop services in accordance with AFI 33-114, *Software Management*, consolidating services to the NOSC as best fits the operational mission.

4.5.7.4. Any new applications and their server(s), core services, network services, or desktop services and storage requirements shall meet the intent of the server consolidation architecture using remote management, co-location or shared hosting consolidation as appropriate to the operational mission in their initial operating capability and full operational capability.

4.5.8. Provide visibility of the MAJCOM network (NIPRNET and SIPRNET) to MAJCOM commanders and directors.

4.5.9. Provide NCCs, within the respective MAJCOM, visibility into NOSC-managed devices for local situational awareness.

4.5.10. Oversee implementation of policies, procedures, and special instructions to NCCs.

4.5.11. Support deployable operations and maintain joint capabilities.

4.5.12. Provide engineering guidance to plan, install, operate, and maintain base network hardware and software.

4.5.13. Perform NOSC-level systems control, maintenance, and administration functions within the MAJCOM network.

4.5.14. Manage MAJCOM electronic mail global address list.

4.5.15. Maintain a data base of workload factor data depicting the number of network users, workstations, servers, and IP addresses to support NOSC manpower requirement. Also, include in this database the building, room, POC, and phone number of the workload factor data. NOSC must be able to provide detailed reports in sorted formats as specified by the appropriate manpower office.

4.6. Network Control Center (NCC) (Air National Guard ROSC). The NCC oversees network operations, helps achieve information assurance, and generates visibility into the base network. Wing and theater air base commanders exercise command and control over their fixed base or deployed site networks and systems via the NCC. Local Area Networks (LAN) and the Metropolitan Area Networks (MAN) on the base are considered part of the base network and managed by the NCC. Thus, the NCC is the central focal point on base for the operation, maintenance, and management of all aspects of the base network to include wireless LANs (NCCs will need to establish a memorandum of agreement with the appropriate

functional community to cover manning and training deficiencies that may exist due to legacy wireless equipment). The NCC provides an on-site technical capability to implement physical network changes and modifications and restoration of faulty network transmission equipment and circuits when directed by the NOSC or AFNOSC. Using network administration, network management, information protection tools, the NCC technicians provide core services to functional system administrators, workgroup managers and users. NCCs will:

4.6.1. Operate 24 hours per day, 7 days per week (with either continuous manning or on-call after-hours response capability).

4.6.2. Ensure presence of on-site personnel when requested by NOSC (or AFNOSC through NOSC) to perform troubleshooting procedures to restore faulty WAN transmission equipment and circuits.

4.6.3. Achieve full operational capability within 4 hours after notification in situations requiring increased operations tempo surge manning. This ensures on-site presence of personnel to meet elevated unit communications requirements. Units will annotate the 4-hour response time in section IIB of AF Form 723, **Status of Resources and Training System (SORTS) Designed Operational Capability (DOC) Statement**, and state AFI 33-115, Volume 1, as the response time source reference document.

4.6.4. Perform Information Dissemination Management.

4.6.4.1. Implement TCNOs according to AFSSI 5021 (will become AFI 33-138), execute changes, or perform “touch labor” as directed by MAJCOM NOSC. Utilize C4 NOTAMs according to AFSSI 5021 (will become AFI 33-138).

4.6.4.2. Draft SITREPs according to AFI 10-206. Draft OPREP3s according to AFI 10-206 to document and report significant network events affecting base-level systems not previously reported in SITREPs.

4.6.4.3. Provide Help Desk services to base-level users and WMs to serve as focal points for network, to include Air Force IT services, problem resolution. Forward lessons learned and situations requiring additional assistance to next upper level tier Help Desk.

4.6.4.4. Escalate problems beyond the capability of the NCC to the NOSC for resolution.

4.6.4.5. Provide situational awareness and visibility of the base-level C4 systems as directed by the AFNOSC, but no less than every 12 hours via NETCOP. As a minimum, NIPRNET, SIPRNET, DSN, ATCALS, ASIM, Weather, DMS and GCCS will be monitored. Other systems may be added as requirements dictate. Forward requirements to HQ AFCA/GCLD.

4.6.4.6. Provide flexible and scaleable levels of service to Functional System Administrators (FSA), WM, and users for Air Force IT services as defined by the AF-CIO.

4.6.5. Perform System and Network Management.

4.6.5.1. Manage internal base DNS (base.majcom.af.mil and base.majcom.af.smil.mil).

4.6.5.2. Manage all base IP address space through utilization of Dynamic Host Configuration Protocol (DHCP). Reserve IP addresses in DHCP for all network servers (including file, print, web, and messaging), network management workstations, Router/Switch interfaces, and Security Management Tools (e.g., VPNs, firewalls, proxy servers, ASIM, etc.). Enable logging to maintain a historical list of IP address assignments. DHCP will allocate dynamic IP addresses for:

4.6.5.2.1. All noncritical workstations connected to the internal base network. Noncritical workstations will have a reservation of 60 days applied to them; this ensures, with relative certainty, that the same IP is assigned to a workstation each time a new reservation is issued.

4.6.5.2.2. Noncritical workstations connected to the internal base networks that have documented IP address shortages, e.g., more than 80% utilization of IP addresses. The DHCP lease time may be adjusted to less than 60 days to recover IP addresses more quickly.

4.6.5.2.3. Remote access clients. Use the Remote Access Server to issue a new IP address each time a remote access client logs in. Do not attempt DHCP through the firewall.

4.6.5.3. In coordination with the NOSC, provide and control all remote dial-in/dial-out communications access services. Place the communications server capable of handling dial-in and dial-out services outside the CITS NO/IA boundary to prevent the possibility of back-door access. This means that organizations will not connect external access devices to the base network. The NCCs control all remote dial-in/dial-out communications services.

4.6.5.4. Provide NTP management. NCCs will use NTP on all systems within the CITS NO/IA boundary to synchronize system clocks with a local GPS receiver. Additionally, ensure that as a minimum run NTP is enabled on all core servers and backbone equipment. Do not allow external NTP sources through the NO/IA boundary due to inherent security problems.

4.6.5.5. Move all Air Force owned networks behind the NCC/NOSC IA boundary. NOSC or NCC will manage and monitor all networked devices using network management and security tools. In all cases, host tenant agreements and service level agreements that result from this requirement must adhere to Air Force policy. The following scenarios apply to non-Air Force units residing on an Air Force base:

4.6.5.5.1. All non-Air Force units on an Air Force installation that use the host base's Core Services (see **Chapter 6**) must be located behind the base boundary protection and comply with the security policy for the host base network.

4.6.5.5.2. Any non-Air Force unit on an Air Force installation not using host base Core Services (see **Chapter 6**) may have their own network separate from the base network. These networks must adhere to the following guidelines:

4.6.5.5.2.1. Physically separate this network from the base network infrastructure. No devices on this network may attach to the base data network in any way.

4.6.5.5.2.2. This network must connect to the NIPRNET outside the base boundary and may only communicate with the base network by coming through the base boundary protection from the outside.

4.6.5.5.2.3. The using organization is responsible for funding any and all network components as well as any costs associated with their connectivity.

4.6.5.5.2.4. The using organization is responsible for complying with all DoD-required IA measures, to include intrusion detection and vulnerability patching.

4.6.5.6. Provide messaging services to base-level users [e.g., DMS and Simple Mail Transfer Protocol (SMTP) electronic mail]. NCCs are not required to do this if the NOSC is performing these duties.

4.6.5.7. Secure and manage the CITS Common Air Force Wireless solution.

4.6.5.7.1. NCCs will control any hardware or software used to provide wireless access to the base network.

4.6.5.7.2. All client devices using the base wireless infrastructure will meet the requirements specified in AFI 33-202 and the CITS common Wireless Local Area Network (WLAN) solution. In addition:

4.6.5.7.2.1. Wireless client devices must be registered with the NCC prior to connecting to the base wireless infrastructure. At the time of registration, the NCC will record a device specific authentication factor - usually the Media Access Control (MAC) address of the device - to be used for hardware authentication.

4.6.5.7.2.2. Lost or stolen wireless devices must be reported to the NCC within 24 hours. Entries for such devices will be removed from all access control lists. If recovered, the device-specific authentication factor will be considered compromised and will be changed before the device is redeployed.

4.6.5.7.2.3. All wireless client devices must run approved Air Force-approved anti-virus software.

4.6.5.7.2.4. All wireless client devices must use a VPN system client (usually software) compatible with the VPN system managed by the NCC.

4.6.5.7.2.5. Wireless client devices will not allow ad hoc wireless networking or direct peer-to-peer wireless networking.

4.6.5.7.2.6. Systems with direct network access (e.g. via Ethernet cable) will not also provide wireless data connectivity. For example, a network-connected computer cannot have a wireless network interface card installed.

4.6.5.7.2.7. Passwords and sensitive information will not be wireless transmitted unless encrypted in accordance with Air Force WLAN policy, and AFMAN 33-223, *Identification and Authentication*. This includes wireless keyboards and wireless terminals, but not pointing devices.

4.6.5.7.3. Wireless Network Operations Requirements.

4.6.5.7.3.1. Must integrate into CITS Information Transport System and Network Management System/Base Information Protect suite at NOSC and/or NCC.

4.6.5.7.3.2. Must have Graphical User Interface and Command Line Interface.

4.6.5.7.3.3. Must have the capability to shut down wireless access points remotely from the NCC and NOSC.

4.6.5.7.3.4. NCCs will expand current network vulnerability scanning procedures to include wireless networks.

4.6.5.8. Provide a core set of office automation application support services.

4.6.5.9. Implement software patches and security fixes as required by the NOSC, AFNOSC, or program manager.

4.6.5.10. Report events not previously detected by the NOSC or AFNOSC.

4.6.5.11. In coordination with NOSC, plan, install, operate, and maintain base network hardware and software.

4.6.5.12. Perform regular day-to-day system backup and recovery operations on NCC managed servers. At a minimum of once a quarter test recovery procedures to ensure procedures are accurate and operational.

4.6.5.13. Develop local restoral and contingency operations plans from existing operations/war plans. Validate restoral plans by testing them on at least a biannual basis.

4.6.5.14. Maintain network and facility configuration, migration, and upgrade plans.

4.6.5.15. Perform fault management for the local base network.

4.6.5.15.1. Dispatch technicians to unmanned or user and subscriber locations when required to test, trouble-shoot, and restore service.

4.6.5.15.2. Coordinate with job control subscribers, local and distant support agencies, and contractors to isolate faults, restore service, and make repairs.

4.6.5.15.3. Ensure a trouble-call process is established.

4.6.5.15.4. System administrators monitor difficulty reports, heads-up messages, and system advisory notices.

4.6.5.15.5. Provide network and small computer maintenance support to WMs and FSAs.

4.6.5.15.6. Maintain Line Replaceable Unit (LRU) stock level and assist users in ordering replacement LRUs.

4.6.5.15.7. Provides technical support to FSA and WM when requested and maintain an electrostatic discharge maintenance area.

4.6.5.15.8. Perform fault isolation to the LRU and line item equipment level. Fault isolation methods include automated diagnostics and sound trouble-shooting techniques.

4.6.5.16. Perform configuration management for the local base network.

4.6.5.16.1. Prepare and update network maps and facility equipment listings. Provide MAJCOM NOSC a copy as required.

4.6.5.16.2. Establish a warranty management program to ensure continuous maintenance support for network hardware.

4.6.5.16.3. Establish a license management program according to AFI 33-114 to ensure authorized usage for base network software.

4.6.5.16.4. Work with Planning/Implementation section and the Systems Telecommunications Engineering Manager (STEM) to participate in the review and planning of base transmission media and telecommunications systems networks. Makes sure replacements for legacy or dumb network devices incorporate remote management capability to improve centralized management, performance, and quality.

4.6.5.16.5. Perform minor application enhancement and software metering.

4.6.5.16.6. Perform automated data processing equipment (ADPE) equipment custodian (EC) duty for NCC equipment.

4.6.5.16.7. Provide assistance, when needed, and performs cryptographic equipment updates on devices under the control of the NCC.

4.6.5.16.8. Provide base network/NCC hardware and software installation service.

4.6.5.16.8.1. Hardware: NCCs install and configure network servers, routers, hubs, bridges, repeaters, and servers. They test and document equipment installation acceptance testing.

4.6.5.16.8.2. Software: NCCs receive and inventory network software, test and validate new software applications and network operating systems.

4.6.5.16.8.2.1. Distribute and install network software releases and updates, and assist customers with software installation and customization.

4.6.5.16.8.2.2. Install and configure SMTP hosts, relays, and gateways.

4.6.5.16.8.2.3. Review site license agreements and remove software from systems when no longer required or authorized.

4.6.5.16.9. Performs base network management (NM) planning.

4.6.5.16.9.1. NCCs maintain the base network characterization and validate the DISA Minimum Essential Circuit Listing (MECL) and the Defense Information Technology Contracting Office (DITCO) database product.

4.6.5.16.9.1.1. Collate local and long-haul customer telecommunications circuit information.

4.6.5.16.9.1.2. Verify current network configurations against other agency databases and forward corrections as required.

4.6.5.16.10. Perform base-wide configuration standardization and interface engineering.

4.6.5.16.10.1. Prepare and update in-station system block diagrams, network maps, and facility equipment listings; maintain network and facility configuration plans; perform minor network engineering; monitor management information base variables; and advise and make recommendations on new systems to customers.

4.6.5.16.10.2. Perform the following in conjunction with the base **Communications and Information Systems Officer** and plans function:

4.6.5.16.10.2.1. Review project support agreements (PSA) and coordinate corrections with the appropriate agencies.

4.6.5.16.10.2.2. Coordinate with Engineering and Installation (EI) teams and/or commercial vendors prior to arrival and prepare the facility for installation team.

4.6.5.16.10.2.3. Escort and assist team chiefs with installation or upgrade projects.

4.6.5.16.10.2.4. Complete DD Form 250, **Material Inspection and Receiving Report**; AF Form 1261, **Communications and Information Systems Acceptance Certificate;** and EI critiques.

4.6.5.16.11. Perform contract management for base network support.

4.6.5.16.11.1. NCCs consolidate and evaluate base-wide NCC-managed network and system components as candidates for contract maintenance support.

4.6.5.16.11.2. Submit inputs to the unit plans function for statement of work development.

4.6.5.16.11.3. Assist the plans function in the preparation of quality assurance surveillance plans and perform contract quality assurance evaluation functions as identified.

4.6.5.16.12. Perform base network budget planning.

4.6.5.16.12.1. Develop/submit budget input and request higher-level funding for all NCC requirements and operations functions.

4.6.5.16.12.2. Monitor base network funds availability and process International Merchant Purchase Authorization Card (IMPAC) requests for hardware and software purchases following approval.

4.6.5.16.13. Remotely perform the functions and duties of a Defense Communications System (DCS) Primary Systems Control Facility (PSCF), patch and test facility, DCS switching center, or other DCS operations function, when it is technically and economically feasible and does not degrade quality of service in accordance with DISA procedures. To support the wing during contingencies, the NCC takes over the responsibility and authority of the PSCF for DCS service control.

4.6.5.17. Conduct performance management for the local base network.

4.6.5.17.1. Consolidate base-level network performance data, security data, and analysis reports, pulling information from the Air Force NETOPS hierarchy as needed. Use the consolidated information to identify causes of service, performance, and security flaws. On the basis of the aggregated analysis, recommends changes in network configurations, hardware or software, procedures, and staff training.

4.6.5.17.2. Monitor and optimize network performance.

4.6.5.17.3. Coordinate installation, acceptance testing, quality assurance, fault isolation, and restoration of the infrastructure with the base's other communications unit functions.

4.6.5.17.4. Maintain capability to filter web sites to meet operational requirements (e.g., MINIMIZE).

4.6.5.17.5. Establish individual circuit and system parameters on non-DCS circuits. Develop the parameters according to DISAC 300-175-9, *DCS Operating Maintenance Electrical Performance Standards*, supplemented by commercial-leased equipment and circuit performance standards.

4.6.5.17.6. Establish initial performance thresholds according to systems and circuit operation specifications and operational or mission requirements.

4.6.5.17.7. Remotely test subscriber equipment, end-to-end circuits, systems, and networks to verify the services provided and input and output signals meet standards.

4.6.5.17.8. Adjust remote network element equipment to optimize service.

4.6.5.17.9. Record configuration data, test data, failure symptoms, coordination efforts, fault isolation steps performed, and any other useful information. Uses this information to evaluate and control operations, service capabilities, and service quality.

4.6.5.17.10. Report to management on quality of infrastructure services.

4.6.5.17.11. Perform system diagnostics and sets global alarm thresholds and system parameters.

4.6.5.17.12. Utilize performance tools to ensure optimum network operation, monitor system logs, analyze bandwidth utilization, and set global parameters to prevent adverse effects to the overall communications network. Core systems must have critical path redundancy.

4.6.5.17.13. Perform network/circuit Quality Control (QC) testing and evaluation.

4.6.5.17.13.1. Generate and update QC schedules.

4.6.5.17.13.2. Plan, provide, coordinate, and verify alternate service during QC testing.

4.6.5.17.13.3. Access and monitor Preventative Maintenance Inspection (PMI) schedules published by the maintenance control work center.

4.6.5.17.13.4. Coordinate in-service/out-of-service QC testing and performance of PMIs with affected work centers and external agencies.

4.6.5.17.13.5. Coordinate and deactivate alternate service once testing/PMIs are completed and original circuit/equipment is verified operational.

4.6.5.17.13.6. Analyze QC performance trend analysis data (collected through in-service/out-of-service QC testing) to identify trends or patterns of circuit/system/network degradation, dispatch to and from user locations when required, and generate and analyze outage reports.

4.6.5.17.13.7. Submit DD Form 1368, **Modified Use of Leased Communication Facilities**, when required, and research, prepare, and submit QC waiver requests when necessary, in the absence of a systems control facility.

4.6.5.18. Conduct security management for the local base network.

4.6.5.18.1. Conduct Information Protection Operations (IPO) according to applicable security publications and TTPs.

4.6.5.18.1.1. Install and set up audit tools.

4.6.5.18.1.2. Perform vulnerability assessments to test and validate security of networks and systems. If vulnerabilities are discovered, provide appropriate systems administrators, unit commanders, DAA, wing and MAJCOM IA offices, and AFNOSC Net Security Division with test results and recommendations. Report vulnerabilities found according to AFSSI 5021 (will become AFI 33-138).

4.6.5.18.1.3. Conduct daily traffic analysis, identify and characterize incidents, and generate incident reports with Air Force approved intrusion detection tools. Investigate each item to clarify and resolve suspicious activity. Report validated suspicious activity in according to AFSSI 5021 (will become AFI 33-138).

4.6.5.18.1.4. Review AFNOSC Net Security Division advisories, and verify systems under NCC control are protected against documented vulnerabilities.

4.6.5.18.1.5. Notify WMs, FSAs, and/or users when their computers have weak configurations, vulnerabilities, and when they have been accessed, exploited, or destroyed by unauthorized persons or machines.

4.6.5.18.1.6. Inform all network users that the NCC has the technical capability to monitor, capture, record, and store all transmissions traversing the network according to AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP*).

4.6.5.18.2. Ensure all systems and networks meet Air Force and local security requirements and have appropriate DAA approval before connecting to the base network infrastructure. Terminate service and/or network connectivity of local systems and networks that fail to comply.

4.6.5.18.3. Provide, manage, and control (in coordination with the AFNOSC when required) access to NIPRNET, SIPRNET, and the Internet.

4.6.5.18.3.1. The NCC, in coordination with the NOSC, will manage any/all security policy enforcement tools installed inside the NCC/base boundary and monitor all networked devices.

4.6.5.18.3.2. Equip all servers within the CITS NO/IA boundary with host-based intrusion detection and network security analysis and scanning tools.

4.6.5.18.4. Identify weak configurations and security holes by auditing and monitoring events occurring on the network.

4.6.5.18.5. Monitor audit and error logs for security violations.

4.6.5.18.6. Test and validate network security to establish and maintain a target baseline for Air Force owned systems.

4.6.5.18.7. Identify and secure computer systems on an affected network. Identify computers with exploited vulnerabilities.

4.6.6. Perform Information Assurance/Computer Network Defense (IA/CND).

4.6.6.1. Provide any network reports requested by the wing IA office required for C&A of base networks and systems.

4.6.6.2. Assist the wing IA office in developing a base-wide network security policy according to AFI 33-202.

4.6.6.3. Coordinate on all base unique Certificate of Networthiness (CoN), Certificate to Operate (CtO), and C&A packages or requests.

4.6.6.4. Develop local procedures to report and respond to computer security and virus incidents according to AFSSI 5021 (will become AFI 33-138). Work with the wing IA office to identify internal actions such as local reporting channels, criteria for determining who is notified, etc.

4.6.6.5. Perform local CND actions and respond to NOSC or AFNOSC direction.

4.6.6.6. Provide physical security for AFEN resources.

4.6.6.7. Analyze customer impact, within the base, of all network incidents, problems and alerts, and develop corrective actions or management changes.

4.6.7. In coordination with the MAJCOM NOSC, take the following measures to meet the intent of the CSAF Server Consolidation effort:

4.6.7.1. Consolidate all e-mail, file, internal (inside the firewall) web and print servers to the NCC, using remote management, co-location or shared hosting consolidation as best fits the operational mission.

4.6.7.2. Consolidate functional community of interest servers that are incapable of supporting DECC or NOSC consolidation to the NCC, using remote management, co-location or shared hosting consolidation as best fits the operational mission.

4.6.7.3. Perform remote management of desktop services in accordance with AFI 33-114 consolidating services to the NCC as best fits the operational mission.

4.6.8. Familiarize and guide FSAs and WMs on local network operations and procedures.

4.6.9. Establish, maintain, control, and enforce the base Internet use policy according to AFI 33-129, *Transmission of Information Via the Internet* (will become Web Management and Internet Use).

4.6.10. Maintain a data base of workload factor data depicting the number of network users, workstations, servers, and IP addresses as described in Air Force Manpower Standard (AFMS) 38DA. Also, include in this data base the building, room, POC, and phone number of the workload factor data. NCCs must be able to provide detailed reports in sorted formats as specified by the appropriate manpower office.

4.7. Functional Systems Administrator (FSA). Functional systems administrators ensure functional communities of interest systems, servers, workstations, peripherals, communications devices, and software are on-line and supported. They must thoroughly understand the customer's mission and be completely knowledgeable of hardware and software capabilities and limitations supporting that functional system. Their AOR is from the user's terminal to the server, but does not include the network backbone infrastructure. FSAs are not normally assigned to the NCC, but are a logical extension of NCC functionality. FSAs are trained and certified according to the appropriate network crew position that best meets their position requirements. FSAs will:

4.7.1. Comply with the policies of this instruction and maintain position certification. Perform the responsibilities delegated by the NCC to optimize performance and quality of service. Consolidate systems administration duties within an organization or a building, if possible, merging them with the NCC based on an SLA, MOA, or MOU.

4.7.2. Ensure servers, workstations, peripherals, communications devices, and operating system/application software are properly configured for network operation, are on-line, and are available to customers.

4.7.3. Periodically review the organization's needs for computer resources.

4.7.4. Define ownership of applications and determine who has permission to read, write, and execute.

4.7.5. Assign and maintain userIDs and passwords according to AFMAN 33-223. Administer user privileges on the system (e.g., which users share files).

4.7.6. Plan for short-term and long-term loss of system hardware and software. In configuring the system, the FSA and network security manager must decide on contingency plans in case of the FSA's absence. This may involve having another FSA administer the system remotely.

4.7.7. Monitor the efficiency of the system (e.g., finding and resolving system bottlenecks).

4.7.8. Perform routine system maintenance such as backing up or archiving application data files and adding application software updates.

4.7.9. Serve as the system trouble-shooter, a critical role in keeping the system operational. Contacts the NCC for hardware maintenance when necessary.

4.7.10. Work with the NCC to implement network security policies and procedures as outlined in the base network security policy.

4.7.11. Ensure end user training is conducted.

4.7.12. Provide user manuals that include sign-on and sign-off procedures, use of basic commands, software policies, user responsibilities, etc.

4.7.13. Implement software patches and security fixes as required by the AFNOSC, or program management office. Tests and validates the proper operation and configuration with appropriate patches and fixes, as required above, prior to restoring any device to the network.

4.8. Workgroup Manager (WM). WMs support a functional community (e.g., work centers, flights, squadrons, or organizations) and serve as the first line of help to resolve customers' administrative and technical problems. WMs are usually not assigned to the NCC, though are logically an extension of the Help Desk team. WMs take direction from the NCC and FSA. NCC direction takes precedence over FSA direction. WMs install, configure, and operate client/server devices. The WM will be a 3A0X1 unless none are assigned. Information managers receive 3-, 5- and 7-skill level training on workgroup management. When a 3A0X1 is not assigned, any AFSC or occupational series can perform WM duties once trained and certified. WMs will:

4.8.1. Comply with the policies of this instruction and maintain WM certification.

4.8.2. Perform the installation of equipment, connection of peripherals, and the installing/deleting of user software.

4.8.3. Configure user software, modify software configuration, and perform basic configuration management functions.

4.8.4. Provide limited software application assistance for commonly used office automation applications purchased from standard Air Force support contracts.

4.8.5. Perform initial system diagnostics and trouble-shooting of systems assigned to them.

4.8.6. Assign, modify and delete passwords and user privileges according to AFMAN 33-223.

4.8.7. Report security breaches and distribute security information

4.8.8. Coordinate support issues with all agencies (e.g., customers, FSA, NCC, etc.).

4.8.9. Notify the unit EC of any hardware relocation and equipment problems.

4.8.10. Obtain an implementation checklist from the MAJCOM, NCC, or FSA, before installing equipment. Assist with installing, testing, and accepting the system according to the terms of the purchase contract and instructions.

4.8.11. Coordinate with the facility manager and the base civil engineer for facility support requirements.

4.8.12. Periodically review the organization's needs for computer resources.

4.8.13. Validate computer equipment requirements the unit EC submits.

4.8.14. When requested, assists the unit EC with computer hardware and software inventories.

4.8.15. Promote user awareness concerning unauthorized or illegal use of computer hardware and software.

4.8.16. Identify organization deficiencies and operational needs that computer use can solve.

4.8.17. Ensure organizations do not use shareware or public domain software until approved for use by the DAA after the Computer Systems Security Officer, WM, or FSA ensures it is free of viruses, hidden defects, and obvious copyright infringements.

4.8.18. Ensure correct management of records created by or stored on computers by coordinating with the unit records manager. These records include information for official use only or information subject to the *Privacy Act of 1974*. AFMAN 37-123, *Management of Records*, gives details on records management for computers. Air Force WEB-RIMS RDS located at **https://webrims.amc.af.mil/rds/index.cfm** provides records disposition guidance.

Chapter 5

AIR FORCE ENTERPRISE NETWORK (AFEN) ACTIVE DIRECTORY MANAGEMENT

5.1. Overview.

5.1.1. Standardization of naming conventions for Win2K directory objects and attributes are critical for interoperability and configuration control reasons.

5.1.2. When trying to decide on common-sense naming conventions for Active Directory, it is important to consider what the consequences are on end-users as well as administrators, from client applications such as Outlook and the Network Browser (My Network Places), to server applications such as Active Directory Users and Computers and Sites and Services.

5.2. Authority.

5.2.1. Per HQ USAF/ILC guidance, "Rigorous central control will be exercised over Active Directory naming conventions." HQ AFCA/ITLD is the lead for all Active Directory concerns to include the responsibility for establishing naming conventions. MAJCOM NOSCs and base-level NCCs are responsible for enforcement of naming conventions. AFEN naming convention guidance can be found at: **https://www.afca.scott.af.mil/win2000/guidance.html**. Some of the naming standards listed in this document are mandatory and some are recommended. If a MAJCOM decides not to use the recommended naming conventions, they must document the naming conventions and consistently enforce them throughout the MAJCOM. MAJCOMs will submit naming conventions to the Infostructure Architecture Council as part of their Active Directory implementation plan. Additional information or questions should be referred to **mailto:afca.itld@scott.af.mil**.

5.2.2. The Air Force will have multiple forests consisting of a single forest per MAJCOM. This requirement holds true for both NIPRNET and SIPRNET. Additional roots will be considered by the Infostructure Architecture Council on a "by exception" basis if there are sound technical grounds. FOAs and DRUs that do not fall under a MAJCOM will need to make arrangements with a MAJCOM to join their root.

5.2.3. HQ AFCA/ITLD is the Air Force focal point for Active Directory requirements, standardization and processing. In all cases, HQ AFCA/ITLD will be formally notified of all Active Directory planning and implementation. MAJCOMs will send a copy of their Active Directory implementation to HQ AFCA/ITLD.

Chapter 6

MISSION AREAS, NOSC OPERATIONS, CREW POSITIONS AND CORE SERVICES

6.1. Mission Areas. Air Force NETOPS Mission Areas are the overarching activities performed by network professionals in various crew positions to maintain and operate the AFEN and contribute to a robust, full-spectrum Defensive Counter-Information (DCI) posture of Air Force operations. These actions promote information assurance and enable crew members to maximize operational availability, optimize performance, and mitigate risks.

6.1.1. Systems and Network Management (S&NM).

6.1.1.1. The S&NM mission area includes the range of computing hosts and applications connected by transmission systems, both wired and wireless, that carry voice, data, sensor, and video throughout the AFEN. It includes switched networks, IP-based data networks, video teleconferencing (VTC) networks, satellite communications networks, and wireless networks. S&NM comprises the functions of Fault, Configuration, Accounting, Performance, and Security (FCAPS) management.

6.1.1.2. This mission area is focused on Assured Resource (System and Network) Availability and on Assured Information Delivery. The objectives of this focus are achieved by configuring and allocating AFEN system and network resources; ensuring effective and efficient processing, connectivity, routing, and information flow; accounting for resource usage; and maintaining robust AFEN capabilities in the face of component or system failure and/or adversarial attack.

6.1.2. Information Dissemination Management (IDM).

6.1.2.1. The IDM mission area provides the right information to the right person in the right format at the right place and time in accordance with commander's information dissemination policies while optimizing the use of information infrastructure resources. IDM, a subset of information management, provides services that address awareness, access, and delivery of information. It involves the operations of compilation, cataloguing, caching, distribution, and retrieval of data; manages the information flow to users, and enables the execution of the commander's information policy. IDM relies on information awareness, information access, delivery management, and dissemination support.

6.1.2.2. This mission area is focused on Assured Information Protection and Assured Information Delivery. The objectives of this focus are achieved through the efficient movement of information into, within, and out of the AFEN; securely storing information; rapidly compiling and cataloging new collections of information and making such information readily available to prospective users through the most efficient and effective modes of information delivery and retrieval—tailored to the needs of the warfighter with access commensurate to information security requirements.

6.1.3. Information Assurance/Computer Network Defense (IA/CND).

6.1.3.1. The IA/CND mission area helps ensure the availability, integrity, identification, authentication, confidentiality, and nonrepudiation of friendly information and information systems while denying the adversaries access to the same information/information systems. It also provides end-to-end protection to ensure data quality and protection against unauthorized access and inadvertent damage or modification.

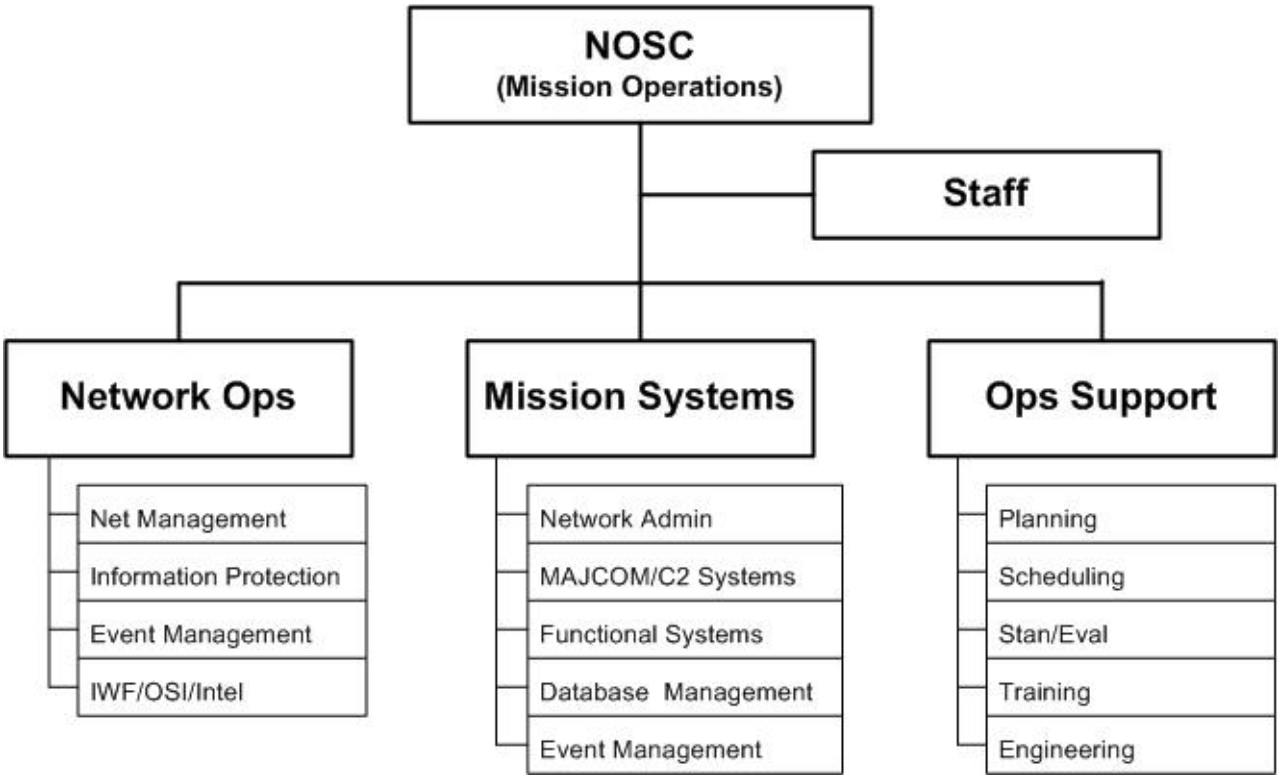
6.1.3.2. This mission area is focused on Assured Resource (Systems and Networks) Availability and on Assured Information Protection. The objectives of this focus are achieved by instituting agile capabilities to resist adversarial attacks, through recognition of such attacks as they are initiated or are progressing, through efficient and effective response actions to counter the attack and safely and securely recover from such attacks; and by reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed.

6.2. NOSC Organization.

6.2.1. NOSC Operations. NOSC Operations are listed here to provide a standard set of operations that the NOSC provides. NOSC Operations are critical to ensuring continuity across the Air Force and to effectively manage the AFEN. **Figure 6.1.** depicts the NOSC operations within their respective Computer Systems Squadron (CSS) or Communications Squadron (CS). It is also possible that these functions may be split across more than one flight within the organization. The Mission Ops area represents the core crew while the Network Ops, Mission Systems, and Ops Support areas represent the supporting functions to the NOSC.

NOTE: **Figure 6.1. This figure does not depict organizational structure, however, it does capture the functions performed within the organization supporting the NOSC.**

Figure 6.1. NOSC Operations.



6.2.1.1. Mission Operations. The Mission Operations element is the core of the NOSC. They are responsible for C2 and maintaining Operational Control (OPCON) over the MAJCOM network. They monitor and report on events affecting their MAJCOM network. They direct changes to the network in order to ensure a sound network defensive posture and efficient movement of data.

6.2.1.2. Network Operations. The Network Operations element consists of the Network Management and Information Protection Operations areas. Together these two areas work hand in hand to operate, defend and respond to events that affect the MAJCOM network. Additionally, within this element are individuals from the Office of Special Investigation, Intelligence, and Information Warfare Flights.

6.2.1.3. Mission Systems. The Mission Systems element consists of the Network Administration (NA) area. This element provides operating system, application, and messaging administration. They are also responsible for server consolidation efforts and maintaining C2, functional, and MAJCOM unique systems. They manage and respond to events with respect to their areas of responsibility.

6.2.1.4. Operations Support. The Operations Support element provides support to the NOSC in the areas of training, standardization/evaluation, engineering (system integration), planning, scheduling and policy.

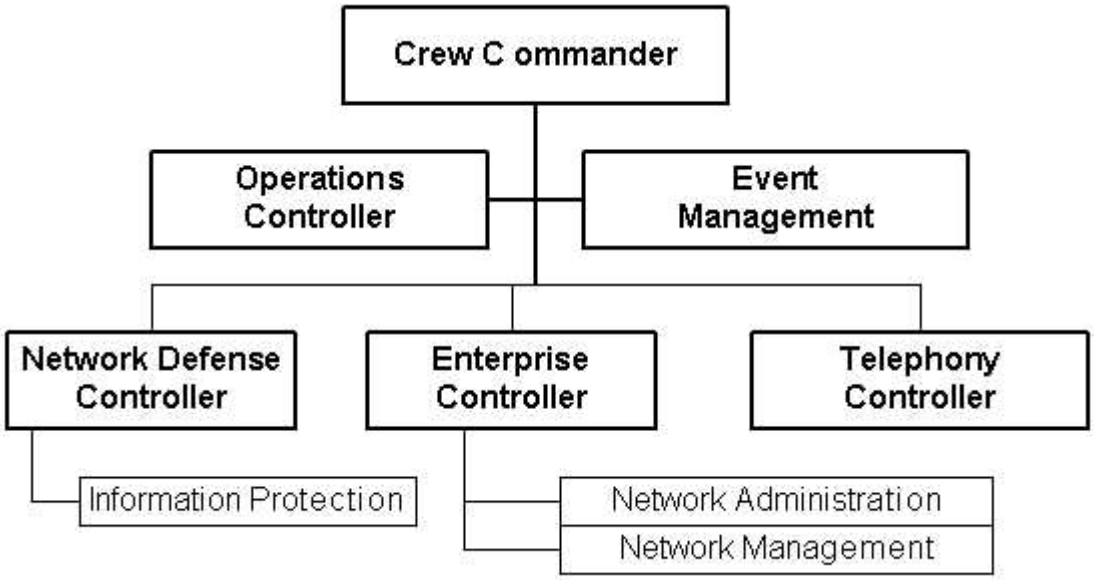
6.3. Crew Positions.

6.3.1. Overview. Crew members coordinate with personnel at their tier or other tiers as necessary in order to provide Core Services to their customers and ensure the availability and security of the AFEN. **Attachment 3** identifies the basic crew positions located at each tier of the network hierarchy. MAJCOMs may augment positions to perform specific functions, as required. Crew members will use standardized tools and software approved for Air Force-wide use in the Infostructure Technology Reference Model (i-TRM). Legacy software tools may also be used, but organizations need to plan how they are going to migrate to the standardized tools.

6.3.2. The original crew position construct was very NCC focused with only four crew positions existing at the MAJCOM level. The CSAF mandate for server consolidation and centralized management at the NOSC now requires NCC crew positions to be replicated at the MAJCOM level.

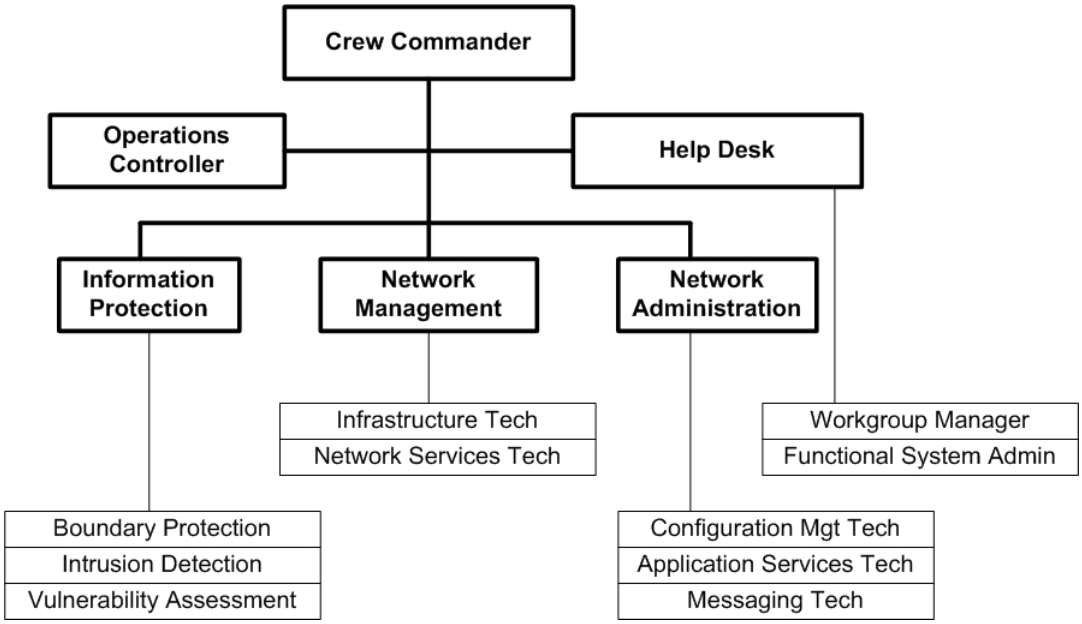
6.3.3. **Figure 6.2.** depicts the crew force relationships within a NOSC. The Crew Commander, Operations Controller, Enterprise Controller, Network Defense Controller, and Voice Controller positions are the foundation of the NOSC. These crew positions monitor and report on events affecting their MAJCOM network. Additionally, certain crew positions (Network Defense Controller and Enterprise Controller) direct the actions of those crew positions subordinate to them. The NOSC is responsible for maintaining operational awareness of the entire MAJCOM network and conducting situational reporting, coordinating event response and network change implementation as necessary.

Figure 6.2. NOSC Crew Position Structure.



6.3.4. The crew positions within an NCC (see **Figure 6.3.**) are set up similarly to that of the NOSC. Over time, as the NOSC assumes management of NCC resources, the number of personnel required to fill a crew position at the NCC may decrease, but the position will still remain. For example, the difference between an Infrastructure Technician within the NM area of the NOSC, versus NCC, lies in the scope of their responsibilities. The Infrastructure Technician at the NOSC may be responsible for the base's external router and switches, whereas the NCC Infrastructure Technician would be responsible for the vast number of routers and switches within the base network.

Figure 6.3. NCC Crew Position Structure.



6.3.5. Crew Position Descriptions. For a complete listing and description of crew positions, please refer to **Attachment 3** .

6.3.6. Training and Certification. Crew members will be certified by position according to AFI 33-115, Volume 2 and Air Force Job Qualification Standards (AFJQS). These establish an Air Force-wide baseline of mandated and enforceable training for network professionals. All individuals filling an Air Force Network Crew Position Role are required to be certified in that position. This is not to be confused with commercial certification (CCNA, MSCE, etc.). Individuals become Air Force certified by following the procedures set forth in AFI 33-115, Volume 2.

6.4. Core Services.

6.4.1. Overview. As stated above, Mission Areas are the overarching activities performed by network professionals. NOSC operations are performed by a highly trained and certified crew force consisting of standard crew positions. Core Services then, are the product, or end result, that is provided by our network professionals to the Air Force community. In addition to core services, NCCs/NOSCs provide desktop and functional services.

6.4.2. Core Services support the Air Force IT services and embody the seamless, secure, and reliable transport of timely and trusted information across the AFEN and the secure, reliable, standards-based, architecturally sound e-mail, file, print, and web services, centrally managed by our AFNOSC/NOSC/NCC Network Professionals. It includes the delivery of organizational and individual e-mail to the desktop, shared file/data storage, a capability to print from the standard desktop to network printers, and centrally managed web services and storage. It includes a single domain for the standard desktop environment, DNS, IP address space management, directory services such as Active Directory, a consolidated Help Desk, appropriate firewalls, Internet Proxy (cache) servers, switched and routed (including wireless) networks, and the metrics and reporting in place to monitor and manage an acceptable level of service.

6.4.3. Desktop services include the common, secure, reliable desktop environment, architecturally compliant and remotely managed by the NOSC/NCC Network Professionals, ensuring data accessibility anywhere within the AFEN. This includes the common desktop environment with standard operating system and office automation software, global access/address book, positive configuration control maintained by the NOSC/NCC, and metrics in place to monitor and manage the service level.

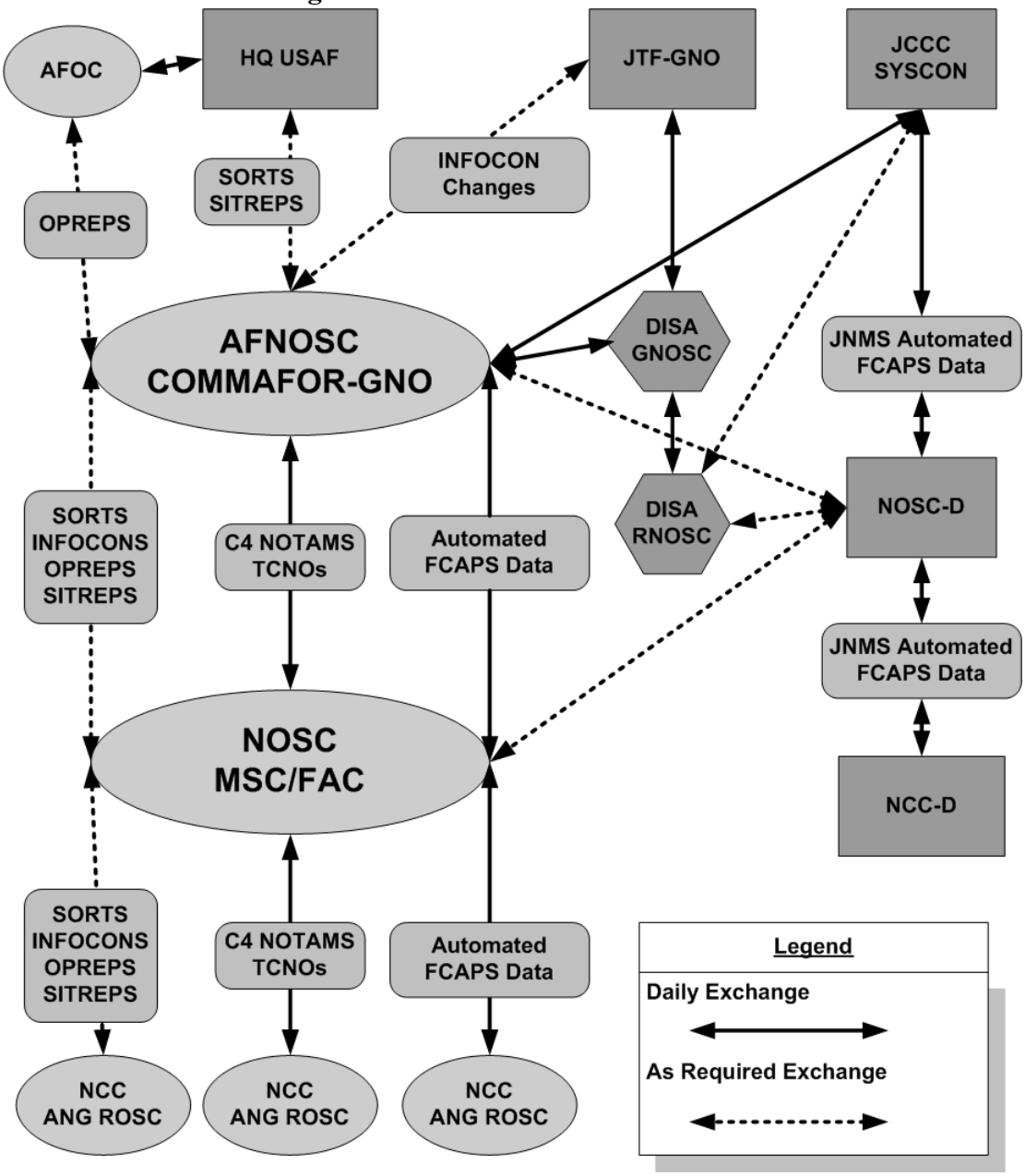
6.4.4. Functional services incorporates hosting functional applications on a reliable, secure platform of AFEN servers centrally managed by NOSC/NCC Network Professionals, enabling the functional workforce(s) to focus on their core competencies. Functional applications will be supported by the functional community in accordance with the SLA, MOA, or MOU between the functional organization and the NOSC/NCC. See **Attachment 2** for policy guidance on SLA.

Chapter 7

INFORMATION EXCHANGES, RELATIONSHIPS, AND REPORTING

7.1. General. Air Force network operations organizations exchange information internally, between each other, and with external agencies. Information is exchanged to facilitate the maintenance and operation of the AFEN, to provide situational awareness, to facilitate integrated Defensive Counter-Information, and to provide commanders with a common operating picture. The picture is developed from information obtained while conducting NETOPS. Generally, the root source of this information comes from "raw" FCAPS data. FCAPS data is monitored, collected, analyzed, processed and reported by the AFNOSC, NOSC, and NCC using software tools that provide a complete view of the AFEN. The primary organizations exchanging information are depicted in **Figure 7.1.**

Figure 7.1. Information Exchanges.



7.2. Network Status and Management Reports. Network status and management actions will be reported via scheduled and unscheduled reports. Unscheduled reports focus on the immediate status of the network and are generally tied to events or incidents. Scheduled reports are associated with information exchange and long-term metric analysis.

7.2.1. Reports and Notifications.

7.2.1.1. Information may be exchanged by network operations organizations internally, between each other, and with external agencies using several types of orders, reports, and/or notices. OPREP3, SITREP, TCNO, and C4 NOTAM are some examples of these (***NOTE***: AFNOSC/NOSC/NCCs may pass informational copies of OPREP3s or SITREPs, but the issuing authority

for OPREP3s and SITREPs is the Wing Command Post). Manually reported information completes the data collection function and provides the critical human element in the network equation. The human element and the need for timely, accurate information are essential. NM software could potentially automate some manual exchanges, as long as network professionals still maintain positive control over the AFEN.

7.2.1.2. Operational Event/Incident Reports (OPREP3). OPREP3s are reported using operational channels, e.g., Command Posts, to notify commanders immediately of any event or incident that may attract international, national, US Air Force, or significant news media interest. They provide immediate up-channel notification of local network intrusions and probes, INFOCON level changes, and network degradations. They are generally tied to events. An NCC may notify the wing Command Post of the need to send an OPREP3, and draft the verbiage, but NCCs do not issue OPREP3s. They only forward the draft to the command post and advise it be sent. For detailed OPREP3 reporting instructions see AFI 10-206.

7.2.1.3. Situation Report (SITREP). SITREPs are submitted through Command and Control channels and are used to report significant outages. This is a narrative report that keeps addressees informed, and enables higher levels of command to prepare for potential effects of ongoing situations. They are submitted at daily, weekly, or monthly intervals, or as directed. Like OPREP3s, an NCC may notify the wing Command Post of the need to send a SITREP, and draft the verbiage, but NCCs do not issue SITREPs. They only forward the draft to the Wing Command Post and advise it be sent. For detailed SITREP reporting instructions see AFI 10-206.

7.2.1.4. Information Operations Condition (INFOCON). INFOCONs are used to define a defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system is a DoD methodology providing a structured approach to react and defend against adversarial attacks on DoD computers and telecommunications systems. This is accomplished by directing actions to establish a heightened or reduced defensive IA posture based on assessed threats or hostilities. INFOCON levels are: NORMAL (normal activity), ALPHA (increased risk of attack), BRAVO (specific risk of attack), CHARLIE (limited attack), and DELTA (general attack). AFI 10-2002 will contain specific instructions on INFOCONs when published.

7.2.1.4.1. DoD-wide INFOCONs are declared by the Commander, United States Strategic Command (USSTRATCOM), and disseminated by the JTF-GNO to the COMAFFOR-CNO via DMS or voice message. The Air Force-wide INFOCON normally mirrors the DoD-wide INFOCON, but may exceed it if conditions warrant. The Air Force Chief of Staff has delegated the authority to set Air Force-wide INFOCONs to the COMAFFOR-CNO.

7.2.1.4.2. Official notification for INFOCON changes come through operational reporting channels in the form of INFOCON Change Alert Messages (ICAM) or OPREP3s. The NOSCs use TCNOs to implement actions to attain INFOCON protection measures. INFOCON level attainment is officially reported by NCCs using SITREPs through command post channels; it is also reported in response to the NOSCs via C4 NOTAM or TCNO compliance. The SITREP is the official operational report, not the TCNO or C4 NOTAM.

7.2.1.4.3. MAJCOM NOSCs will ensure subordinate bases comply with directed INFOCON actions via TCNO and track compliance. AFNOSC will compile an Air Force-wide report and forward it to the COMAFFOR-CNO as appropriate. Subordinate Air Force units (i.e., MAJ-

COM, NAF, wing, or base level) may declare a higher INFOCON if local conditions warrant. Up-channel reporting of all local or MAJCOM INFOCON changes according to AFI 10-2002 when available.

7.2.1.5. Time Compliance Network Order (TCNO). TCNOs are downward-directed operations, security, or configuration management-related orders issued by the AFNOSC or MAJCOM NOSCs. The TCNO provides a standardized mechanism to issue one "order" amongst AFNOSC/NOSC/NCCs, telling them how to run and make changes to the AFEN. TCNOs do not replace INFOCONs, OPREP3s, SITREPs, or Time Compliance Technical Orders (TCTO). In some cases this may mean dual reporting is required.

7.2.1.5.1. TCNOs may be generated internally to direct the implementation of an operational or a security vulnerability risk mitigation procedure or fix action (i.e., software patch), or issued in response to DISA-generated Information Assurance Vulnerability Assessments (IAVA). TCNOs are used to address Air Force or MAJCOM wide incidents/problems, and not for isolated internal incidents unless impact is determined to be system-wide.

7.2.1.5.2. See AFSSI 5021 (will become AFI 33-138) for TCNO reporting and compliance details and formats.

7.2.1.6. Command, Control, Communications, and Computers Notice to Airmen (C4 NOTAM). C4 NOTAMs are informative in nature and are not used to direct actions. They are used by all organizations within the NETOPS hierarchy. They are the primary means for disseminating network information that does not require specific actions to be taken, or compliance to be tracked. However, in some cases, acknowledging receipt of a C4 NOTAM may be required. There are four types of C4 NOTAMs. They are: Informative, Scheduled Event, Unscheduled Event, and Summary. For descriptions of each type of C4 NOTAM and procedures on use refer to AFSSI 5021 (will become AFI 33-138).

7.2.2. Helpdesk, Trouble Resolution and Reporting.

7.2.2.1. The Help Desk is an operation that provides technical information to customers and solves technical problems by providing support and information. The Help Desk should provide an efficient and effective means to answer customers' questions and solve their problems. At the heart of a Help Desk operation is a sophisticated database that contains all the information necessary to handle events. The Help Desk is the Workgroup Manager providing end-user support, a NCC or NOSC working to resolve a network outage, or the AFNOSC providing senior leadership with situational awareness of the AFEN. The Help Desk is actually a global repository of information about customers, vendors, hardware, software, locations, networks, service level agreements, problems and solutions. The database also identifies the interrelationships among these items.

7.2.2.2. The Help Desk will provide network assistance and trouble resolution and will be based on a fully integrated trouble ticketing system. The trouble ticketing system should be able to automatically assign priorities and set response times and escalation timelines based on the criticality of the system being reported on. The trouble ticketing system will be able to share and communicate fix actions across all three network tiers. The Help Desk system should also be integrated with an Automated Call Distribution (ACD) system wherever possible.

7.2.2.3. The Help Desk consists of three different levels. Each of these levels exist at each tier of the Network Operations Hierarchy outlined in **Chapter 2** . These Help Desk levels are:

7.2.2.3.1. Level 1. Level 1 support should have end-to-end responsibility for each customer request. The help desk technician should be empowered to resolve as many requests as possible. Level 1 provides a single point of contact to the customers for servicing a request.

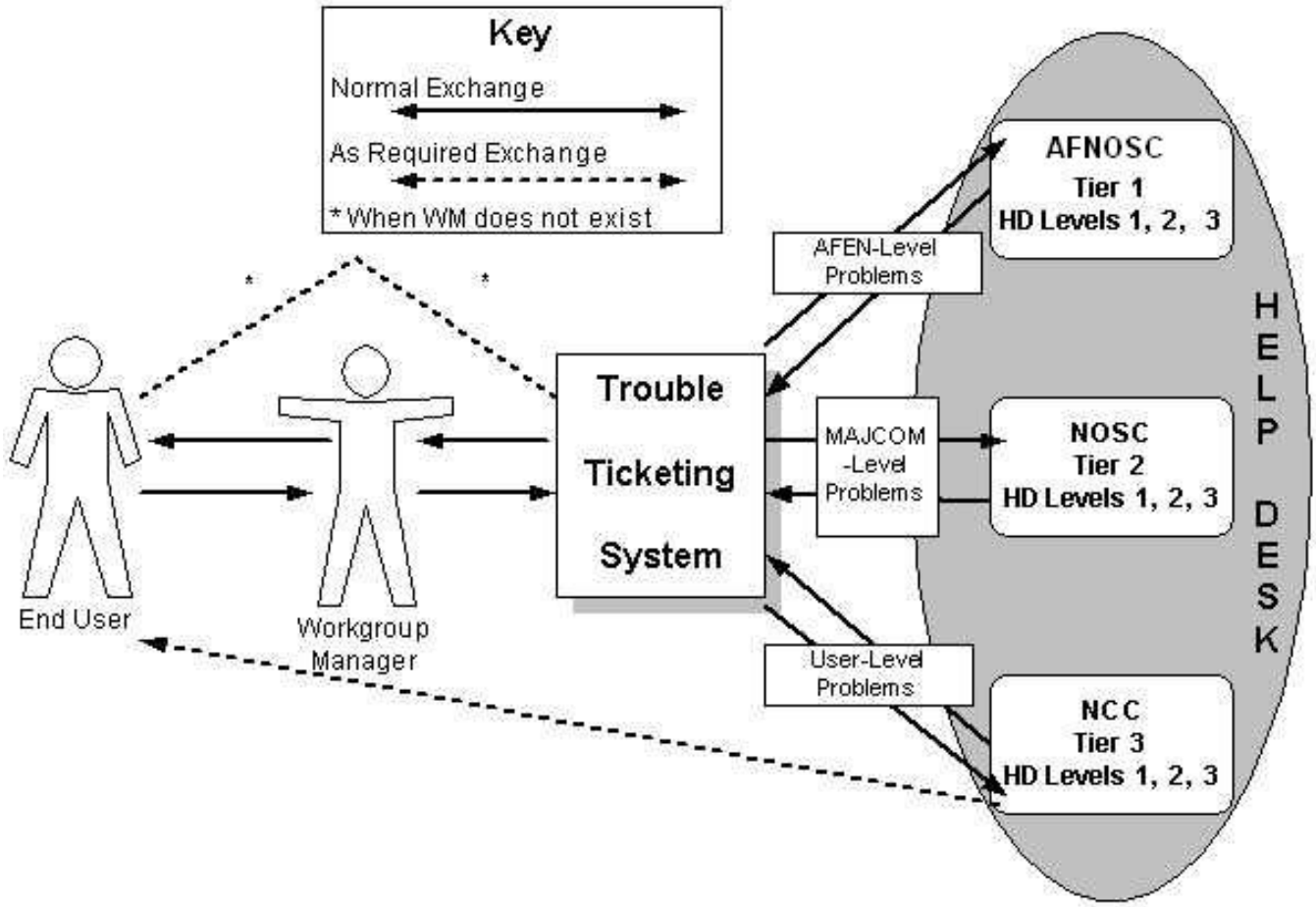
7.2.2.3.2. Level 2. Level 2 client support provides advanced technical expertise to level 1. Their responsibility is to analyze the requests routed to them and resolve the problems. Resources at this level are typically those individuals working in the functional areas outlined in **Attachment 3** .

7.2.2.3.3. Level 3. Level 3 support is composed of highly specialized technical experts. Calls which cannot be solved at levels 1 and 2 are routed to this level. Resources at this level are typically composed of engineers, system integrators and/or third-party providers/vendors.

7.2.2.3.4. In the absence of a fully automated system, ensure a system is implemented to manually link trouble tickets. An example of how this could be accomplished would be by recording the appropriate ticket number of the organization that has assumed responsibility for the service interruption at each level as the ticket is escalated.

7.2.2.4. Base-level users experiencing problems with network Core Services (see **Chapter 6**) or systems (including common office applications) will first contact their WM. If the local WM is unable to fix the trouble, the WM will enter a trouble ticket into the Help Desk system or contact the Help Desk by phone for ticket submission. WMs and users will be able to automatically track and view the status of troubles submitted by them. Help Desk personnel will resolve problems by identifying fix actions to the WM or customer by web interface, e-mail, phone, or by attempting a remote fix action. If local physical access or replacement of equipment is required, the Help Desk will dispatch appropriate base-level personnel. Trouble resolution for many network Core Services or systems will be orchestrated by the regional NOSC Help Desk. The AFNOSC Help Desk will handle all trouble tickets related to or affecting Air Force-level systems. The trouble resolution process and information exchanges are shown below in **Figure 7.2.**

Figure 7.2. Trouble Ticket Reporting and Tracking.



Chapter 8

AIR FORCE TECHNICAL ORDERS

8.1. General.

8.1.1. The purpose of the Air Force Technical Order (TO) system is to provide concise but clear instructions for safe and effective operation and maintenance of centrally-acquired and managed Air Force military systems. All Air Force personnel are responsible for controlling and using TOs as organizational property in conjunction with official duties. Compliance with Air Force TOs is mandatory.

8.1.2. Technical publications are essential for network support to function properly and to provide the operations activity with accurate information. Technical publications include TOs, commercial manuals, and specialized publications. Set up and maintain these publications according to AFPD 21-3, *Technical Orders*, and 00-5 series technical orders.

8.2. Maintaining Air Force TOs.

8.2.1. Publications Manager.

8.2.1.1. AFNOSC, MAJCOM NOSCs, Base NCCs and any other organization utilizing CITS equipment will appoint a primary and alternate publications manager. This function could be consolidated with Maintenance Support Flight if available as identified in AFI 21-116, *Maintenance Management of Communications-Electronics.*

8.2.1.2. The Publications Manager will be responsible for:

8.2.1.2.1. Establishing an independent TO account with the base Technical Order Distributing Office (TODO). Ensure that the account is on requirement for both the TO and any additional TCTO.

8.2.1.2.2. Maintaining those TOs required for support of all CITS equipment. Maintain additional T.O.s required for training and deploying.

8.2.1.2.3. Ensuring TOs are adequate, accurate and readily available to Network Professionals (TO 00-5-2). Maintaining sufficient requirement to support operational load. TOs should not be removed from the primary work locations simply to accommodate the staff.

8.2.1.2.4. Identifying any errors, contradictions, or procedures requiring clarification, by following specific procedures in TO 00-5-1, *AF Technical Order System*. See TO 00-5-1 for specific guidance on preparing AFTO Form 22, **Technical Manual (TM) Change Recommendation and Reply**.

8.2.1.2.5. Ensuring TCTOs are managed and issued in accordance with procedures in TO 00-5-15, *Air Force Time Compliance Technical Order Process*. TCTOs are military orders issued by order of the Secretary of the Air Force and as such, shall be complied with as specified in the TCTO.

8.2.1.2.6. Utilizing AFMQCC 200-6 (current version) Technical Order Control Check Sheet and other applicable guidance to aid units in maintaining technical order programs.

Chapter 9

SERVICE LEVEL AGREEMENTS (SLA)

9.1. Service Level Agreements (SLA). The NCC or NOSC will establish SLAs with customers whose network support requirements exceed the core services defined in paragraph **6.4.** or the Air Force IT service defined by the AF-CIO. SLAs define division of responsibilities for network operations and services to minimize duplication of effort between organizations. SLAs define resources each party will provide to support delivery of negotiated services. SLAs are just one method of accomplishing the intent of this paragraph. Additionally, a MOA or MOU may be used as long as they capture the intent of this paragraph. The management process for implementing SLAs and a sample SLA are in **Attachment 2** .

9.2. Information Collections, Records, and Forms or Information Management Tools (IMT).

9.2.1. Information Collections. No information collections are created by this publication.

9.2.2. Records. Records pertaining to operational capability reporting are created by this publication (paragraph **4.5.3.**). Retain and dispose of these records according to Air Force WEB-RIMS RDS , Table 11-4 (will become Table 10-16), located at **https://webrims.amc.af.mil/rds/index.cfm**.

9.2.3. Forms or IMTs (Adopted and Prescribed).

9.2.3.1. Adopted Forms or IMTs. DD Form 250, **Material Inspection and Receiving Report**; DD Form 1368, **Modified Use of Leased Communication Facilities;** AF Form 723, **SORTS DOC Statement**; AF Form 847, **Recommendation for Change of Publications**; AF Form 1261, **Communications and Information Systems Acceptance Certificate; and** AFTO Form 22, **Technical Manual (TM) Change Recommendation and Reply.**

9.2.3.2. Prescribed Forms or IMTs. No forms or IMTs are prescribed by this publication.

DONALD J. WETEKAM, Lt Gen, USAF
DCS/Installations and Logistics

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Paperwork Reduction Act of 1995

Privacy Act of 1974

DISAC 300-175-9, *DCS Operating Maintenance Electrical Performance Standards*

AFPD 21-3, *Technical Orders*

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

AFI 10-206, *Operational Reporting*

AFI 10-2002 , *Information Operations Conditions* (Draft—to be published)

AFI 21-116, *Maintenance Management of Communications-Electronics*

AFI 33-114, *Software Management*

AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-129, *Transmission of Information Via the Internet* (will become Web Management and Internet Use)

AFI 33-202, *Network and Computer Security*

AFI 33-207, *Computer Security Assistance Program*

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

AFMAN 33-223, *Identification and Authentication*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

AFI 36-2201, Volume 3, *Air Force Training Program, On The Job Training Administration*

AFCAT 36-2223, *USAF Formal Schools*

AFMAN 37-123, *Management of Records*

AFI 63-127, *Command, Control, Communications, Computers, and Intelligence Support Planning (C4ISP)* (Draft--to be published)

AFSSI 5021, *Time Compliance Network order and Vulnerability and Incident Reporting* (will become AFI 33-138, *Enterprise Network Operations Notification and Tracking)*

TO 00-5-1, *Air Force Technical Order System*

TO 00-5-15, *Air Force Time Compliance Technical Order Process*

Air Force Network Operation (NETOPS) CONOPS

Joint Network Operations CONOPS (ver 2.40)

Abbreviations and Acronyms

ADPE—Automatic Data Processing Equipment

AEF—Air Expeditionary Forces

AETC—Air Education and Training Command

AF—Air Force (Forms Only)

AFC2ISRC—Air Force Command and Control & Intelligence, Surveillance, and Reconnaissance Center

AFCA—Air Force Communications Agency

AF-CIO—Air Force Chief Information Officer

AFEN—Air Force Enterprise Network

AFFOR—Air Force Forces

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFJQS—Air Force Job Qualification Standard

AFMAN—Air Force Manual

AFMC—Air Force Materiel Command

AFMS—Air Force Manpower Standard

AFNOSC—Air Force Network Operations and Security Center

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFSN—Air Force Systems Network

AFSSI—Air Force Systems Security Instruction

ANG—Air National Guard

AOR—Area of Responsibility

ASIM—Automated Security Incident Measurement

ATCALS—Air Traffic Control and Landing Systems

C2—Command and Control

C4—Command, Control, Communications, and Computer

C4ISP—Command, Control, Communications, Computers and Intelligence Support Plan

C4ISR—Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

C&A—Certification and Accreditation

CITS—Combat Information Transport System

CNA—Computer Network Attack

CND—Computer Network Defense

CNO—Computer Network Operations

COMAFFOR—Commander, Air Force Forces

COMAFFOR-CNO—Commander, Air Force Forces-Computer Network Operations

CoN—Certificate of Networthiness

CONOPS—Concept of Operations

CS—Communications Squadron

CSAF—Chief of Staff of the Air Force

CSS—Computer Systems Squadron

CtO—Certificate to Operate

DAA—Designated Approving Authority

DCI—Defensive Counter-Information

DCS—Defense Communications System

DCS—Deputy Chief of Staff (Signature Block Only)

DECC—Defense Enterprise Computer Center

DHCP—Dynamic Host Configuration Protocol

DII—Defense Information Infrastructure

DIICC—Defense Information Infrastructure Control Concept

DIRLAUTH—Direct Liaison Authority

DISA—Defense Information Systems Agency

DITCO—Defense Information Technology Contracting Office

DMS—Defense Message System

DNS—Domain Name Service

DOC—Designed Operational Capability

DoD—Department of Defense

DRU—Direct Reporting Unit

DSN—Defense Switched Network

EC—Equipment Custodian

FAC—Functional Awareness Cell

FOA—Field Operating Agency

FCAPS—Fault, Configuration, Accounting, Performance, and Security

FSA—Functional System Administrator

GAL—Global Address List

GCCS—Global Command and Control System

GIG—Global Information Grid

GNO—Global Network Operations

GPS—Global Positioning System

IA—Information Assurance

IAVA—Information Assurance Vulnerability Alerts

IDM—Information Dissemination Management

INFOCON—Information Operations Condition

IP—Internet Protocol

IPO—Information Protection Operations

i-TRM—Infostructure Technology Reference Model

JCCC—Joint Communications Control Center

JNMS—Joint Network Management System

JTF—Joint Task Force

LAN—Local Area Network

LRU—Line Replaceable Unit

MAJCOM—Major Command

MAN—Metropolitan Area Network

MECL—Minimum Essential Circuit Listing

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

MSC—Mission Support Center

NA—Network Administration

NAF—Numbered Air Force

NCC—Network Control Center

NETCOP—Network Common Operating Picture

NETOPS—Network Operations

NIPRNET—Non-secure Internet Protocol Router Network

NM—Network Management

NO/IA—Network Operations and Information Assurance

NOSC—Network Operations and Security Center

NOSC-D—Network Operations and Security Center Deployed

NOTAM—Notice to Airmen

NTP—Network Time Protocol

OPCON—Operational Control

OPREP3—Operational Event/Incident Reports

OPTN—Operationalizing and Professionalizing the Network

ORM—Operational Risk Management

PMI—Preventive Maintenance Inspection

POM—Program Objective Memorandum

PSCF—Primary Systems Control Facility

QC—Quality Control

RDS—Records Disposition Schedule

ROSC—Regional Operations and Security Center

S&NM—Systems and Network Management

SDP—Service Delivery Point

SECAF—Secretary of the Air Force

SIPRNET—Secret Internet Protocol Router Network

SITREP—Situation Report

SMTP—Simple Mail Transfer Protocol

SLA—Service Level Agreement

SORTS—Status of Readiness and Training System

SYSCON—Systems Control

TAC—Tactical Internet Protocol

TACON—Tactical Control

TCNO—Time Compliance Network Order

TCTO—Time Compliance Technical Order

TO—Technical Order

TODO—Technical Order Distributing Office

TTP—Tactics, Techniques, and Procedures

VPN—Virtual Private Network

VPS—Voice Protection System

WAN—Wide Area Network

WLAN—Wireless Local Area network

WM—Workgroup Manager

Attachment 2

SERVICE LEVEL AGREEMENT

A2.1. Sample. The following is a sample of a SLA format between the service provider and the customer. The sample agreement shows only minimum topics that should be addressed; however, ensure the SLA covers NCC Core Services (see **Chapter 6**).

1. Introduction. Parties (organizations) involved:

a. Service provider: (i.e., DAA or NCC).

(1) POC names.

(2) Location or office symbol.

(3) Telephone numbers.

b. End-user organization.

(1) POC names.

(2) Location or office symbols.

(3) Telephone numbers

2. Purpose. The purpose of this SLA is to state the relationship between the service provider and the end-user organization. It specifies the services and commitments of the NCC as well as the expectations and obligations of the end-user organization.

3. Responsibilities of Service Provider (Name of the Organization). The service provider agrees that it will:

a. Specify what resources it will use.

b. Describe how they will inform the customer of infrastructure changes and new or changed service.

c. State security methods that they will use to protect infrastructure resources from unauthorized access, monitoring, or tampering.

d. Describe process used to notify and coordinate with end-user organization about planned outages of connectivity, equipment, or electricity.

e. Explain the coordination process for service degradation or failure correction and state how customer will be kept informed of status.

f. Describe materials that will be provided to customer to minimize procedural errors.

g. Explain customer support performance criteria and workload limitations (e.g., hours of operation, response times, and expected maximum calls).

h. Describe what performance data and analysis reports they will provide to the customer organization to show service quality and level of customer support provided.

i. State what customer training is available and what role the service provider's will play in customer training.

j. Perform periodic surveys to monitor customer satisfaction.

k. State the security measures they will use to protect infrastructure resources from unauthorized access, monitoring, or tampering.

l. Describe the process used to notify end-users of planned outages of connectivity, equipment, or electricity.

4. Responsibilities of End-User Organization.

a. The end-user organization agrees that it will:

(1) Describe the process used to ensure end-users know procedures for getting help.

(2) Coordinate with service provider on any major configuration changes (e.g., network installation/expansion, TCP/IP port requirements, changes in topology, system upgrades, relocation, etc.).

(3) WMs and SAs will provide, upon request, equipment layout, network schematic, network connectivity (attached via backbone or stand alone), and their exact location.

(4) Describe how they will use the performance and trend analysis data from service provider and provide feedback to improve service.

(5) Develop end-user contingency operations plans and capabilities.

(6) Identify what resources they will matrix or transfer to the service provider.

(7) Provide service provider with access to equipment both electronically and physically as needed.

(8) Agree to perform the certification effort and comply with wing or NCC security policy.

b. During a trouble call, the end users will:

(1) Contact organization's WM first, if available.

(2) Describe what minimum information they will provide (e.g., name, organization, location, telephone number, equipment number, user-id, e-mail address).

(3) Provide service provider with a description of problem, its priority, and potential mission impact.

(4) Work with the service provider during fault isolation process, as needed.

(5) Negotiate for increased workload/expansion for contingencies or new support.

5. Customer Escalation Procedures. The two parties agree to the following procedures in case they need to escalate resolution of the problem (i.e., when the customer is not satisfied with the service provided).

a. Escalation Levels, To Whom, and Phone Numbers.

(1) 1st

(2) 2nd

(3) 3rd

6. Conclusion.

a. Parties agree that the terms of this agreement will remain in effect for (5 years, 6 months, etc.) are subject to review (annually, semiannually, etc.).

b. The parties agree to the following mechanism for initiating an out-of-cycle SLA review:

c. Service levels and procedures established herein were agreed to by parties represented by the undersigned.

_____ _____

(Service Provider Representative Signature) (End-User Organization Signature)

Attachments (add as needed):

1. Hours of Operation.
2. Definitions of Terminology.
3. Lists of Support Equipment and Software.
4. Summaries of Applicable Contracts.
5. Contingency Plan.

Attachment 3

CREW POSITIONS

A3.1. General. This attachment identifies the crew positions located at each network operations level. Table A2.1 illustrates the relationship between tiered-level crew positions and specific NETOPS Mission Areas. Crew Positions are grouped into three functional areas. These areas are Information Protection Operations (IPO), Network Management (NM), and Network Administration (NA).

A3.2. Functional Area Descriptions.

A3.2.1. Network Administration (NA) Positions. This functional area is responsible for central management of server hardware, operating systems and applications. Responsibilities include some of the core services (as outlined in **Chapter 6**) provided by the NOSC/NCC to the base or MAJCOM populace. The individuals assigned to this functional area are the base experts in system administration and also provide technical assistance to FSAs and WMs who provide administration support from their servers to their end-user workstations. NA positions are divided into three positions: Configuration Management Technician, Application Services Technician, and Messaging Technician.

A3.2.2. Network Management (NM) Positions. This functional area provides proactive and reactive management of resources by monitoring and controlling the network infrastructure, available bandwidth, hardware, and distributed software resources. Responsibilities include some of the core services (as outlined in **Chapter 6**) provided by the NOSC/NCC to the base or MAJCOM populace. NM responds to detected security incidents, network faults (errors) and user reported outages. NM is further divided into two positions: Infrastructure Technician and Network Services Technician.

A3.2.3. Information Protection Operations (IPO) Positions. This functional area 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 (IS) and network security intrusions. This area conducts IPO employing hardware and software tools to enhance the security of their networks. The personnel in this area install, monitor, and direct proactive and reactive network information protection defensive measures to ensure the availability, integrity, and reliability of base networked and stand-alone information resources. Information Protection Operations are divided into three crew positions: Boundary Protection Specialist, Intrusion Detection Specialist, and Vulnerability Assessment Specialist.

A3.3. Unit Level Positions.

A3.3.1. Workgroup Manager (WM). Workgroup Managers support a functional community (e.g., work centers, flights, squadrons, or organizations) and serve as the first line of help to resolve customers' administrative and technical problems. WMs are usually not assigned to the NCC, though are logically an extension of the Help Desk team. WMs take direction from the NCC and FSA. NCC direction takes precedence over FSA direction. Workgroup managers install, configure, and operate client/server devices. The WM will be a 3A0X1 unless none are assigned. Information managers receive 3-, 5- and 7-skill level training on workgroup management. When a 3A0X1 is not assigned, any AFSC or occupational series can perform WM duties once trained and certified.

A3.3.2. Functional Systems Administrator (FSA). FSAs ensure functional communities of interest systems, servers, workstations, peripherals, communications devices, and software are on-line and

supported. They must thoroughly understand the customer's mission and be completely knowledgeable of hardware and software capabilities and limitations supporting that functional system. Their area of responsibility is from the user's terminal to the server, but does not include the network backbone infrastructure. Functional system administrators are not normally assigned to the NCC, but are a logical extension of NCC functionality. Functional system administrators are trained and certified according to the appropriate network crew position that best meets their position requirements.

A3.4. NCC and NOSC Crew Positions.

A3.4.1. Configuration Management Technician. Installs and configures the network operating system for all servers to Air Force specifications. Establishes print services and maintains standardized file storage directory structures. Creates user accounts in accordance with Air Force standard naming conventions and provides file, print, and messaging access. Maintains directory services supporting the Air Force Directory, performs preventive maintenance and ensures data recovery capability through proper data backup scheduling and execution.

A3.4.2. Application Services Technician. Installs, configures, operates, and maintains network-launched user applications and the trouble ticketing system and its database.

A3.4.3. Messaging Technician. Installs, configures, operates, and maintains network messaging applications. Maintains accuracy of the Global Address List (GAL) as well as local address lists supporting the Air Force Directory and Air Force White Pages.

A3.4.4. Network Services Technician. Maintains the NM systems to include back up of these systems. They are responsible for collecting and archiving the data necessary to conduct detailed infrastructure mapping and analysis, producing time-sensitive displays and threshold alerts, and developing course of action scenarios. Controls all base IP address space through use of Dynamic Host Configuration Protocol (DHCP), or static configuration. Maintains DNS servers for internal and external name resolution.

A3.4.5. Infrastructure Technician. Modifies switch, router, and hub configurations to ensure optimum network performance. Configures access control lists to grant/restrict network access to authorized users and processes. Uses approved network management software and tools to perform their tasks. Infrastructure technicians are experts in operating and configuring routers and switches, in addition to a variety of hubs and transmission media.

A3.4.6. Intrusion Detection Specialist. Uses Air Force standard automated security tools to deter, detect, isolate network intrusions, and recover compromised systems after attack.

A3.4.7. Vulnerability Assessment Specialist. Performs internal network security assessments, using Air Force standard automated security tools to minimize and/or eliminate threat of network intrusion by proactively probing network defenses to identify vulnerabilities. Ensures systems are compliant with TCNO requirements and updates/reports status. Determines and reports the information protection posture of the base network. Ensures all current network security tools and patches are implemented across all internal base systems. Base will maintain ability to monitor, detect, analyze, summarize, report, control, isolate, contain, recover and correct vulnerabilities.

A3.4.8. Boundary Protection Specialist. Installs, configures, and maintains the CITS IA suite. Operates and maintains firewall(s), web proxy and caching servers, and E-mail gateway server to protect base information resources from internal and external threats.

A3.5. AFNOSC and NOSC Positions.

A3.5.1. Network Defense Controller. Network defense controllers oversee intrusion detection, boundary protection and vulnerability assessment operations to defend the AFEN. Network defense controllers develop a network defense visibility display, direct time sensitive adjustments to the network security posture to minimize or counter operational risk, and collect and store the data and metrics necessary to conduct Operational Risk Management (ORM). They also direct security measures such as identification/authentication controls, internal encryption, and intrusion detection for the NOSC or NCCs under their control.

A3.5.2. Enterprise Controller. Enterprise Controllers oversee network administration and network management operations for the AFEN. They are responsible for monitoring network management software and generating ad hoc queries for network assistance, and directing courses of action. Enterprise controllers maintain a "watch" on network performance characteristics and infrastructure centers of gravity, and recommend adjustments. They centrally monitor server, user, and server-launched applications to ensure efficient use. They also create and report appropriate metrics within their area of responsibility.

A3.5.3. Voice Controller. Voice Controllers are responsible for operating, managing, and maintaining the Voice Protection System (VPS) system and help provide situational awareness of all MAJCOM voice networks (e.g. DSN, public switched telephone network, and Federal Telecommunications System 2001). Voice Controllers develop VPS security policies, custom report development, recurring and ad-hoc report generation, moves/adds/changes associated with VPS policy, troubleshooting and system maintenance, upgrades system backups, and regular administrative reporting. They are also responsible for coordinating VPS-related issues with individual bases.

A3.6. Crew Positions at All Levels.

A3.6.1. Crew Commander. Crew Commander is the only officer crew position. They serve at all three levels of NETOPS hierarchy; the AFNOSC, NOSC, and NCC. NCCs with limited manning may utilize Operations Controllers in place of Crew Commanders. Responsibilities include successful mission execution, maintaining crew integrity, and ensuring crew members are trained and certified. Crew Commanders conduct changeover briefings and prepare daily standup briefings. They coordinate with wing/base-level OPSEC and counterintelligence (AFOSI) personnel on DCI plans/operations, and de-conflict CND activities with on-going aerospace operations and missions. Additionally, they maintain daily logs, coordinate with external customers, and review SITREPs, OPREP3s, INFOCONs, TCNOs, and C4 NOTAMs. Crew commanders maintain restoration and recovery plans and procedures and ensure positive control over network defense operations. In short, they maintain tactical and operational control over their assigned crew.

A3.6.2. Operations Controller. Operations Controllers serve at each tier of the network operations hierarchy. They are required at the AFNOSC and NOSC, but optional at the NCC. The Operations Controller cannot be duel hatted with another crew position (e.g., they cannot fill an Enterprise Controller position and Operations Controller position during the same shift). Operations Controllers are seasoned network professionals (preferably a senior NCO) and certified in at least one crew position. They are the right-hand of the Crew Commander. They advise Crew Commanders of critical situations and recommend courses of action. Additionally, they help maintain daily logs, and review SITREPs, OPREP3s, INFOCONs, TCNOs, and C4 NOTAMs. Operations Controllers help Crew Commander ensure positive control over their assigned crew.

A3.6.3. Help Desk Technician/Event Manager. Help Desk technicians are in essence event managers. At the NCC level Help Desk Technicians are the WM and FSA point of contact to the NCC. They utilize a standard trouble ticketing database for inputting, assigning, resolving and closing trouble tickets. Event Managers are responsible for maintaining a real-time view of the base network, MAJCOM network, or AFEN ability to perform its designed functions. Event managers also prepare monthly metrics showing operational performance. Help Desk Technicians and Event Managers must be certified in at least one crew position.

Table A3.1. Network Operations Mission Areas.

				Systems and Network Management	Information Dissemination Management	Information Assurance
CREW POSITIONS	UNIT		Functional Systems Administrator			
			Workgroup Manager			
	NCC		Help Desk Technician			
		Network Admin Positions	Configuration Management Technician			
			Application Services Technician			
			Messaging Technician			
		Information Protection	Boundary Protection Specialist			
			Intrusion Detection Specialist			
			Vulnerability Assessment Specialist			
		Network Mgt	Infrastructure Technician			
			Internet Services Technician			
			Crew Commander			
	NOSC		Network Defender			
		Information Protection Operations	Boundary Protection Specialist			
			Intrusion Detection Specialist			
			Vulnerability Assessment Specialist			
			Enterprise Controller			
		Network Admin Positions	Configuration Management Technician			
			Application Services Technician			
			Messaging Technician			

				Systems and Network Management	Information Dissemination Management	Information Assurance
CREW POSITIONS	NOSC	Network Mgt	Infrastructure Technician			
			Internet Services Technician			
		Event Manager/Help Desk				
		Voice Controller				
		Crew Commander				

Network Operations Mission Areas					
CREW POSITIONS			Systems and Network Management	Information Dissemination Management	Information Assurance
	AFNOSC	Network Defense Controller			
		Enterprise Controller			
		Event Manager/Help Desk			
		Crew Commander			