BY ORDER OF THE SECRETARY
OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-115

16 SEPTEMBER 2014

ANDERSEN AIR FORCE BASE
Supplement

12 AUGUST 2016

Communications and Information

AIR FORCE INFORMATION
TECHNOLOGY (IT) SERVICE
MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **http://www.e-publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6CS

Certified by: SAF/A6C
(Maj Gen Earl Matthews)

Supersedes: AFI33-115V1, 24 May 2006,
AFI33-115V2, 14 April 2004,
AFI33-115 V3, 15 April 2004,
AFI33-129, 3 February 2005,
AFI33-138, 28 November 2005

Pages: 50

(ANDERSONAFB)

OPR: 36 CS/SCOO

Certified by: 36 MSG/CC
(Col Eric S. Turner)

Pages: 4

This Air Force Instruction (AFI) defines AF IT Service Management and assigns responsibilities for standardization and management of IT Services in the AF. This instruction implements AF Policy Directive (AFPD) 33-1, *Cyberspace Support,* Department of Defense (DoD) Instruction (DoDI) 8410.01, *Internet Domain Name Use and Approval*, DoDI 8410.02, *NetOps for the Global Information Grid (GIG),* DoDI 8410.03, *Network Management (NM)* and DoDI 8550.01, *DoD Internet Services and Internet-Based Capabilities*. This instruction is consistent with AFPD 33-2, *Information Assurance (IA) Program;* AFPD 33-3, *Information Management;* AFPD 33-4, *Information Technology Governance;* and AFPD 10-17, *Cyberspace Operations*. This instruction provides guidance, direction and assigns responsibilities for the Air Force

Information Networks (AFIN) as the Air Force provisioned portion of the DoD Information Networks (DoDIN). This directive applies to all military and civilian Air Force personnel, the Air Force Reserve (AFR), and Air National Guard (ANG). This publication shall be applied to contractors or other persons through the contract or other legally binding agreement with the Department of the Air Force. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Send recommended changes or comments to the Air Force Cyberspace Strategy & Policy Division (SAF/A6CS) using AF Form 847, *Recommendation for Change of Publication.*

Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). See **Attachment 1** for a glossary of references and supporting information.

(ANDERSONAFB) Air Force Instruction (AFI) 33-115, 16 September 2014, is supplemented as follows. This supplement applies to all assigned, attached, and tenant units supported by AFNET and Andersen Air Force Base (AFB), and separate operating locations supported by AFNET and Andersen AFB. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional' s chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

SUMMARY OF CHANGES

This is a total revision of AFI 33-115. Information from AFI 33-115 Volume 1, *Network Operations*, AFI 33-115 Volume 2, *Licensing Network Users and Certifying Network Professionals*, AFI 33-115 Volume 3, *Air Force Network Operating Instructions*, AFI 33-129, *Web Management and Internet*, and AFI 33-138, *Enterprise Network Operations Notification and Tracking*, were incorporated in this document. AFMAN 33-152, *User Responsibilities and Guidance for Information Systems*, provides guidance for responsible use of the Internet that was previously covered by AFI 33-129 and user certification requirements previously covered by AFI 33-115V2. Network professional certification requirements are covered by AFMAN 33-285, *Information Assurance (IA) Workforce Improvement Program.* Methods and Procedures Technical Order (MPTO) 00-33A-1109, *Vulnerability Management*, provides vulnerability notification and tracking processes and procedures previously covered by AFI 33-138. AFPD 10-17, *Cyberspace Operations*, and supporting AFIs, provides AF policy and assigns responsibility for the planning and execution of Cyberspace Operations including DoDIN

Operations. AFI 10-1701, *Command and Control (C2) of Cyberspace*, provides Command and Control (C2) guidance for DoDIN Operations within the AF.

1. Purpose. This instruction defines AF IT Service Management and assigns responsibilities for the configuration, provisioning, maintenance, and management of AFIN using an IT Service Management (ITSM) framework to further integrate capabilities and maintain configuration control of AF networks and data servers. This instruction serves as the single reference for AF IT Service Management policy and applies to all personnel who manage, configure, operate, maintain, defend, or extend any portion of the AFIN or provide support within the AF for the DoDIN and the Joint Information Environment (JIE).

1.1. Procedural guidance supporting this AFI is contained in Methods and Procedures Technical Orders (MPTOs) directing standard processes for management, standardization, and maintenance of AF IT Services applicable to all AF personnel, see **paragraph 7.3**.

1.2. Cyberspace operational orders as defined in AFI 10-1701 (e.g., AF Cyber Tasking Orders, Cyber Control Orders, AF Time Compliance Network Orders) shall take precedence over information contained in this AFI and supporting MPTOs if there is a conflict.

2. Objectives. The primary objective of this AFI is to establish and define AF IT Service Management with roles and responsibilities to ensure the AFIN is designed, built, configured, secured, operated, maintained, and sustained to meet mission requirements. This AFI also provides guidance regarding migration of AF enterprise capabilities (core services, applications, and systems) to the JIE according to DoD guidance. AF IT Service Management integrates, secures, and manages the AFNET/AFNET-S with processes and capabilities to enable the seamless, secure, and reliable exchange of information across the AFIN and the DoDIN. The AFNET is the AF's underlying unclassified network that enables AF operational capabilities and lines of business. AFNET-S is the secure AFNET.

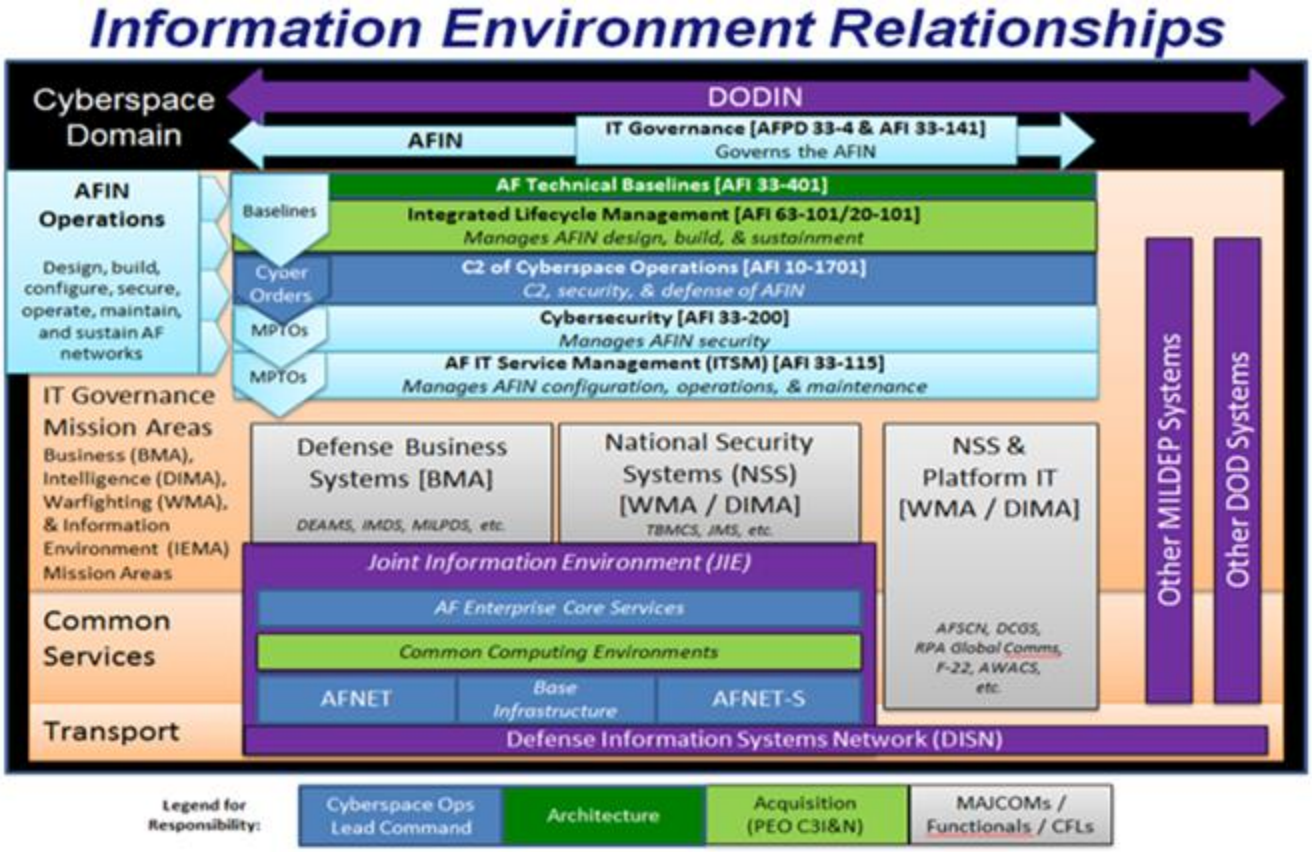
2.1. This AFI and supporting 00-33 series MPTOs shall not alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) systems or intelligence, surveillance, reconnaissance mission and mission support systems or higher authoritative guidance governing Special Access Program (SAP) systems. When DNI or SAP authorities fail to address areas covered by this AFI, this AFI and associated MPTOs will be followed. If there is conflict between this AFI and associated MPTOs with guidance issued by DNI or SAP authorities, DNI or SAP guidance will take precedence.

2.2. For this instruction, the term Major Command (MAJCOM) also applies to Numbered Air Force (NAF), Field Operating Agency (FOA) and Direct Reporting Unit (DRU) when not assigned to a MAJCOM.

2.3. All AF organizations will follow this policy when extending AF IT Services.

3. Background. The AF Information Environment consists of AF unique information capabilities across the IT Governance Mission Areas: Business (BMA), Warfighting (WMA), Defense Intelligence (DIMA) and Information Environment (IEMA). The AF Information Environment includes the IT systems, components and networks of the Defense Business Systems, National Security Systems (NSS), Platform IT, Enterprise Core Services and Common Computing Environments as depicted in **Figure 1**. The AFIN is the globally interconnected, end-to-end set of AF unique information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security. The AFIN can be considered the networked AF Information Environment. Where known, this AFI will depict the specific AF capabilities and services which will transition to DoD’s secure joint information environment (JIE). JIE is comprised of shared IT infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies.

Figure 1. Information Environment Relationships.


Information Environment Relationships
Cyberspace Domain
DODIN
AFIN
IT Governance [AFPD 33-4 & AFI 33-141]
Governs the AFIN
AFIN Operations
Design, build, configure, secure, operate, maintain, and sustain AF networks
Baselines
AF Technical Baselines [AFI 33-401]
Integrated Lifecycle Management [AFI 63-101/20-101]
Manages AFIN design, build, & sustainment
Cyber Orders
C2 of Cyberspace Operations [AFI 10-1701]
C2, security, & defense of AFIN
MPTOs
Cybersecurity [AFI 33-200]
Manages AFIN security
MPTOs
AF IT Service Management (ITSM) [AFI 33-115]
Manages AFIN configuration, operations, & maintenance
IT Governance Mission Areas
Business (BMA), Intelligence (DIMA), Warfighting (WMA), & Information Environment (IEMA) Mission Areas
Defense Business Systems [BMA]
DEAMS, IMDS, MILPDS, etc.
National Security Systems (NSS) [WMA / DIMA]
TBMCS, JMS, etc.
NSS & Platform IT [WMA / DIMA]
AFSCN, DCGS, RPA Global Comms, F-22, AWACS, etc.
Other MILDEP Systems
Other DOD Systems
Common Services
Joint Information Environment (JIE)
AF Enterprise Core Services
Common Computing Environments
AFNET
Base Infrastructure
AFNET-S
Transport
Defense Information Systems Network (DISN)
Legend for Responsibility:
Cyberspace Ops Lead Command
Architecture
Acquisition (PEO C3I&N)
MAJCOMs / Functionals / CFLs

3.1. AF IT Service Management enables a robust and resilient net-centric environment providing the means to establish and extend the AFIN. AF IT Service Management supports rapidly evolving mission processes and warfighter requirements which require an optimized, stable, and enterprise managed AFIN postured to integrate with and support the JIE. AF IT Service Management encompasses management of common IT functions, actions, and capabilities to provide Common Computing Environments, Application Support Services, and Enterprise Core Services. Additionally, AF ITSM standardizes select ITSM processes for all information systems (e.g., Vulnerability Management).

3.2. AF IT Service Management is aligned with the Defense Information Technology Infrastructure Library (ITIL) as it transitions to the Defense Enterprise Service Management Framework (DESMF), and DoD Directive (DoDD) 8000.01, *Management of the Department of Defense Information Enterprise*. These services and the standard methods and procedures in the supporting MPTOs will continue to evolve to support the AF's management of IT under the JIE construct. These services must align with high level guidance and strategic goals of the AF Enterprise Architecture. For more information on enterprise architecture, see AFI 33-401, *Air Force Architecting.*

3.3. AFI 10-1701 implements the C2 of Cyberspace Operations and while this AFI directs specific ITSM functions which support DoDIN Operations. Together, these two instructions direct operations and support of the AFIN for the business and warfighting mission areas including the Cyberspace Operations mission. Capabilities to secure and protect the AFIN must be integrated throughout AF networks and systems following Cybersecurity policy (previously known as IA). Cybersecurity inherent in AF networks and systems are further enhanced by Defensive Cyberspace Operations (DCO) under Cyberspace Operations. DCO may be integrated with or direct changes to cybersecurity in AF networks and systems under C2 of Cyberspace Operations as it directs AFIN operations and defense. Note: DoD defines DoDIN Operations as the actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation.

4. Roles and Responsibilities. Roles and responsibilities for AF IT Service Management are a coordinated effort between all organizations providing, supporting, and utilizing IT in the AFIN, the DoDIN, and the JIE. AF functional communities or DoD organizations such as Defense Information Systems Agency (DISA) or AFSPC will have primary or supporting roles when AF IT Services are consolidated at the DoD-enterprise level and JIE. Roles and responsibilities for C2 of Cyberspace within AFI 10-1701 provides clear command and control over these collaborative relationships and is to be used in conjunction with this AFI.

4.1. **Chief, Information Dominance and Chief Information Officer (SAF/CIO A6).** SAF/CIO A6 has overall responsibility for the AFIN, information technology (IT), IT Service Management responsibilities for National Security Systems (NSS), defense business systems, and information resource management matters according to AFPD 33-1. SAF/CIO A6 will:

4.1.1. Provide strategy, policy, guidance, and oversight for the AF portion of the DoD information enterprise, including communications, spectrum management, network management, information systems, and cybersecurity.

4.1.1.1. Develop AF strategy and policy on the operation and protection of all AF IT and information systems within the AFIN as the AF provisioned portion of the DoDIN, including development and promulgation of enterprise-wide architecture requirements and technical standards, and enforcement, operation, and maintenance of systems, interoperability, collaboration, and interface between AF and non-AF systems, and investment and cost effectiveness of information system acquisition and sustainment.

4.1.1.2. Maintain a consolidated inventory of AF mission-critical and mission-essential information systems, identify interfaces between these systems, and ensure the development and test of contingency plans for responding to disruptions in the operation of any of these information systems.

4.1.1.3. Provide guidance and oversight for AF network management, including the standards for day-to-day security and protection of AF information networks; AF IT support to joint missions; and resilience and reliability of information and communication networks.

4.1.1.4. Provide guidance and oversight on the administration of AF Internet services, use of Internet-based capabilities, and all Internet domain-related functions.

4.1.1.5. Develop strategy, policy, and guidance for AF use of private and public cloud computing services in support of the AFIN. Review DISA's security model for commercial cloud services and coordinate any modifications needed for alignment between the DoD cloud security model and the AFIN technical architecture security controls provided in the Target Baseline according to AFPD 33-4, *Information Technology Governance*.

4.1.2. Provide governance of IT according to AFPD 33-4, *Information Technology Governance*, including oversight for compliance with the Target Baseline (TB), Implementation Baseline (IB), and Operational Baseline (OB).

4.1.3. Define the AF IT Service Management for the AFIN and ensure Enterprise Core Services for the AF are in-line with the DoD Enterprise Services under the DoDIN and/or JIE.

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

4.1.5. Fulfill AF CIO responsibilities of DoDI 8550.01, *DoD Internet Services and Internet-Based Capabilities.*

4.1.6. Provide oversight and guidance for personnel development, career field management, and training of AF Cyberspace career fields according to AFI 36-2640, *Executing Total Force Development*.

4.1.7. Provide AF unique requirements to the DoD Enterprise Cloud Service Broker (ECSB) for commercial cloud providers for interoperability with AF implementations of Controlled Unclassified Information and the Enterprise Records Management Plan.

4.1.8. Work with Air Force Office of the Judge Advocate General (AF/JA), the Air Force Office of Special Investigations (AFOSI), the Air Force Office of the Inspector General (SAF/IG), the Intelligence Community, and the Acquisition Division of the Air Force General Counsel (SAF/GCQ) to provide requirements to the DoD ECSB to ensure that tools and processes to protect sensitive information and adequate law enforcement tools are available for commercial cloud services.

4.1.9. Work with Air Force Legal Operations Agency (AFLOA), SAF/GC, AF/JAA and SAF/AQC to provide requirements to the DoD ECSB for Software-as-a-Service (SaaS) compliance with AF e-Discoveryrequirements according to AFMAN 33-363, *Management of Records.*

4.1.10. Act as the approval authority for waiver requests to deviate from the requirements of this publication.

4.1.11. Act as the central AF approval authority for obligations to acquire servers, data centers, and IT technology therein, IAW AFI 33-150, *Management of Cyberspace Support Activities,* Attachment 2.

4.2. **IT Governance Executive Board (ITGEB) will:**

4.2.1. Approve the data centers (Installation Processing Node [IPN], Installation Services Node [ISN], Special Purpose Processing Node [SPPN]) to serve as AF data center infrastructure. ITGEB-approved data centers are the only authorized data centers for the AF to employ application hosting and provisioning of private cloud services. See AFPD 33-4 for more information on the ITGEB.

4.2.2. Oversee the execution of application rationalization and migration across the AF to ensure compliance with DoD guidance regarding hosting within IPNs, CDC, and DISA commercial cloud brokered services. This includes directing the capture and reporting of metrics reflecting decommissioned servers and data centers in accordance with the Federal Data Center Consolidation Initiative (FDCCI).

4.2.3. The scope for the ITGEB includes the entire AF IT enterprise for business and mission capabilities, including business and national security systems (NSS), and excluding the embedded software in support of weapons platforms. This team shall focus on the commoditization and operational configuration management of a baseline IT infrastructure and the business practices to exploit that IT infrastructure for AF users. The details of membership and processes can be found in AFPD 33-4.

4.3. **Secretary of the Air Force Office of Public Affairs (SAF/PA) will:**

4.3.1. Develop guidance for the integration of public web sites into the Air Force Public Web Program. Serve as chair of the Air Force Public Web Policy Board.

4.3.2. Develop guidance governing the public communication program.

4.3.3. Review and approve/disapprove waiver requests for AF public Web sites hosted outside the scope of the Air Force Public Web Program.

4.4. **Assistant Secretary of the Air Force for Acquisition (SAF/AQ).** As the Senior Acquisition Executive, SAF/AQ will**:**

4.4.1. Oversee the acquisition and sustainment of capabilities that support the AFIN.

4.4.2. Work with SAF/CIO A6 and AFSPC to procure, develop, integrate and test the AFIN components and systems in accordance with the Implementation Baseline.

4.4.3. Collaborate with SAF/CIO A6 in developing the Implementation Baseline (IB) defined in AFPD 33-4. Ensure AF acquisition programs comply with the established IB requirements.

4.4.4. Ensure AF acquisition programs leverage, to the maximum extent possible, the use of JIE Enterprise Core Services, and promote sharing of data, information, and knowledge throughout the AF corporate structure.

4.4.5. Work with SAF/CIO A6 to develop strategy, policy, and guidance to provide an AF enterprise approach for acquiring commercial cloud computing services utilizing the DoD ECSB.

4.4.6. Ensure all Acquisition Category (ACAT) programs address the requirements of National Defense Authorization Act (NDAA) Fiscal Year 2012 Section 2867 and AFI 33-150, *Management of Cyberspace Support Activities*, Attachment 2, in the acquisition of servers, data centers, and IT technology.

4.5. **Air Force Material Command (AFMC).** As the Implementing Command defined by AFI 63-101/20-101, AFMC has overall responsibility for supporting the design, build, and sustainment of the AFIN. AFMC will:

4.5.1. In coordination with AFSPC, provide technical assistance to SAF/CIO A6 to develop policy and guidance for the AFIN.

4.5.2. Provide integration and test capability for IT components to support the development environment of new capabilities and troubleshooting performance issues with fielded capabilities, as required.

4.5.3. Provide direction and guidance to ensure all Program Executive Offices (PEOs) comply with the single AF approach for cloud computing and establish the AF Cloud Service Lead according to **paragraph 4.6.5**.

4.5.4. Oversee the work performed by PEO C3I&N on the commoditized infrastructure Implementation Baseline.

4.5.5. In coordination with AFSPC, oversee the deployment of all AF IT services.

4.5.6. Oversee the standup of the IT lifecycle integration and test capability.

4.6. **The Program Executive Office for Command, Control, Communications, Intelligence and Networks (PEO C3I&N).** PEO C3I&N will:

4.6.1. Perform Service Design and Development to include engineering, architecture, and provisioning support for AFNET, AFNET-S, and PEO C3I&N-provided systems within the AFIN and JIE in coordination with SAF/CIO A6 and AFSPC. Provides integration of AF IT across all systems centers (e.g., Air Force Life Cycle Management Center, Space and Missile Systems Center, Air Force Medical Support Agency, Air Force Nuclear Weapons Center).

4.6.2. Establish, publish, and maintain the commoditized infrastructure Implementation Baseline in accordance with AFPD 33-4.

4.6.3. Facilitate the standup and operation of an IT lifecycle integration and test capability supporting the development, test, and delivery of new warfighter capabilities utilizing the Implementation Baseline. Leverage existing DoD, AF and Contractor resources to establish a virtual, distributed system development, integration and test capability supporting the delivery of new warfighter capabilities.

4.6.4. Support mission capabilities offices in configuring and provisioning the Implementation Baseline to meet requirements. Support mission capabilities offices with transitioning their newly developed capabilities into the Implementation Baseline integration environment leading to deployment.

4.6.5. Serve as the AF Cloud Service Lead:

4.6.5.1. Review and validate all cloud computing technical requirements prior to engaging with DISA as the DoD cloud broker.

4.6.5.2. Assist AF acquisition programs to define requirements and capabilities that can be implemented utilizing DoD ECSB approved cloud offerings.

4.6.6. Ensure a standardized AF process is adhered to for common computing environments and cloud services, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) as detailed in **paragraph 5.3.** Fully leverage DoD efforts to provide a DoD Enterprise Cloud Environment under the JIE in accordance with DoD CIO Memorandum, *DoD Cloud Computing Strategy Memorandum*, 5 July 2012 and DoD CIO Supplemental Guidance Memo, 16 December 13.

4.6.6.1. Review all AF cloud computing technical requirements for consistency with the AF framework to cloud computing prior to engaging with DISA as the DoD ECSB.

4.6.6.2. Work with the DoD ECSB, in conjunction with SAF/AQ and AFMC organizations to ensure a clear, tailorable cost model is established and made available for use of and migration to commercial cloud services.

4.6.7. Implement Network Management (NM) data schemas and net-centric sharing mechanisms to support the development of Service Level Agreements (SLAs), and support the implementation of network management security according to DoDI 8410.03, *Network Management (NM)*.

4.6.8. Ensure that all AF Commercial Cloud Contracts address the additional issues in the DoD Cloud Issue Matrix according to DoD CIO Supplmental Guidance Memo, 16 December 2013.

4.7. **Commander, Air Force Space Command (AFSPC/CC)**. In accordance with AFPD 10-17, AFSPC/CC is responsible for the overall command and control, security and defense of the AFIN. AFSPC/CC is responsible for the command, control, implementation, security, operation, maintenance, sustainment, configuration, and defense of the AFNET/AFNET-S. These day-to-day authorities may be delegated. In addition to those responsibilities outlined in 10-series AFIs, AFSPC will:

4.7.1. Assist SAF/CIO A6 to develop policy and guidance for the AFIN and AF adoption of JIE capabilities.

4.7.2. Establish and maintain the Operational Baseline in accordance with AFPD 33-4.

4.7.3. Develop and submit to SAF/CIO A6 and HQ AETC requirements for initial, advanced, supplemental, and qualification training for cyberspace career field members.

4.7.4. Fulfill DoDIN Operations responsibilities for the AFNET/AFNET-S in support of DoDI 8410.02, *NetOps for the Global Information Grid (GIG)*, while remaining consistent with AFPD 10-17, *Cyberspace Operations*, and AFI 10-1701, *Command and Control for Cyberspace Operations*.

4.7.4.1. Establish and provide the necessary resources to ensure compliance with SLAs and memorandums of agreement (MOAs) among DoDIN and JIE service providers and users.

4.7.4.2. Participate in the DoDIN Operations Community of Interest (COI) to share information, promote standards, and resolve DoDIN Operations issues.

4.7.4.3. Participate in the DoD CIO and SAF CIO/A6 Enterprise Architecture (EA) efforts described in DoDI 8410.02 and AFPD 33-4.

4.7.4.4. Ensure all AF contractors and other entities operating AF-owned information systems and AF-controlled information systems on behalf of the Air Force that receive, process, store, display, or transmit AF information, regardless of classification or sensitivity, comply with DoDI 8410.02.

4.7.5. Provide Network Management for the AFNET/AFNET-S with automated Configuration Management and Policy Based Network Management (PBNM) according to DoDI 8410.03.

4.7.6. Ensure the operation of the AF's DoD Internet Services and official use of Internet-based Capabilities (IbC) according to DoDI 8550.01.

4.7.7. Ensure that all DoD Internet services and IbC used by the AF to disseminate unclassified DoD information are assessed at least annually for compliance with DoDI 8550.01.

4.7.8. Provide technical procedures, and standards for the AFIN.

4.7.8.1. Develop MPTOs for AF ITSM to configure, operate, and maintain AF IT established in **Section 5**, AF IT Services Framework.

4.7.8.2. Provide life cycle management of AF ITSM MPTOs with technical content management (TCM) by 24 AF, other subordinate units, AF Program Management Offices (PMOs), or System Program Offices (SPOs) as needed.

4.7.8.3. Serve as the Command Control Point for MPTOs supporting AF ITSM to include technical content management according to TO 00-5-1, *AF Technical Order System*, and TO 00-5-3, *AF Technical Order Lifecycle Management*.

4.7.9. Develop and implement metrics and measures of effectiveness for the AFNET/AFNET-S and AF IT Service Management.

4.7.10. Develop processes and implement policies including MPTOs to manage all AF-owned networks and platform IT interconnections behind appropriate cybersecurity boundaries as defined in the Baselines and according to AFI 33-210, *Air Force Certification and Accreditation Program*. Review and approve Service Level Agreements for non-AF owned networks on AF installations.

4.7.11. As the AF Authorizing Official (AO) (previously known as Designated Accrediting Authority [DAA]) in accordance with AFI 33-200, assess networthiness and serve as the waiver approval authority for web servers, services, applications, or capabilities supporting the AF to be hosted on commercial servers or services (including cloud computing services) outside of military or government cybersecurity boundaries. Approval requires coordination with the AF Cloud Broker Lead and DoD ECSB. The AF AO has responsibility over AF networks, applications and systems as well as the connection approval authority for non-AF systems and applications that will integrate into the AFIN.

4.7.12. Prior to JIE transitions, manage all networks under a One AF-One Network policy by directing the operation, maintenance, and configuration of all AFNET and AFNET-S components (see **Chapter 7**). Serve as the waiver approval authority for allowing management of networks outside of the lead MAJCOM.

4.7.13. Support and facilitate management of the Standard Desktop Configuration (SDC)/Defense Server Core Configuration (DSCC) by Air Force Enterprise Configuration Management Office (AFECMO).

4.7.14. Ensure records management procedures are implemented and sustained for all enterprise storage services.

4.7.14.1. Ensure technology solutions meet requirements to support eDiscovery capabilities according to DoD 5012.02-STD, *Electronic Records Management Software Applications Design Criteria Standard* and the Federal rules of Civil Proceedure.

4.7.14.2. Implement policy, advocate for resources, and organize, train, and equip cyberspace forces to identify, locate, protect, and produce electronically-stored information in response to litigation requirements.

4.7.14.3. Cooperate with Air Force Legal Operations Agency and the Air Force Records Office directing actions to locate and preserve electronic records as well as non-record electronically stored information which become subject to a litigation hold.

4.7.14.4. Cooperate with Air Force Office of Special Investigations (AFOSI) when an investigation requires the location, acquiring and or preservation of electronic records as well as non-record electronically stored information, IAW AFPD 71-1.

4.7.15. Assist AFMC with the development, integration, testing, and fielding of new systems and services, as required (e.g., step 4 of the SDDP to be published or when requested to determine causes of and solutions to deployment and performance issues).

4.7.16. Incorporate AF IT Services into the Core Functions Support Plan (CFSP), as the CFL for Cyberspace Superiority.

4.7.17. Work with MAJCOM/A6s and Mission/Functional process owners to ensure technical consistency of IT solutions across the AFIN in accordance with AFSPC's roles and responsibilities as CFL for Cyberspace Superiority.

4.7.18. If a specific approval authority is not identified (see **paragraph 4.1.11**), act as the AFIN approval authority for:

4.7.18.1. System/equipment waiver requests (i.e., purchases, documentation, preventative maintenance inspections).

4.7.18.2. Proposed temporary modifications, known as T-1 modifications to the AFNET/AFNET-S system/equipment modifications according to AFI 63-131, *Modification Program Management*.

4.7.19. Manage and administer Domain Name Service (DNS) subdomains assigned to the AF by DISA or approved for AF use according to DoDI 8410.01.

4.7.19.1. Manage AF-level (af.mil and af.smil.mil) DNS and naming convention for the AF according to the MPTO for Directory Services. Maintain a Name Server (NS) record for all AF name servers in the af.mil zone and provide technical support for the af.mil and af.smil.mil domain and sub-domains.

4.7.19.2. Annually verify administrative and technical contact information is correct in the registrations maintained at the DoD Network Information Center/Secret Internet Protocol Router Network (SIPRNET) Support Center (DoD NIC/SSC) and at the General Services Administration's Government Domain Registration and Services Web site at **http://www.dotgov.gov**.

4.7.20. Review and update AF-level SLAs with external agencies and supported MAJCOMs as required.

4.7.21. Provide network integration and engineering services for the AFNET/AFNET-S and development of JIE capabilities.

4.7.21.1. Ensure operational systems do not introduce vulnerabilities to the AFNET/AFNET-S or disrupt existing functions, while creating a resilient network environment that preserves operational advantage.

4.7.21.2. Perform networthiness consultation, validation, compliance and assessments of risk to the AFIN to enforce standards for functional and cyberspace systems, applications, and products requiring connection to the AFIN.

4.7.21.3. Develop and implement the AFNET Integration Process to verify compliance with security, interoperability, supportability, sustainability, usability regulations of systems, applications, and/or products, and readiness review criteria.

4.7.21.4. Collaborate with organizations to integrate all AF-owned, contracted or developed systems into the AFNET/AFNET-S.

4.7.21.5. Develop integration and implementation plans for AFIN & AFNET evolution to current and future JIE capabilities.

4.7.22. Provide the AF's engineering center of excellence for developing and implementing technical solutions for the AFIN via subordinate organizations such as the 38th Cyberspace Engineering Installation Group (38 CEIG) and AF Network Integration Center (AFNIC).

4.7.22.1. Document Main Operating Base AFIN infrastructure, including system life-cycle information, via the Cyberspace Infrastructure Planning System (CIPS) (Reference MPTO 00-33D-3003, *Managing the Cyberspace Infrastructure with the Cyberspace Infrastructure Planning System*).

4.7.22.2. Provide AFIN network operations with enterprise engineering services according to AFI 33-150, *Management of Cyberspace Support Activities*.

4.7.22.3. Develop and analyze cyberspace requirements and associated impacts on operational architectures and capabilities, and convert AF and DoD technical specifications into standard AFIN and joint solutions to facilitate convergence on a single robust and defensible architecture.

4.7.22.4. Provide network health and vulnerability assessments as coordinated and directed by 24 AF/AFCYBER, including network security and optimization assistance as well as event-driven response action teams.

4.7.22.5. Develop and maintain the AFNET Infrastructure Roadmap and AFNET Concept of Operations to serve as an input to the Target Baseline and show how the Operational Baseline would evolve into the Target Baseline. The Roadmap and Concept of Operations will address Cyber, Situational Awareness of the network, and Network Management capabilities as well as operational roles and responsibilities.

The Infrastructure Roadmap will contain the collected and prioritized set of requirements.

4.8. **24th Air Force (24 AF (AFCYBER)).** 24 AF is the AF component to USCYBERCOM. AFSPC/CC may delegate certain authorities to 24 AF/CC IAW AFI 10-1701, Command and Control for Cyberspace Operations.

4.8.1. In coordination with AFSPC, maintain and administer the Operational Baseline including the AFNET/AFNET-S.

4.8.2. Serve as liaison between the AFECMO and the operational community to facilitate the development and implementation of the SDC/DSCC.

4.8.3. Direct the security, operations, and defense of cloud computing services operated for the AF outside of AF network boundaries but logically a part of the AFIN, using authorities designated by the Cyber C2 structure in AFI 10-1701.

4.8.4. Provide assessments of impact to the AFIN in response to requests for web servers, services, applications, or capabilities to be hosted on commercial servers or services outside of military or government cybersecurity boundaries.

4.8.5. In coordination with AFSPC, review and approve/disapprove MAJCOM unique applications, communications systems, and IT Services requests/needs to ensure compatibility with AF IT Services. Include recommended changes affected by use of commercial servers or services (including cloud computing services).

4.8.6. Provide enterprise-level management of AF IT Services.

4.8.7. Monitor subordinate units' compliance with orders issued and provide assistance on compliance issues when resolution is beyond their scope and/or resources.

4.9. **624th Operations Center (624 OC).** 624 OC is the operational-level C2 organization for 24 AF (AFCYBER), providing strategy, planning, execution monitoring and assessment of Air Force cyber operations. 624 OC directs AF cyber operations and the activities of subordinate 24 AF cyber units via the Cyber Tasking Order (CTO) and other cyber orders. In addition to duties specified in 10-series AFIs and applicable CYBERCOM orders, 624 OC is responsible for the following:

4.9.1. Develop options and directs operational configuration changes, Information Operations Condition (INFOCON) changes (see AFI 10-710, *Information Operations Condition (INFOCON)*), and changes to security postures in response to vulnerabilities and incidents, AF and CCMD operations, USCYBERCOM direction, and outages that cross MAJCOMs, affect the preponderance of the AFIN, or are time critical in nature.

4.9.2. Perform trend analysis and correlation of threat, performance, and compliance metrics as it relates to Vulnerability Management.

4.10. **Major Commands (MAJCOMs)/Functionals.** MAJCOMs/Functionals implement AF guidance concerning the operation and maintenance of mission specific MAJCOM/Functional unique applications, communications systems, and IT. MAJCOMs/Functionals will:

4.10.1. Manage and provide support for command/functional-unique programs and systems/IT. **(T-1)**.

4.10.1.1. Ensure command/functional-unique programs and systems/IT integrate with, but do not conflict with applicable AF IT Services. **(T-1)**.

4.10.1.2. Ensure command/functional-unique applications do not duplicate infrastructure, services or capabilities provided by the AFIN, AFNET, AFNET-S or JIE, by reviewing the Target, Implementation, and Operational Baselines for planned or existing services or capabilities. Exceptions must be approved by SAF/CIO A6. **(T-1)**.

4.10.1.3. Conduct application rationalization within their portfolios for business and mission systems to eliminate duplicity and ensure proper alignment with their business process in accordance with AFI 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review*. **(T-1)**.

4.10.1.4. Ensure new applications and systems are fielded within IPNs or CDCs IAW DoD guidance. **(T-0)**.

4.10.2. Utilize only AFECMO produced standard configurations for command-unique systems. Cloning, repackaging, adding, or removing software from AFECMO standard images with the intent of producing a customized image is strictly prohibited except as waived by the AF AO (previously known as DAA) according to **paragraph 4.15.2**. **(T-1)**.

4.10.3. Submit requests to change an Operational Baseline Configuration Item (CI) such as new software or an equipment upgrade. **(T-1)**.

4.10.3.1. For non-program office fielded systems, follow the Change Management process by using the change request module of the Enterprise Information Technology Service Manager (EITSM), a.k.a. Remedy, or via AFTO Form 265, *Request for Change*, according to MPTO 00-33A-1100, *Change Management*,.

4.10.3.2. For program office fielded systems and equipment, submit AF Form 1067 according to AFI 63-131, *Modification Program Management*.

4.10.4. Plan, program, and budget for the capability to respond to orders released according to AFI 10-1701, that impact command/functional-unique programs and systems/equipment including end user workstations and/or network servers and localized infrastructure supporting command-unique requirements. **(T-1)**.

4.10.5. Designate a MAJCOM/AF Forces Communications Control Center (M/ACCC) or equivalent organization to function as the MAJCOM's advocate for mission impacts to the user community (MAJCOM only). **(T-1)**.

4.11. **MAJCOM/AF Forces Communications Control Centers (M/ACCCs) will:**

4.11.1. As an operational element of the MAJCOM Commander's staff , combine situational awareness of networks and information systems supporting the MAJCOM with an in-depth MAJCOM-unique understanding of how those networks and systems are used to accomplish the mission of the command. **(T-2)**.

4.11.2. Generate and disseminate near-real time situational awareness of how MAJCOM missions are being delayed, disrupted, degraded, or terminated due to events associated with the underlying communications networks critical to those missions. **(T-2)**.

4.11.3. Serve as the information dissemination point of contact to the Integrated Network Operations and Security Centers (I-NOSCs), Enterprise Service Units (ESUs), and AF Enterprise Service Desk (ESD) on mission impacts and/or degradation to the mission and its user community. **(T-1)**.

4.11.4. Elevate issues beyond the bases' responsibility or capability to the respective enterprise service support organization. **(T-2)**.

4.12. **Communications Focal Point (CFP) within the Communications Squadron or equivalent will:**

4.12.1. Serve as the conduit for the AF ESD to resolve communications systems and equipment issues at base level. The AF ESD is responsible for all AFNET users, but will delegate some of that responsibility to the CFPs via the Federated Administrative Rights (FAR). Tools such as Information Assurance Officer Express (IAO Express) and Virtual ESD (vESD) will automate certain functions, then re-route tickets that cannot be handled by the tool to either the CFP for Tier 1 or Tier 2 support, as appropriate and/or depending on the FAR authorized, or to the ESD backshop for further processing/support. Tickets that are routed to the CFP will then be routed (by the CFP) to the appropriate production work center for resolution. **(T-1)**.

4.12.2. Operate systems and the AFNET/AFNET-S in the IPN according to AFIN baseline management processes and AF IT Services MPTOs. **(T-1)**.

4.12.3. Maintain accountability of all AFIN components physically present on the installation regardless of the organization operating the equipment. (T-1).

4.12.4. Execute control of production procedures prescribed by AFI 33-150 and MPTO 00-33A-1001, *General Cyberspace Support Activities Management Procedures and Practice Requirements*. Execute control of production on AFNET/AFNET-S components when requested by the operating organization, such as the 26 NOS, I-NOSCs or 33 NWS. Control of production includes planning and scheduling production, ordering and managing materials, and maintaining Automated Information Systems (AISs). **(T-2)**.

4.12.5. Serve as or assign a performing workcenter to provide preventive and touch maintenance on AFNET/AFNET-S, functional, and PMO equipment only as directed by the owning organization (e.g., I-NOSC, ESU, 26 NOS, 33 NWS, MAJCOM, PMO). **(T-1)**.

4.12.6. Utilize only AFECMO produced standard configurations (e.g., SDC, DSCC). Cloning, repackaging, adding, or removing software from AFECMO standard images with the intent of producing a customized image is strictly prohibited except as waived by the AF AO (previously known as DAA) according to **paragraph 4.15.2**. **(T-1)**.

4.12.7. Provide detailed maintenance records in a transferable system such as Remedy for preventive and touch maintenance on AFNET/AFNET-S equipment when directed to execute such maintenance by the owning organization. Utilize Integrated Maintenance Data System (IMDS) for all maintenance data tracking and actions completed on the AISs within physical control of CFP, according to MPTO 00-33A-1001. **(T-2)**.

4.12.8. Elevate issues beyond the base's responsibility or capability to the respective enterprise service support organization. **(T-1)**.

4.12.9. Execute actions to comply with Cyber C2 orders according to **paragraph 7**. **(T-1)**.

4.12.9.1. Identify information systems controlled by a PMO which will only be patched or modified upon approval of the PMO or system owner. **(T-1)**.

4.12.9.2. For command/functional systems, coordinate with Functional System Administrators (FSAs) to take action to comply with Cyber C2 orders. **(T-1)**.

4.12.10. Where remote administration/connectivity fails to resolve an end user service incident or fulfill a AF ITSM responsibility (e.g., Vulnerability Management), the CFP can be assigned network permissions and responsibilities to troubleshoot and resolve end user service incidents or fulfill AF ITSM responsibilities. Perform actions within local control requiring a touch labor solution as directed. **(T-1)**.

4.12.10.1. Document tasking and effort using Service Incident Management and Problem Management where appropriate.

4.12.11. Identify and resolve network threats, vulnerabilities, and attacks in coordination with the I-NOSCs, so as to minimize risks to operations. **(T-1)**.

4.12.12. Inform base leadership and base populace on network threats, vulnerabilities, and actions. **(T-2)**.

4.12.13. Notify/coordinate Authorized Service Interruptions (ASI) to minimize impact on base-level mission. **(T-1)**.

4.12.14. Maintain situational awareness of their portion of the AFIN. Notify I-NOSCs and M/ACCCs of any issues regarding equipment under CFP control or that may affect base users. **(T-1)**.

4.12.15. Report communications systems/equipment issues to MAJCOM and other higher headquarter functions as required. The CFP will provide situational awareness to the M/ACCC according to MAJCOM or Combatant Commanders guidance. **(T-1)**.

4.12.16. Coordinate, correlate, assess de-conflict and eradicate suspicious/malicious activity through appropriate authorities FSAs, M/ACCC, 561 NOS, 83 NOS, 299 NOSS and 33 NWS. **(T-2)**.

4.12.17. Perform information dissemination management. **(T-2)**.

4.12.18. Follow compliance reporting requirements as specified in each Cyber C2 order. Orders may require compliance-based, task-based, or asset-based reporting. **(T-1)**.

4.12.19. Develop and exercise COOPs. **(T-3)**. The Communications Squadron/equivalent Plans office will take lead on the development and maintenance of COOPs and/or Disaster Recovery Plan (DRP) for managed services. Work centers will assist the Plans office with the COOP/DRP development for services under their responsibility. COOP will focus on restoring an organization's mission-essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. See National Institute of Standards and

Technology (NIST) Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, for more details.

4.12.20. Up channel information that may help C2 of the AFIN. **(T-2)**.

4.13. **AF Enterprise Configuration Management Office (AFECMO).**

4.13.1. AFECMO will provide configuration management of the Standard Desktop Configuration (SDC), Defense Server Core Configuration (DSCC), Systems Center Configuration Manager (SCCM) and associated Group Policies, software components and TOs. **(T-1)**.

4.13.2. AFECMO is the only organization authorized to make changes to the SDC and DSCC installation image/configuration, baseline group policy, or the SCCM configuration baseline except as approved by the AFSPC Operational Baseline process or directed through orders released according to AFI 10-1701. Any organization cloning, repackaging, adding, or removing software from AFECMO standard images with the intent of producing a customized image is strictly prohibited except as waived by the AF AO (previously known as DAA). **(T-1)**.

4.14. **Air Force Program Management Offices (PMOs), System Program Offices (SPOs), and Organizations Developing, and/or Managing, Operating non-core IT Services, Applications or Capabilities.** Note: In accordance with the acquisition chain of authority and acquisition requirements specified in AFI 63-101/20-101, tiering of the acquisition requirements does not apply and waiver authority resides with the program execution chain. This does not relieve the program execution chain of complying with IT Services requirements specified in AFI 33-115. These organizations will:

4.14.1. Design, build, and sustain AFIN components and systems in accordance with the Implementation Baseline. Ensure infrastructure, services or capabilities are not duplicated from those provided by the AFIN or the JIE, by reviewing the Target, Implementation, and Operational Baselines for planned or existing services or capabilities. Exceptions must be approved by SAF/CIO A6. **(T-1)**.

4.14.2. Design, build, and sustain systems and associated IT according to IT baseline management processes, AF IT Services MPTOs, systems TOs, and guidance for Integrated Life Cycle Management (ILCM) provided by AFPD 63-1/20-1, *Integrated Life Cycle Management*. **(T-1)**.

4.14.2.1. Ensure information systems environments are developed and maintained consistent with the AFIN technical architecture published as the Target, Implementation, and Operational Baselines according to AFPD 33-4, where applicable, for AF capabilities built on cloud services.

4.14.2.2. Evaluate cloud computing solutions in accordance with **paragraph 5.3**, as part of their planning process when developing new applications or evaluating changes to the hosting of existing applications. Rationalize existing application needs, virtualize, and migrate existing applications to approved data centers and/or cloud services to support AF data center consolidation goals. The requiring program office is responsible for the acquisition and funding of cloud computing as supporting infrastructure. **(T-0)**.

4.14.3. Comply with all Cyber C2 orders according to **paragraph 7**. **(T-1)**.

4.14.4. Implement all actions required by Cyber C2 orders directing AF ITSM (e.g., Vulnerability Management) and report compliance/non-compliance according to the orders and applicable methods and procedures. **(T-1)**.

4.14.5. Host, tenant, and Geographically Separated Unit (GSU) organizations will coordinate all IT actions with potential impact on the network or other IT services or capabilities with their servicing CFP. **(T-1)**.

4.14.6. Utilize AFECMO produced standard configurations (e.g., SDC, DSCC). Cloning, repackaging, adding, or removing software from AFECMO standard images with the intent of producing a customized image is strictly prohibited except as waived by the AF AO (previously known as DAA) according to **paragraph 4.13.2**. **(T-1)**.

4.14.7. Conform to a One AF-One Network policy (see **paragraph 7.6**) managed by AFSPC. All systems on the network must be configured to operate within this construct or possess a waiver from the lead MAJCOM. **(T-1)**.

4.14.8. Utilize base CFP, ESU, I-NOSC, DISA, or other government enterprise managed network services and Enterprise Core Services. IT capabilities or data servers residing outside the protections of government networks and data centers require a waiver from the lead MAJCOM. **(T-1)**.

4.14.8.1. Manage all data servers and associated computing infrastructure in the data center (IPN, SPPN) as approved by the ITGEB in support of federal and AF efforts to reduce operating costs by consolidating data centers. **(T-0)**.

4.14.8.2. Submit requirements for required approvals of data servers and associated IT using CIPS through the base level Cyberspace Systems Integrator (CSI) according to AFI 33-150, Attachment 2. Obligation requests must be submitted to **usaf.pentagon.saf-cio-a6.mbx.a3c-a6c-afdcc-workflow@mail.mil** and approved by the servicing lead command or MAJCOM A6. **(T-1)**.

4.14.9. Provide Information Support Plans to AFIN Operations activities as required by AFI 63-101/20-101, *Integrated Life Cycle Management,* for any IT system that exchanges information external to itself, and/or is connected to the DoDIN.

4.15. **Functional Systems Administrator (FSA) will:**

4.15.1. Ensure functional communities of interest systems, servers, workstations, peripherals, communications devices, and software are on-line and supported. **(T-2)**.

4.15.2. Manage and maintain their functional systems. Provide an interface between program representatives and the CFP, CDC, or IPN. **(T-1)**.

4.15.3. Create a SLA or MOA for any transfer of administrative responsibilities to an IPN. **(T-2)**.

4.15.3.1. Implement all actions required by Cyber C2 orders as approved by each system's configuration control authority according to **paragraph 7**. **(T-1)**. Coordinate order implementation with servicing CFP, I-NOSC, users, and external agencies.

4.15.3.2. Follow compliance reporting requirements as specified in each Cyber C2 order. Orders may require compliance-based, task-based, or asset-based reporting.

4.15.4. Work with the CFP to:

4.15.4.1. Eradicate malicious logic from networks, information systems, and stand-alone computing devices. **(T-1)**.

4.15.4.2. Assess the scope of unauthorized network activities or incidents. **(T-1)**.

4.15.4.3. Review and upchannel I-NOSC-run vulnerability reports to the owning PMO.

4.15.5. Utilize AFECMO produced standard configurations (e.g., SDC, DSCC). Cloning, repackaging, adding, or removing software from AFECMO standard images with the intent of producing a customized image is strictly prohibited except as waived by the AF AO (previously known as DAA) according to **paragraph 4.13.2**. **(T-1)**.

4.16. **All Unit Commanders will:**

4.16.1. Ensure assigned personnel use government provided equipment, government IT services, or Internet-based Capabilities accessed from government equipment for official, authorized, or limited authorized personal use according to AFMAN 33-152 and DoDI 8550.01. **(T-0)**.

4.16.2. Maintain the security, integrity, and accountability of AF information on the Internet by establishing and maintaining public websites/capabilities inside the network demilitarized zone (DMZ) and private websites/capabilities inside the protections of government network security. Any AF website, servers, services, applications, or capabilities to be hosted on commercial servers or services outside of military or government cybersecurity boundaries requires AFSPC lead command approval. **(T-0)**.

4.16.3. Ensure all publically accessible DoD Internet Services managed by the organization comply with applicable cybersecurity controls, information security procedures, OPSEC measures, and DoDI 8550.01 requirements including registration and dissemination guidance. **(T-0)**.

4.16.4. Control content on public websites through the Public Affairs (PA) office according to AFI 35-107, *Public Web Communications* and AFI 35-102, *Security and Policy Review Process*. **(T-0)**.

4.16.5. Ensure all public websites and capabilities within the organization span of control are submitted to wing/base PA offices for review prior to their launch. ANG units will coordinate with their unit Public Affairs Officer (PAO) prior to their launch. ANG geographically separated units use their host wing for PAO support. **(T-0)**.

4.16.6. Obtain all Internet connectivity and web services through the supporting base CFP except as excluded by **paragraph 7.4. (T-2)**.

4.17. **Air Force Office of Special Investigations Cyber Investigations and Operations (AFOSI CI&O).** AFOSI conducts cyber investigations and operations in, through, and beyond cyberspace to identify, exploit, and neutralize criminal, terrorist, and intelligence threats to the AF, DoD, and US Government (USG). Air Force Mission Directive (AFMD) 39, *Air Force Office of Special Investigations (AFOSI)*, and Air Force Policy Directive

(AFPD) 71-1, *Criminal Investigations and Counterintelligence*, both implement DoDD O-5240.02, *Counterintelligence*, and define AFOSI's role as the Air Force's sole agency for conducting counterintelligence (CI) investigations, and offensive counterintelligence operations (OFCO) and as such is the only Air Force agency authorized to do so in cyberspace. AFOSI is also responsible for initiating and conducting independent criminal investigations per AFMD 39 and AFPD 71-1. The CI&O program is AFOSI's primary cybercrime investigative and operations capability. For the purposes of this paragraph, AFOSI is a DoD intelligence component as defined in DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*. AFOSI CI&O will:

4.17.1. Be the focal point for Law Enforcement (LE) and Counterintelligence activities in cyberspace and the AFIN.

4.17.2. Provide Law Enforcement support to AFCYBER/CC for matters occurring in or impacting the AFIN.

4.17.3. Provide Cyber Counterintelligence support to AFCYBER/CC and the AF for matters occurring in or impacting the AFIN.

4.18. **(Added-ANDERSONAFB)** . **Network Control Center (NCC) within the Communications Squadron or equivalent will:**

4.18.1. **(Added-ANDERSONAFB)** . The 36th Communications Squadron (36 CS) NCC is to email the Base System Administrator (SA) applicable action items based on NOTAMS received from Air Force Mission Assurance Center (AMAC) OPC. The NCC will report compliance information for all patches and NOTAMs within their AOR only.

4.18.2. **(Added-ANDERSONAFB)** . The SA will coordinate with 36 CS NCC to ensure their systems are compliant IAW AFNET and AFNET-S requirements. NOTAM compliance for Program Management Office (PMO) systems will be coordinated with PMOs. NCC will report compliance information for all patches and NOTAMs within their AOR only. Implementation of patches by SAs will be coordinated with their PMO and compliance will be reported through those channels. PMO systems or functional systems that are not compliant must have an approved POA&M coordinated with the AMAC.

4.18.2.1. **(Added-ANDERSONAFB)** . Vulnerabilities identified on devices that cannot be managed by the 36 CS (i.e., non-clients) are the responsibility of the SA of those network devices. Failure to maintain system patch compliance under 2.5 vulnerabilities per system may result in denial of network service to systems/computers. The 36th Communications Squadron Commander (36 CS/CC) will make a risk assessment and, if warranted, recommend disconnection to the 36th Wing Commander (36 WG/CC) and the Air Force Space Command Commander (AFSPC/CC), who is the AF Authorizing Official. If the 36 WG/CC approves disconnection actions, the PC/laptop/server will be quarantined temporarily to prevent any vulnerabilities to penetrate the network. Restoration actions will need to be coordinated by the SA through the NCC, or SAs/users can call the Communications Focal Point at 366-2666 to get put back online once the system is patched to an approved security baseline.

4.18.3. **(Added-ANDERSONAFB)** . Andersen Vulnerability Scan process: the 36 CS NCC is responsible for conducting a vulnerability scan, using an AF approved vulnerability scanner. The scans conducted by the NCC are performed for compliance reporting and identification of failed patch automation actions. Weekly scans occur Tuesday and Wednesday for SIPRNET. NIPRNET scans are started on Monday. SAs are responsible for ensuring their squadrons SIPR computers are online from 0730 through 1630 for vulnerability scanning. Systems found to be high risk for vulnerabilities due to not meeting uptime windows, will have a risk assessment done by the 36 CS to send a recommendation to the 36th Wing Commander (36 WG/CC) to either accept risk based on mission requirements, or disconnect the device based on network security implications. uptime requirements may be temporarily denied network access until top vulnerabilities are patched. NCC weekly scan results can be made available on request by the appropriate SA for situational awareness and compliance validation efforts.

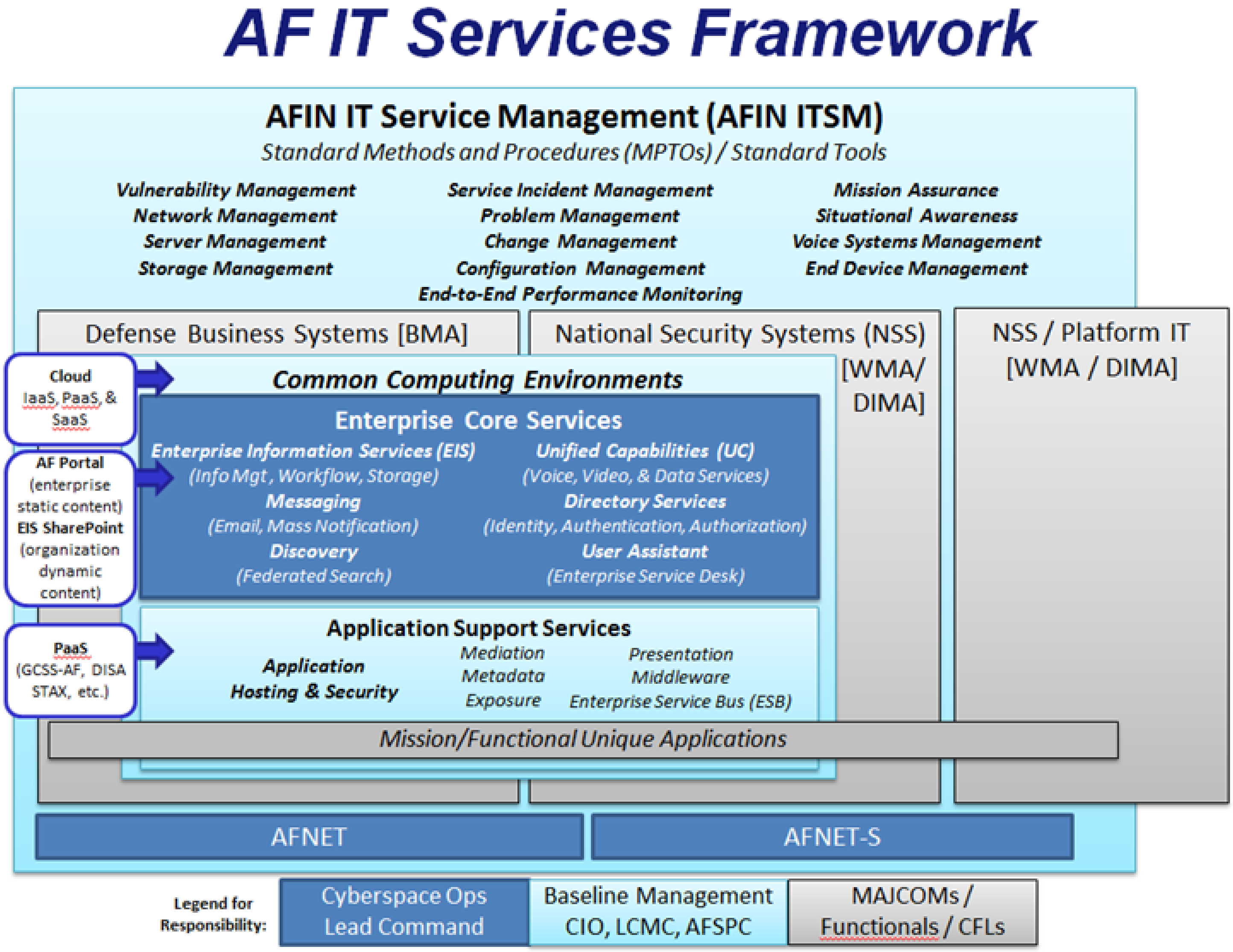
4.18.3.1. **(Added-ANDERSONAFB)** . Andersen NCC will process an 'all audits' scan on AFNET and AFNET-S during the first week of each month; results of these scans are published to a vulnerability file share on NIPRNET and on SIPRNET before the end of the week. If vulnerability scanning tools are unavailable due to technical issues, the most recent valid scan takes precedence and will be uploaded instead. Scorecards for each PMO are placed into this file share for PMOs to review and take action. Andersen SAs are responsible for reviewing the results of the 'all audits' and score cards and take actions to meet compliance requirements by the end of the second week of each month.

4.18.3.2. **(Added-ANDERSONAFB)** . Andersen SAs must take actions to coordinate any POA&M requests if needed by the end of the third week of each month. Failure to review and take actions before the end of the third week may result in the identified systems being subject to the actions specified in paragraph 4.18.2.1 of this instruction. Andersen NCC will review and continue to process any/all POA&M requests and assist with patching efforts during the fourth week of each month.

4.18.4. **(Added-ANDERSONAFB)** . NIPRNET AND SIPRNET computers inactive for 30 days or more will be subject to actions specified in paragraph 4.18.2.1 of this instructions.

5. AF IT Services Framework. The AF IT Services Framework, as an ITSM framework, provides foundation which integrates and manages the AFIN, enterprise core services, and solutions to support the AF portion of the DoDIN and the DoD Information Enterprise as defined by DoDD 8000.01. AF IT Services are functionally aligned to the Defense Information Enterprise Architecture and its activities. AF IT Services may not be provided by a single entity but are instead a federated, shared capability among several organizations. The services will be developed, operated and maintained in accordance with the Target, Implementation, and Operational Baselines and the processes defined by this publication and supporting MPTOs. Mission/Functional Unique Applications may be supported and defined as a new AF IT Services as their usage and scope increases across the enterprise supporting the AF usage of a previously functional unique application. Additional AF IT Services will be initially designated in the Target or Implementation Baseline as appropriate with requests and changes to the Baselines managed by the Air Force Consolidated Enterprise Information Technology Baseline (AF CEITB).

Figure 2. AF IT Services Framework.


AF IT Services Framework
AFIN IT Service Management (AFIN ITSM)
Standard Methods and Procedures (MPTOs) / Standard Tools
Vulnerability Management
Network Management
Server Management
Storage Management
Service Incident Management
Problem Management
Change Management
Configuration Management
End-to-End Performance Monitoring
Mission Assurance
Situational Awareness
Voice Systems Management
End Device Management
Defense Business Systems [BMA]
National Security Systems (NSS) [WMA/ DIMA]
NSS / Platform IT [WMA / DIMA]
Cloud IaaS, PaaS, & SaaS
AF Portal (enterprise static content) EIS SharePoint (organization dynamic content)
PaaS (GCSS-AF, DISA STAX, etc.)
Common Computing Environments
Enterprise Core Services
Enterprise Information Services (EIS)
(Info Mgt, Workflow, Storage)
Messaging
(Email, Mass Notification)
Discovery
(Federated Search)
Unified Capabilities (UC)
(Voice, Video, & Data Services)
Directory Services
(Identity, Authentication, Authorization)
User Assistant
(Enterprise Service Desk)
Application Support Services
Application Hosting & Security
Mediation
Metadata
Exposure
Presentation
Middleware
Enterprise Service Bus (ESB)
Mission/Functional Unique Applications
AFNET
AFNET-S
Legend for Responsibility:
Cyberspace Ops Lead Command
Baseline Management CIO, LCMC, AFSPC
MAJCOMs / Functionals / CFLs

5.1. **AF IT Services Management (AF ITSM).** AF IT Service Management is established as IT components, infrastructure, and processes (e.g., Network Management, Vulnerability Management) enabling effective operations and defense of the AFIN and the IT services. AF IT Service Management creates a trusted environment capable of protecting and maintaining the integrity, quality, and availability of the AFIN. All terrestrial, space and airborne networks will inherit the capabilities of AF IT Service Management, reference AFPD 33-5, *Warfighting Integration* for establishment of a fully integrated, flexible and net-centric family of systems, networks and architectures bridging theater warfighting, combat support, global/functional capabilities and infrastructure enterprises. Non-traditional services that are being migrated onto the Internet Protocol (IP) network (e.g., IP telephony, video teleconferencing) will need to be managed for both non-standard or legacy systems and newer IP-based implementations until all legacy systems are removed from the AF.

5.1.1. **Vulnerability Management**. Vulnerability Management is established as the practice of identifying AFIN hardware and software vulnerabilities, performing risk analysis, prioritizing mitigation actions based on levels of risk deemed acceptable by an appropriate commander, and remediating and/or mitigating the vulnerabilities to proactively prevent exploitation. This service area includes all AFIN systems and components, and the complete cycle of identification, classification, remediation, and mitigation of vulnerabilities. Vulnerability Management also includes patching, tracking, and testing. *Note: Special precautions are taken with Command, Control, Intelligence, Surveillance, and Reconnaissance mission systems and non-standard or legacy systems to ensure automated vulnerability fix actions do not degrade operational missions.* Specific methods and procedures are in MPTO 00-33A-1109, *Vulnerability Management*.

5.1.2. **Network Management**. Network Management is established as the ability to monitor, control, configure, and optimize networks, systems, services and the underlying physical assets that provide end-user services, as well as connectivity to enterprise application services all in accordance with the applicable DISA Security Technical Implementation Guides (STIGs). Network Management includes the activities, methods, processes, procedures, capabilities, tools, and resources that pertain to the operation, administration, logging, maintenance, and provisioning of networked systems. Network Management begins with the background situational awareness of network configuration and performance of networks. Network Management shall have and use automated Configuration Management and PBNM according to DoDI 8410.03. Specific procedures are in MPTO 00-33A-1106, *Air Force Information Network (AFIN) Network Management*.

5.1.3. **Server Management**. Server Management is established as the activities, methods, processes, procedures, capabilities, tools, and resources that pertain to the operation, administration, monitoring, configuration, and maintenance of the hardware and software components of a server in accordance with the applicable DISA STIGs. Server Management includes coordination of server requirements for environmental and facility support, installation and deployment, monitoring, configuration, and security. Specific methods and procedures for Server Management are in MPTO 00-33A-1113, *AFIN Server/Storage Management and Application Hosting*.

5.1.4. **Storage Management**. Storage Management is established as the activities, methods, processes, procedures, capabilities, tools, and resources that provide for the storage, retrieval, availability, backup and recovery, destruction, labeling, quota management, security, and confidentiality of user data on the AFIN in accordance with the applicable STIGs. Storage Management also includes the administration, configuration, and monitoring of the storage media and devices. Specific methods and procedures for Storage Management are in MPTO 00-33A-1113, *AFIN Server/Storage Management and Application Hosting*.

5.1.5. **Service Incident Management**. Service Incident Management is established as the activities, methods, processes, procedures, capabilities, tools, and resources used to restore normal service operations as quickly as possible. A service incident is any event (network security, network management, etc.) which is not part of standard operations and causes an interruption or reduction of the quality of service. A service incident is categorized under three major ticket models as Standard (applications, services, networks, etc.), Major (accelerated workflow with reduced escalation timelines), or Security (handling follows security incident guidance) with separate procedures and workflows for each major type. The goal of Service Incident Management is to minimize the adverse effect on operations, ensuring the best possible levels of service and availability are maintained. Service Incident Management is directly linked to management of the physical infrastructure and should focus on identifying infrastructure issues and documenting corrective actions or changes needed to prevent incidents in the future. Specific procedures for Service Incident Management are in the MPTO 00-33A-1112, *Air Force Network Enterprise Service Desk Service Incident Management*. Security incident procedures will be published in MPTO 00-33B-5007, *Security Incident Management for Information Systems.* Cyber incident procedures will be published in AFI 10-1702, *Cyber Incident Handling*.

5.1.6. **Problem Management**. Problem Management is established as the activities, methods, processes, procedures, capabilities, tools, and resources used to identify and resolve the root causes of service incidents and prevent their recurrence. A "problem" is a condition typically identified as a result of multiple service incidents that exhibit common symptoms, share related mission impacts, or share a common root cause. Problem Management includes event correlation, trend analysis, problem diagnosis, root cause analysis, and knowledge basing to provide a user-level knowledge base of answers and resolutions to common user-level issues. Specific procedures for Problem Management are in MPTO 00-33A-1114, *AFIN*ictect*Problem Management*.

5.1.7. **Change Management**. Change Management is established as standardized activities, methods, processes, and procedures used to effectively manage and control all changes to the AFIN Operational Baseline, minimizing risk, disruptions in service and adverse impacts to operational users. A "change" is the addition, modification or removal of anything that could have an effect on IT services, configuration, processes, security, etc. Change Management focuses on documenting changes to the network. This includes documenting updates made to maps, drawings, network layouts, Virtual Local Area Network (VLAN) Architectures, IP addresses, and network configurations. Linkages identified such as base level drawings must be included in the CSI blueprint. The change management process must begin at the base level and extend to the AF level to ensure all requirements are contained in one process. Multiple change management processes must be consolidated and a governing group be formed to focus on change management. Change management and configuration management must be a dynamic process. Any change to the network must be automatically reflected in the visualization of the network configuration. It is critical to clarify the relationship between change management and vulnerability management. Vulnerability management is change management responsiveness to security-directed changes. Specific procedures for Change Management are published in MPTO 00-33A-1100, *AF-GIG Operational Change Management Process*.

5.1.8. **Configuration Management**. Configuration Management is established as the activities, methods, processes, procedures, capabilities, tools, and resources which establish and maintain thorough, documented baselines of the hardware and software configuration items of the AFIN, including the features, attributes, technical configuration, and documentation of the components. Configuration Management defines those items that are configurable, those items that require formal change control, and the process for controlling changes to such items. Configuration Management is vital to network and system stability and will be automated to support Network Management according to DoDI 8410.03. Before changes are introduced into a network or system, they must be properly reviewed, approved and documented following Change Management methods and procedures. Specific procedures for Configuration Management will be in the *Configuration Management MPTO.*

5.1.9. **End-to-End Performance Monitoring**. End-to-End Performance Monitoring is established as deliberate, proactive monitoring and capacity planning of all the hardware and software components of the AFIN which enables all AF IT Services including mission/functional unique applications. It supports mission assurance by including the end user experience and the warfighter's ability to access critical information. End-to-End Performance Monitoring includes the activities, methods, processes, procedures, capabilities, tools, and resources which allow cyber professionals to rapidly identify, isolate, and resolve service incidents before they cause significant degradation or poor performance resulting in mission impact. Monitoring, measuring, performance analysis, and optimizing networks and networked systems are included in the scope. Capacity Planning includes the long trend analysis of network devices including servers, and should be performed in order to identify future constraints with the results incorporated into either future Technical Baselines. Service and application performance is affected by both the performance of the network and performance of the servers and applications providing the service. As the operator of the network, 24 AF has the ultimate responsibility for determining the network elements to be monitored, the thresholds that must be established, and the appropriate responses to results that fall outside the established thresholds. 24 AF must coordinate with the network owner (e.g., DISA, Army, etc.) if monitoring spans networks outside of AF control. End-to-End Performance Monitoring applies to the NIPRNET and the SIPRNET, and all other terrestrial, space and airborne networks – anywhere a network can be hosted – for all entities (Active, Guard, & Reserve). Specific procedures for End-to-End Performance Monitoring will be in the *End-to-End Performance Monitoring MPTO.*

5.1.10. **Mission Assurance**. Mission Assurance is established as the actions taken to ensure operational users can leverage AFIN systems and command/functional unique systems to execute operational missions. This includes activities, methods, processes, procedures, capabilities, tools, and resources that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Continuity of operations, disaster recovery, risk management, and “fighting through an attack” are also critical aspects of Mission Assurance. Mission Assurance requires traceability of mission dependencies on cyberspace capabilities to provide prioritization of all other AFIN activities and provide the mission context for Situational Awareness. This applies to all components of the AF IT Services Framework. Specific procedures for Mission Assurance will be in the *Mission Assurance and Situational Awareness MPTO.*

5.1.11. **Situational Awareness**. Cyberspace Situational Awareness (SA) is the requisite current and predictive knowledge of cyberspace and the operating environment upon which cyberspace operations depend, including all factors affecting friendly and adversary cyberspace forces (JP 3-12). Situational Awareness is enabled by the activities, methods, processes, procedures, capabilities, tools, and resources which provide meaningful and relevant end-to-end visibility incorporating data from End-to-End Performance Monitoring and other management data into a common operational picture by providing the operating status, location, performance, and utilization of AFIN hardware and software, both (a) within context as AFIN resources and (b) within the context of the mission(s) those resources are supporting. Specific procedures for Situational Awareness will be in the *Mission Assurance & Situational Awareness MPTO.*

5.1.12. **Voice Systems Management.** Voice Systems Management is established as the ability to monitor, control, configure, and optimize voice systems. Voice Systems Management includes the activities, methods, processes, procedures, capabilities, tools, and resources that pertain to the operation, administration, maintenance, and provisioning of voice systems. Voice Systems Management will be undergoing significant change as a part of the DoD category of Unified Capabilities (UC), as stated in the AF UC Master Plan and DoDI 8100.04, *DoD Unified Capabilities (UC)*. To optimize support of real-time voice (video, etc.) requirements in the future, systems and data networks must be optimized to meet the unique requirements of UC while eliminating specific system stovepipes to provide quality of service (QoS) needs for Voice over Internet Protocol (VoIP) and UC. Additional guidance for Voice Systems Management is available in AFMAN 33-145, *Collaboration Services and Voice Systems Management.* Specific procedures for Voice Systems Management will be in MPTO 00-33A-1108 *Voice Systems Management.*

5.1.13. **End Device Management**. End Device Management is established as the installation and deployment, monitoring, configuration, maintenance, and security of end devices on the AFIN. End devices are items such as desktop PCs, laptops, notebooks, tablet PCs, smartphones, executive mobile devices, VoIP phones, IP-enabled sensors/alarms, etc. Specific procedures for End Device Management will be in the *End Device Management MPTO.*

5.2. **Enterprise Core Services**. Enterprise Core Services are standard IT capabilities available to all users on the AFIN. Enterprise Core Services support DoD Net-Centric strategies for data and services by enabling users to safeguard, compile, catalog, discover, cache, distribute, retrieve, and share data in a collaborative environment across the AF and DoD enterprises. As DoD establishes joint enterprise services under JIE, the AF will evaluate the transition of AF enterprise core services when appropriate. 24AF will operate AF enterprise services not provided by JIE, and/or those JIE enterprise services being provided by the AF to all DoD customers.

5.2.1. **Collaboration**. Collaboration services are established as the capabilities and resources that allow communications and interactions across the AFIN enterprise, including voice, video, data, and visual representation. This includes those capabilities which may be bundled into Unified Capabilities (UC). UC are defined as the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities (DOD Unified Capabilities Requirements 2013). Examples may include web conferencing, application and desktop sharing, presence, chat, video teleconferencing, VoIP, white boarding, chat rooms, and online forums. Additional guidance for Collaboration is in AFMAN 33-145, *Collaboration Services and Voice Systems Management* and DoDI 8100.04, *DoD Unified Capabilities* (*UC*).

5.2.2. **Messaging**. Messaging services are established as the exchange of electronic message traffic between all users and organizational entities on the AFIN. Messaging services include the ability to compose, read, store, forward, manage, prioritize, digitally sign/encrypt, and track delivery/receipt of electronic messages. The AF is transitioning messaging services to cloud services utilitzing DISA Enterprise Email (DEE). Examples may include email, Instant Messaging and Voicemail. Specific user procedures for Messaging are in AFMAN 33-152, *User Responsibilities and Guidance for Information Systems* and incorporated in UC covered by AFMAN 33-145.

5.2.3. **Discovery**. Discovery services are established as the capabilities and resources that enable users to identify, search, locate, and retrieve information across the AFIN. Discovery services include the ability to catalog and index information, identify applicable data repositories, formulate search queries/criteria, and retrieve/deliver relevant information to users in a timely fashion. This is a critical capability enabler for change management, configuration management, policy based management, and performance analysis as described above. Specific procedures for Discovery will be in the *Discovery and Information Management MPTO.*

5.2.4. **Enterprise Information Services (EIS)**. Enterprise Information Services will provide a solution across the entire AF by enabling organizations to communicate and collaborate vertically and horizontally with all EIS capabilities, optimizing the use of available bandwidth by using the most effective capabilities for the operational environment. Warfighters will utilize Knowledge Operations (KO) capabilities to drive operational effects through improved decision-making processes. Warfighters will pull required information and knowledge smartly, push information for continuous collaboration across the unified communications domain, and receive the right information at the right time and in the right format through advanced collaboration techniques (i.e., integrated people, processes and technology) via a proactive push from all integrated operations and support functions. Enterprise Information Services effectively capitalize upon KO performed by commanders, who integrate all AF functional areas into refined staff organizations, internal battle rhythms, and routine interactive sessions with subordinate commanders worldwide. The KO vision of a “One AF—One Enterprise” to fundamentally change the way the AF uses, delivers, and manages knowledge to perform peacetime missions and wartime operations across an integrated AF enterprise recognizes the imperative for a proactive means to promote collaboration, the sharing of ideas, and to find solutions to common problems across the entire AF. It also promotes the ability to learn, innovate, decide, and act, faster than our adversaries while operating in a condition of persistent conflict. Enterprise Information Services are established as the capabilities and resources supporting the security, reliable storage, timely delivery and deduplication of information across the AFIN enterprise. Examples include common and private data/file service, workflow management service, and enterprise print service. These services will be implemented and sustained according to AFPD 33-3, *Information Management*. Specific procedures for Information Management will be in the *Discovery and Information Management MPTO.*

5.2.5. **Knowledge Management (KM)**. Knowledge Management (KM) is the capturing, organizing, and storing of knowledge and experiences of individual workers and groups within an organization and making this information available to others in the organization. KM is the art of creating, organizing, applying, and transferring knowledge to facilitate situational understanding and decision making. (AFSPC Enabling Concept for Knowledge Operations, May 2011)

5.2.6. **Application Hosting.** Application Hosting services are established as hosting environments that are architecturally compliant, consistent, reliable, and secure computing environments (consisting of application software and associated utilities) supporting AF IT Services, Enterprise Core Services, Application Support Services, and mission/functional unique applications and systems. All Application Hosting will migrate to Common Computing Environments and Cloud Services, see **paragraph 5.3**, no later than end of Fiscal Year (FY) 2018 (FY18) according to DoD guidance. Specific procedures for Application Hosting are in MPTO 00-33A-1113, *AFIN Server/Storage Management and Application Hosting.*

5.2.7. **User Assistant.** User Assistant services are established as the personnel, activities, methods, processes, procedures, capabilities, tools, and resources providing an interface to AFIN users for customer service functions, including service incident/problem reporting, IT service requests, service incident prioritization, operational impact reporting, and escalation to mission/functional unique application help desks. The primary AFIN organization designated for user assistance is the AF ESD. Specific Procedures are in the MPTO 00-33A-1112, *Air Force Network Enterprise Service Desk Service Incident Management.*

5.2.8. **Directory Services.** Directory Services are established as the activities, methods, processes, procedures, capabilities, tools, and resources that provide, operate, and maintain a global directory of AFIN users, objects, and resources. Directory services include appropriate identity and attribute information, allowing effective enterprise-wide identity management, authentication, and authorization to AFIN resources. Directory Services are sourced from and rely on a number of AF and DoD organizations for account management and data accuracy. Specific procedures for Directory Services will be in the *Directory Services MPTO.*

5.3. **Common Computing Environments and Cloud Services.**

5.3.1. The DoD CIO Cloud Computing Strategy (2012) provides Federal and DoD mandates for cloud computing adoption and identifies the three major benefits as efficiency, agility, and innovation. The DoD Cloud Computing Goal is to *"implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the Department's mission, anywhere, anytime, on any authorized device."*

5.3.2. Common computing environments authorized for hosting AF core enterprise services, applications, and systems are limited to IPNs, CDCs, and cloud services provisioned by DISA.

5.3.3. The DoD and the AF must take advantage of the commoditized IT functions and transform the way in which they acquire, operate, and manage IT in order to realize increased efficiency, effectiveness, and security. The DoD has begun this transformation in a reengineered information infrastructure called the Joint Information Environment (JIE). The JIE is comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs). The DoD Enterprise Cloud Environment is a key component to enable the DoD to achieve JIE goals.

5.3.4. Cloud computing supports the DoD JIE and provides capabilities for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) as described in DoD CIO Memorandum, *DoD Cloud Computing Strategy Memorandum*, 5 July 2012.

5.3.4.1. Infrastructure as a Service (IaaS) - Virtualized systems operated on fundamental computing resources (e.g., processing, storage, network) managed as a cloud service with the AF retaining control of operating systems, storage, and deployed applications.

5.3.4.2. Platform as a Service (PaaS) - A cloud computing platform providing operating systems, database systems, web servers, security, etc. for hosting of AF unique applications. The AF is only retaining control of the hosted unique application(s) and not the operatiosn systems, database systems, web servers, security, etc.

5.3.4.3. Software as a Service (SaaS) - All aspects of standard applications are provided as a cloud service to the AF. The AF does not retain control over the applications, platform or infrastructure.

5.3.5. Organizations will work with Managed Services Office within PEO C3I&N, as the AF Cloud Service Lead, to coordinate all cloud computing technical requirements prior to engaging with DISA as the DoD cloud broker. Once DISA has developed cloud solutions across the ECSB Security Model and a waiver process, all AF cloud activities will be coordinated with the cloud broker.

5.3.5.1. Cloud computing requirements will be grouped by the DoD ECSB Security Model to maximize data types of Unclassified-Public, Unclassified-Private, Controlled Unclassified Information (CUI), and Classified. The priority of effort should focus on requirements for unclassified cloud computing in alignment with initial DoD ECSB efforts.

5.3.5.2. Program managers will ensure that cloud computing technical requirements for their acquisition programs are in compliance with the DoD Enterprise Cloud Environment. Submit cloud computing technical requirements for review to PEO

C3I&N as the AF Cloud Service Lead: AFLCMC/HNI Workflow, **aflcmc.hni.workflow2@us.af.mil.**

5.3.6. Organizations will maintain responsibility for their application and capabilities built on a cloud service and/or identified as a government responsibility in any applicable documentation for cybersecurity or approvals to operate for the cloud service.

5.3.6.1. Maintain AFIN networthiness by complying with AF AO (previously known as DAA) direction for executing secure operations functions within their operated portions of the AFIN extending to cloud services.

5.3.6.2. Ensure information systems and applications utilizing cloud computing services follow the DoD Provisional Authroization process and receive Certification and Accreditation (C&A) from the AF AO or designated Functional AO according to AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*. C&A will utilize cybersecurity control inheritance for cybersecurity controls provided by the cloud service. SaaS with a full C&A decision from the DoD ECSB's AO does not require further C&A review.

5.3.6.3. Ensure Computer Network Defense Service Provider (CNDSP) and cybersecurity continuous monitoring requirements are met for cloud services used by the organization. Provide any additional resources required for a CNDSP to meet these requirements.

5.3.6.4. Web servers, services, applications, or capabilities for processing non-public information to be hosted on commercial servers or services (including cloud computing services) outside of military or government cybersecurity boundaries requires DoD Provisional Authorization and AF AO approval for use regardless of applicability of C&A requirements.

5.4. **Application Support Services**. Application Support Services should be provided by the Common Computing Environments. Application Support Services are the middleware and common services which enable cross-community of interest (COI) sharing of information and capabilities (exposure services, metadata repositories, mediation/translation, etc.). Application Support Services provide a set of tools, capabilities, processes, and methodologies to support enablement of a Service Oriented Architecture (SOA) for the AF and DoD enterprises.

5.4.1. **Mediation.** Mediation services are established as data aggregation, correlation, or transformation processing; data translation or fusion; negotiation services (brokering, trading and auctioning services); subscription and publication services, and workflow coordination services. Typically, mediation services intercept and modify messages that are passed between existing services (providers) and clients (requesters).

5.4.2. **Metadata.** Metadata is descriptive information about a particular data set, object, or resource, including how it is formatted, and when and by whom it was collected. Metadata services are established as procedures, guidelines, and methods for effective data planning, analysis, standards, modeling, configuration management, storage, retrieval, protection, validation, and documentation of metadata. Metadata will follow the DoD Metadata specification according to DoDI 8410.03. Although metadata most commonly refers to web resources, it can be about either physical or electronic resources.

5.4.3. **Exposure.** Exposure services are established as procedures, guidelines, and methods for making web services visible and discoverable. This exposure or visibility allows web services to be discovered or searched using service registries. Once web services are exposed and discovered or searched, a data or service consumer (person or machine user) can determine if the service/data is viable for consumption and use.

5.4.4. **Presentation.** Presentation services are established as the presentation layer for user access to an application. The presentation layer of an application can vary from a simple Web-based front end to a heavy client that has the user interface.

5.4.5. **Middleware.** Middleware services are established as the computer software that connects software components or people and their applications. The software consists of a set of services that allows multiple processes running on one or more machines to interact. This technology evolved to provide for interoperability in support of the move to coherent distributed architectures, which are most often used to support and simplify complex distributed applications. It includes web servers, application servers, and similar tools that support application development and delivery. Middleware is especially integral to modern information technology based on eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), Web Services, and Service Oriented Architecture (SOA).

5.4.6. **Enterprise Service Bus (ESB).** The Enterprise Service Bus is established as the construct for a standards-based integration platform that combines messaging, web services, data transformation, and intelligent routing to reliably connect and coordinate interactions of significant numbers of diverse applications across extended enterprises with transactional integrity. ESB integration fabric infrastructure shall include highly distributed, scalable service containers; event-driven change invocation; centralized management of distributed integration configurations; diverse client connectivity and support for multiple protocols; seamless, dynamic routing of data across physical deployment boundaries; unified security and access control model; distributed configuration and caching of deployment resources, such as Extensible Stylesheet Language Transformations (XSLT) documents and routing rules; scriptable and declarative environment.

5.5. **Mission/Functional Unique Applications (MFUAs)**. Mission and Functional-Unique Applications are IT applications and/or systems which provide a mission-specific capability to one or more communities of interest, funded and managed by the requirements' owners. MFUAs rely on services from AF ITSM, Enterprise Core Services, and Application Support Services to function. Owners of MFUAs must use the information within this AFI and corresponding MPTOs to ensure their systems can efficiently interface with and leverage all applicable AF IT Services. MFUAs will adhere to applicable Baseline standards in accordance with **paragraph 6** and AFPD 33-4. MAJCOMs are responsible for managing and sustaining MAJCOM-unique systems. MFUA owners are responsible for reporting information, cost, plans, and status of applications to their respective MAJCOMs, SAF CIO, and Cyber CFL when requested.

6. AFIN Baseline Management. The Target, Implementation, and Operational Baselines address the technical standards, protocols and guidance to establish a consistent environment for IT capability engineering, development, deployment and support, see AFPD 33-4 for more information. The Baselines are prescriptive and include those things required to ensure a repeatable and predictable process by which to develop and deploy IT capabilities and of the infrastructure on which they operate. The Baselines apply to both AF-controlled portions of the NIPRNET and SIPRNET environments. Future technical standards, protocols, guidelines, and implementation constraints are provided by the Target Baseline. Selected products and their informed/allowed configurations are provided by the Implementation Baseline. Currently operational AF IT Services and their usage are provided by the Operational Baseline.

7. Operation of AF IT Services within the AFIN.

7.1. **Command and Control (C2) of the AFIN.** C2 of the AFIN is conducted to operate, secure, defend, maintain, and control the AFIN for the purposes of DoDIN Operations and Defensive Cyberspace Operations (DCO).

7.1.1. Operational type orders for C2 of the AFIN are defined and issued according to AFI 10-1701.

7.1.2. Operational type orders, AF TCTOs, and TCNOs issued for C2 of the AFIN take precedence over TOs, MPTOs, and TCTOs issued by PMOs, SPOs, and other organizations directing the standard operation and maintenance of the AFIN.

7.2. **Technical Orders (TOs).** The purpose of the Air Force Technical Order (TO) system in supporting AF IT Service Management is to provide clear and concise instructions for safe and reliable operation, inspection and maintenance of centrally acquired and managed AF systems and commodities.

7.2.1. Technical publications are essential for the proper function of AFIN Operations and to provide the operations activity with accurate information. Technical publications include TOs, MPTOs, commercial manuals, and specialized publications.

7.2.2. Technical publications for AF IT Service Management are developed and verified according to AFI 63-101, TO 00-5-1, *AF Technical Order System,* and TO 00-5-3, *AF Technical Order Life Cycle Management.*

7.2.3. All organizations supporting AF IT Service Management order TOs following procedures in TO 00-5-1.

7.2.4. Report any errors, contradictions, or procedures requiring clarification, by following procedures in TO 00-5-1 on preparing AFTO Form 22, *Technical Manual (TM) Change Recommendation and Reply***.**

7.2.5. Compliance with AF IT Service Management TOs is mandatory, except as explained in TO 00-5-1.

7.3. **Method and Procedure Technical Orders (MPTOs).** Air Force 00-series MPTOs are procedure-oriented and provide general methods and procedures standardizing processes across the AF and are used to standardize AF IT Service Management. MPTOs are available for ordering through the Enhanced Technical Information Management System (ETIMS) application on the AF Portal, per TO 00-5-1. Contact unit Technical Order Distribution Office (TODO) for assistance.

7.3.1. AF IT Service Management MPTOs standardize AFIN ITSM processes and procedures and may integrate the operation of individual systems under AF IT Services. A full list of MPTOs directed by this AFI is located within **Attachment 1**.

7.3.2. TOs published for specific systems take precedence over AF IT Services MPTOs.

7.4. **Time Compliance Technical Orders (TCTOs).** TCTOs document all permanent modifications, update changes and retrofit changes to standard Air Force systems and commodities.

7.4.1. TCTOs are managed and issued according to TO 00-5-15, *Air Force Time Compliance Technical Order Process*.

7.4.2. TCTOs are military orders issued by order of the SECAF and as such, shall be complied with as specified in the TCTO.

7.5. **Time Compliance Network Orders (TCNOs).** TCNOs are downward-directed security or vulnerability-related orders issued by the AF.

7.5.1. TCNOs are generated internally to the AF or in response to an Information Assurance Vulnerability Alert (IAVA) or Information Assurance Vulnerability Bulletin (IAVB) to direct the implementation of an operational or security vulnerability risk mitigation procedure or fix action (countermeasure).

7.5.2. TCNOs are managed and issued according to MPTO 00-33A-1109, *Vulnerability Management* and under the authority of AFI 10-1701.

7.6. **One AF-One Network.** The lead command for Cyberspace Operations directs the operation, maintenance, configuration, and control of AF network infrastructure with the goal and objective of providing a single network for the AF that is managed, commanded/controlled, and fully compatible with a seamless DoD network.

7.6.1. **Core Data Center (CDC):**

7.6.1.1. CDCs are highly capable, highly resilient data centers providing standardized hosting and storage services to the enterprise within the Single Security Architecture (SSA) now being implemented. CDCs are the backbone of JIE and approved by DoD CIO.

7.6.1.2. CDCs also enable a significant reduction in the total number of DoD data centers by serving as consolidation points for computing and storage services currently hosted across hundreds of Component Facilities in accordance with DoD CIO memorandum, *Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration*, 11 July, 2013.

7.6.1.3. All AF organizations will plan for systems to be hosted within an approved CDC NLT end of FY18, (T-0).

7.6.2. **Area Processing Center (APC):**

7.6.2.1. An APC is a facility which provides enterprise and regional computing and data centers supporting Enterprise Core Services and provides Application Hosting as an Enterprise Core Service for Mission/Functional Unique Applications.

7.6.2.2. Per DoD CIO guidance (1 Nov 2012), APCs will either convert to IPNs or close as approved by the ITGEB. APCs will meet DoD standards for facility and network infrastructure, security, technology and operations, and adhere to DoD enterprise governance, (T-0).

7.6.2.3. If not designated as a CDC, organizations will plan for transition of systems to a designated CDC under JIE construct, (T-0).

7.6.3. **Installation Processing Node (IPN):**

7.6.3.1. An IPN is a facility which provides a consolidated base-level computing and data processing node for all NIPRNET and SIPRNET systems which are unable to be hosted at a DoD enterprise-level data center (e.g., CDC) based upon validated Disconnected, Intermittent, Limited (DIL) requirements.

7.6.3.2. IPNs will be designated by the ITGEB when sites are approved as an AF data center, (T-0).

7.6.3.3. IPNs will provide 24-hour, 7-days a week on-site hardware maintenance, environmental control, space utilization, and physical security of the base-level processing node.

7.6.3.4. IPNs will conform to the AF's implementation of FDCCI.

7.6.4. **Installation Services Node (ISN):**

7.6.4.1. An ISN is the required localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the enterprise.

7.6.4.2. Potential services include anomaly detection, audit functions, Active Directory (AD), DNS, Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), and print services. In addition, ISNs may also host unified capabilities (UC) that must remain on the Installation to enable emergency services even when the connection is interrupted.

7.6.5. **Special Purpose Processing Node (SPPN):**

7.6.5.1. A SPPN is a facility which provides a fixed processing node supporting data servers and special purpose functions that cannot be supported by a IPN, CDC, or other DoD enterprise-level data center due to its association with mission specific infrastructure or equipment.

7.6.5.2. SPPNs will be designated by the ITGEB when sites are approved as an AF data center, (T-0).

7.6.5.3. SPPNs will be supported and maintained by the functional community of interest requiring the SPPN.

7.7. **Cybersecurity (previously known as Information Assurance[IA]).** All systems (e.g., centrally managed applications) will comply with AF Cybersecurity program guidance in AFI 33-200, *Information Assurance (IA) Management*, DOD Cybersecurity program guidance, and U.S. Strategic Command (USSTRATCOM) warning and tactical directives/orders (e.g., Information Assurance Vulnerability Management (IAVM) program, security incident handling program, and other responsibilities outlined in CJCSI 6510.01, *Information Assurance (IA) and Support to Computer Network Defense (CND)*).

7.7.1. Authorizing Official (AO) (previously known as Designated Accrediting Authority [DAA]**)** Approval. All systems must receive accreditation and authorization to operate by the appropriate AO prior to operational use according to AFI 33-210.

7.7.2. Reciprocity, Reuse, and Inheritance. The AF recognizes and fully supports reciprocity and reuse according to AFI 33-210. In order to minimize certification and accreditation (C&A) workload and paperwork, AOs and Information Systems Security Manager (ISSM), (previously known as IAM) will fully embrace and support inheritance in which AF IT Services and mission/functional unique applications inherit security controls and other Cybersecurity attributes as reuse from other associated services, hosting environments, security solution, etc., as appropriate. Cybersecurity policy takes precedence if Cybersecurity policy provides specific guidance for inheritance in the future.

7.8. **Commercial Internet Service Provider (ISP) Connections and DoDIN Wavier Process.**

7.8.1. A DoDIN Waiver (previously known as DOD GIG Waiver) is required for any internet connection not utilizing the DoDIN infrastructure/transport services to allow a direct unfettered and non-attributable connection to the public Internet in the performance of DoD/AF missions. For more information about DoDIN Waivers and commercial ISPs refer to AFI 33-200. The commercial ISP connection cannot be connected to the NIPRNET (Use of an approved hardware/software secure tunnel across a commercial ISP circuit to connect to the NIPRNET/DoDIN is allowed).

7.8.2. **Quality-of-Life (QoL) Internet Services**. The QoL Internet Services may be established for "patron" activities such as the Family Support Center, library, dormitories, medical treatment facilities, lodging, and other services facilities.

7.8.2.1. For Morale, Welfare and Recreation (MWR) Category A, B, and C activities, refer to AFI 65-106, *Appropriated Fund Support of Morale, Welfare, and Recreation (MWR) and Nonappropriated Fund Instrumentalities (NAFIS)*.

7.8.2.2. For QoL internet access in Dormitories, refer to AFI 32-6005, *Unaccompanied Housing Management*.

7.8.2.3. These systems shall not be connected to the base network/NIPRNET with the privileges of ".mil" registered users.

7.8.2.4. Official business activities and administrative offices in these QoL locations may require and are authorized NIPRNET connectivity through the base network according to AFI 65-106. Refer to AFI 65-106 for the funding of NIPRNET installation, sustainment and management in MWR facilities.

7.8.2.5. Certification and Accreditation (C&A) is not required for QoL Internet Services.

7.8.2.6. Commercial ISPs used as Quality of Life (QoL) internet service for patrons are exempted from the DoDIN Waiver process.

7.8.3. Portions of the AF Services' mission must be conducted outside of the NIPRNET to comply with AF Cybersecurity policies. Although some patron-based activities are supported by the QoL networks, the vast majority of services user base, systems support organizations, and management activities are not permitted to operate on the NIPRNET, but still require identity authentication. AFPC Services Directorate is authorized to connect to commercial ISP nodes to support and manage the Services NAFIS that are not allowed on the NIPRNET according to AFI 65-106.

7.8.4. DOD Dependent Schools and Base Education Offices. Only government personnel and/or government contractors are authorized Internet access through NIPRNET. Internet access for classroom education or civilian education institutions must be through a commercial ISP (or DISA's Private ISP when available) and cannot be connected to the NIPRNET.

7.8.5. Headquarters Air Education and Training Command (HQ AETC) and the United States Air Force Academy (USAFA). HQ AETC and USAFA require academic networks that provide students, faculty, and staff IT services that are not available on the AFNET (i.e., conduct research and scientific collaborations). Consequently, HQ AETC and USAFA are authorized to operate networks specifically designed to IT enable their education and training missions.

7.8.6. Geographically Separated Unit (GSU). The GSU owning MAJCOM is required to provide funding to the supporting base, MAJCOM or AFSPC for any network circuit(s) required for the GSU connectivity. GSUs will comply with all policies and directives of their servicing AFIN Operations activities including the CFP supporting their network circuit.

7.8.7. When available, DISA's Private ISP Service (through AF Guest Network) will be the default method for obtaining direct, unfettered, and non-attributable access to the public Internet in the performance of DoD/AF missions (not MWR or QoL). DISA Private ISP connections will be exempt from the DoDIN Waiver requirements as DISA is the service provider.

7.9. **Sharing Data, Information, and Information Technology Services.** All Authoritative Data Sources (ADSs) should be exposed as Data-as-a-Service (DaaS).

7.9.1. Data shall remain as closely controlled as possible by the ADS steward to ensure its currency and accuracy.

7.9.2. Systems and services shall reference ADSs rather than duplicate or provision external source data for anything beyond short-term consumption or proxying for performance or security reasons.

7.9.3. Sharing of data, information, and IT services shall be managed according to DoDD 8320.02.

7.9.4. Data authentication and control shall be managed according to DoDI 8520.03, *Identity Authentication for Information Systems*.

7.10. **Service Level Agreements (SLA), Memorandums of Agreement (MOA), Memorandums of Understanding (MOU).** SLAs will be established by AFSPC for AF IT

Services to define division of responsibilities for network operations and services to minimize duplication of effort between organizations.

7.10.1. Enterprise service SLAs will be established for ESUs and the AF ESD with approval by the ITGEB.

7.10.2. An MOA, MOU, or Operational Level Agreement (OLA) will be established as appropriate for organizations or users whose network support requirements exceed the standards of an enterprise service SLA.

7.10.3. Whenever possible, SLAs will identify the minimum levels of support required by the users rather than acceptable failure rates (uptime rates as opposed to downtime rates). SLAs will also describe the prioritization of systems and services to meet mission assurance requirements.

7.11. **AFIN Operations Training.** Refer to AFI 33-154, *Air Force On-The-Job Training Products for Cyberspace Support Enlisted Specialty Training* and MPTO 00-33A-1001, for policy and procedures for AFIN Operations training. Cyberspace Operations Training is covered under AFPD 10-17 and AFI 10-1703 Volume 1 *Cyberspace Operations Cyber Crew Training.*

MICHAEL J. BASLA, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

(ANDERSONAFB)

DOUGLAS A. COX, Brig Gen, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

National Defense Authorization Act (NDAA) Fiscal Year 2012, § 2867, *Data Servers and Centers*, 31 December 2011

CJCSI 6510.01, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, 9 February 2011

CNSSI 4009, *National Information Assurance (IA) Glossary*, 26 April 2010

DoD 5012.02-STD, *Electronic Records Management Software Applications Design Criteria Standard*, 25 April, 2007

DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, 10 February 2009

DoDI 5000.02, *Operation of the Defense Acquisition System*, 25 November 2013

DoDI 8100.04, *DoD Unified Capabilities (UC)*, 9 December 2010

DoDI 8320.02, *Sharing Data, Information, and Technology (IT) Services In The Department Of Defense*, 5 August 2013

DoDI 8410.01, *Internet Domain Name Use and Approval*, 14 April 2008

DoDI 8410.02, *NetOps for the Global Information Grid (GIG)*, 19 December 2008

DoDI 8410.03, *Network Management (NM)*, 29 August 2012

DoDI 8520.03, *Identity Authentication for Information Systems*, 13 May 2011

DoDI 8550.01, *DoD Internet Services and Internet-Based Capabilities*, 11 September 2012

DoD CIO Memo, *Approvals/Waivers for Obligation of Funds for Data Servers and Centers*, 26 June 2012

DoD CIO Memo, *Exemption for Obligation of funds for Data Servers and Data Centers Related to the High Performance Computing Modernization Program*, 25 January 2013

DoD CIO Memo, *Approvals/Waivers for Obligation of Funds for Data Servers and Centers*, 9 May 2013

DoD CIO Memo, *Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration*, 11 July 2013

AFPD 10-17, *Cyberspace Operations*, 31 July 2012

AFPD 33-1, *Cyberspace Support*, 9 August 2012

AFPD 33-2, *Information Assurance (IA) Program*, 3 August 2011

AFPD 33-3, *Information Management*, 8 September 2011

AFPD 33-4, *Information Technology Governance*, 17 January 2013

AFPD 33-5, *Warfighting Integration*, 11 January 2013

AFPD 63-1/20-1, *Integrated Life Cycle Management*, 3 July 2012

AFPD 71-1, *Criminal Investigations and Counterintelligence*, 6 January 2010

AFI 10-1701, *Command and Control (C2) of Cyberspace,* 5 March 2014

AFI 10-701, *Operations Security (OPSEC),* 8 June 2011

AFI 10-710, *Information Operations Condition (INFOCON) (FOUO),* 10 August 2006

AFI 33-141, *Air Force Information Technology Portfolio Management and IT Investment Review*, 23 December 2008

AFI 33-150, *Management of Cyberspace Support Activities,* 30 November 2011

AFI 33-154, *Air Force On-The-Job Training Products for Cyberspace Support Enlisted Specialty Training*, 1 May 2013

AFI 33-200, *Information Assurance (IA) Management,* 23 December 2008

AFI 33-210, *Air Force Certification and Accreditation Program (AFCAP),* 23 December 2008

AFI 33-360, Publications and Forms Management, 25 September 2013

AFI 33-401, *Air Force Architecting,* 17 May 2011

AFI 35-102, *Security and Policy Review Process*, 20 October 2009

AFI 35-107, *Public Web Communications*, 21 October 2009

AFI 36-2640, *Executing Total Force Development*, 16 December 2008

AFI 63-101/20-101, *Integrated Life Cycle Management*, 7 March 2013

AFI 63-131, *Modification Program Management*, 19 March 2013

AFI 65-106, *Appropriated Fund Support of Morale, Welfare, and Recreation (MWR) and Nonappropriated Fund Instrumentalities (NAFIS),* 6 May 2009

AFMAN 33-145, *Collaboration Services and Voice Systems Management*, 6 September 2012

AFMAN 33-152, *User Responsibilities and Guidance for Information Systems,* 1 June 2012

AFMAN 33-153, *IT Asset Management*, 19 March 2014

AFMAN 33-363, *Management of Records*, 1 March 2008

Air Force Performance Plan for Reduction of Resources Required for Data Servers and Centers, 31 January 2012

TO 00-5-1, *AF Technical Order System*

TO 00-5-3, *AF Technical Order Life Cycle Management*

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

(Added-ANDERSONAFB) MTO 2014-311-006, *Ensure All Devices with Microsoft Operating System within AFIN and SIPR Domains have an Operational Microsoft System Center Configuration Manager Client Installed*

(Added-ANDERSONAFB) NOTAM 2015-233-005A, *Updated Process for Submitting Plans of*

Action & Milestones (POA&Ms)

MPTO 00-33A-1001 *General Cyberspace Support Activities Management Procedures and Practice Requirements*

MPTO 00-33A-1100, *AF-GIG Operational Change Management Process*

MPTO 00-33A-1106, *Air Force Information Network (AFIN) Network Management*

MPTO 00-33A-1108, AFIN *Voice Systems Management*

MPTO 00-33A-1109, *Vulnerability Management*

MPTO 00-33A-1112, *Air Force Network Enterprise Service Desk Service Incident Management*

MPTO 00-33A-1113, AFIN *Server/Storage Management and Application Hosting*

MPTO 00-33A-1114, AFIN *Problem Management*

MPTO 00-33A-XXXX, *Directory Services*

MPTO 00-33A-XXXX, *Mission Assurance and Situational Awareness*

MPTO 00-33A-XXXX, *Discovery and Information Management*

MPTO 00-33A-XXXX, *End-to-End Performance Monitoring*

MPTO 00-33B-5007, *Security Incident Management for Information Systems*

MPTO 00-33D-2002, *Engineering Installation and Cyberspace Readiness Activities Management*

MPTO 00-33D-3003, *Managing the Cyberspace Infrastructure with the Cyberspace Infrastructure Planning System*

Prescribed Forms

No prescribed forms are implemented by this publication.

Adopted Forms

AFTO Form 22, *Technical Manual (TM) Change Recommendation and Reply*

AFTO Form 265, *Request For Change*

AF Form 847, *Recommendation for Change of Publication*

AF Form 1067, *Modification Proposal*.

Abbreviations and Acronyms

ADS—Authoritative Data Source

AETC—Air Education and Training Command

AF-GIG—Air Force-Global Information Grid

AF CEITB—Air Force Consolidated Enterprise Information Technology Baseline

AFCAP—Air Force Certification and Accreditation Program

AFECMO—Air Force Enterprise Configuration Management Office

AF ESD—Air Force Enterprise Service Desk

AFFOR—Air Force Forces

AFI—Air Force Instruction

AFIN—Air Force Information Networks

AFMAN—Air Force Manual

AFMC—Air Force Material Command

AFNET—Air Force Network

AFNIC—Air Force Network Integration Center

AFPD—Air Force Policy Directive

AFR—Air Force Reserves

AFSPC—Air Force Space Command

AIRCOM—Air Communications

AIS—Automated Information Systems

(Added-ANDERSONAFB) AMAC—Air Force Mission Assurance Center

ANG—Air National Guard

AO—Authorizing Official (previously known as DAA)

(Added-ANDERSONAFB) AOR—Area of Responsibility

APC—Area Processing Center

ASI—Authorized Service Interruptions

C-NAF—Component Number Air Force

C&A—Certification and Accreditation

C2—Command and Control

C3I&N—Command, Control, Communications, Intelligence and Networks

CCB—Configuration Control Board

CCMD—Combatant Command

CDC—Core Data Center

CEIG—Cyberspace Engineering Installation Group

CFL—Core Function Lead

CFP—Communications Focal Point

CI—Counter Intelligence

CIO—Chief Information Officer

CIPS—Cyberspace Infrastructure Planning System

CND—Computer Network Defense

COI—Community of Interest

COOP—Continuity of Operations Plan

COTS—Commercial of the Shelf

CSAF—Chief of Staff of the Air Force

CSI—Cyber Systems Integrator

DaaS—Data-as-a-Service

DAA—Designated Accrediting Authority (now refered to as AO)

DCO—Defensive Cyberspace Operations

DESMF—Defense Enterprise Service Management Framework

DIL—Disconnected, Intermittent, Limited

DIMA—Defense Intelligence Mission Area

DISA—Defense Information Systems Agency

(Added-ANDERSONAFB) DITPR—DoD Information Technology Portfolio Repository

DMZ—Demilitarized Zone

DNI—Director of National Intelligence

DNS—Domain Name Service

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDIN—Department of Defense Information Networks

DOTMLPF—Doctrine, Organization, Training, Material, Leadership & Education, Personnel & Facilities

DRU—Direct Reporting Unit

DSCC—Defense Server Core Configuration

EA—Enterprise Architecture

ECSB—Enterprise Cloud Service Broker

EITSM—Enterprise Information Technology Service Manager

(Added-ANDERSONAFB) eMASS –—Enterprise Mission Assurance Support Service

ESB—Enterprise Service Bus

ESD—Enterprise Service Desk

ESI—Enterprise Software Initiative

ESU—Enterprise Services Unit

FOA—Field Operating Agency

FSA—Functional System Administrator

GIG—Global Information Grid

GSU—Geographically Separated Unit

HQ—Headquarters

IA—Information Assurance

IaaS—Infrastructure-as-a Service

IAVA—Information Assurance Vulnerability Alert

IAVB—Information Assurance Vulnerability Bulletin

IAVM—Information Assurance Vulnerability Management

IbC—Internet-based Capabilities

IB—Implementation Baseline

IC—Intelligence Community

ILCM—Integrated Life Cycle Management

IMDS—Integrated Maintenance Data System

INFOCON—Information Condition

I-NOSC—Integrated Network Operations and Security Center

IP—Internet Protocol

IPN—Installation Processing Node

IS—Information Systems

ISN—Installation Services Node

IT—Information Technology

ITGEB—IT Governance Executive Board

ITIL—Information Technology Infrastructure Library

ITS—Information Transport System

ITSM—Information Technology Service Management

JIE—Joint Information Environment

JTF—Joint Task Force

KO—Knowledge Operations

(Added-ANDERSONAFB) MAC—Media Access Control

MAJCOM—Major Command

M/ACCC—MAJCOM/Air Force Forces Command Coordination Center

MFUA—Mission/Functional Unique Applications

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

MPA—Military Personnel Appropriation

MPTO—Methods and Procedures Technical Order

MWR—Morale, Welfare, and Recreation

NAF—Numbered Air Force

NAFIS—Non-Appropriated Fund Instrumentalities

NetD—Network Defense

NetOps—Network Operations

NIPRNET—Non-Secure Internet Protocol Router Network

NM—Network Management

NOS—Network Operations Squadron

(Added-ANDERSONAFB) NOTAMS—Notice to Airman

NS—Name Server

NSS—National Security System

OLA—Operational Level Agreement

PA—Public Affairs

PAO—Public Affairs Officer

OPR—Office of Primary Responsibility

PaaS—Platform-as-a-Service

PBNM—Policy Based Network Management

PEO—Program Executive Office

PMO—Program Management Office

(Added-ANDERSONAFB) POA&M—Plan of Action & Milestones

QoL—Quality of Life

QoS—Quality of Service

RDS—Records Disposition Schedule

(Added-ANDERSONAFB) SA—System Administrator

SAF—Secretary of the Air Force

SAP—Special Access Program

SCCM—Systems Center Configuration Manager

(Added-ANDERSONAFB) SCCM—System Center Configuration Manager

SCI—Sensitive Compartmented Information

SDC—Standard Desktop Configuration

SECAF—Secretary of the Air Force

SDDP—Service Development and Delivery Processes

SINE—Single Integrated Network Environment

SIPRNET—SECRET Internet Protocol Router Network

SLA—Service Level Agreement

SOA—Service Oriented Architecture

SOAP—Simple Object Access Protocol

SPO—System Program Office

SPPN—Special Purpose Processing Node

T.O—Technical Order

TB—Target Baseline

TCM—Technical Content Management

TCNO—Time Compliance Network Order

TCTO—Time Compliance Technical Order

TM—Technical Manual

UC—Unified Capabilities

USAF—United States Air Force

USAFA—United States Air Force Academy

USCYBERCOM—United States Cyber Command

VLAN—Virtual Local Area Network

VoIP—Voice Over Internet Protocol

XML—Extensible Markup Language

XSLT—Extensible Stylesheet Language Transformation

Terms

Air Force Information Networks (AFIN)—The globally interconnected, end-to-end set of AF unique information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security.

AFIN Operations—Operations to design, build, configure, secure, operate, maintain, and sustain AF networks to create and preserve information assurance on the AF information networks.

AF IT Services—The IT networks, systems, processes, and capabilities which enable the seamless, secure, and reliable exchange of information across the AFIN.

Air Force Network (AFNET)—The AF's underlying Non-Secure Internet Protocol Router Network (NIPRNET) that enables AF operational capabilities and lines of business.

AFNET-S—The AF's underlying Secret Internet Protocol Router Network that enables AF operational capabilities and lines of business.

Authoritative Data Source (ADS)—A source of data or information that is recognized by members of a Community Of Interest to be valid or trusted because it is considered to be highly reliable or accurate or is from an official publication or reference.

Core Data Center—The backbone of the JIE, CDCs are highly capable, highly resilient data centers providing standardized hosting and storage services to the enterprise within the Single Security Architecture (SSA). CDCs also enable a significant reduction in the total number of DoD data centers by serving as consolidation points for computing and storage services currently hosted across hundreds of Component Facilities. (DoD CIO memorandum, *Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration*, 11 July 2013)

Cyber Incident—Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. (CNSSI 4009)

Cyberspace Operations—The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. (AFPD 10-17)

Data Center—Accordingly, under the FDCCI, a data center is now defined as a closet, room, floor or building for the storage, management, and dissemination of data and information. Such a repository houses computer systems and associated components, such as database, application, and storage systems and data stores.' A data center generally includes redundant or backup power supplies, redundant data communications connections, environmental control (air conditioning, fire suppression, etc.) and special security devices housed in leased (including by cloud providers), owned, collocated, or stand-alone facilities. Under this revised definition, neither square footage nor Uptime Institute tier classifications are required to define a facility as a data center. (OMB memorandum, *Implementation Guidance for the Federal Data Center Consolidation Initiative (FDCCI)*, 19 March 2012)

Department of Defense Information Network (DoDIN)—The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security (formerly known as GIG). (JP 3-12)

DoDIN Operations—Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 3-12)

Enterprise Core Services—Standard IT capabilities available to all users on the AFIN. Enterprise Core Services support DoD Net-Centric strategies for data and services by enabling users to safeguard, compile, catalog, discover, cache, distribute, retrieve, and share data in a collaborative environment across the AF and DoD enterprises.

Implementation Baseline—The Implementation Baseline is the baseline of acquisition selected products and their informed/allowed configurations that implement the architecture, standards and protocols and guidelines specified in the Target Baseline. The Implementation Baseline informs the Operational Baseline of the acquisition selected products and how they are to be configured to support deployment of user applications across the infrastructure topology. The Implementation Baseline governs the implementation of the Development and Integration/Test environments (AFPD 33-4).

Information Enviroment (IE)—The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment, which includes cyberspace, consists of three interrelated dimensions that continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive. (JP 3-13 and Draft DoDI 8115.02)

Information Processing Node—A fixed DoD data center serving a single DoD installation and local area (installations physically or logically behind the network boundary) with local services that cannot (technically or economically) be provided from a CDC. There will be no more than one IPN per DoD installation but each IPN may have multiple enclaves to accommodate unique installation needs (e.g., Joint Bases)

Information Technology—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (CNSSI 4009)

Infrastructure-as-a-Service (IaaS)—Virtualized systems operated on fundamental computing resources (e.g., processing, storage, network) managed as a cloud service with the AF retaining control of operating systems, storage, and deployed applications.

Installation Services Node (ISN)—An Installation services node is the required localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the enterprise. Potential services include anomaly detection, audit functions, Active Directory (AD), DNS, Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), and print services. In addition ISNs may also host unified capabilities (UC) that must remain on the Installation to enable emergency services even when the connection is interrupted.

Internet—An informal global collection of government, military, commercial, and educational computer networks. The global collection of interconnected local, mid-level, and wide area networks that use IP as the network layer protocol.

Internet-based Capabilities—All public information capabilities or applications available across the Internet from locations not directly or indirectly controlled by DoD or the Federal government (i.e., locations not owned or operated by DoD or another Federal agency or by contractors or others on behalf of DoD or another Federal agency).

Internet Service Provider—A commercial entity providing data connectivity into the Internet.

Joint Information Environment—A secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies. JIE is operated and managed per the Unified Command Plan (UCP) using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs).

Operational Baseline—The Operational Baseline is the set of components of the Implementation Baseline appropriately configured and deployed across the topology of the AFIN infrastructure that implements the architecture, standards and protocols and guidelines specified in the Target Baseline and provide the required warfighter capabilities and performance. It specifies the exact laydown and configurations of hardware and software within all facilities in the AF infrastructure topology.

Platform-as-a-Service (PaaS)—A cloud computing platform providing operating systems, database systems, web servers, security, etc. for hosting of AF unique applications.

Security Incident—An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (CNSSI 4009 - *Security Incident refers to Incident*)

Server—A hardware platform (computer) that houses software providing service to other computers or programs to satisfy client requests and needs.

Service Incident—Any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service. (ISO 20000 – *ITSM definition of Incident*) An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set. (ITIL Version 3 Service Operation)

Service Oriented Architecture—A set of principles and methodologies for designing and developing software in the form of interoperable services.

Service Request—A request from a user for information, or advice, or for a standard change or for access to an IT Service. For example to reset a password, or to provide standard IT Services for a new user. Service Requests are usually handled by a Service Desk, and do not require an request for change to be submitted. (ITIL Version 3 Service Operation)

Software-as-a-Service (SaaS)—All aspects of standard applications are provided as a cloud service to the AF.

Special Purpose Processing Node (SPPN)—A fixed data center supporting special purpose functions that cannot (technically or economically) be supported by CDCs or IPNs due to association with infrastructure or equipment (e.g., communication and networking, manufacturing, training, education, meteorology, medical, modeling & simulation, test ranges, etc.). No general purpose processing or general purpose storage can be provided by or through a SPPN. SPPNs do not have direct connection to the Global Information Grid (GIG); they must connect through a CDC or IPN. (DoD CIO memorandum, "Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration," 11 July, 2013)

Target Baseline—The Target Baseline specifies the standards, protocols, guidelines and implementation constraints for the future state of the AFIN infrastructure. It is used to inform the development of the Implementation Baseline. The Target Baseline is thoroughly documented and continually updated based upon emerging industry standards and the evolving AF enterprise architecture.

Unified Capabilities (UC)—The integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. (DODI 8100.04)

User—The individual who operates the computer or uses application software.