DEPARTMENT OF THE AIR FORCE

WASHINGTON, DC

OFFICE OF THE SECRETARY

AFI17-120_AFGM2016-01

28 October 2016

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Air Force Guidance Memorandum (AFGM) to Air Force Instruction (AFI) 33-150, MANAGEMENT OF CYBERSPACE SUPPORT ACTIVITIES.

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately changes Air Force Instruction 33-150, *Management Of Cyberspace Support Activities*, 30 November 2011. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with (IAW) AFI 33-360, *Publications and Forms Management*. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

As a result of the publication of AF Policy Directive(AFPD) 17-1 *Information Dominance and Cyberspace Governance and Management*, which supersedes AFPD 33-1, *Cyberspace Support*, dated 9 Aug 2012; AFI33-150 is hereby renumbered as AFI 17-120. This Memorandum also renumbers AFI33-150; the title and the rest of the content remain unchanged. I hereby direct the Office of Primary Responsibility (OPR) for AFI33-150 to conduct a special review in accordance with AFI33-360 to align its content with AFPD17-1. This will result in a rewrite or rescind action of AFI33-150.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon rescinding or rewrite of AFI33-150, whichever is earlier.

WILLIAM J. BENDER, Lt Gen, USAF
Chief, Information Dominance and
Chief Information Officer

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-150

30 NOVEMBER 2011

Incorporating Change 1, 18 December 2014

Communications and Information

MANAGEMENT OF CYBERSPACE SUPPORT ACTIVITIES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6ONI

Certified by: SAF/A6ON
(Col Daniel Elmore)

Pages: 29

Supersedes: AFI33-150, 26 November 2008 and
AFI33-104, 10 May 2001

This Air Force Instruction (AFI) implements Air Force Policy Directive AFPD 33-1, *Cyberspace Support.* It establishes the management of cyberspace resources to include systems, equipment, personnel, time, and money and provides the directive guidance for Air Force cyberspace support activities. This publication applies to all military and civilian Air Force personnel, members of the Air Force Reserve Command (AFRC), Air National Guard (ANG), third-party governmental employee and contractor support personnel in accordance with appropriate provisions contained in memoranda support agreements and Air Force contracts. In this document, the term "cyberspace support activity" is defined as any action taken to restore communications systems/equipment to operational status, to perform preventive maintenance inspections (PMI) on communications systems/equipment and/or components, or to install or remove communications systems/equipment. The term cyberspace infrastructure refers to equipment and network infrastructure to provide the internet, network operations and command and control, and embedded processors and controllers. The term "Communications systems/equipment" is defined as: transmission, switching, processing, systems-control, and network management systems, as well as equipment, software, and facilities, fixed and deployable, that supports a mission area. The intent of this instruction is to ensure only qualified personnel perform cyberspace support activities and prevent damage to communications hardware, software, stored information, and current mission operations. One or more paragraphs of this AFMAN may not apply to non-AF-managed joint service systems. These paragraphs are marked as follows: *(NOT APPLICABLE TO NON-AF-MANAGED JOINT SERVICE SYSTEMS).* 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 using AF Form 847, *Recommendation for Change of Publication*, to Cyberspace Strategy and Policy Division (SAF/A6SS), 1030 Air Force Pentagon, Washington DC 20330-1030. When collecting and maintaining information protect it by the Privacy Act of 1974 authorized by 10 U.S.C. 8013. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records* and disposed of in accordance with Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). See Attachment 1 for a glossary of references and supporting information.

SUMMARY OF CHANGES

This interim change (1) incorporates responsibilities of Installation Communication Squadron (CS) Commanders and Tenant Unit Commanders previously documented in AFI 33-101, *Commanders Guidance and Responsibilities* (rescinded); (2) adds AF Data Center Consolidation responsibilities and guidance previously identified via AF Guidance Memorandum; (3) updates office symbol and responsibilities for 38th Cyberspace Engineering Installation Group (38 CEIG); (4) adds requires for AFTO Form 747, *Cyberspace Infrastructure Systems Acceptance*, and AFTO Form 229, *Engineering Installation Assistance*; (5) adds Tier waiver approval authorities according to AFI 33-360; (6) removes ATCALS references based on transfer to AF/A3. A margin bar (|) indicates newly revised material.

1. Purpose. This instruction implements new communications systems/equipment activity guidelines and changes or eliminates the requirement to complete redundant procedures and practices. Guidance in this publication is intended to assist Air Force personnel in identifying activities required to support Air Force communications. This instruction is an initiative to reduce the number of SAF/CIO A6 departmental- level publications by changing their publications from "stove-piped" system/program-based to audience/role-based focus. Specific procedural information is located in the more detailed Methods and Procedures Technical Orders (MPTO) or specialized publications. Common core communication services for standard user information (e.g., e-mail, phone, messaging, etc.) are located in AFMAN 33-152, *Users Responsibilities and Guidance for Information Systems*. Guidance for acquisition and sustainment planning is located in AFI 63-101, *Integrated Life Cycle Management.*

1.1. **Objectives**. The primary objectives of cyberspace support activities are to ensure continuous security, operational availability, and reliability of systems and equipment supporting the Air Force mission. This instruction outlines unit roles and responsibilities to ensure communications systems/equipment are serviceable and properly configured to meet mission requirements.

1.2. **Intent.** This instruction mandates the use of MPTO 00-33A-1001, *General Cyberspace Support Activities Management Procedures and Practice Requirements*, which establishes implementation guidance and procedures; MPTO 00-33D-3003, *Managing the Cyberspace Infrastructure with the Cyberspace Infrastructure Planning System*, which explains how to use the Cyberspace Infrastructure Planning System (CIPS) to document, fund, distribute, implement, and manage the cyberspace infrastructure; and MPTO 33D-2002, *Engineering, Implementation, and Cyberspace Readiness Activities Management,* which defines the processes and procedures for the management of Engineering Installation (EI) and Cyberspace Readiness activities to include providing Major Commands (MAJCOMs) and bases with the necessary information to process EI requirements for funding via the Air Force (AF) EI Work Plan in CIPS. These elements support the objectives in **paragraph 1.1**. **Note:** This AFI and supporting MPTOs cannot 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. This AFI and supporting MPTOs cannot alter or supersede higher authoritative guidance governing Special Access Program (SAP) systems, counterintelligence or law enforcement collection operations, or investigations involving communication systems. When DNI or SAP authorities fail to address areas covered by this AFI, this AFI and associated MPTOs need 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 precedence. TOs are available for ordering through the Enhanced Technical Information System (ETIMS) application on the AF Portal, per TO 00-5-1, Air Force Technical Order System. Contact unit Technical Order Distribution Office (TODO) for assistance.

2. Roles and Responsibilities. Note: For this instruction, the term major command (MAJCOM) also applies to Numbered Air Forces (NAF), Field Operating Agencies (FOA) and Direct Reporting Units (DRU).

2.1. **Chief Information Dominance and Chief Information Officer(SAF/CIO A6).** Develops and publishes cyberspace support activities, strategy, policy, tactical doctrine, and programs to integrate warfighting and combat support capabilities, and oversees implementation of enterprise information, information resources, and data management capabilities for Joint, Coalition and Air Force warfighters. Coordinates with military services, MAJCOMs and any additional government agencies as applicable. In addition, SAF/CIO A6 will:

2.1.1. Manage cyberspace operations career fields.

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

2.1.3. DELETED.

2.1.4. Appoint executive agent for IT emerging technologies.

2.1.5. Establish overall guidance, act as approval authority for plans, and resolve proposed consolidation actions for Centralized Repair Activities (CRA).

2.1.6. Act as the approval authority for:

2.1.6.1. Proposed temporary T-1 AFNET system/equipment modifications according to AFI 63-131, *Modification Management*.

2.1.7. Will oversee management and disposition of all AF data centers as described in **paragraph 3**, to include the data center components of weapons systems.

2.1.7.1. Ensure all requirements support the Federal Data Center Consolidation Initiative (FDCCI) IAW **paragraph 3**.

2.1.7.2. Coordinate with AFSPC and other Lead MAJCOMs to determine if existing capabilities across the AF or DoD will satisfy the requirement. Requests satisfied by existing capabilities will be disapproved and returned to the requestor along with appropriate rationale and recommended alternatives IAW **paragraph 3**.

2.2. **Air Force Space Command (AFSPC).** As Lead Command for all Air Force Cyberspace Operations via the 24AF(AFCYBER), AFSPC will be the Air Force focal point for establishment, operation, maintenance, defense, exploitation, and attack Cyberspace Operations. AFSPC coordinates the prioritization of all Cyberspace Infrastructure requirements. In addition, AFSPC will:

2.2.1. Control the membership of the Engineering and Installation Governance Structure (EIGS).

2.2.2. Coordinate the establishment of and the schedule for the EIGS composed of representatives from all MAJCOMs for the review, prioritization, and funding of EI projects Air Force-wide.

2.2.3. Ensure program information is documented in the CIPS.

2.2.4. Manage and distribute the consolidated funding for EI projects.

2.2.5. Manage and distribute the consolidated Military Personnel Appropriation (MPA) man-days for ANG implementation of projects.

2.2.6. In coordination with 38th Cyberspace Engineering Installation Group (38 CEIG), monitor the execution of cyberspace projects approved for implementation.

2.2.7. In coordination with the A6 community, develop, manage, and defend EI Program Objective Memorandum (POM) inputs with the information that resides in CIPS.

2.2.8. Support FDCCI goals and objectives when managing and distributing the consolidated funding for Engineering Installation (EI) projects.

2.3. **Air Force Network Integration Center.** As a Direct Reporting Unit to AFSPC, AFNIC is designated as the United States Air Force (USAF) lead agency to develop policy and guidance for cyberspace support activities and related areas to shape, provision, integrate and sustain the AF Cyber Network in all four domains: terrestrial, air, space and cyberspace. In addition, AFNIC will:

2.3.1. AFNIC Enterprise Systems Policy, Procedures and Support Division (ESP) will:

2.3.1.1. Manage assigned cyberspace support activities policy, procedures, and MPTO 00-33A-1001.

2.3.1.2. Manage all waiver requests relating to cyberspace support activities.

2.3.1.3. Manage the Air Force Communications Quality Control Checklist (AFCQCC) program.

2.3.1.4. Represent the communications personnel/community as members of workgroups, integrated process/product teams as required.

2.3.1.5. Serve as focal point for Air Force guidance and directives regarding communication systems/equipment modifications except when MAJCOM is designated as the Air Force Lead or lead command per paragraph 2.4.5.

2.3.1.6. Under direction from SAF/A6SF, develop compliance inspection criteria for the Air Force Inspector General (TIGs).

2.3.1.7. Act as focal point for Standard Reporting Designator assignment for non-Air Force Material Command (AFMC) centrally managed commercial items and/or Government-Off-The-Shelf (GOTS) equipment.

2.3.1.8. Manage Depot Purchased Equipment Maintenance, Low Density Level (LDL) assets, non-airborne Readiness Spares Packages (RSP), and provide material management assistance to units.

2.3.1.9. Provide enterprise level equipment analysis capability metrics, such as reliability, availability, and maintainability, utilizing approved automated information system (AIS).

2.3.1.10. Perform unit-funded staff assistance visit (SAVs) upon request and availability of manpower.

2.3.1.11. Manage Information Technology (IT) hardware asset accountability according to AFMAN 33-153, *Information Technology (IT) Asset Management (ITAM)*.

2.3.2. AFNIC Enterprise Systems Cyber Force Strategies (ESF) will:

2.3.2.1. Manage training resources in support of formal courses, upgrade training, certification training and newly integrated technology training.

2.3.2.2. Support cyberspace operations career fields and systems providing/managing computer based training, instructor led training, and virtual instructor led training.

2.3.3. AFNIC Enterprise Systems Maintenance Management (ESM) will:

2.3.3.1. Perform system management duties and responsibilities as specified in current Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), and Service Level Agreements (SLA).

2.3.3.2. Review MAJCOM recommended changes to Air Force-managed programs, systems/equipment.

2.3.3.3. Assess, evaluate, and ensure compliance with governing directives for communications systems/equipment, as directed or requested.

2.3.3.4. AFNIC Integration Engineering (EN) will:

2.3.3.5. Direct engineering standards and solutions to configuration manage, control, integrate, and optimize Air Force network (AFNet) Cyberspace operations and the core services it provides.

2.3.3.6. Provide engineering analysis and assessment to characterize and resolve AFNet performance, integration, and interoperability issues to meet customer quality of service delivery expectations.

2.4. **Major Commands (MAJCOMs).** MAJCOMs implement Air Force guidance concerning their communications systems/equipment. MAJCOMs will:

2.4.1. Manage and provide support for command-unique programs and systems/equipment.

2.4.2. Coordinate MAJCOM policy, procedures, and Technical Order (T.O.) supplements for implementation consideration affecting cyberspace support activities, subject to the following conditions:

2.4.2.1. Supplements must not be less restrictive than higher level publications or the basic publications being supplemented, and must not contradict or conflict with Air Force-wide policy, procedure, or publications according to AFI 33-360, *Publications and Forms Management*.

2.4.2.2. Supplements must contain only MAJCOM unique material.

2.4.2.3. Recommended MAJCOM supplements to Air Force publications, forms, and checklists. Also, proposed changes to Air Force-wide communications systems/programs/equipment must be coordinated with the appropriate OPR or lead command.

2.4.3. DELETED.

2.4.4. Ensure logistics support and life-cycle management plans are developed for MAJCOM-acquired/ procured commercial-off-the-shelf (COTS) communications systems and equipment.

2.4.5. When designated as Air Force Lead (early development) or as lead command, serve as focal point to develop/implement Air Force guidance and directives concerning communications systems/ equipment.

2.4.6. Review and forward all waiver requests relating to communications systems/equipment activities to AFNIC/ES via AFSC 3DXXX Functional Managers.

2.4.7. Act as approval authority for MAJCOM-developed Local Communications Quality Control Checklist (LCQCCs) for command-unique programs, systems and equipment, IAW T.O. 00-33A-1001.

2.4.8. Provide quality assurance (QA) guidance, if required.

2.4.9. Manage and act as approval authority for support/maintenance assistance requests. Assistance requests may be accomplished if unit-funded and manpower is available.

2.4.10. Establish focal point for CRA management, if applicable.

2.4.11. Prioritize their own work plan(s) and provide representatives to the EIGS for the review, prioritization, and funding of projects Air Force-wide. Reference **paragraph 2.5** for EIGS structure and TO 33D-2002 for AF EI work plan process.

2.4.12. Designate appropriate system functional managers.

2.4.13. MAJCOMs owning, managing, or operating data centers as defined by OMB (servers in any form, except for those expressly exempted by this AFI) will ensure these facilities are documented in Data Center Inventory Management System (DCIMS) and all obligations to acquire IT are approved IAW the process in **paragraph 3**.

2.4.14. Coordinate any Defense Information Systems Network (DISN) Long-Haul Communications changes required to support data center and data server requests according to AFMAN 33-116, *Long-Haul Communications Management*.

2.5. **Engineering and Installation Governance Structure (EIGS).** EIGS organizations include the EIGS Council (composed of MAJCOM two-letter representatives), the EIGS Board (MAJCOM three-letter level), and the EIGS Group (MAJCOM four-letter level) which prioritize and approve EI requirements Air Force-wide. In addition, the EIGS will:

2.5.1. Provide senior leader guidance to Cyberspace program planners to help determine project priorities.

2.5.2. Develop minimum submission criteria, provide guidance, and set the schedule for cyberspace infrastructure work plans.

2.5.3. Establish the funding "cut line" for the EI PEC (Program Element Code) 27436F based on the amount disbursed.

2.5.4. Review the priorities, adjust them if needed, and approve a single consolidated Air Force-wide centralized EI work plan, considering both contractual implementation and organic implementation.

2.5.5. In coordination with 38th Cyberspace Engineering Installation Group (38 CEIG), monitor execution of approved EI requirements.

2.6. **38th Cyberspace Engineering Installation Group (38 CEIG).** The 38 CEIG and its squadrons plans, engineers, and delivers a survivable and resilient infrastructure to establish the cyberspace domain and assist the Air Force mission to conduct offensive and defensive air, space, and cyberspace operations. They provide engineering, planning, implementation, management, and consultation support to enable establishment of forward operating bases, combatant command, Air Force, and Joint service net-centric environment. Reference MPTO 00-33D-2002 for all 38 CEIG services and processes. In addition, the 38 CEIG will:

2.6.1. Provide Air Force-wide cyberspace infrastructure and health assessments to identify shortfalls and vulnerabilities.

2.6.2. Provide specialized engineering, operational engineering, and emergency maintenance/restoral.

2.6.3. Develop and maintain the Technology Infrastructure component of the AFNet Enterprise Architecture, describing and identifying the physical layer including, the functional characteristics, capabilities, and interconnections of the hardware, software, and communications.

2.6.4. Provide Combatant Commanders a Designated Operational Capability (DOC)-tasked 72-hour rapid-response EI force that is deployable worldwide.

2.6.5. Provide a specialized contracting activity that executes responsive acquisition strategies and compliant sourcing solutions in support of the AF Cyberspace Mission, and the Air Force Work Plan.

2.6.6. Provision, budget, and manage inter-base Long Haul Communications (reference AFMAN 33-116), DISN Subscription Services (DSS), Mobile Satellite Services (MSS) and Teleport Management, GSA FTS2001/Networx Requirements Manager, common user network connectivity oversight, last half-mile connectivity task orders, and AF's MAJCOM Circuit Management Office (CMO) (reference AFI 33-134, *Mobile Satellite Services Management*).

2.6.7. Provide enterprise system management support to base communications squadrons/flights, MAJCOMs, Lead Commands, and Air Staff, to include field technical expertise on systems and policy interpretation.

2.6.8. Provide Cyberspace Information Technology acquisition support, project and program implementation services, and requirements review, preparation, and processing to the AF, Numbered Air Force (NAF)/Air Force Forces (AFFOR), DoD, and other government agencies IAW AFPD 16-5, *Planning, Programming, Budgeting, and Execution Process*.

2.6.8.1. DELETED.

2.6.8.2. DELETED.

2.6.9. As the CIPS Program Management Office (PMO), chairs the CIPS Oversight Group.

2.6.9.1. DELETED.

2.6.9.2. DELETED.

2.6.9.3. DELETED.

2.6.10. DELETED.

2.6.11. DELETED.

2.6.12. DELETED.

2.6.13. DELETED.

2.6.14. DELETED.

2.7. **Program Managers.**

2.7.1. Program managers will document their program information in CIPS according to MPTO 00-33D-3003 and AFI 63-101. **(T-1).** However, information regarding data center infrastructure must be documented in DCIMS according to **paragraph 3**. **(T-0)**

2.7.2. Address data center consolidation, according to **paragraph 3**, in acquisition planning and plan for end state disposition prior to the next major increment or modification. **(T-0)**

2.7.3. All Program Offices owning, managing, or operating data centers as defined by OMB (servers in any form, except for those expressly exempted by this AFI) will ensure these facilities are documented in DCIMS and all obligations to acquire IT are approved IAW the process in **paragraph 3**. **(T-0)**

2.8. **Engineering and Installation (EI) Total Force Group (TFG).** The TFG consists of: one (1) Active-Duty Air Force unit (85 EIS), 15 Air National Guard (ANG) Squadrons, National Guard Bureau (NGB)/A6 EI Functional Area Manager (FAM), 251 CEIG, 253, CEIG, and 38 CEIG. The TFG provides the process to implement funded cyberspace infrastructure projects with organic resources. TFG enterprise oversight is the responsibility of NGB/A6 EI FAM and 38 CEIG. In addition, the TFG will:

2.8.1. Review EIGS prioritized projects and make recommendations for organic implementation.

2.8.2. Dispense EIGS approved projects for organic implementation.

2.9. **Communications Unit Commanders or Equivalent.**

2.9.1. Implement all applicable programs listed in MPTO 00-33A-1001. MPTO 00-33A-1001 topics include Quality Assurance Program, Control of Production, Communications Inspection, Corrosion Prevention and Control Program (CPCP), Historical Record Management, Life Cycle Management, Material Management, Publications Programs, Antenna Identification, Tool Management, Performance Metrics and Algorithms for Communications, Centralized Repair Activities (CRA), System Managers, Specialized Communications Teams (SCT), Common Communications Procedures, and Climbing Training Requirements, Equipment Control. **(T-2)**

2.9.2. Establish a QA work center directly under the Communications Unit Commander or Operations Group as appropriate. **(T-3)**

2.9.3. Assign an individual as the Wing/Base 3A1XX Administration Functional Manager for accession, training, classification, utilization, and career development of enlisted (3A1XX) personnel. NOTE: These personnel operate in every functional area and often do not work in the Wing/Base communications unit. Nevertheless, they are specialized extensions of the total capability for cyber support to the Air Force mission. **(T-1)**

2.9.4. Process and sign the AFTO Form 747, *Cyberspace Infrastructure Systems Acceptance*, for all cyberspace infrastructure installation actions. **(T-2)**

2.9.5. Serve as the focal point for the installation's cyberspace systems, equipment, and programs. **(T-2)**

2.9.5.1. Ensure applications, systems, and core enterprise services are hosted only in SAF/CIO A6-approved facilities as defined by **paragraph 3.2.3**. **(T-0)**

2.9.5.2. Ensure all systems/equipment supported by cyberspace support activities is tracked in the approved AIS to include antennas. **(T-2)**

2.9.5.3. Ensure only Air Force-approved AIS such as Integrated Maintenance Data System (IMDS), Remedy, Telephone Management System (TMS), CIPS, and Training Business Area (TBA) are used for all customer service requests/work orders and training documentation unless granted a higher headquarters waiver. **Note**: Follow approved security classification guide or authoritative SAP and DNI guidance when applicable. **(T-2)**

2.9.6. Meet the mission needs of assigned tenant units and geographically separated units (GSUs) not receiving support from another host wing, command, or Service. **(T-2)**

2.9.6.1. Manage the infrastructure for host systems and tenant systems as defined in support agreements. **(T-2)**

2.9.6.2. Review and assist with the development of tenant plans involving communications and information resources or activities. **(T-3)**

2.9.7. Develop cyberspace infrastructure annexes and appendices, for installation specific contingency plans and support plans. **(T-3)**

2.9.8. Validate the base blueprint in CIPS prior to Installation commander's endorsement (reference AFTO Form 330, *Base Blueprint Endorsement Checklist*). **(T-3)**

2.9.9. Be the "Approval Authority" for CIPS accounts IAW MPTO 00-33D-3003. **(T-3)**

2.9.10. Coordinate CSI visits with installation level Functional Area Managers (FAMs) and installation Civil Engineering Squadron planners. **(T-3)**

2.9.11. Manage and document base cyberspace infrastructure projects in CIPS for current and out years. Reference MPTO 00-33D-3003. **(T-2)**

2.9.11.1. Manage all Communications and Information Systems Installation Records (CSIR) for Cyber Operations and Transport Systems per MPTO 00-33A-1001 until CIPS is enhanced to provide that capability. **(T-2)**

2.9.11.2. Manage the Cable and Antenna Systems Communications Mission Data Set (CMDS) layer in the CIPS Visualization Component (CVC) per MPTO 00-33D-3004. **(T-2)**

2.9.11.3. Prioritize and approve projects on Work Plan submissions in CIPS as applicable.

2.9.11.4. Follow the process in MPTO 00-33D-2002 for including Cyberspace Infrastructure requirements in the AF EI Work Plan process. **(T-2)**

2.9.12. Initiate and process the AFTO Form 229, *Engineering Installation Assistance*, to request services not identified or funded on the AF EI Work Plan as defined in MPTO 00-33D-2002. **(T-2)**

2.9.13. DELETED.

2.10. **Flight Commander/Flight Chief or equivalents.** At a minimum, the Flight Commander and Flight Chief of cyberspace personnel will:

2.10.1. DELETED.

2.10.2. Direct PMIs to be accomplished IAW appropriate or established T.O.s or in the absence of T.O.s, commercial manuals or publications.

2.10.3. Publish local workcards (LWC) and/or checklists if required.

2.10.4. Waive the accomplishment or approve deviations of scheduled inspections (e.g., PMIs) under conditions listed in MPTO 00-33A-1001.

2.10.5. Increase frequency or scope of scheduled inspections (e.g., PMIs) or individual inspection requirements when, and if, required.

2.10.6. Coordinate with applicable agencies/units for cyberspace support activities impacting operations.

2.10.7. Authorize use of local CQCCs.

2.10.8. Manage cyberspace deployment processes for equipment, personnel and technical documents.

2.10.9. Serve as approval authority for cannibalization or controlled substitution activities.

2.11. **Work center Supervisors.** At a minimum, work center supervisors of cyberspace personnel will:

2.11.1. Ensure compliance with directives, technical publications, and supplements.

2.11.2. Ensure customer service requests and work orders reflect current system/equipment status.

2.11.3. Understand supervisors' roles and responsibilities in the QA program.

2.11.4. Secure and control government property to include tracking warranty information.

2.11.5. Coordinate scheduled support actions (e.g., Time Change Item (TCI), and Time Compliance Technical Order (TCTO), Time Compliance Network Order (TCNO), Maintenance Tasking Order (MTO), Network Tasking Order (NTO), etc.) with Communications Focal Point (CFP).

2.11.6. Appoint project coordinator [e.g., EI, self-help, Specialized Communications Team (SCT), CIPS], and ensure required duties are accomplished.

2.11.7. Manage test, measurement, and diagnostic equipment and other test equipment.

2.11.8. Establish a comprehensive safety program to include such programs as Radio Frequency Radiation, Hazard Material, Hazard Communication, confined space, facility grounding, lock out/tag out, and climbing training.

2.11.9. Manage work center corrosion prevention and control program (CPCP) and electrostatic discharge program according to MPTO 00-33A-1001.

2.11.10. Ensure work center logistics support management responsibilities are accomplished.

2.11.11. Maintain historical files and master inventories on communications systems/equipment in applicable AIS.

2.11.12. DELETED.

2.12. **Communications Focal Point (CFP).** In the base communications squadron/flight, the CFP is the combination of the Maintenance Operations Center (MOC), telephone helpdesk and the traditional network helpdesk functions. The CFP function has tactical control (TACON) of the client service team (CST) Work center. The CST unit commanders retain administrative control of CSTs. The CST Work center retains TACON of all CSTs assigned to the base. A separate MOC may exist at bases where cyber systems are assigned to an Operations Group in addition to equipment/systems assigned to Communications Group/Squadron. The standalone MOC will comply with applicable CFP responsibilities contained in TO 00-33A-1001. **Note:** CFP and Enterprise IT Service Desk (ESD) integration is contained in MPTO 00-33A-1001. The CFP will:

2.12.1. Manage customer service requests, work orders, and equipment status reporting.

2.12.1.1. Manage service requests, trouble tickets, and/or service incidents according to Control of Production procedures in MPTO 00-33A-1001.

2.12.1.2. Manage work orders according to procedures in TO 00-33D-3003. **Note:** Work Order Management System (WOMS) is an integrated tool that permits users to create, track, and process work orders within CIPS at both the base and MAJCOM levels, while keeping work orders and infrastructure requirements as separate business objects.

2.12.2. Provide a 24-hour contact number to customers/users and base Command Post.

2.12.3. Manage/review approved AIS management products for accuracy and analyzes data for negative trends.

2.12.4. Manage reports (e.g., situational reports (SITREP), communications statistics, etc.) and disseminate to appropriate personnel for action. The CFP will disseminate monthly ticket and activities information to the unit commander.

2.12.5. Document and control removal/replacement/cannibalization actions.

2.12.6. Act as focal point for depot maintenance requests.

2.12.7. Ensure master PMI schedule is entered into the AIS and includes antennas.

2.12.8. Review, direct, and monitor accomplishment of scheduled and unscheduled support actions (e.g., TCI, TCTO, TCNO, MTO, NTO, outages, etc).

2.12.9. Serve as focal point (i.e., sub-system manager) for the Air Force-approved AISs (e.g., IMDS, Remedy, etc.).

2.12.10. Develop procedures to sustain operations in the event of power failure, communications outage, etc.

2.12.11. Review all SLAs, MOAs, or MOUs for applicability and impact to current cyberspace support activities according to AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures*.

2.12.12. Provide customers with reporting procedures for communications systems outages/problems.

2.12.13. Perform the Logistics Service Center (LSC) liaison duties of Mission Capable and Turn-Around (TRN) Monitors.

2.12.14. Act as the main interface with the AFNet ESD.

2.12.15. Forward all CIPS requirements to the appropriate authority for implementation.

2.13. **Quality Assurance (QA).** The QA program is responsible directly to the commander or deputy. The QA program applies to all cyberspace AFSCs who sustain systems. At a minimum, QA personnel will:

2.13.1. Provide assistance, advice, and authoritative references to work center supervisors and unit leadership.

2.13.2. Establish and maintain a technical publications program (e.g., technical orders, Air Force Network Standard Operating Procedures, etc.).

2.13.3. Manage Quality Assessments and Trend Analysis activities using Air Force approved systems.

2.13.4. Process material and T.O. deficiencies.

2.13.5. Review work center facility, systems installation, and equipment records management.

2.13.6. Perform technical reviews of modifications proposals and process valid proposals according to applicable directives.

2.13.7. Perform CPCP and electrostatic discharge (ESD) focal point duties according to MPTO 00-33A-1001.

2.13.8. Review locally devised checklists, operating instructions, publications, and directives annually.

2.13.9. Submit changes to various publications, T.O.s and other guidance.

2.13.10. Review statements of work where cyberspace support activities are outsourced.

2.13.11. Complete Air Force Job Qualification Standard (AFJQS) 3DXXX-201G, *Quality Assurance*, within 180 days of assuming responsibilities unless previously completed and documented. Use this AFJQS as a guide for training Quality Assurance Representative (QAR) personnel.

2.13.12. Validate and manage LWCs.

2.13.13. Use applicable AFCQCCs during evaluations according to MPTO 00-33A-1001.

2.13.14. Perform in-process, acceptance, deactivation, or transfer inspections on equipment/systems being overhauled, repaired, installed, removed, or newly acquired.

2.14. **Tenant Unit Commanders (or equivalent)** will:

2.14.1. Appoint a tenant communications responsible officer to serve as their single focal point and accountable officer for the cyberspace support systems of their respective activities. **(T-2)**

2.14.2. Define specific tenant and installation communications squadron commander (or equivalent) responsibilities in the support agreement or similar document. Upon appointment, unit commanders (or equivalent) notify the installation communications squadron commander (or equivalent). **(T-2)**

2.14.3. Coordinate with the installation communications squadron commander (or equivalent) to ensure their systems will integrate and interoperate, when necessary, with the DODIN, AFIN, AFNET or host base systems. **(T-2)**

2.14.4. Identify to the host installation, MAJCOM, and lead MAJCOM for Cyberspace Operations, the special engineering, installation, operation and/or maintenance requirements for NSS, SAP or SCI or other federal agency systems that are used by the tenant. **(T-2)**

2.15. **All Organizations.** All organizations owning, managing, or operating servers in any form (data centers as defined by OMB), except for those expressly exempted by **paragraph 3.2.1** or **paragraph 3.3.1** will work with the SAF/CIO A6 DCC Team (see **paragraph 3.4**) to ensure these facilities are documented in DCIMS and all obligations are approved IAW the process in **paragraph 3**. **(T-0)**

3. Data Servers And Data Centers Approval Process.

3.1. **AF Data Center Infrastructure Management.** Under the FDCCI, OMB defines a data center as a closet, room, floor or building for the storage, management, and dissemination of data and information. This definition has been further defined by the DOD CIO to include single and multiple server instantiations regardless of adherence to Uptime Institute or TIA-942 standards. While it is generally recognized that weapon systems may not be data centers, most weapon systems have an IT component that may constitute a data center or reside in a data center. Thus, a weapon system designation , in and of itself, does not justify an exemption from FDCCI, related data center legislation, DOD guidance, or the guidance contained in this AFI. The SAF/CIO A6 will oversee management and disposition of all AF data centers under the purview of aforementioned guidance, to include the data center components of weapons systems.

3.2. **AF Data Center Consolidation.** The DOD CIO, working under the purview of FDCCI guidance, requires all data centers (exceptions are noted below) to be documented in DCIMS. Records will be created and maintained by data center owners IAW guidance and training provided by the AF Data Center Consolidation team within SAF/CIO A6. Data center end states (discussed below) submitted by data center owners will be adjudicated and approved by SAF/CIO A6.

3.2.1. DCIMS Exemptions. The following items are exempt from FDCCI and do not require entry into DCIMS:

3.2.1.1. IT components constituting a data center that are onboard airborne platforms.

3.2.1.2. IT components constituting a tactical data center such as those contained in shelters.

3.2.1.3. IT components constituting a data center where the metadata (location, configuration, owner, etc.) is classified. Those systems are inventoried separately by the Director of National Intelligence.

3.2.2. Data Center End States. The following data center end states are defined by the DOD CIO and approved for use in DCIMS:

3.2.2.1. Core Data Center (CDC) – These locations are selected by the DOD CIO and operated by DISA.

3.2.2.2. Installation Processing Node (IPN) – Data centers required to host applications required for base operations where access does not transit the base boundary. IPNs will not allow connections from one base to another and there shall be no more than one (1) IPN per base or installation.

3.2.2.3. Special Purpose Processing Node (SPPN) – Servers connected to special purpose IT or non-IT equipment that cannot be moved due to technical requirements (such as flight simulators) or servers hosting applications critical to Air Force, DOD, or combatant command missions.

3.2.2.4. Closed – Data centers not identified as one of the three categories above must be projected to close no later than 2018. Applications hosted within these data centers must be migrated to a data center approved by SAF/CIO A6 as noted below.

3.2.3. Application Designations. Applications and/or systems that do not require base boundary transit for use are designated local and may reside in an IPN approved by SAF/CIO A6. All other applications and/or systems are designated enterprise and must be hosted in an enterprise data center approved by SAF/CIO A6 NLT 4th quarter of Fiscal Year 2018 (QTR4FY18). Exceptions may be granted by SAF/CIO A6 for those instances where migration to an enterprise location would introduce risk to mission or an approved business case analysis shows migration to be cost prohibited. Application owners must coordinate with appropriate organizations as directed in Air Force Guidance Memorandum 33-04, Common Computing Environment.

3.2.3.1. DISA Core Data Center/MilCloud (any app, system, or service).

3.2.3.2. Commercial Cloud (any app, system, or service) with a DoD Provisional Authorization for the corresponding data level.

3.2.3.3. IPNs approved by SAF/CIO A6 (base local apps only).

3.2.3.4. SPPNs approved by SAF/CIO A6 (SPPN specific apps only).

3.3. Obligation of Funds Related to Data Centers (10 USC §2223a, Data Servers and Centers). Obligations, regardless of appropriation, other required approvals, or other granted authorities to acquire servers and/or equipment related to data centers (items specified below) as defined above must be approved by SAF/CIO A6 prior to execution. Exemptions are outlined below; however, data centers exempted under 10 USC §2223a, Data Servers and Centers must still be documented within the DCIMS, including IT components of weapons systems.

3.3.1. Exemptions to 10 USC §2223a, Data Servers and Centers:

3.3.1.1. Items acquired using National Intelligence Program (NIP) funds. This does not include Military Intelligence Program fund.

3.3.1.2. Items acquired using High Performance Computing Modernization Program (HPCMP) funds.

3.3.1.3. Items within data centers exempted from FDDCI as described in **paragraph 3.2.1**.

3.3.2. Items Covered Under 10 USC §2223a, Data Servers and Centers. This guidance applies to obligations of any and all funds to: construct or modify existing data center buildings, facilities, or rooms; or acquire items in the categories listed below regardless of appropriation, requirement, and/or originator.

3.3.2.1. Servers of any type.

3.3.2.2. Server software of any type.

3.3.2.3. Virtual Suites.

3.3.2.4. Storage to include Storage Area Networks (SAN), Network Attached Storage (NAS), and Direct Attached Storage (DAS).

3.3.2.5. Racks.

3.3.2.6. Uninterruptable Power Supply (UPS).

3.3.2.7. Generators.

3.3.2.8. Routers, switches, etc. (unless deployed in a facility separate from a data center or servers such as a wiring closet).

3.3.2.9. Cooling systems and environmental monitoring capabilities.

3.3.2.10. Backup capabilities, regardless of medium.

3.3.2.11. End user devices (e.g., desktops, laptops, tablets, mobile devices), and associated software and services used within a data center.

3.3.2.12. Service, support, and maintenance contracts (e.g., warranty support, preventive, routine, and emergency maintenance) for existing data center capabilities.

3.4. Data Servers and Centers Submission Preparation. Requests for obligation authority under 10 USC §2223a, Data Servers and Centers, must support a data center having an approved record in the DCIMS with a valid DOD identification number. All data centers must also have a corresponding and populated record in the Enterprise Information Technology Data Repository (EITDR). All requests for obligation authority and queries, to include requests for templates or support, must be submitted to the SAF/CIO A6 DCC team via the MAJCOM or FOA A6 to the AF Data Center Consolidation organizational mailbox: **usaf.pentagon.saf-cio-a6.mbx.a3c-a6c-afdcc-workflow@mail.mil.**

3.5. Data Servers and Centers Submission Process. Organizations must submit a spend plan for each data center maintained in DCIMS NLT 31 July of each year. Data centers in DCIMS without an approved spend plan on file with SAF/CIO A6 will be considered noncompliant. Spend plans must detail individual acquisitions for items listed in **paragraph 3.3.2** planned for the upcoming year and provide the information listed below in **paragraphs 3.5.1-3.5.7**. Organizations requiring acquisition of items not detailed on approved spend plans must submit an out of cycle request for approval to include the items listed below in **paragraphs 3.5.1-3.5.7**. Spend plans will be approved annually by SAF/CIO A6 to satisfy requirements under the purview of 10 USC §2223a:

3.5.1. Obligation Detail Matrix (format provided by SAF/CIO A6 DCC team).

3.5.2. Brief description for each acquisition.

3.5.3. A description of how each acquisition supports consolidation of infrastructure (FDCCI) and the JIE.

3.5.4. Individual purchase request or spreadsheet that shows item, quantity, and unit cost for each acquisition.

3.5.5. An approval memo signed by the wing commander, MAJCOM A6, PMO, or PEO and the approver/signer must be O6/GS-15 or higher. Approval memos must also certify that no capability exists within the base, MAJCOM, or program to satisfy the approved requirement.

3.5.6. All spend plans against a data center with an end state of "Closed" must be accompanied by an approved POAM, which clearly depicts closure before end of FY18. Moreover, the acquisitions for these data centers must clearly depict actions to realize closure.

3.5.7. A description of efficiencies realized including current and project savings in dollars or personnel, reduction in required floors space, or reduction in energy usage.

3.6. Approval Process and Timeline. The SAF/CIO A6 goal for completing review and granting approval or disapproval is 10 working days; however, this can be affected due to unforeseen circumstances. The "10 day clock" starts when all required inputs have been received and validated from the requestor. An approval code assigned by SAF/CIOA6 is required prior to execution of contracts or obligation of any and all funds for each item relating to those described in **paragraph 3.3.2**. Approval codes and associated items will be listed on the Obligation Detail Matrix attached to the SAF/CIO A6 approved spend plan and sent to the requestor.

3.6.1. Out of cycle approval codes may be obtained by sending an electronic message to the AF DCC Team at **usaf.pentagon.saf-cio-a6.mbx.a3c-a6c-afdcc-workflow@mail.mil.** Requests received prior to 1600 EST will generally be approved the same day with approval codes returned to the requestor. Requestors must present the validation e-mail provided by SAF/CIO A6 personnel via the "USAF Pentagon SAF-CIO A6 Mailbox A3C-A6C AFDCC Workflow" electronic mailbox along with the out of cycle approval code for funds to be obligated by a contracting officer. A SAF/CIO A6 approval memorandum and attached Obligation Detail Matrix must be provided for all obligations relating to items in **paragraph 3.3.2**, regardless of approval code disposition.

3.7. Requestor Reporting Requirements. All changes to data center configurations (e.g. shutting down a data center) must be reported within 30 days of the event occurring. Actual obligation amounts must be reported within 30 days of the event occurring for each item on the Obligation Detail Matrix attached to approved spend plans. Failure to comply with these instructions or instructions issued in approval memoranda results in noncompliance for the data center.

WILLIAM T. LORD, Lt Gen, USAF
Chief of Warfighting Integration and Chief
Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures,* 18 October 2013

AFI 25-201, *Supports Agreements Procedures*, 1 May 2005

AFI 33-134, *Mobile Satellite Services Management*, 10 February 2005

AFI 33-360, *Publications and Forms Management*, 18 May 2006

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

AFI 33-590, *Radio Management*, 8 April 2013

AFI 36-2619, *Military Personnel Appropriation (MPA) Man-Day Program,* 22 July 1994

AFI 38-101, *Air Force Organization,* 16 March 2011AFI 63-101, *Acquisition and Sustainment Life Cycle Management,* 17 April 2009

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

10 U.S.C. §2223a, Data Servers and Centers

AFMAN 23-110, *USAF Supply Manual,* 1 April 2009

AFMAN 33-116, *Long-Haul Communications Management*, 16 May 2013

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

AFMAN 33-153, *Information Technology (IT) Asset Management (ITAM),* 19 March 2014

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

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

AFPD 16-5, *Planning, Programming, Budgeting, and Execution Process,* 27 September 2010

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

AFPD 33-1, *Information Resources Management,* 27 June 2006

AFPD 33-3, *Information Management*, 28 March 2006

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

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

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

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

MPTO 00-33A-1001 *General Communications Activities Management Procedures and Practice Requirements,* 31 March 2010

MPTO 00-33A-1001 *General Cyberspace Support Activities Management Procedures and Practice Requirements*, 1 May 2014

MPTO 33D-2002-WA, *Cyberspace Engineering, Implementation, and Readiness Activities Management*, 30 May 2014

MPTO 00-33D-3003, *Managing the Cyberspace Infrastructure with the Cyberspace Infrastructure Planning System*, 30 December 2010

MPTO 00-33D-3004-WA, *Managing Cable and Antenna with the Cyberspace Infrastructure Planning System (CIPS) Visual Component (CVC)*, 16 July 2012

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

Public Law 112-81

T.O. 32-1-101, *Use and Care of Hand Tools and Measuring Tools*, 1 December 2004

Prescribed Forms

No forms are prescribed by this publication

Adopted Forms

AFTO Form 229, *Engineering Installation Assistance*

AFTO Form 747, *Cyberspace Infrastructure Systems Acceptance*

AFTO Form 330, *Base Blueprint Endorsement Checklist*

AF Form 673, *Air Force Publication/Form Action Request*

AF Form 847, *Recommendation for Change of Publication*

See MPTO 00-33A-1001, for other adopted forms.

Abbreviations and Acronyms

AF—Air Force (as used in forms)

AFC2IC—Air Force Command and Control Integration Center

AFCQCC—Air Force Communications Quality Control Check sheet

AFEMS-AIM—Air Force Equipment Management System-Asset Inventory Management

AFFOR—Air Force Forces

AFI—Air Force Instruction

AFIN—Air Force Information Networks

AFJQS—Air Force Job Qualification Standard

AFMAN—Air Force Manual

AFMC—Air Force Material Command

AFNIC—Air Force Network Integration Center

AFPD—Air Force Policy Directive

AFRC—Air Force Reserves Command

AFSC—Air Force Specialty Code

AFSPC—Air Force Space Command

AFTO—Air Force Technical Order

AIM—Asset Inventory Management

AIS—Automated Information System

ALC—Air Logistics Center

ANG—Air National Guard

BIN—Budget Identification Number

CDC—Core Data Center

CEIG—Cyberspace Engineering Installation Group

CFETP—Career Field Education and Training Plan

CFP—Communications Focal Point

CIO—Chief Information Officer

CIPS—Cyberspace Infrastructure Planning System

CITS—Combat Information Transfer Systems

CMDS—Communications Mission Data Set

CMO—Circuit Management Office

COTS—Commercial-off-the-shelf

CPCP—Corrosion Prevention and Control Program

CRA—Centralized Repair Activity

CS—Communications Squadron

CSC—Client Service Center

CSI—Cyberspace Systems Integrator

CSIR—Communications and Information Systems Installation Records

CST—Client Service Team

CVC—CIPS Visualization Component

DAS—Direct Attached Storage

DCIMS—Data Center Inventory Management System

DECC—Defense Enterprise Computing Center

DISN—Defense Information Systems Network

DNI—Director of National Intelligence

DOC—Designated Operational Capability

DOD—Department of Defense

DODIN—Department of Defense Information Networks

DRA—Defense Reporting Activity

DRU—Direct Reporting Unit

DSS—DISN Subscription Services

EI—Engineering and Installation (also E&I)

EIGS—Engineering and Installation Governance Structure

EITDR—Enterprise Information Technology Data Repository

ESD—Enterprise IT Service Desk

ETIMS—Enhanced Technical Information System

FAM—Functional Area Manager

FDDCI—Federal Data Center Consolidation Initiative

FOA—Field Operating Agency

GOTS—Government Off-The-Shelf

GSU—Geographically Separated Units

HPCMP—High Performance Computing Modernization Program

IAW—In Accordance With

IMDS—Integrated Maintenance Data System

IPN—Installation Processing Node

IT—Information Technology

ITAM—Information Technology Asset Management

JIE—Joint Information Environment

JTRS—Joint Tactical Radio System

LDL—Low Density Level

LSC—Logistics Service Center

LWC—Local Workcards

MAJCOM—Major Command

MOA—Memorandum of Agreement

MOC—Maintenance Operations Center

MOU—Memorandum of Understanding

MPA—Military Personnel Appropriation

MPTO—Methods and Procedures Technical Order

MSS—Mobile Satellite Services

MTO—Maintenance Tasking Order

NAF—Numbered Air Force

NAS—Network Attached Storage

NGB—National Guard Bureau

NIP—National Intelligence Program

NLT—No Later Than

NSS—National Security System

NTO—Network Tasking Order

O&M—Operations and Maintenance

OMB—Office of Manpower and Budget

OPR—Office of Primary Responsibility

PEC—Program Element Code

PMI—Preventative Maintenance Inspection

PMO—Program Management Office

POM—Program Objective Memorandum

QA—Quality Assurance

QAR—Quality Assurance Representative

RDS—Records Disposition Schedule

RSP—Readiness Spares Packages

SAF—Secretary of the Air Force

SAN—Storage Area Network

SAP—Special Access Program

SAV—Staff Assistance Visit

SCI—Sensitive Compartmented Information

SCT—Specialized Communications Team

SITREPS—Situational Reports

SLA—Service Level Agreement

SPPN—Special Purpose Processing Note (SPPN)

TACON—Tactical Control

TBA—Training Business Area

TCI—Time Change Item

TCNO—Time Compliance Network Order

TCTO—Time Compliance Technical Order

TFG—Total Force Group

TMS—Telephone Management System

T.O.—Technical Order

TODO—Technical Order Distribution Office

TRN—Turn-Around

UPS—Uninterruptable Power Supply

USAF—United States Air Force

WOMS—Work Order Management System

Terms

Air Force-Approved AIS—An Air Force-approved automated information system is any system that the Air Force maintains and operates at an enterprise level such as Cyberspace Infrastructure Planning System (CIPS), Integrated Maintenance Data System (IMDS), Training Business Area (TBA), Remedy, and Telephone Management System (TMS). MAJCOM-unique systems are not Air Force-level AISs.

Air Force Communications Special Instructions—AFCSIs provide a means to temporarily issue inspection and servicing requirements, operational performance checks, and special instructions related to standard communications equipment for which formal T.O. procedures are not yet published. They may also provide a means to issue optional or temporary modifications on communications equipment. They are only published for equipment that is applicable to more than one MAJCOM and until applicable T.O. can be developed.

Air Force-Global Information Grid (AF-GIG)—The Air Force-provisioned portion of the Global Information Grid (GIG) that the Air Force has primary responsibility for the procurement, operations, and defense. It provides global connectivity and services, in addition to C2 of that connectivity and those services that enable Air Force commanders to achieve information and decision superiority in support of Air Force mission objectives. The AF-GIG consists of fixed, mobile, and deployable facilities, and equipment, as well as processes, trained personnel and information.

Assets/Commodities—Refers to the list of communications categories that provide a communications capability: Distribution Systems, Data, Flight Support Systems, Long Haul Comm., Network Control Center, Premise Wiring, Public Address, Radio, Security, Video, and Voice Switching Systems. This includes equipment and infrastructure.

Cannibalization—Cannibalization is the removing of parts from one end item and placing the removed parts into another like item. This is done to restore systems/equipment quickly. The part is then ordered and installed into the item which the part was removed from to restore the first item.

Centralized Repair Activity (CRA)—Consolidates support and supply resources at designated locations to support dispersed equipment. It integrates support, supply and other logistics elements providing a cohesive support program that enhances logistics responsiveness and operational effectiveness while reducing costs (see AFMAN 23-110 Volume 2, Part 2, Chapter 21, Section 21N).

Certified Personnel—Certified personnel are qualified personnel who have completed hands-on performance training designed to qualify an airman in a specific position (duty position or skill-level), however they have been evaluated by an outside source (e.g., QA, Stan/Eval, Cisco, Microsoft, etc). In the CFETP, the task certifier block is used to document third party certifications if required by your Air Force Career Field Manager (AFCFM). Not all tasks require certification on the CFETP however once that specific task has been certified by an outside source, it can reflect that certification. Also to certify ATCALS equipment and systems, the qualified personnel needs to be certified on the equipment or systems being ATCALS certified.

Client Service Center (CSC)—The Client Service Center (CSC) is the work center that will perform the following functions Communications Focal Point, Voice/Video/Data/Personnel Wireless Communications System Appliances, Account Management, and Asset Management. These functions are responsible issuing and tracking communications systems/equipment.

Commercial-Off-The-Shelf (COTS)—COTS systems or equipment are products/items designed and manufactured for commercial use, purchased, and used "as-is" by the military.

Cyberspace—Defined in JP 1-02 as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers." Air Force considers cyberspace to be a physical domain and therefore subject to all physical laws of nature. In a physical sense, the Air Force considers cyberspace to include things such as the internet (Global Information Grid or GIG), telecommunications networks (combat communications, satellite communications), computer systems, network operations and command and control [e.g., Air Force Network Operations Center, Integrated Network Operations Security Centers (I-NOSC)], and embedded processors and controllers.

Cyberspace Infrastructure Requirement—Add a new capability in the form of a new system, asset, or a change to the network/cyberspace infrastructure configuration that affects the Communications Mission Data Set (CMDS).

Cyberspace support activity—Any actions taken to restore communications systems/equipment to operational status, to perform preventive maintenance inspections (PMI) on communications systems/equipment, and/or component, or to install or remove communications systems/equipment.

Communications Focal Point (CFP)—CFP is the consolidation of help desk, telephone trouble tickets and Maintenance Operations Center. This function tracks all communications systems/equipment and/or component outages and resides with the Client Service Center (CSC) work center.

Communications systems/equipment—Any item maintained, restored, installed or removed by cyberspace personnel to include circuits. "Communications systems" are defined as: transmission, switching, processing, systems-control, and network management systems, as well

as equipment, software, and facilities, fixed and deployable, that supports a mission area. Examples include: base telephone switches, cable plants, cable television, Automated Message Handling System (AMHS), Defense Message System (DMS), antennas, land mobile radio systems and cryptographic systems. The Air Force-provisioned portion of the Global Information Grid (GIG) that the Air Force has primary responsibility for the procurement, operations, and defense. It provides global connectivity and services, in addition to C2 of that connectivity and those services that enable Air Force commanders to achieve information and decision superiority in support of Air Force mission objectives. The AF-GIG consists of fixed, mobile, and deployable facilities, and equipment, as well as processes, trained personnel and information. This document implements DoD Directive (DoDD) 8100.1, *Global Information Grid (GIG) Overarching Policy*, and defines Air Force roles and responsibilities for protecting and maintaining the AF-GIG; and also encompasses terrestrial, space and airborne networks [networks are defined as all wired and wireless information (data/voice/video) exchange systems - even if not Internet Protocol (IP)-based].

Cyberspace-C—Defined in JP 102 as "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers." Air Force considers cyberspace to be a physical domain and therefore subject to all physical laws of nature. In a physical sense, the Air Force considers cyberspace to include things such as the internet (Global Information Grid or GIG), telecommunications networks (combat communications, satellite communications), computer systems, network operations and command and control [e.g., Air Force Network Operations Center, Integrated Network Operations Security Centers (I-NOSC)], and embedded processors and controllers.

Cyberspace Infrastructure—Refers to the equipment and network infrastructure to provide the internet, telecommunications network, network operations, command and control and embedded processors and controllers.

Engineering Installation—Program that provides engineering, implementation, restoral, removal and reconstitution of Air Force cyberspace infrastructure. The program focuses on the highest priority cyber infrastructure requirements impacting the Air Force.

Executive Agent—Indicates a delegation of authority by a superior to a subordinate to act on behalf of the superior. An agreement between equals does not create an executive agent. Designation as executive agent, in and of itself, confers no authority. The exact nature and scope of the authority delegated must be stated in the document designating the executive agent. An executive agent may be limited to providing only administration and support or coordinating common functions or it may be delegated authority, direction, and control over specified resources for specified purposes.

Flight Commander and Flight Chief—Any officer, enlisted or civilian member fulfilling those duties serving over the flight of personnel.

Global Information Grid (GIG)—The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as

defined in section 3542(b) (2) of Title 44 United States Code (U.S.C.). The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. It includes any system, equipment, software, or service that meets one or more of the following criteria: transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services; provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services; processes data or information for use by other equipment, software, or services. (10 U.S.C. 2513).

Government Off-The-Shelf (GOTS)—Equipment, systems, and/or products that are typically developed by the technical staff of the government agency for which it is created. It is sometimes developed by an external entity, but with funding and specification from the agency. Because agencies can directly control all aspects of GOTS products, these are generally preferred for government purposes.

Hands-on—Any activity involving active participation to include actual performing the task at hand.

Joint Tactical Radio System (JTRS)—A Defense Department-wide initiative to develop a family of revolutionary software-programmable tactical radios that will provide the warfighter with voice, data and video communications, as well as interoperability across the joint battle space. The JTRS radios envisioned by DoD, expected to begin coming on line in the 2011 or 2012 timeframe, are based on software development that enables one radio to handle various waveforms.

IT Lean Process—The Information Technology Lean (IT Lean) process is a tailored version of the DOD 5000 series acquisition process specifically designed for small IT programs, and applies to systems in acquisition or sustainment including upgrades or modernizations. See AFI 63-101 for use of IT Lean in conjunction with the Security, Interoperability, Supportability, Sustainability and Usability (SISSU) process using EITDR to manage the acquisition process. See AFI 33-210 for use of IT Lean in certification and accreditation, and for scope and limitations of the IT Lean process.

Local Commercial Services—Telecommunications Services provided by the local exchange carrier (LEC) within the local area transport access (LATA).

Low Density Level (LDL)—Low density parts which are positioned at a LSC based on the number of TRNs submitted. There are very few of these parts available and it is a first come, first serve basis request. LSC manages this process in coordination with the unit.

Lead Command—The MAJCOM, DRU, or FOA assigned as the Air Force user advocate.

Maintenance Tasking Order (MTO)—Used by the AFCYBER community to assign workload to a field technician.

Network Tasking Order (NTO)—Used to direct changes to the Air Force-Global Information Grid (AF-GIG).

Quality Assessments—An element in the Quality Assurance (QA) program. Its purpose is to provide assurances, through some type of evaluation, that the Quality System functions are effective. Quality Assessment activities can be categorized as either internal or external assessments, evaluations, audits, or certifications. The QA program may use technical, personnel, and managerial evaluations to fill these requirements.

Quality Assurance (QA)—Embodies a leadership philosophy that creates and inspires trust, teamwork, and a quest for continuous, measurable improvement throughout the working/production environment in the organization. It is the commander's tool for ensuring that a process, end item or service is of the type and quality to meet or exceed requirements for effective mission operations. It performs regular evaluations on unit personnel, equipment, and programs to ensure unit is adhering to the instructions and technical publications and properly maintaining system/equipment. QA program consists of three essential elements: Quality System, Quality Assessments, and Trend Analysis. These three elements create an environment supporting the key objective of continuous process improvement.

Quality Assurance Representative (QAR)—Appointed by the commander, complete required training, then assist the QA work center in the accomplishment of evaluations.

Qualified Personnel—Personnel who have completed hands-on performance training designed to qualify an airman in a specific position (duty position or skill-level). Qualifications training occur both during and after upgrade training to maintain up-to-date qualifications and are used to determine qualified personnel. This does not mean personnel are certified.

Situational Reports (SITREPS)—Reports generated by a command and control authority/function that advises leadership of a situation.

Specialized Communications Team (SCT)—Provides a specialized maintenance and training capability above those normally found in the O&M units. SCTs perform emergency restoral of failed or degraded facilities, systems, or equipment and provide follow-on training to prevent recurrence of the problem.

Support Activities—Any actions or processes (e.g., publication management, time change management) that assist personnel with supporting the communications systems/equipment. The activities minimize fraud waste and abuse and provide common practices among all cyberspace personnel no matter the duty location.

System Affiliate—A MAJCOM or agency designated by a negotiated formal agreement with the lead.

Systems/equipment—See Communications systems/equipment.

Time Change Item (TCI)—Scheduled actions that personnel perform to support a piece of equipment. They are listed in the technical publications and occur as deemed. For example: replacement of the oil after 3000 hours of operation.

Time Compliance Network Order (TCNO)—Generated by AFCYBER/Air Force Combat Communications Center (AFCCC) and direct a change to systems/equipment. Air Force level TCNOs are converted to TCTOs if required by the Program Management Office (i.e., Combat Information Transport System [CITS], etc.).

Time Compliance Technical Order (TCTO)—Directs a modification or change to a system or piece equipment and are published by the Program Management Office (PMO).

Tools—Any device used to restore, repair, change, modify, clean, etc. a piece of communications equipment. Tools can be physical items such as a screwdriver, pad, resistor, junction boxes, hammer, pre-made cabling, etc., as well as software items such as restoral disks, software imaging disks, drivers, program software, disk duplicator, etc. These items need to be stored and maintained according to MPTO 00-33A-1001, T.O. 32-1-101 and unit guidance/policy.