1BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 17-2101

22 MAY 2018

Communications and Information

LONG-HAUL COMMUNICATIONS MANAGEMENT

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/CIO A6SE

Certified by: SAF/CIO A6S
(Maj Gen Higby)

Supersedes: AFMAN33-116, 16 May 2013

Pages: 26

This Air Force Manual defines Air Force (AF) Long-Haul Communications (LHC) and assigns responsibilities for standardization and management of Long Haul Communications in the AF. This instruction implements Department of Defense (DOD) Directive (DODD) 8000.01, Management of the Department of Defense Information Enterprise, Joint Publication 6-0, Joint Communication System, 10 June 2015, CJCSI 6211.02D, Defense Information System Network (DISN) Responsibilities, 24 January 2012 and consistent with AFPD 17-1, Information Dominance Governance and Management. It describes the procedures to provision, process and manage AF Long-Haul Communications in accordance with the Defense Information Systems Agency (DISA) circulars and documents referenced in Attachment 1. This manual applies to all AF military, civilians, and contractor personnel under contract by the Department of Defense

(DOD) who develop, use, operate, or manage AF communications and information systems. Unless otherwise specified, the term major command (MAJCOM) includes AF level field operating agencies (FOA) and direct reporting units (DRU). This publication applies to the to all AF military, civilian and contractor personnel to include Air National Guard (ANG) and the AF Reserve. 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. Send questions or comments on the content of this manual through appropriate command channels to the SAF/CIO A6S and the Air Force Long Haul Comm Flight, 38th Cyberspace Readiness Squadron (CYRS)/SCC. Refer recommended changes and conflicts between this and other publications to SAF/CIO A6S, using AF Form 847, Recommendation for Change of Publication, with information copy to AF Cyberspace Strategy & Policy Division (SAF/A6SS). 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 IAW the Air Force Records Disposition Schedule (RDS) in the Air Force Records Information Management System (AFRIMS). See Attachment 1 for a glossary of references and supporting information.

SUMMARY OF CHANGES

This manual was rewritten and must be completely reviewed. This rewrite updates the entire manual: Chapter 1, Long-Haul Communications Management; Chapter 2, Roles and Responsibilities; Chapter 3, Commercial Internet Service Provider; and Attachment 1, Supporting Information.

Chapter 1

AF LONG-HAUL COMMUNICATIONS (AF LHC) MANAGEMENT

1.1. Overview. Long Haul Telecommunications is all general and special purpose long-distance telecommunications, facilities and services (including commercial satellite services, terminal equipment and local circuitry supporting the long-haul service) to or from the base, post camp or station switch and/or main distribution frame (except for trunk lines to the first-serving commercial central office for local communications services).

1.1.1. The AF centrally provisions, manages and funds the AF enterprise Long Haul Communications transport portion of the DOD network and services called the Defense Information Systems Network (DISN) and the AF segment called the AF Information Networks (AFIN) which uses the DISN for transport.

1.1.2. DOD policy assigns Defense Information Systems Agency (DISA) the responsibility to provide end-to-end DOD Information Network (DODIN) infrastructure and to provision, manage and sustain DISN transport, services, facilities, and equipment in direct support of DOD missions, the Joint warfighter and AF operational readiness.

1.1.2.1. DOD Chief Information Officer (CIO) policy mandates all DOD Service Components and Agencies provision and fund the shared DOD network and services from DISA to promote Joint interoperability.

1.1.3. The AF Information Network (AFIN) is the AF managed segment of the DoD network known as the DODIN and its subcomponent, that is called the DISN.

1.1.3.1. The DISN is comprised of Non-Secure Internet Protocol Router Network (NIPRNET) also referred to as "Sensitive but Unclassified IP Data" and Secure Internet Protocol Router Network (SIPRNET) also referred to as "Secret IP Data".

1.1.3.2. The AF Network (AFNET) is the AF’s underlying unclassified network that enables AF operational capabilities and lines of business.

1.1.3.3. AFNET-S is the secret level AFNET also known as the classified network (Secret) that enables AF operational capabilities and lines of business.

1.1.4. The AF Long Haul Communications Flight, 38th Cyberspace Readiness Squadron (CYRS)/SCC, executes and manages all facets of the DISN Enterprise Long Haul Communications Program on behalf of the AF.

1.1.4.1. AF LHC provisioning and management guidance can be found in the AF LHC Management Handbook located on AF LHC Community of Practice (CoP):

1.1.4.2. DISA connection process guidance on DISN connectivity can be found in the DISN Connection Process Guide at:

https://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Process-Guide.

1.2. DISN Cost Recovery Overview . DISN Infrastructure Services (DISN IS) is the method established by DOD CIO and DOD-Comptroller to allocate and fund the total cost of the DISN between all DOD Military Departments (MILDEPs) and Agencies.

1.2.1. The AF's fair share of DISN cost is directed by DOD-Comptroller and released in Program Budget Decision action and paid through the Defense Working Capital Fund .

1.2.2. AF LHC portion of DISN costs support both Regular Air Force, Guard, Reserve and COCOM utilization of: DISN IS Transport Services and IP Voice/Video/Data network services plus DISA overhead costs associated with Network Operations, Network Management, Cyber Security, Information Assurance, Network Support Services, Operational Support Systems, DISA Gateway Infrastructure, DISA Satellite Standard Tactical Entry Points (aka STEP Sites), and DOD Internet Access Points.

1.2.2.1. AF funded DISN IS Voice/Video/Data network services are: Transport (aka bandwidth) between two (2) DISN Node locations, Sensitive but Unclassified (SBU) Voice (VOIP and DSN), Voice over Secure IP, Global Video Service, SBU IP Data/SECRET IP Data (formerly DISN NIPRNET/SIPRNET), and DISN Virtual Private Network Services.

1.2.3. All AF organizations, as management headquarters, provision and budget for unique and base-level non-DODIN/DISN infrastructure, systems, and services.

1.3. Evolution of DOD and AF AFIN/DODIN Networks.

1.3.1. "Everything over Internet Protocol (IP)". DoD CIO mandated DISA and the MILDEPs/Agencies transition to IP due to evolving Information Technologies (IT) requirements, increasing cyber security needs, and drive to reduce the cost of the DISN. Part of this effort is the elimination of all legacy technologies and equipment from the DISN.

1.3.1.1. Ensure AF alignment with established DoD waiver process for those DOD and AF mission systems that still require legacy transport.

1.4 Automated Tools for Provisioning, Tracking and Funding Management. The following systems provide AF users the ability to provision, manage, fund and track all circuit and services associated with their AF LHC provisioning requests. AF users requiring access to the following tools can register for an account and request appropriate role(s).

1.4.1. AF Telecommunications Certifications Office Support System (TCOSS): AF LHC Flight manages and sustains the web enabled TCOSS tool that provides the real time availability of funds prior to the approval of provisioning actions. Funding Officials can monitor and track AF corporate and DOD customer LHC expenditures. The TCOSS database repository supports electronic DISA/DITCO circuit provisioning and acquisition messages (current and historic) needed to manage worldwide AF LHC circuit and service actions.

1.4.2. AF Technical Control Administrative Tool Set (TCATS): AF LHC Flight developed and manages TCATS, a web enabled tool that is automated and integrated within TCOSS to leverage its' database of current and historic provisioning actions. TCATS provides AF users the ability to manage, track, report and analyze AF provisioned circuit and trunk information to increase the quality of management decisions and outage reporting data for Air Force, Army, Navy, and Marine Technical Control Facilities (TCF) world-wide. TCATS replaced the stand alone version of Facility and Circuit Information Tracking (FaCIT).

1.4.3. DISA StoreFront: DISA developed and manages as a suite of tools used to request telecommunication circuits, services and products.

1.4.4. DISA Telecommunication Services Enterprise Acquisition Services (TSEAS) Inventory and Billing Information (TIBI): TIBI application provides DISA customers the ability to monitor their Telecom and IT inventory and billing information.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Air Force. The Department of the Air Force in accordance with DOD Directive 5100.01 shall organize, train, equip, and provide air, space, and cyberspace forces for the conduct of prompt and sustained combat operations, military engagement, and security cooperation in defense of the Nation, and to support the other Military Services and joint forces. Long Haul Communication is an enabler for air, space and cyberspace forces, the Air Force responsibilities for DISN LHC are:

2.1.1. Program, budget, fund, and provide support for the DISN, and the DODIN as required.

2.1.2. Coordinate with DISA on all activities related to DISN Command, Control, Communications, and Computers and information systems for which DISA has development, execution, review, integration, testing, or support responsibilities.

2.1.3. Identify support requirements for DISA networks, telecommunications, and IT systems, services, and capabilities to the Director, DISA, in accordance with DoDD 5105.19.

2.1.4. Centrally manage, procure, operate, manage, and maintain their portion of the DODIN, and the supporting infrastructure, establish, and extend AFIN services.

2.1.5. Per Joint Pub 6-0 - Service components and assigned support organizations should designate a single office within their communications staffs to coordinate with joint force J-6. All Service component communication support organizations should:

2.1.5.1. Formulate and publish plans, orders, and internal operating instructions for the use of their communications systems.

2.1.5.2. Ensure their technical control facilities perform network control and reconfiguration. For example, they change circuit paths, direct troubleshooting to resolve problems, and provide status information.

2.1.5.3. Account for traffic management in a packet-routed environment and execute circuit management functions.

2.2. Headquarters Air Force/Secretary of the Air Force.

2.2.1. The Assistant Secretary for Acquisition (SAF/AQ):

2.2.1.1. Coordinates with the SAF/CIO A6 to ensure all procured and developed AFIN components and systems clearly identify and program for DISN and DODIN bandwidth requirements and costs.

2.2.1.2. Coordinates with SAF/CIO A6 and the Deputy Under Secretary of Air Force, Management (SAF/MG) to develop and publish guidance and processes to ensure the bandwidth efficiency of systems that impact the AFIN infrastructure.

2.2.1.3. Provides policy and direction to ensure efficient procurement of LHC resources.

2.2.2. The Assistant Secretary for Financial Management (SAF/FM):

2.2.2.1. Ensures AF LHC corporate bill is funded in the execution year.

2.2.2.2. Ensures compliance with requiring Economic Analysis as identified in AFI 65-501 which dictates the inclusion of all costs associated with DISN bandwidth.

2.2.3. The Chief of Information Dominance and Chief Information Officer (SAF/CIO A6), through their assigned staff support:

2.2.3.1. Provides policy and direction to ensure effective and efficient management of LHC resources including circuits, services, systems, equipment, and personnel.

2.2.3.2. Approves or disapproves DODIN waivers in accordance with CJCSI 6211.02, enclosure D, sections 10 and 11, and DISA's connection process guide **http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Process-Guide**.

2.2.3.3. Programs Element Monitor's (PEM's) for Program Element 33126 will coordinate with AF LHC Flight/38 CYRS/SCC to ensure funding requirements are appropriately programed and funded through the corporate structure.

2.3. AF Long Haul Communications Flight, 38th Cyberspace Readiness Squadron/SCC (38 CYRS/SCC). The AF LHC Flight is the Air Force's DISN LHC Program manager who:

2.3.1. Executes Program Manager responsibilities for the DISN LHC on behalf of the Headquarters, Air Force to include the planning, programming and budgeting for the LHC program and management of the AF corporate DISN LHC requirements.

2.3.2. Serves as the AF LAFO.

2.3.3. Serves as the AF Top Registration Authorized Official in DISA StoreFront for approving roles (Registration Official, LAFO, and Routing List Official).

2.3.4. Assists SAF/CIO A6 in the development of AF policy and procedural guidance on the acquisition and management of DISN LHC services.

2.3.5. Provides AF customers guidance on how to process DoDIN waivers. Details on the DOD Waiver process can be found in DISN Connection Process Guide appendix G located at **https://www.disa.mil**.

2.3.6. Manages the Consolidated MAJCOM Circuit Management Office (CMO) for all MAJCOMs and executes the consolidated MAJCOM CMO duties as identified in Chapter 2, paragraph 2.8.2.

2.3.7. Manages the AF Enhance Mobile Satellite System (EMSS), Inmarsat, and Teleport Program providing subject matter expertise assistance to AF users and recommendations to SAF CIO on commercially leased DISN satellite services.

2.3.8. Manages and sustains TCOSS repository for: all current and historical AF/Army provisioning documents; financial management and tracking of all AF/Army requirements; tracking of all commercially leased AF EMSS and Inmarsat services; and Networx/ Enterprise Infrastructure Solutions commercially leased long distance voice services.

2.3.9. Develops, releases, manages and sustains the TCOSS integrated TCATS tool to assist AF communication offices alignment with DOD/DISA policy directing management of their LHC responsibilities.

2.3.10. Provides direct provisioning oversight and management of all corporately funded enterprise SBU IP Data (formerly NIPRNET), Secret IP Data (formerly SIPRNET) and DISN Virtual Private Network (VPN) requirements for all MAJCOMs.

2.3.11. Provides direct management oversight on corporate AF LHC funding appropriations and MAJCOM dedicated funding. The AF LHC Financial Analysts:

2.3.11.1. Serve as AF Program Designator Code (PDC) manager. Reviews local funded codes created by Management Headquarters, Agencies, Units and COCOMs.

2.3.11.1.1. Establish a line of accounting and funding for all new PDCs with an AF Form 406, Miscellaneous Obligation/Reimbursement Document (MORD), and ensure all new PDCs are loaded by Defense Information Technology Contracting Office (DITCO) in the billing system.

2.3.11.1.2. Create, manage, and track PDC(s) for all AF corporately funded and MAJCOM dedicated LHC circuits and services.

2.3.11.3. Ensure Defense Finance and Accounting Services posts expenditures correctly and expeditiously.

2.3.11.4. Manage AF LHC Program Element 33126F.

2.3.11.4.1. Project and submit AF LHC Future Year Defense Program (FYDP) budget estimate.

2.3.11.4.2. Develop and implement current year spend plan.

2.3.11.4.3. Coordinate with AF LHC Core Function Lead Integrator to rectify shortages or overages in execution year.

2.3.11.5. Receive financial/execution plan (D-22s) from MAJCOMs. Ensures that financial/execution (D-22) transfers cover costs for existing requirements.

2.3.11.5.1. Pay MAJCOM dedicated LHC bills on behalf of their command.

2.3.11.6. Manage the DISA and the OSD Statistical Sampling Report.

2.3.11.6.1. Receive OSD Statistical Sampling Report from DITCO.

2.3.11.6.2. Forward report to appropriate Lead Authorized Funding Official (LAFO) / Authorized Funding Official for validation.

2.3.12. Assists SAF/CIO A6 as SME in support of AF and Major Command IG teams.

2.3.13. Serves as the AF customer interface and focal point with DISA, DITCO, and the General Services Administration (GSA) for long-haul circuit and service requirements.

2.3.14. Coordinates with DISA, DITCO, GSA, commercial venders, and users to resolve management, acquisition, and technical issues with LHC systems, circuits, equipment, and services. Identifies problems, facilitates solutions, and requests changes and improvements to the AF, the DISA, and DOD long-haul process.

2.3.15. Serves as the AF Transition Lead and Designated Agency Representative Administrator for GSA's Networx/Enterprise Infrastructure Solutions (EIS) contracts by acting as the:

2.3.15.1. AF focal point for registration and maintenance of Agency Hierarchy Codes through DITCO and requesting user entitlements to vendor web-based portal applications directly from the vendor.

2.3.15.2. AF lead manager for Networx/EIS Fair Opportunity Source Selection activities and subsequent contracts.

2.3.15.3. AF Networx/ EIS inventory transition manager.

2.3.16. Denies/terminates DISN LHC requests when it is in the best interest of the AF. This activity will not be accomplished indiscriminately and shall be coordinated with the customer.

2.3.17. Represents the AF at meetings, conferences, workshops and surveys with civilian, government, DOD, Joint Chiefs of Staff, Major Commands, FOA, DRU, and Joint agencies pertaining to DISN LHC.

2.3.18. Represents the AF with government and DOD procurement actions involving long-haul requirements and participates in contract evaluation panels.

2.3.19. Participates in working groups internal and external to AF, providing LHC technical and/or procedure SME recommendations and guidance.

2.3.20. Coordinates with all appropriate organizations (DISA, the AF customers/mission system managers, sister services, COCOMs and other DOD Agencies) regarding contract transitions which affect circuits, equipment, and services.

2.3.21. Forwards National Security Emergency Preparedness (NS/EP) appointment letters to Department of Homeland Security TSP Program Office. (**tsp@hq.dhs.gov**)

2.3.22. Manages the expired/expiring Communications Service Authorization (CSA) program to ensure commercial circuits and services are re-awarded or discontinued IAW DISA Global Contract Re-award Actions Tactics, Techniques, and Procedures.

2.4. Major Commands, Management Headquarters (MHQ), AF level Organizations will:

2.4.1. Execute LAFO duties as detailed in Chapter 2, paragraph 2.11 of this AFMAN.

2.4.2. Appoint a Long Haul Comm point of Contact (POC) for circuit management and LHC related issues and forward appointment letter to AF Long Haul Communication Flight, 38 Cyberspace Readiness Squadron/SCC. (T-3)

2.4.3. Appoint a LAFO and alternate and forward appointment letter to 38 CYRS/SCC. If the LAFO and alternate are identified as the LHC POC state that in the LAFO appointment letter.

Note: AF-level FOAs and DRUs that do not have LHC requirements (circuits and services) do NOT need to appoint a LHC POC or LAFO and alternate.

2.4.4. Appoint one or more Telecommunications Service Priority (TSP) NS/EP Invoking Officials in writing IAW NCS Directive 3-1 Telecommunications Service Priority.

(TSP) System for National Security Emergency Preparedness (NS/EP); NCS Manual 3-1-1 TSP Service User Manual for the Telecommunications Service Priority (TSP) Systems; DISAC

310-130-1 Submission of Telecommunications Service Requests; and DISAC
310-130-4 Defense User's Guide to the Telecommunications Service Priority (TSP) System

2.4.3.1. Invoking Officials validate and authorize all NS/EP provisioning requests for telecommunications services before invoking NS/EP procedures in accordance with DISAC 310-130-4, Chapter 6.

2.4.4. Identify programmed funds during the Fiscal Year Execution Plan that will be transferred to 38 CYRS/SCC using the Functional Realignment process, commonly known as financial/execution plan (D-22) transfers. Transfer additional funds during the Fiscal Year when financial/execution plan (D-22) transferred funds are insufficient to cover additional or changing requirements.

2.4.5. Ensure all subordinate organization(s) contractor DISN SBU IP DATA and SECRET IP DATA connection(s) align with all guidance in the DISA DISN Connection Process Guide (CPG).

2.4.6. Ensure AF Management HQ's and subordinate organization(s) whose transport requirements exceed existing available DISN capabilities are funded to cover those requirements for up to two years until AF corporate adjusts Program Objective Memorandum (POM) submission.

2.4.7. Work with non-AF tenants to coordinate cost impact of LHC requirements that exceed available DISN infrastructure.

2.4.8. Validate, approve and transmit AF Top Secret/Sensitive Compartmented Information (TS/SCI) TS/SCI IP DATA and NSANet requirements and network connections

2.5. AF Installations will:

2.5.1. Ensure AF main operating bases (MOBs) have a DISN presence as stated in CJCSI 6211.02 and provide requisite site support (known as Title 10 responsibilities) for DISN equipment located on bases, posts, camps, and stations.

2.5.1.1. Provide Title 10 responsibilities of power, physical security, floor space, and onsite support coordination for the base DISN network Point of Present.

2.5.1.2. Provide Base Operations Support to DISN LHC infrastructure installed on the base. The AF Installation may delegate appointed responsibilities to the base Communications Squadron/Flight. The main authority/delegated authority:

2.5.1.2.1. Appoint a DISN Node Site Coordinator (NSC) and alternate in accordance with DISAC 310-55- 9 paragraph C2.1.2, for base level support of the DISN on AF installations where DISN equipment resides. The appointment letter must be updated and resubmitted when any of its content changes and verified at least annually.

2.5.1.3. Manage base LHC functions (both DISA-provided transport/services and commercial long distance services) obtained through GSA, Networx/EIS and/or other government-wide DOD-authorized contracts, in accordance with DISACs and this AFMAN.

2.5.1.4. Implement procedures to safeguard all DISA-owned DISN equipment assigned to the installation against loss, damage, destruction, misuse, or pilferage.

2.6. All AF Organizations that own/fund DISN LHC circuits/services must:

2.6.1. Appoint an Authorized Funding Official (AFO) in writing to their management headquarters Lead Authorized Funding Official (LAFO). The AFO is the unit level individual responsible for managing LHC funding/paying for circuits and services.

2.6.2. Execute AFO duties as detailed in Chapter 2, paragraph 2.10 of this AFMAN.

2.6.3. Submit requests to terminate unused AF funded circuits or services when no longer required.

2.7. All Air Force Centers, Agencies, and Other Key Stakeholder will:

2.7.1. Validate centrally funded SBU IP DATA and SECRET IP DATA transport connections, and Internet Protocol addressing, on-site assistance requests and systems configuration. This responsibility includes conducting Review & Revalidation on connections every 2 years.

2.7.1.1. Submit requests to terminate unused AF funded SBU IP DATA and SECRET IP DATA connections when no longer required.

2.7.2. Program Management Offices:

2.7.2.1. Ensure networked systems that use LHC transport are bandwidth-efficient and include implementation of software and/or hardware compression/acceleration technologies where possible.

2.7.2.2. Determine system LHC bandwidth requirements by base/site and submit circuit bandwidth requirements according to the AF LHC Requirements Process.

2.7.2.3. Review/revalidate bandwidth requirements prior to initial fielding.

2.7.2.4. Program for DISN LHC costs as part of overall lifecycle costs and Program Objective Memorandum.

2.8. Functional LHC Circuit Management Office (CMO) Responsibilities.

2.8.1. MAJCOM level CMO workload responsibilities were consolidated under the AF LHC Flight at 38 CYRS/SCC.

2.8.2. All CMO not part of the MAJCOM CMO’s consolidation effort retain their CMO responsibilities to:

2.8.2.1. Provision, track, and manage LHC circuits and service throughout their life cycle.

2.8.2.2. Register and obtain appropriate role assignments in DISA StoreFront provisioning tool and AF TCOSS for their respective organizations. All CMO’s will:

2.8.2.2.1. Prepare, review, validate, approve, and/or reject Service Requests in DISA StoreFront for long-haul circuits, services, and equipment submitted by subordinate organizations.

2.8.2.2.2. Assist and guide subordinate organizations on LHC management which include (but not limited to user account registration in DISA StoreFront and AF TCOSS required to manage LHC circuits, services and funding.

2.8.2.2.3. Prepare orders in accordance with DISAC 310-130-1 and DISA Provisioning Notices.

2.8.2.3. Identify and obtain special circuit considerations (i.e. diversity, avoidance, redundancy, and survivability) to meet mission specifications.

2.8.2.4. Identify proper TSP level (DISAC 310-130-4 and DISAC 310-130-1).

2.8.2.5. Ensure TS/SCI connections (TS/SCI IP DATA, NSANet) are submitted for validation and approval to the appropriate A2 designated office.

2.8.2.6. Ensure all Defense Service Network (DSN) dedicated precedence service requests are approved in accordance with CJCSI 6211.02.

2.8.2.7. Manage expired/expiring CSA program to ensure commercial circuits and services are re-awarded or discontinued in accordance with DISA Global Contract Reaward Actions.

2.8.2.7.1. Ensure DOD CIO endorsed DISA/DITCO policy is followed which states zero tolerance for expired CSAs. DISA/DITCO intent is to issue vendors a non-revocable termination letter within two weeks of CSA expiration date.

2.8.3. Technical Control Facility (TCF), Patch and Test Facility (PTF), and/or Circuit Actions.

2.8.3.1. Responsible for base LHC management in accordance with all DOD Directives and Instructions, DISA Circulars (DISACs), DISA Notices, and AF policies.

2.8.3.1.1. Technical Control Facilities and Patch and Test Facilities in the Pacific area should follow the Pacific area guidance in DISAC 310-70-1 DISA PAC Supplement 1 and DISA PAC C 310-70-58 along with other DISA PAC circulars as they apply.

2.8.3.1.2. TCFs identified as Facility Control Offices or Intermediate Facility Control Offices should follow DISAC 310-70-1 DISA PAC Supplement 1 guidance.

2.8.3.2. Register, at a minimum, two Authorized Requesting Officials in DISA StoreFront provisioning tool who:

2.8.3.2.1. Prepare, submit, manage, and track Service Requests (SRs) in DISA StoreFront for long-haul comm circuits, services, Networx/ Enterprise Infrastructure Solutions requirements and equipment requests for the Base and supported Geographically Separated Units (GSU) that receive AF LHC services from the installation.

2.8.3.3. TCF's and PTF's must establish and maintain:

2.8.3.3.1. Provisioning records and permanent/temporary circuit history folders.

2.8.3.3.2. Site specific systems diagrams that depict signal flow through the facility readily available in the operations area of the Tech Control Facility (TCF), Patch and Test Facility (PTF), or Network Control Center (NCC) to aid restoration and troubleshooting efforts.

2.8.3.3.3. Circuit Layout Records which is a drawing that depicts the physical layout of trunks and circuits.

2.8.3.3.4. Master Station Log which is a record of information on significant events occurring within the area of assigned responsibility.

2.8.3.4. Track facility, link, trunk, circuit, channel, equipment outages, and HAZCONs within the activity area of responsibility. Outage and restoration records are maintained in accordance with DISAC 310-70-1 and DISAC 310-55-1.

2.8.3.5. Establish a trend analysis program on all circuits, trunks for which they are the Circuit Control Office (CCO) or servicing activity, and on all circuits and trunks which terminate at their station in accordance with DISAC 310-70-1 and DISAC 310-130-2.

2.8.3.6. Maintain an inventory of all base telecommunications equipment and services in accordance with CJCSI 6211.02. (T-0)

2.8.3.7. Review and revalidate all requirements for base telecommunications equipment and services. (T-0)

2.8.3.7.1. Terminate services that are uneconomical or no longer needed in accordance with CJCSI 6211.02. (T-0)

2.8.3.8. Coordinate Authorized Service Interruptions (ASIs) with Subordinate units, affected AF customers and tenant organizations. Submit concurrence or non- concurrence to the base Communications Focal Point for SBU I DATA, SECRET IP DATA, and 24 AF designated mission critical circuits. All other ASI's are coordinated directly with DISA and guidance in DISAC 310-55-1, Status Reporting. (T-3)

2.8.3.9. Coordinate and schedule power outages (i.e. base Civil Engineering) with DISA, Major Commands, Cyber Operations Flight/690 Network Support Squadron, and affected AF customers that will impact communication facilities, rooms, racks, and equipment.

2.8.3.10. Within 30 days of new circuit activation and annually thereafter, send DODIN user notification letters to each user in accordance with DISAC 310-70-1. (T-3)

2.8.4. ANG/AFRC Bases without Technical Control Facility/Patch and Test Facility

2.8.4.1. ANG/AFRC tenant units collocated on main operating bases do not have to accomplish the Tech Control Facility/Patch and Test Facility roles and responsibilities defined above since the host base provides that support.

2.8.4.2. ANG/AFRC tenant units can be a CCO/CMO and can accomplish CCO/ CMO duties as detailed in the located on the AF LHC Community of Practice (CoP).

2.9. AF DISN Node Site Coordinator (NSC) responsibilities with DISN equipment presence.

2.9.1. Appropriate base level organization appoints a primary and alternate DISN NSC in accordance with DISAC 310-55-9, paragraph C2.1.2.1.

2.9.1.1. Email copy of the NSC appointment letter to the appropriate DISA theater office and to the AF LHC Flight, 38 CYRS/SCC.

2.9.2. The NSC will support DISA and accomplish their roles and responsibilities identified within CJCSI 6211.02, DISAC 310-55-9, and DISAC 310-70-1. AF units located in the Pacific and Europe theater should follow the additional guidance provided in the DISA Pacific and Europe Field Commands supplements to DISAC 310-70-1.

2.9.3. Training. All NSC's are required to complete the DISA NSC training in accordance with DISAC 310-55-9. The NSC appointment letter must be up-to-date, and on file with DISA theater coordinator to register and obtain training. A Node Site Coordinator appointee who requires training will contact their DISA theater coordinator and once verified, submit training request to HQ DISA POC.

2.10. Authorized Funding Official (AFO) for organizations who fund and own DISN AF LHC circuits and/or services must:

2.10.1. Appoint an AFO in writing to their Headquarters level LAFO. An AFO is a civilian or military personnel at unit level responsible for approving and managing LHC funding for circuits and services. AFOs can only request access to their assigned PDC's.

2.10.1.1. AFO's will:

2.10.1.1.1. Update at the start of each fiscal year the funding PDC with a certified MORD number, Line of Accounting (LOA), and Customer Account Information in TIBI (T-0)

2.10.1.1.2. Approve and/or disapprove DISA StoreFront Service Requests.

2.10.1.1.3. Reconcile LHC invoices for all DISN ordered telecommunications equipment and services, CSA's and/or other acquisition documents before authorizing payment. (T-0)

2.10.1.1.4. Submit PDC requests to 38 CYRS/SCC Financial Analyst point of contact.

2.10.1.1.5. Validate OSD/DITCO Quarterly Statistical Sampling invoice in TIBI when requested by 38 CYRS/SCC Financial Analyst. (T-0)

2.11. Lead Authorized Funding Official (LAFO) are located at:

2.11.1. Headquarter level organization who fund and own DISN LHC circuits/services must appoint a Headquarters level primary and alternate LAFO in writing to AF LHC Flight, 38 CYRS/SCC Circuit Management Office.

2.11.1.1. A LAFO is a civilian or military personnel who is responsible for approving and managing LHC funding for DISN circuits and services. The LAFO provides management oversight to their units AFO and the Authorized Billing Officials (ABO) along with process guidance in regard to management of DISN LHC funding.

2.11.1.2. The LAFO responsibilities are to:

2.11.1.2.1. Ensure unit's under their purview reconcile their monthly LHC invoices for telecommunications equipment and service inventories, CSA's, and/or other acquisition documents before authorizing payment.

2.11.1.2.2. Ensure units obtain access to Networx/Enterprise Infrastructure Solutions (EIS) vendor on-line systems for commercial long distance usage and billing data by contacting the AF EIS Program Administrator at AF LHC Flight, 38 CYRS/SCC.

2.11.1.2.3. Approve role requests under their command within two business days of receiving role request notification. (T-3)

2.11.1.2.4. Approve role requests to an AFOs assigned funding PDC's.

Note: Only AF level LHC personnel have access to all AF PDC’s. A LAFO may approve an ABO role requests with (%) TIBI access to multiple funding codes.

2.11.1.2.5. Ensure all AFO contact information is up-to-date for primary and alternate AFOs in TIBI database for local funded program codes under their Headquarters. (T-3)

2.11.1.2.6. Submit locally funded PDC worksheet to AF LHC Flight Financial Managers.

2.11.1.2.7. Provide training to AFO’s under their area of responsibility.

Chapter 3

COMMERCIAL INTERNET SERVICE PROVIDER (ISP)

3.1. Commercial Internet Service Provider (CISP) Connection

3.1.1. Types. CISP connections do not connect to the AF Information Network infrastructure and require authorization through the DoD and AF DISN waiver process. Information Services (ISs) that process, store and transmit DoD data using a CISP connection must perform categorization in accordance with DoDI 8510.01 tailored appropriately to determine the set of security controls to be implemented with the approval of the IS's Authorizing Official (AO). Tailoring of security controls must take into account the sensitivity of the data being processed, stored, and transmitted (e.g., controlled DoD data, publically releasable data) and protection of the supporting IS. The CISP connection cannot be connected directly to the DISN. Use of an approved hardware/software secure tunnel (IPSEC only) such as an AF- approved, virtual private network (VPN) across a CISP circuit to connect to the DISN/AF Information Network (AFIN) is allowed. Tunneling classified data via a CISP requires a DODIN waiver based in DoD Policy. These systems shall not be connected to the base network/NIPRNET with the privileges of ".mil" registered users. CISPs will not be used to host classified systems directly, a CISP connect can only be used to tunnel the classified connection.

3.1.1.1. Controlled unclassified DoD data can be authorized over CISP based upon the following use cases conditions. The Authorizing Official must stipulate appropriate security controls for the supporting IS as state in DODI 8510.01. For AF guidance see AFI 17-101, Risk Management Framework (RMF) for AF Information Technology (IT).

3.1.1.1.1. Training Connections. Commercial training circuits are connections used to exercise COOP, military operations, or contingency plans, or as a secondary communication link for force protection. These connections are normally less than 90 days and the requirement formally documented.

3.1.1.1.2. Temporary Facilities/Urgent or Ad Hoc Missions. Provisional commercial connections installed to support temporary facilities or missions due to DoD employee relocation caused by military construction, natural disaster, or unforeseeable events where the AFIN is not available or would be cost-prohibitive to install due to the temporary nature of the need.

3.1.1.1.3. Infrastructure Non-availability. Interim commercial connections installed to support AF IT requirements due to loss of telecommunication infrastructure (Outside plant cabling system, communication nodes, etc.) caused by natural disaster, significant equipment refresh, repairs, or unforeseeable events where the AFIN is not available or would be cost- prohibitive to install due to the temporary nature of the need.

3.1.1.1.4. Stabilization and Reconstruction, Disaster Relief (SRDR), and Humanitarian and Civic Assistance Operations. Per reference (DODI 8220.02), United States task forces may support civil-military partners in SRDR and civic assistance operations. These operations may include extending IT services to Foreign National First Responders and other International health care organizations and assistance organizations. To ensure security of the AFIN, these connections will normally be commercial in nature and include Wireless Access Points (WAPs), SATCOM, links, or terrestrial connections on Foreign telecommunication infrastructure for emergency response trucks/trailers and mobile emergency operations centers.

3.1.1.1.5. Recruiting. Due to the location (e.g., strip malls, commercial buildings), number of users (5 – 7), and mobile quality of recruiting stations (recruit from the youth population), it is cost prohibitive to procure anything but commercial connections for recruiting offices; however, these connections will comply with all DoD cybersecurity policies.

3.1.1.1.6. Force Protection and Public Safety. DoDI 5535.10, Coordination of DoD Efforts to Identify, Evaluate, and Transfer DoD Technology Items, Equipment, and Services to Federal State, and Local First Responders, directs DoD entities to support interagency efforts with the Department of Homeland Security (DHS) and other Federal, State, and local agencies to combat threats to the homeland. Coordination and information sharing with civil First Responders in an accessible information environment is necessary to protect and defend tenants onboard, and directly adjacent, to DoD Installations to enable emergency management activities. All commercial connections deemed necessary to support these requirements will be documented in an Installation Emergency Management (IEM) plan in accordance with DODI 6055.17, DoD Emergency Management (EM) Program. CISP connections will comply with applicable Federal and Civil or Tribal government mandates, standards, or regulations.

3.1.1.1.7. Civil Authority Databases. Connections to data repositories such as National Crime Information Center (NCIC), Terrorist Screening Database, Department of Homeland Security database (E-Verify and U.S. VISIT), and other authoritative data sources to vet the claimed identity and to determine fitness to access an Installation or site to remain in compliance with Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control. Connections to global crime databases for criminal justice information (CJI) retrieved through DoD Identity Management Capability Enterprise Services Application (IMESA) used and acted upon in accordance with existing law enforcement procedures.

3.1.1.1.8. Payment Card Industry. AF organizations processing Automatic Teller Machine (ATM) or Point of Sale (POS) transactions must connect to civilian financial institutions and credit card companies to process these requests. At a minimum, protect financial transactions conducted via the internet (e.g. Defense Travel System, transient housing or Morale Welfare & Recreation (MWR) hotels, Defense Exchange Commissary Agency (DECA), etc.) in accordance with Payment Card Industry Data Security Standards (PCI DSS) using Federal Information Processing Standard (FIPS) 140-2 encryption.

3.1.1.2. Publically releasable DoD data can be authorized over CISP based upon the following use cases conditions. The Authorizing Official will tailor the appropriate security controls for the supporting IS in accordance with DODI 8510.01.

3.1.1.2.1. Community Relations Events/Public Affairs. CISP connections to support community relations events or Public Affairs may be temporary or permanent. Temporary CISPs are connections to support events held to extend good will to communities located adjacent to AF Installations. Permanent CISPs are connections to support requirements that cannot be supported by a DISN connection. Permanent CISP connections are often required to support Public Affairs Offices and Service Broadcast Television Stations for shared data exchange with commercial entertainment institutes and activities.

3.1.1.2.2. Non-Appropriated Fund Instrumentalities (NAFIs). NAFIs may not be fully funded with appropriated funds; therefore, commercial connections are usually procured and funded with NAF to ensure compliance. Further guidance on the level of support and types of NAFIs that may be partially supported with appropriated funds are found in DODI 1015.10, Military Morale, Welfare, and Recreation (MWR), and DODI 1015.15, Establishment, Management, and Control of Nonappropriated Fund Instrumentalities and Financial Management of Supporting Resources.

3.1.1.2.2.1. The Quality-of-Life (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.

3.1.1.2.2.2. 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).

3.1.1.2.2.3. For Internet access in dormitories, refer to AFI 32- 6005, Unaccompanied Housing Management.

3.1.1.2.3. Morale, Welfare and Recreation (MWR) Activities. Internet-based Capabilities (IbCs) are generally internet services for military exchanges, internet cafes, and lodging programs, provided by MWRs, for use by authorized patrons, see DoDI 8550.01, DoD Internet Services and Internet-Based Capabilities, for guidance. Other examples of IbCs include Wounded Warrior housing, hospitals/clinics, Wounded Warrior fundraising events, etc.

3.1.1.2.4. DoD Dependent Schools and Base Education Offices. Internet access for classroom education or civilian education institutions must be through a commercial ISP (or DISAs Private ISP when available) and cannot be connected to NIPRNET.

3.1.1.2.5. Headquarters Air Education and Training Command (HQ AETC) and the United States AF 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.

3.1.1.2.5.1. Authorizing Official Approval is required for AETC and USAFA operated education and training academic networks.

3.1.1.2.5.2. AETC and USAFA operated education and training academic networks are exempt from the DoD Information Network (DODIN) Waiver process if they do not process, store, or transmit sensitive information.

3.1.1.2.5.3. AETC Recruit, Training, and Education Action Officer (RT&E) developed an in-house DODIN Waiver Exemption Process that precludes the need to go through the DODIN Waiver process if unit meet certain criteria similar to quality of life (e.g. education/training centric, no For Official Use Only data, no malware).

3.1.1.2.6. Geographically Separated Unit (GSU). The GSU owning Major Command or Management Headquarters will fund any network circuit(s) required for GSU connectivity. GSUs will comply with all policies and directives of servicing AFIN Operations activity including Comm Focal Point supporting their network circuit.

3.1.1.3. Requirements. Devices using the CISP must be physically or logically separated from the AFIN network and comply with applicable Security Technical Implementation Guides (STIG), Security Recommendation Guides (SRG), and other DoD cyber security policies. Register the CISP in the Systems/Networks Approval Process (SNAP) database.

3.1.1.3.1. Protect controlled DoD, Personally Identifiable Information (PII), Law Enforcement, and Criminal Investigative information from access by unauthorized personnel using role-based access methodology and FIPS 140-2 encryption for data in transit.

3.1.1.3.2. The CISP connection complies with applicable STIGs, SRGs, and other DoD cyber security policies when the application of those policies and standards will not adversely affect the mission need for the CISP.

3.1.1.3.2.1. The authorized Cyber Security Service Provider (CSSP) or other monitoring solution appropriate for the mission monitors the CISP used for controlled unclassified information (CUI) in accordance with STIGs, SRGs, and other DoD cyber security policies.

3.1.1.3.2.2. Perform annual reviews to determine if they are still needed and for compliance with the security controls and the authorization to operate (ATO).

3.1.1.3.2.3. Configure wireless technologies (access points, routers, cellular “hot spot” devices) for Wi-Fi Protected Access version 2 (WPA2) encryption.

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

3.2.1. Authorizing Official Approval is required for AETC and USAFA operated education and training academic networks.

3.2.2. AETC and USAFA operated education and training academic networks are exempt from the DoD Information Network (DODIN) Waiver process if they do not process, store, or transmit sensitive information.

3.2.2.1. AETC Recruit, Training, and Education Action Officer (RT&E) developed in-house DODIN Waiver Exemption Process precludes need to go through the DODIN Waiver process if unit meet certain criteria similar to quality of life (e.g. education/training centric, no For Official Use Only data, no malware).

BRADFORD J.SHWEDO, Lt Gen, USAF
Chief, Information Dominance
and Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Joint Publication 3-12, Cyberspace Operations, 5 February 2013

Joint Publication 6-0, Joint Communication System, 10 June 2015

CJCSI 6211.02D, Defense Information System Network (DISN) Responsibilities, 24 January 2012

DoDI 5000.64, Accountability and Management of DoD Equipment and other Accountable Property, 27 April 2017

DoDI 8010.ab, Department of Defense Information Network (DODIN) Transport, draft

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

ASD (C3I) Memo, Policy Clarification Letter – Long-Haul and Regional Telecommunications Systems and Services for the Department of Defense (DoD), 5 May 1997

NCS Directive 3-1, Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NS/EP), 10 Aug 2000

NCS Manual 3-1-1, TSP Service User Manual for the Telecommunications Service Priority (TSP) Systems, 5 May 2000

DISAC 310-55-1, Enterprise Operational Reporting for the Department of Defense Information Network 9 Dec 2014

DISAC 310-55-9, Base Level Support for the Defense Information System Network Services, 4 April 2014

DISAC 310-70-1, Global Information Grid (GIG) Technical Control, 21 April 2012

DISAC 310-130-1, Submission of Telecommunications Service Requests, 19 August 2009

DISAC 310-130-2, Management Thresholds (MT5) and Performance Objectives (POs), 1 October 2012 DISAC 310-130-4, Defense User's Guide to the Telecommunications Service Priority (TSP) System, 21 October 2014

DISA-DITCO Procurement Guide for Telecommunications January 2017 replaces Circular 350-135-1,

Commercial Communications, Defense Commercial Communications Acquisition Procedures, 12 Feb 1996, includes Change 11, 14 Aug 2013

Procurement Guide – Telecommunications, January 2017

DISA/DAF Memorandum of Agreement, Property Accountability of DISA-owned Equipment (MPS- 12-011), December 2012 in effect until December 2021

AFPD 17-2, Cyberspace Operations, 12 April 2016

AFI 17-210, Radio Management, 26 May 2016

AFI 65-501, Economic Analysis, 29 Aug 2011

Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DOD Physical Access Control.

DoDI 1015.10, Military Morale, Welfare, and Recreation (MWR)

DoDI 1015.15, Establishment, Management, and Control of Non-Appropriated Fund Instrumentalities and Financial Management of Supporting Resources

DoDI 5535.10 Coordination of DoD Efforts to Identify, Evaluate, and Transfer DoD Technology Items, Equipment, and Services to Federal State, and Local First Responders

DODI 6055.17, DoD Emergency Management (EM) Program

DODI 8220.02, Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations

DODI 8510.01, Risk Management Framework

DoDI 8550.01, DoD Internet Services and Internet-Based Capabilities

Federal Information Processing Standard (FIPS) 140-2 encryption

AFI 17-101, Risk Management Framework (RMF) for AF Information Technology (IT), 02 Feb 2017

AFI 32-6005, Unaccompanied Housing Management, 29 Jan 2016

AFI 65-106, Appropriated Fund Support of Morale, Welfare, and Recreation (MWR) and Nonappropriated Fund Instrumentalities (NAFIS), 06 May 2009

Prescribed Forms

No forms are prescribed by this publication

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 406 *Miscellaneous Obligation/Reimbursement Document (MORD)*

Abbreviations and Acronyms

ABO—Authorized Billing Official

ADO—Address Directory Official

AFO—Authorized Funding Official

AHC—Agency Hierarchy Code

ARO—Authorized Requesting Official

ASI—Authorized Service Interruption

ATC—Authority to Connect

ATO—Authority to Operate

CCO—Circuit Control Office

CCSD—Command and Control Service Designated

CFLI—Core Function Lead Integrator

CIO—Chief Information Officer

CIPS—Cyberspace Infrastructure Planning System

CJCS—Chairman of the Joint Chiefs of Staff

CMO—Circuit Management Office

COCOM—Combatant Command

CIPS—Cyberspace Infrastructure Planning System

CJCS—Chairman of the Joint Chiefs of Staff

CMO—Circuit Management Office

COCOM—Combatant Command

CoP—Community of Practice

CSA—Communications Service Authorization

DCN—DISA Control Number

DISA—Defense Information Systems Agency

DISAC—Defense Information Systems Agency Circular

DISN—Defense Information Systems Network

DITCO—Defense Information Technology Contracting Office

DODIN—Department of Defense Information Networks

DSAWG—Defense Information Assurance Security Accreditation Working Group

DSF—DISA StoreFront

DSR—Delayed Service Report

DWCF—Defense Working Capital Fund

DWP—DODIN Waiver Panel

EA—Economic Analysis

EXC—Exception Report

FYDP—Future Year Defense Program

HAZCON—Hazardous Conditions

IbCs—Internet-based Capabilities

IER-In—Effect Report

IS—Internet Service

ISP—Internet Service Provider

IT—Information Technology

LAFO—Lead Authorized Funding Official

LHC—Long Haul Communications

LOA—Line of Accounting

MHQ—Management Headquarters

MILDEP—Military Departments (aka sister services)

MOB—Main Operating Base

MORD—Miscellaneous Obligation Reimbursement Document

MRC—Monthly Recurring Charge

NCS—National Communications System

NRC—Non-Recurring Charge

NSC—Node Site Coordinator

NS/EP—National Security/Emergency Preparedness

PDC—Program Designator Code

POM—Program Objective Memorandum

POP—Point of Presence

PTF—Patch and Test Facility

R&R—Review and Revalidation

RFU—Ready for Use

SAM—Status of Acquisition Message

SBU—Sensitive but Unclassified

SDB—Satellite Data Base

SDP—Service Delivery Point

SR—Service Request

SRG—Security Recommendation Guides

STIG—Security Technical Implementation Guide

TCF—Technical Control Facility

TCOSS—Telecommunications Certification Office Support System

TIBI—Telecommunication Services Enterprise Acquisition Services (TSEAS) Inventory and Billing Information

TRAO—Top Registration Authorization Official

TSEAS—Telecommunications Services Enterprise Acquisition Services

TSO—Telecommunications Service Order

TSP—Telecommunications Service Priority

TSR—Telecommunications Service Request

UC—Unified Capabilities

Wi-Fi—Wireless Fidelity