



DEFENSE INFORMATION SYSTEMS AGENCY

P.O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

DISA CIRCULAR 310-45-1

23 June 2008

ORGANIZATION

Single System Manager (SSM)
for the Defense Switched Network (DSN)

1. **Purpose.** This Circular prescribes policy and describes organizational roles, responsibilities, and functions for the Single System Manager (SSM) for the Defense Switched Network (DSN).
2. **Applicability.** This Circular applies to the Defense Information Systems Agency (DISA), the military departments (MILDEPs), and other activities of the Department of Defense (DoD) and government agencies responsible for implementing procedures (implementers) and providing DSN services (providers) to authorized users.
3. **Authority.** This Circular is published in accordance with the authority contained in DoD Directive 5105.19, Defense Information Systems Agency (DISA), 25 July 2006.
4. **Glossary of Terms.** A glossary of terms is provided in [enclosure 1](#).
5. **Policy.** This Circular is the governing directive for exercising single system management of the DSN.
6. **Circular Composition.** A summary of the history and mission of DISA and an overview of the communications relationships affecting DISA as the DSN SSM are provided in [enclosure 2](#). The SSM management of the DSN is described in [enclosure 3](#). Organizational responsibilities associated with DSN SSM are outlined in [enclosure 4](#).

FOR THE DIRECTOR:


ALAN R. LYNN
Brigadier General, USA
Chief of Staff

OPR: GS
DISTRIBUTION: W

Return to:

[Top of DISAC 310-45-1](#)
[DISAC 310-45-1 Enclosure 1](#)
[DISAC 310-45-1 Enclosure 2](#)
[DISAC 310-45-1 Enclosure 3](#)
[DISAC 310-45-1 Enclosure 4](#)
[Publications Listing](#)
[DISA Home Page](#)

cio-pubs@disa.mil - Last Revision: 23 June 2008

Enclosure 1: DISAC 310-45-1

**GLOSSARY OF TERMS FOR THE SINGLE SYSTEM MANAGER (SSM)
FOR THE DEFENSE SWITCHED NETWORK (DSN)**

APL	Approved Products List
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)
C2	command and control
C3I	command, control, communication and intelligence
C&A	certification and accreditation
CCB	Configuration Control Board
CENTREX	Central Exchange
CIO	Chief Information Officer
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CM	configuration management
CMP	Configuration Management Plan
CONUS	continental United States
DATMS	DISN Asynchronous Transfer Mode Services
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DSS	DISN Subscription Service
DVS	DISN Video Services
GIG	Global Information Grid
GoS	grade of service
IA	information assurance
ICTO	interim connection to operate
IO	interoperability
IP	Internet Protocol
JITC	Joint Interoperability Test Command
JROCM	Joint Requirements Oversight Council Memorandum
MAN	metropolitan area network
MILDEP	military department
MUF	military unique feature
NIPRNet	Unclassified but Sensitive IP Router Network

NMCS National Military Command System
NPO network performance objective
NSS National Security Systems

O&M operations and maintenance
OCONUS outside the continental United States
OSD Office of the Secretary of Defense

QA quality assurance

RFP request for proposal
RTS real time services

SIPRNet Secret Internet Protocol Router Network
SM System Manager
SMO System Management Office
SSM Single System Manager

VCAO Voice Connection Approval Office
VoATM Voice over Asynchronous Transfer Mode
VoIP Voice over Internet Protocol
VTC video teleconferencing

Return to:

[Top of DISAC 310-45-1](#)
[DISAC 310-45-1 Enclosure 1](#)
[DISAC 310-45-1 Enclosure 2](#)
[DISAC 310-45-1 Enclosure 3](#)
[DISAC 310-45-1 Enclosure 4](#)
[Publications Listing](#)
[DISA Home Page](#)

cio-pubs@disa.mil - Last Revision: 23 June 2008

**OVERVIEW OF THE SINGLE SYSTEM MANAGER (SSM)
FOR THE DEFENSE SWITCHED NETWORK (DSN)**

1. **History and Mission of DISA.** The Defense Information Systems Agency (DISA) was established as a Department of Defense (DoD) agency in 1960. By authority of the Secretary of Defense, DoD Directive (DoDD) 5105.19, Defense Information Systems Agency (DISA), places DISA under the direction, authority, and control of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO). The mission of DISA is described as being "responsible for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions to serve the needs of the President, the Vice President, the Secretary of Defense, and the DoD Components, under all conditions of peace and war."

2. **Communications Relationships Affecting the DSN SSM.**

The Defense Switched Network (DSN) is a worldwide network. For management purposes, it is subdivided into four major theaters of operation: Western Hemisphere, Europe, Pacific, and Central (Southwest Asia). The DSN is an interbase, nonsecure, and secure command and control (C2) telecommunications system for C2 and non-C2 authorized users in accordance with national security directives.

2.1 **Global Information Grid (GIG).** To accomplish its mission, DISA operates the Global Information Grid (GIG). The GIG is a 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, policymakers, 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 (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. 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.

2.2 Defense Information System Network (DISN). The DISN is the DoD global end-to-end information transfer infrastructure providing the communications infrastructure and services needed to satisfy national defense and command, control, communications, and intelligence (C3I) requirements and corporate defense requirements. The DISN includes the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet); the Secret Internet Protocol Router Network (SIPRNet); the Defense Red Switch Network (DRSN); the Defense Switched Network (DSN); the DISN Video Services (DVS); Transport Services; and DISN Asynchronous Transfer Mode ATM Services (DATMS).

2.3 Defense Switched Network (DSN). The DSN is an interbase, nonsecure or secure DoD telecommunications system that provides dedicated telephone service, voice-band data, and dial-up video teleconference (VTC) for end-to-end command use and DoD authorized C2 and non-C2 users in accordance with national security directives. Nonsecure dial-up voice (telephone) service is the system's principal service. The Director, DISA, is the designated Single System Manager (SSM) for the DSN based on DoDD 5105.19 and DoDD 8100.1, Global Information Grid (GIG) Overarching Policy; DoD Instruction (DoDI) 8100.3, Department of Defense (DoD) Voice Networks; and Chairman of the Joint Chiefs of Staff (CJCSI) 6215.01C, Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS).

2.3.1 The primary function of the DSN is to provide nonsecure voice (i.e., telephone and video conferencing) service. The DSN differs from all other circuit switched networks through the provisioning and utilization of military unique features (MUFs). A MUF consists of network and telecommunication switch features that are above and beyond those supported by commercial telephony carrier services to the general public. A MUF is intended to ensure the most critical calls receive preferential treatment in terms of call completion. Specifically, the use of precedence and preemption classmarks ensure critical calls access hardware and software resources and supplant calls of less importance when required. (MUFs are defined in detail in CJCSI 6215.01C.)

2.3.2 The DSN includes the end instruments, switches on the installations, backbone and tandem switches, transmission connectivity between and among the installations, Central Exchange (CENTREX) partitioned switches providing DSN service, network management system, timing and synchronization system,

and signaling system. Voice processing and transport technologies (e.g., Voice over Internet Protocol [VoIP] or Voice over Asynchronous Transfer Mode [VoATM]) shall also be considered as elements of the DSN for meeting end-to-end performance requirements.

Return to:

[Top of DISAC 310-45-1](#)

[DISAC 310-45-1 Enclosure 1](#)

[DISAC 310-45-1 Enclosure 2](#)

[DISAC 310-45-1 Enclosure 3](#)

[DISAC 310-45-1 Enclosure 4](#)

[Publications Listing](#)

[DISA Home Page](#)

cio-pubs@disa.mil - Last Revision: 23 June 2008

**MANAGEMENT OF THE SINGLE SYSTEM MANAGER (SSM)
FOR THE DEFENSE SWITCHED NETWORK (DSN)**

1. **General.** The Defense Switched Network (DSN) is unique among the Defense Information System Network (DISN) networks in that the assets which make up the network (switches) are owned, operated, and maintained by the military departments (MILDEPs). DISA provides the global oversight, guidance, network management system, and staffing down to the theater level as required to manage the DSN. Single system management is the process used by DISA, in collaboration with the MILDEPs, to manage the DSN over its entire life cycle. The process allows concurrent sustainment of the existing system, adaptation to changing requirements, and introduction of new procedures and technologies. The principal impetus for the process is to accomplish these activities while continually meeting performance metrics required by the Joint Requirements Oversight Council Memorandum (JROCM) 202-02, Global Information Grid (GIG) Mission Area Initial Capabilities.

1.1 In the role of the DSN Single System Manager (SSM), the Director, DISA, delegates authority to the DSN System Manager (SM) to implement appropriate policies and practices to manage the architecture, design, program planning, development, implementation, operation, interoperability (IO), and replacement of DSN elements to provide end-to-end command and control (C2) communications.

1.2 The DSN SM serves as the focal point for all DSN policies and procedures, working in conjunction with the Joint Staff, the combatant commands, and the DISN theater field offices. The DSN policies are issued to provide management guidance for the DSN. The DSN procedures are issued to provide the standardized methodologies required to implement the policies.

2. Stakeholders.

2.1 **Management Stakeholder.** DISA is the primary "management" stakeholder in the effective management of the DSN, and the Director, DISA, has delegated management authority for the DSN to the DSN SM. The roles and responsibilities of the DSN SM and staff are delineated in detail in enclosure 4 of DISAC 310-45-1.

2.2 Operational Stakeholder. The MILDEPs are the "operational" stakeholders and are tasked with responsibility for the procurement, installation, operation, and maintenance of individual DSN switches worldwide, in accordance with DSN SSM guidance. The DoD components and contracted commercial telecommunications companies are responsible for obtaining and maintaining interoperability and security of switches under their immediate control. According to CJCSI 6215.01C, Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS), it is their responsibility to ensure switches are operated in a manner that does not introduce vulnerabilities to the DSN.

2.3 Utilization Stakeholder. The DSN user community is the "utilization" stakeholder, depending on the network to provide all circuit-switched services required. Per CJCSI 6215.01C, the DSN is the first choice solution for all new and existing circuit switched telecommunications requirements. CJCSI 6215.01C defines three classes of DSN users as special C2 users, C2 users, and non-C2 users. These users must exercise telecommunications discipline utilizing the network for official use only, regulating use of military unique features (MUFs); such as, multilevel precedence and preemption, only as needed, and reporting service issues through their appropriate reporting chain.

3. Areas of Emphasis. The full spectrum of management issues is addressed by single system management across the life cycle of the network, to include development of policies and procedures, centrally managing numbering and routing, managing circuit provisioning, and many other disciplines. There are, however, specific management areas that receive particular attention.

3.1 Interoperability (IO) Certification and Information Assurance (IA) Accreditation. Any piece of equipment connected to the DSN must be both IO certified and IA accredited. As the DSN SSM, DISA develops processes, procedures, and technical standards that ensure DSN systems and components satisfy defined requirements for IO and supportability. Further, as the DSN SSM, DISA has overall responsibility for end-to-end operational integrity of the DSN. DISA develops procedures and technical standards to ensure DSN systems and components are tested to satisfy defined requirements for IA certification and accreditation (C&A). Connection to the DSN is approved by the Voice Connection Approval Office (VCAO) for IO and IA certified equipment. In accordance with DoDI 8100.3, Department of Defense (DoD) Voice Networks, only the Assistant Secretary

of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO) can approve IO and IA waivers or a request for an interim connection to operate (ICTO) approval. Requests for waivers or for an ICTO shall be submitted via the Service or Agency chain of command to the ASD(NII)/DoD CIO stating the reason compliance is not possible. (Specific procedures to request a waiver or ICTO are detailed in subparagraph 6.4 of DoDI 8100.3.)

3.2 Technology Migration. In accordance with CJCSI 6215.01C, the DSN SSM is "the voice standards and voice processing/ transport technology migration coordinator to ensure end-to-end global voice quality, interoperability, and visibility for all voice C2 services." All voice transport and processing initiatives shall be coordinated with the DSN SSM. The impact of emerging voice processing and transport technology on global end-to-end DSN performance and C2 services shall routinely be assessed by the DSN SSM.

3.3 Performance Metrics. Performance metrics for the DSN are specified in CJCSI 6215.01C for network performance objectives (NPOs) and voice quality.

3.3.1 The NPOs are intended to satisfy user requirements and reduce costs and are recommended by DISA in coordination with the DoD components, validated by the Joint Staff, and approved by the ASD(NII)/DoD CIO. Commercial standards and practices are employed by the NPOs, when practical, to satisfy mission requirements. There are two general categories of NPOs--throughput and availability.

3.3.1.1 Currently, the throughput objective for routine precedence calls traversing the network is an intratheater grade of service (GoS) of P.07 (the probability of seven calls out of 100 being blocked during the busy hour expressed as a percentage) and an intertheater GoS of P.09 as measured during normal business hours of the theaters.

3.3.1.2 Network availability is a composite of switch availability and transmission availability. DISA, in conjunction with the operations and maintenance (O&M) commands, collects outage data across the network and compiles reports of network availability utilizing that data. An availability objective of 99.8 percent is the NPO.

3.3.2 While availability and throughput are all important factors, voice quality can be considered paramount. A connected call is of no use if the conversation between the two parties is unintelligible. Quality checks are performed on the current system, looking for echo and other factors that impact voice quality. With the pending conversion of current time division multiplexed voice services to a converged Internet Protocol (IP)-based packet network, new quality assurance (QA) checks are being implemented for factors such as latency.

4. **Annual Assessment.** An annual assessment on the impact of emergent voice processing and transport technology on global end-to-end voice performance and C2 services will be provided by the DSN SSM to the Joint Staff and the DSN Configuration Control Board (CCB).

Return to:

[Top of DISAC 310-45-1](#)
[DISAC 310-45-1 Enclosure 1](#)
[DISAC 310-45-1 Enclosure 2](#)
[DISAC 310-45-1 Enclosure 3](#)
[DISAC 310-45-1 Enclosure 4](#)
[Publications Listing](#)
[DISA Home Page](#)

cio-pubs@disa.mil - Last Revision: 23 June 2008

Enclosure 4: DISAC 310-45-1

**RESPONSIBILITIES FOR THE SINGLE SYSTEM MANAGER (SSM)
FOR THE DEFENSE SWITCHED NETWORK (DSN)**

Organizational responsibilities for the DSN are detailed in the following paragraphs. The assignment of Lead (L) and Support (S) roles and responsibilities for various DSN-related activities is summarized in [table 1](#).

1. Defense Information Systems Agency (DISA). The DISA SSM prescribes policy, provides procedures, assigns responsibilities, establishes technical requirements, monitors testing, and conducts certification and accreditation (C&A). The SSM also handles leases and procurements, installations, connections, and operations of telecommunications switches and services affecting the DSN. DISA will:

1.1 Act as DSN SSM by providing operational direction and management control of the DSN.

1.2 Chair and manage the DSN Configuration Control Board (CCB) and implement approved and funded DSN CCB actions.

1.3 Biennially update the DSN Program Plan (to include world-wide DSN topology), Network Configuration Management Plan (CMP), DSN Security Guide, DSN Classification Guide, DSN System Interface Criteria, Generic Switching Center Requirements, interoperability (IO) certification and information assurance (IA) test plans, and Worldwide Numbering and Dialing Plan and submit through the Joint Staff for validation and to Office of the Secretary of Defense (OSD) for approval.

1.4 Provide systems engineering system management of the DSN in response to validated, approved, and funded DSN Program Plan requirements.

1.5 Manage the effectiveness of the DSN on a 24-hour-per-day, 7-day-per-week basis, and evaluate operations and maintenance (O&M) practices and procedures ensuring command and control (C2) requirements are being met.

1.6 Report status and operational effectiveness of the DSN to the Joint Staff quarterly or more frequently if issues exist that may have a major effect on the network.

- 1.7 Recommend DSN performance objectives and establish interface criteria in coordination with DoD components and forward to the Joint Staff for approval.
- 1.8 Publish implementation documents for approved DSN objectives in coordination with DoD components.
- 1.9 Review, process, and implement approved requests for DSN telecommunications service. (If any request for service has potential to harm the network, DISA will forward the request to the Joint Staff for resolution regardless of designated approval level shown in CJCSI 6215.01C, Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS).
- 1.10 Use exercises to verify readiness of the DSN and its ability to support user missions over the full range of stress scenarios.
- 1.11 Coordinate and assess funding amounts under the DISN Subscription Service (DSS) process.
- 1.12 Coordinate and review Command, MILDEP, and Agency policies and procedures on DSN use, where requested.
- 1.13 Review Command, MILDEP, and Agency DSN switch hardware and software, requests for proposals (RFPs), and contracts for compliance with configuration management (CM) and IO policy, where requested.
- 1.14 Process and implement approved DSN service agreements with foreign governments.
- 1.15 Provide technical evaluations for proposed schemes for automatic interconnection onto the DSN from public switched networks and forward a recommendation to the Joint Staff for approval or disapproval.
- 1.16 Implement network management procedures.
- 1.17 Produce, update, and distribute the DSN Directory.
- 1.18 Recommend DSN consolidation and modification to improve network effectiveness or reduce costs.

1.19 Operate a DSN testing facility and maintain documentation pertaining to connection approval and interface standards. The Joint Interoperability Test Command (JITC) will test or witness testing of all DSN components and interfaces before integration with the DSN; conduct developmental, operational, IO, environmental, and qualitative DSN testing; perform ongoing comprehensive evaluations throughout DSN program development; provide guidance to DSN users regarding test plans and conduct; certify tested entities for operation or IO with the DSN; document all test results and certifications; and provide lists of certified DSN components and configurations.

1.20 Ensure only those switches and software loads that have been certified as interoperable by JITC and that have received security C&A are introduced into the DSN.

1.21 Disseminate specific instructions for operation of switching centers to the MILDEPs.

1.22 Maintain a database of all contractor DSN access requests, approvals, and terminations.

1.23 Approve or disapprove establishment of Metropolitan Area Networks (MANs), as proposed by combatant commands and MILDEPs, and maintain a list of approved metropolitan calling areas notifying the combatant commands and MILDEPs when biennial revalidation is required.

1.24 Implement controls necessary to limit DSN network access to those authorized by this Circular.

1.25 Maintain a database of all combatant command approvals for outside the continental United States (OCONUS) Class B service and notify the combatant commands of the biennial revalidation requirement.

1.26 Provide an annual assessment of the impact of emerging voice processing and transport technology on global end-to-end voice performance and C2 services to Joint Staff and the DSN CCB.

1.27 Develop and maintain intraswitch and interswitch dialing plans to ensure standardization across the network.

2. **Combatant Commands.**

2.1 Define, validate, coordinate, and approve requirements for DSN service within their areas of purview.

2.2 Forward approved DSN requirements, priorities, and precedence service to DISA and supporting MILDEPs for implementation and provide planning support for incorporation into the DSN Program Plan.

2.3 Provide policy guidance and procedures in conformance with DISAC 310-45-1 and in coordination with the MILDEPs and DISA for the use of the DSN within their respective areas of responsibility.

2.4 Provide acquisition, operation, maintenance, and logistics support for DSN customer premises equipment within facilities for which the combatant command is operationally responsible.

2.5 Coordinate with DISA before approval to determine if a DSN service request would degrade network performance.

2.6 Implement, control, and monitor use of precedence, on- and off-netting, and unofficial use of the DSN to prevent fraud, waste, or abuse.

2.7 Support DISA in contingencies, crises, and exercises involving operational elements of the DSN, as required.

2.8 Review and validate operational requirements for the DSN to meet requirements of operations, concept, and contingency and exercise plans.

2.9 Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability after DISA technically evaluates the request to determine potential network performance degradation and revalidate these requirements biennially.

2.10 Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval, in accordance with CJCSI 6215.01C.

2.11 Participate as nonvoting members of DSN CCB.

2.12 Provide copies of all contractor DSN access requests, approvals, and terminations to DISA.

2.13 Forward proposals for metropolitan calling areas or MANs to DISA for approval and revalidate OCONUS metropolitan calling areas biennially.

2.14 Approve OCONUS local commander requests for Class B service and notify the DISA DSN System Management Office (SMO) of approvals, as required by CJCSI 6215.01C.

2.15 Develop and implement policies and procedures to limit DSN use to that authorized by DISAC 310-45-1.

2.16 Coordinate all emerging technology base, post, camp, and station voice transport and processing initiatives with the DSN SMO.

3. Department of Defense (DoD) Components.

3.1 Define, validate, coordinate, and approve requirements for DSN services, in accordance with CJCSI 6215.01C.

3.2 Participate in the DSN CCB as a voting member.

3.3 Forward approved DSN requirements and priorities to DISA for coordination or implementation and provide planning requirements for incorporation into the DSN Program Plan.

3.4 Program, budget, acquire, operate, maintain, and fund assigned portions of the DSN for telecommunications services provided by the DSN and maintain switch hardware and software within three versions of the most current DISA IO certified and IA accredited release.

3.5 Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability after DISA technical evaluation to determine potential network performance degradation and revalidate the requirements biannually. (See DoDD 4640.13, Management of Base and Long-Haul Telecommunications Equipment and Services, and DoDI 4640.14, Base and Long-Haul Telecommunications Equipment and Services.)

3.6 Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval, in accordance with CJCSI 6215.01C.

3.7 Provide acquisition, operation, maintenance, logistics,

and funding support for customer premises equipment and terminal equipment.

3.8 Provide training and periodic technical evaluations to ensure facilities, equipment, and personnel meet DSN performance objectives and interface requirements.

3.9 Provide policy, implement controls for, and monitor use of precedence, on- and off-netting, and unofficial use of the DSN to prevent fraud, waste, or abuse.

3.10 Support DISA during exercises involving operational elements of the DSN.

3.11 Review and validate operational requirements for DSN switches under their operational control.

3.12 Verify only the new hardware and new software loads that have been certified as interoperable and IA accredited and placed on the Approved Products List (APL) by JITC are introduced into the DSN and verify all older existing hardware and software in the end-to-end DSN global network will be IO certified and IA accredited upon upgrade, replacement, or relocation of equipment in support of new users.

3.13 Operate respective switching centers per directions disseminated by DISA.

3.14 Provide copies of all contractor DSN access requests, approvals, and terminations to DISA.

3.15 Forward proposals for metropolitan calling areas or MANs to DISA for approval or disapproval and revalidate continental United States (CONUS) metropolitan calling areas biennially.

3.16 Develop and implement policies and procedures to limit DSN use to that authorized by DISAC 310-45-1.

3.17 Coordinate all emerging technology post, camp, or station voice transport and processing initiatives with the DSN System Manager (SM).

3.18 Maintain DISA intraswitch and interswitch dialing plans for end users and implement the DSN access codes.

4. National Military Command System (NMCS) and the Joint Staff.

4.1 Define, validate, coordinate, and approve DSN telecommunications services requirements, in accordance with CJCSI 3170.01E, Joint Capabilities Integration and Development System.

4.2 Forward approved, planned DSN requirements and priorities for coordination and implementation.

4.3 Review and approve FLASH and FLASH OVERRIDE precedence calling requirements as validated by the combatant commands, Services, and Agencies.

4.4 Ensure FLASH OVERRIDE and FLASH user missions continue to receive high precedence levels of service and initiate action to discontinue such access when mission needs change.

4.5 Review, validate, and approve DSN service requirements that might adversely affect the network but are required for mission accomplishment.

4.6 Review the operational effectiveness of the DSN. (Matters having a major effect on the network will be reported by the Joint Staff to OSD.)

4.7 Validate the biennial DSN Program Plan and submit to OSD for approval.

5. **Non-Department of Defense (DoD) Agencies.**

5.1 Define, validate, coordinate, and approve DSN requirements and priorities for telecommunications services.

5.2 Respond to DSN SSM guidance and direction.

5.3 Forward approved DSN requirements and priorities for coordination and implementation.

Return to:

[Top of DISAC 310-45-1](#)
[DISAC 310-45-1 Enclosure 1](#)
[DISAC 310-45-1 Enclosure 2](#)
[DISAC 310-45-1 Enclosure 3](#)
[DISAC 310-45-1 Enclosure 4](#)
[Publications Listing](#)
[DISA Home Page](#)

TABLE 1. DEFENSE SWITCHED NETWORK (DSN) RESPONSIBILITY MATRIX

RESPONSIBILITIES	DISA	COMBATANT COMMANDS	DOD COMPONENTS	NMCS AND JOINT STAFF	NON-DOD AGENCIES
Manage DSN contracts	L	S	S		
Manage DSS revenue	L	S	S	S	
Manage DSN program resources	L	S	S	S	
Oversee DSN operations	L	S	S	S	S
Manage DSN revenue generation	L	S	S		
Develop and support DSN policy	L	S	S	S	
Approve requirements and priorities	S	L	S	S	
Approve requirements for telecomm services	S		L		
Approve requirements that might affect DSN	S		S	L	
Forward requirements to DISA	S	L	L	L	L
Provide combatant policy guidance	S	L	S	S	
Develop DSN concepts	L	S	S	S	S
Publish DSN Program Plan	L	S	S	S	S
Provide logistics planning and policy	S		L		L
Conduct switch inventory	S		L	S	L
Manage security	L	S	S	S	S
Manage connection approval process	L	S	S	S	S
Engineer developmental systems and components	L		S		S
Engineer operational systems and components	L		S		S
Provide technical assistance and insertion	L		S		S
Engineer system changes	L		S		S
Manage network configuration	L		S		S
Manage network implementation, transition, and execution	L		S		S
Manage interface development and implementation	L		S		S
Develop network system management (ADIMSS)	L		S		S
Implement topology and connectivity	L		S		S
Administer network O&M	L		S		S
Test and certify DSN and components	L	S	S		S
Provide operations direction and control	L		S	S	
Evaluate DSN O&M	L		S	S	
Support operations working groups	L	S	S	S	S
Review and approve Flash/Flash Override	S	S	S	L	
Change switch designation (i.e., MFS, EO, PBX)	S		S	L	

Legend: L - Lead Role (to guide the action); S - Support Role (to maintain the action)

Return to:

[Top of DISAC 310-45-1](#)

[DISAC 310-45-1 Enclosure 1](#)

[DISAC 310-45-1 Enclosure 2](#)

[DISAC 310-45-1 Enclosure 3](#)

[DISAC 310-45-1 Enclosure 4](#)

[Publications Listing](#)

[DISA Home Page](#)

cio-pubs@disa.mil - Last Revision: 23 June 2008
