CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6211.02A
DISTRIBUTION: A, B, C, J, S 22 May 1996

DEFENSE INFORMATION SYSTEM NETWORK
AND CONNECTED SYSTEMS

References: See Enclosure C.

1. Purpose. This instruction establishes policy and delineates responsibilities for life-cycle management of the Defense Information
System Network (DISN). It details policy for management and use of the DISN, DISN services, and connected systems. Specific policies governing the satellite component of the DISN are covered in CJCS MOP 37, "Military Satellite Communications Systems."

2. Cancellation. CJCSI 6211.02, 23 June 1993, “Defense Information System Network and Connected Systems, is cancelled.

3. Applicability. This instruction applies to the Joint Staff, Services, CINCs, and Defense agencies.

4. Policy. The DISN is DOD’s consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. All DOD activities requiring telecommunications services will use the DISN when those services are available and are technically and economically feasible to the Department of Defense. See Enclosure A for general guidance on DISN management and use.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Procedures. This instruction provides policy guidance and, where required, tasks the appropriate agencies to develop and publish detailed procedures.

8. Summary of Changes. This instruction establishes the DISN as the primary DOD end-to-end telecommunications network for supporting military operations. Subparagraph 6.e, of Enclosure A incorporates

language from Change 2 of the Joint Ethics Regulation, DOD 5500.7, regarding the use of the DISN for health, morale, and welfare telephone calls and other authorized uses. This paragraph, as changed, also will change subparagraph 10a of Enclosure A of CJCSI 6215.01, 1 February 1996 to be in agreement with DOD 5500.7

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

\Signature\
WALTER KROSS
Lieutenant General, USAF
Director, Joint Staff

Enclosures:
A--General Guidance
Appendix--Guidelines for the DISN Requirements Committee
B--Organizational Responsibilities
C--References
GL--Glossary

DISTRIBUTION

	Copies
Distributions A, B, C, and J plus the following:	
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)	4
Director, National Security Agency/Chief, Central Security Service	4
Director, Joint Interoperability Test Center	2
Director, Inter-American Defense Board	2
Chairman, US Section US-Canada Military Cooperation Committee	2

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

ENCLOSURE A

GENERAL GUIDANCE

1. System Concept

a. The DISN is DOD's worldwide protected network that allows the warfighter to exchange information in a seamless, interoperable, and global battlespace. Its underlying infrastructure is composed of three major segments or blocks:

(1) The sustaining base (i.e., base, post, camp, or station) C4I infrastructure (to include legacy systems) that will interface with the long-haul network in order to support the deployed warfighter (reach-back services).

(2) The long-haul telecommunications infrastructure, which includes the Defense Communications System (DCS) and the communication systems and services between the fixed environment and the deployed joint task force (JTF) and combined task force (CTF) warfighter.

(3) The deployed warfighter and associated commander in chief (CINC) telecommunications infrastructures that support the JTF and/or CTF.

b. The DISN long-haul infrastructure is an integrated network, centrally managed and configured to provide intersite and interelement/block information transfer services for all DOD activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, and video services in support of national defense C4I decision support requirements and corporate information management (CIM) functional business areas.

c. The DISN provides the global transfer infrastructure by integrating separate CINC, Service, and Defense agency networking requirements into a DOD enterprise-wide network to meet common-user and special purpose information transfer requirements.

d. DISN information transfer facilities will support secure transmission requirements for subnetworks such as the Global Command and Control System (GCCS), Defense Red Switch Network, the Joint Worldwide Intelligence Communications System, and the Defense Message System (DMS).

2. Required Features. DISN will:

a. Be global in scope.

b. Be interoperable between all infrastructure segments or blocks.

c. Support multiple information transfer services for DOD users, including (1) dedicated point-to-point; (2) switched voice and data, currently Unclassified but Sensitive IP Router Network (NIPRNET), and Secret IP Router Network (SIPRNET); and (3) video services.

d. Be capable of rapid expansion or reconfiguration (minutes and hours) and extension to the tactical environment, and be interoperable with tactical systems. Bandwidth capacity for surge will be engineered and allocated based on contingency requirements and Joint Staff validation and direction.

e. Support automatic rerouting and restoral of circuits by priority in accordance with existing National Security-Emergency Preparedness (NSEP) procedures, Telecommunications Service Priority (TSP) procedures, and other procedures as required to ensure network performance and user requirements are met.

f. Be operated, maintained, and managed under the full control of military and DOD civilian personnel.

g. Be robust, adaptive, and reliable by employing network and configuration management, diverse routing, and automatic rerouting features.

h. Provide subnetwork and component survivability commensurate with the supported command or mission.

i. Support multilevel precedence and preemption (to meet assured connectivity requirements) and all classifications of information.

j. Support value-added services, such as messaging and conferencing, and allow for the addition of new services and technologies.

k. Provide a secure information environment for the processing, storage, transfer, and use of information in accordance with the DISN security policy.

l. Be capable of detecting attempts to access the network by unauthorized users. Support automatic denial of such access

attempts and automated reporting of such attempts to the DISN management structure.

3. Use. In accordance with procedures outlined in reference b, all DOD long-haul communications requirements will be submitted to DISA. DISA will use the appropriate DISN service to satisfy DOD long-haul and wide-area network information transfer requirements. Sustaining base and deployable requirements will be processed in accordance with reference b and the supporting components' procedures.

4. Connection Requirements Identification. Each DOD system or application device having a requirement for long-haul common-user information transfer services will be identified to DISA for DISN planning purposes. DOD activities will identify these systems and requirements to DISA as soon as requirements for these services have been validated.

5. Access and Connection Approval. The Chairman of the Joint Chiefs of Staff, Chiefs of the Services, CINCs, directors of Defense agencies, or their designated representative will validate operational requirements before requesting connection approval from DISA. Requirement validation and approval should ensure mission requirements are best satisfied via the DISN. DISA will make final approval for all DISN connections ensuring operational requirements have been validated; connections meet all technical and interoperability requirements; and subnetworks, systems, and other connected components provide adequate security and have been accredited by the proper authority. Requirement conflicts will be resolved by the DISN Requirements Committee or similar forum using guidelines in the Appendix.

6. Specific Provisions for Access and Connection

a. DOD Activities. DISA, in conjunction with the Services and agencies, will develop, coordinate, and publish DISN connection criteria and approve new connections for all DISN services for all activities.

b. Non-DOD Federal, State, and Local Government Activities. Requirements of non-DOD Federal, State, and local government activities will be submitted to the Director for Command, Control, Communications, and Computer Systems (J-6), Joint Staff, for validation and then forwarded for OSD approval.

c. Foreign Governments and Allied Organizations. In addition to first meeting the access and connection requirements for non-DOD US activities, use of the DISN by foreign governments and allied organizations must be approved under the provisions of reference c.

d. Civilian Contractor Activities. Requirements for access of contractor-controlled systems to DISN must be validated by the Joint Staff and approved by OSD. Based on a US Government contract, authorized contractor personnel may use DOD-controlled systems with access to DISN when performing contractual responsibilities. The sponsoring agency validates and arranges funding for the requirement.

e. Health, Morale, and Welfare (HMW). DISN shall be for official use and authorized purposes only.

(1) Official use includes emergency communications and any other communications that the CINC determines are necessary in the interest of DOD. In the interest of morale and welfare, CINCs may approve communications by DOD employees and military members to their family members at home from locations to which they are deployed for extended periods of time on official business.

(2) Authorized purposes include, for example, brief communications made by military members and DOD employees during official travel to notify family members of transportation or schedule changes. Reasonable personal communications (such as auto or home repair appointments or brief Internet searches) from the military member or DOD employee at his or her workplace are also authorized when the CINC or Agency Designee permits categories of such communication and after determining that such communications:

(a) Do not adversely affect the performance of the DOD organization or the official duties of the military member or DOD employee.

(b) Are of reasonable duration and frequency, and whenever possible, made during the employee’s or military member’s personal time such as after normal duty hours or during lunch periods.

(c) Serve a legitimate public interest, such as enabling DOD employees or military members to stay at their desks rather than requiring them to depart the work area to use commercial systems, or improving the morale of military members and DOD employees stationed away from home for extended periods of time.

(d) Would not reflect adversely on DOD, such as uses involving pornography, chain letters, unofficial advertising or soliciting, inappropriate handling of classified information, etc.

(e) Do not overburden the communication system, create no significant additional cost to DOD, and in the case of long distance communications are:

1. Charged to the DOD employee's home telephone number or other non-Federal Government number (third number call).

2. Made to a toll-free number.

3. Reversed to the called party if a non-Federal Government number (collect call).

4. Charged to a personal telephone credit card.

5. Otherwise reimbursed to DOD or the DOD component in accordance with established collection procedures.

7. Security. DISN will support and employ security services, protection mechanisms, and procedures in accordance with referenced and subsequent revisions of the DISN security policy. The DISN Security Accreditation Working Group will provide, interpret, and approve DISN security policy and, under Defense Information System Security Program (DISSP) sponsorship, will make accreditation recommendations to the four designated approval authorities (DAAs) (the Directors of DISA; NSA/Chief, CSS; DIA; and the Joint Staff) for the DISN.

a. Connected systems will be secured commensurate with the sensitivity of the information (both classified and unclassified) being processed.

b. Users must comply with DOD security requirements as described in references e and f for those systems processing Sensitive Compartmented Information (SCI) and implementing Service and Defense agency directives.

c. Connection to any other automated information system or data communication network or subnetwork, while connected to DISN, is strictly prohibited without appropriate documentation from the DAAs of the connected networks.

d. Security requirements for DISN elements and connected systems accessing DISN will be contained in reference d, subsequent revisions, and guidance provided by DISA's Center for Information System Security (CISS).

8. Cost Recovery. In accordance with OSD direction, DISN non-Defense Satellite Communication System costs will be recovered

through the Defense Business Operating Fund (DBOF) Communication Information Services Activity (CISA) through a billing scheme that is published by DISA. Non-DOD activities will be billed through the respective Service or Defense agency approval authority.

9. New DISN Services. DISA will continually assess the technical, programmatic, and operational feasibility of adding new services and capabilities to the DISN. The CINCs, Services, and agencies will provide similar assessments regarding the sustaining base and deployable infrastructure. New services and capabilities will be added in response to validated user requirements and via planned technology insertion.

10. Survivability. Survivability enhancements in transmission paths, routing, equipment, and associated facilities will normally be limited to systems supporting units with critical missions that justify the additional cost.

APPENDIX TO ENCLOSURE A

GUIDELINES FOR THE DEFENSE INFORMATION SYSTEM NETWORK REQUIREMENTS COMMITTEE

1. Purpose. To provide a forum for resolution of requirement issues for the DISN.

2. Representation. The committee will consist of representatives of the Joint Staff, Services, Defense agencies, unified commands, and DISA. The Director, J-6, will appoint the committee chair.

   a. Representatives should be O-6 or civilian equivalent.

   b. CINCs will participate but may arrange to delegate their issues to the Joint Staff for resolution. Services and Defense agencies should coordinate issues with the supported CINC.

   c. All representatives are expected to present the staffed viewpoint of their parent organization.

3. Meetings. The committee will meet as required to resolve unsettled DISN requirements issues.

4. Resolution Process. Unresolved issues will be forwarded to the Military Communications-Electronics Board (MCEB) for resolution through the MCEB process.

(INTENTIONALLY BLANK)

ENCLOSURE B

ORGANIZATIONAL RESPONSIBILITIES

1. The Chairman of the Joint Chiefs of Staff is responsible for operational network policy and overall direction. The Director, Joint Staff, serves as one of the four DAAs for DISN accreditation issues. Authority for operational DISN policy and direction is delegated to the Director, J-6, Joint Staff, who will:

   a. Monitor the operational and management effectiveness of the network and report significant items (e.g., major mission degradation) to the Chairman of the Joint Chiefs of Staff.

   b. Use the requirements committee and the MCEB to resolve requirements conflicts and issues referred to the Joint Staff. Guidelines for the requirements committee are delineated in the Appendix to Enclosure A.

   c. Coordinate and assign funding responsibility for joint requirements to the appropriate Service.

   d. Validate unified command, Service, or Defense agency subnetworks.

   e. Validate non-DOD Federal, State, and local government requirements.

2. The CINCs will:

   a. Define, validate, and coordinate DISN candidate information system requirements.

   b. Review and submit service restoration priority requests in accordance with NSEP and TSP procedures.

   c. Delegate validation authority, as deemed appropriate, to supporting Services and Defense agencies.

   d. Ensure approved systems efficiently use DISN services to meet mission requirements and enforce user compliance with DISN policy and procedures.

   e. With the exception of USCINCSOC, submit their validated DISN requirements through Service channels to DISA. USCINCSOC will submit service requirements directly to OSD.

3. The Director, DISA, is assigned overall responsibility as DISN network manager and, in accordance with reference g, will:

a. Provide operational management for the DISN and will be responsive to the validated operational requirements of the Joint Staff, CINCs, Services, and Defense agencies.

b. Establish a management structure for DISN and exercise operational direction, including day-to-day network management and configuration management of the DISN (i.e., maintaining an accurate and appropriately classified data base of existing DISN users, including non-DOD activities, and monitoring system service restoral to ensure compliance with NSEP and TSP procedures).

c. Perform required system engineering and modeling to achieve optimal network design and implementation approach, and identify performance standards for DISN services (i.e., availability and response time).

d. Continuously monitor the effectiveness of the DISN and provided services in satisfying user requirements. Be responsive to CINC requests for reports on system performance.

e. Refer to the Joint Staff any matters that significantly degrade the network.

f. Provide Joint Staff, Services, Defense agencies, and CINCs appropriate periodic status and programmatic updates.

g. In coordination with the Joint Staff, and the appropriate CINCs, Services, and Defense agencies, analyze and satisfy requests for new DISN services.

h. Specify interoperable interface protocol standards, in coordination with the CINCs, Services, and Defense agencies.

i. Coordinate changes, through the requirements committee, that impact user interfaces.

j. Establish and publish DISN connection requirements identification and accreditation procedures and publish to the unified commands, Services, and Defense agencies.

k. Develop and maintain a coordinated Test and Evaluation Master Plan and provide operational test and evaluation through the Joint Interoperability Test Center to ensure user network requirements are being met. Additionally, DISA will chair periodic working groups with Service and DOD agency

representatives on all DISN-related network level acquisitions and changes.

l. Ensure that the DISN security architecture meets the needs of DISN users.

m. Develop and maintain DISN planning and program management process and documentation.

n. Ensure security measures and plans and accreditation policies are based on threat assessments validated by the appropriate member(s) of the DOD Intelligence Community.

o. Serve as one of the four DAAs for the DISN.

4. The Services and Defense agencies will:

a. Review long-haul common-user transmission requirements and forward all requirements not needing unified and specified command, Joint Staff, or OSD approval to DISA for development of a technical solution, coordination, and implementation. In accordance with DISA provided criteria, systems requirements must be identified far enough in advance to ensure a timely acquisition of network components to satisfy the required operational date.

b. Review and submit, as delegated by the supported CINC, requirements for service restoral capability with sufficient information as prescribed in reference h.

c. Program, budget, fund, and provide support for assigned portions of the DISN through the PPBS, including approved contractor and foreign government systems.

d. Provide sufficient local data distribution capability to meet the CINC’s validated connectivity requirements. (These systems must be focused on supporting operational requirements of the parent Service and be capable of supporting a joint task force headquarters to support contingencies.)

e. Apply applicable information, communications, and physical security measures and ensure installation requirements continue to meet the requirements of the DISN security policy.

f. Ensure that approved systems use DISN services to meet mission requirements and ensure user compliance with DISN policy and procedures.

g. Coordinate with the theater commander and DISA before submitting long-range requirements for DISN access within a geographic region of responsibility of a theater unified command. Conflicting views among the requesting activity, DISA, and the concerned commander of a unified command will be forwarded to the J-6, Joint Staff, for resolution.

h. Maintain direct management responsibility to coordinate, install, test, and accept their users' host and terminal access circuits according to DISA-established criteria. Services and DOD agencies will provide representatives to joint, DISA-chaired working groups on related topics.

i. Provide requisite site support for the DISN equipment located on their respective bases, posts, camps, and stations. Site support requirements will be specified by DISA in appropriate procedural documentation and coordinated with the Services and Defense agencies. Support required will include, but is not limited to, providing power, physical security, floor space, and on-site coordination for the DISN data networks points of presence located on their respective bases, posts, camps, and stations.

j. Manage DISN subnetworks when authorized by the Director, J-6, Joint Staff.

k. Provide information, as requested, to DISA for DISN billing, management, and inventory purposes.

l. Identify representatives to the DISN Requirements Committee and its subcommittees, as required.

m. Implement and comply with the policies and procedures required in references a and b.

5. The Director, NSA/Chief, CSS, will:

a. Provide guidance on required security services and features necessary to meet DISN operational requirements.

b. Recommend basic doctrine, methods, and procedures to minimize DISN information security vulnerabilities in accordance with the provisions of references i and e.

c. Validate all requirements for, manage, and accredit all NSA/CSS cryptologic systems in accordance with references e and f.

d. Serve as one of the four DAAs for the DISN.

e. Develop, acquire, and certify COMSEC equipment.

6. The Director, DIA, will:

a. In accordance with established agreements with DISA, implement, operate, and manage Joint Worldwide Intelligence Communications System (JWICS) components and facilities on the DISN.

b. Serve as one of the four DAAs for the DISN.

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

a. DODD 4640.13, 5 December 1991, "Management of Base and Long-Haul Telecommunications Equipment and Services" (currently under revision)

b. DODI 4640.14, 6 December 1991, "Base and Long-Haul Telecommunications Equipment and Services" (currently under revision)

c. CJCS MOP 43, 11 March 1992, "Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations"

d. DISN Long-Haul Security Policy, 14 December 1995

e. DODD 5200.28, 21 March 1988, "Security Requirements for Automated Information Systems (AISs)"

f. DCID 1/16, 19 July 1988, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks"

g. DODD 5105.19, 25 June 1991, "Defense Information Systems Agency"

h. DISA Circular 310-130-4, 18 August 1993, "Defense User's Guide to the Telecommunications Service Priority (TSP) System"

i. DODD C-5200.5, 21 April 1990, "Communications Security (COMSEC)"

j. DODD S-5100.19, 19 March 1959, "Implementation of National Security Council Intelligence Directive No. 7"

k. CJCS MOP 37, 14 May 1992, "Military Satellite Communications Systems"

(INTENTIONALLY BLANK)

GLOSSARY

application devices. Devices (e.g., computer terminals, personal computers, mini and mainframe computers, and facsimile machines) that provide a capability to process information from various input mechanisms.

data communications. Information exchanged between end systems in machine-readable form.

Defense Business Operations Fund (DBOF), Resource Management Committee. Committee which coordinates the funding of the DCS.

Defense Information System Network (DISN). A subelement of the Defense Information Infrastructure, the DISN is the DOD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

Defense Satellite Communications System (DSCS). Composed of DOD operated and maintained satellites and earth terminals, operating in the SHF frequency band, that provide communications transmission capability.

Designated Approving Authority (DAA). Responsible for weighing the security risks of operating an automated information system versus the benefits it may provide and deciding whether or not to approve operation of the system.

DISN user. An individual assigned to an organization having devices directly or indirectly connected to the DISN.

Military Communications-Electronics Board. A decision making body chaired by the Joint Staff, J-6, and composed of the C4 heads of the Services, DIA, and NSA and the Director, DISA.
This body deals with issues of interoperability and standardization between the Department of Defense and US allies.

subnetwork. A logical partition of a network amenable to separate management, control, and provisioning because of functional or geographic reasons.

system. A generic term for a collection of equipment connected to the DISN. It may refer to a host, a group of hosts, or a network.

validation. The confirmation, by designated authority, that a request for access and use of the DISN is necessary to meet that organization's mission requirements.

Warner-Exempt. Guidelines used to determine if system acquisition must be conducted through GSA. As a general guideline, systems that directly or indirectly support a warfighting mission are considered Warner-Exempt and do not require acquisition through GSA.