CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6215.01C
DISTRIBUTION: A, B, C, J, and S 9 November 2007

POLICY FOR DEPARTMENT OF DEFENSE (DOD) VOICE NETWORKS WITH REAL TIME SERVICES (RTS)

Reference(s): See Enclosure F.

1. Purpose. This instruction establishes policy consistent with DODI 8100.3 (reference oo) and prescribes responsibilities for use and operation of the DOD voice networks, to include but not be limited to the Defense Switched Network (DSN), the Defense RED Switch Network (DRSN), Defense Video Services (DVS) and all Defense Information Systems Networks (DISN) that provide RTS.

2. Cancellation. CJCSI 6215.01B, 23 September 2001, is canceled.

3. Applicability. This instruction applies to Office of the Secretary of Defense, the Military Services, Chairman of the Joint Chiefs of Staff, combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, the DOD Field Activities and all other organizational entities in the Department of Defense (referred to hereafter collectively as "the DOD components") in peacetime, crisis situations, and wartime. This instruction also identifies policy and responsibilities concerning non-DOD governmental, foreign government, and civilian organizational requests for DSN, DRSN and DISN Assured RTS support (DARTS). Requests for waivers this instruction will be forwarded through the DOD component chain of command to the Joint Staff, stating the reason compliance is not possible. This instruction is applicable to:

a. All telecommunications switches leased, procured (whether systems or services), or operated by any DOD component of the Department of Defense.

b. The hardware or software for sending and receiving voice, data, or video signals across a network that provides customer voice, data, or video

equipment access to the DSN, DRSN or public switched telephone networks (PSTN).

c. End-to-End services (e.g., phone-to-phone, video-to-video units, fax-to-fax; secure terminal equipment (STE-to-STE) to include tactical applications.

d. All technologies i.e. (circuit switch, voice over Asynchronous Transfer Mode (ATM), and Voice over Internet Protocol (VoIP)) that use DSN or DRSN phone numbers; or that are otherwise incorporated into the DSN or DRSN numbering or routing plans via area code, access code, Internet Protocol (IP) addressing scheme, etc. for the origination and reception of voice, dial-up video, and dial-up data for routine and precedence subscribers.

e. The DOD component's planning, investment, development, operations, and management of telecommunications switches connected to the DSN or DRSN for processing voice, dial-up video and dial-up data.

f. All networks that provide DISN RTS.

4. Policy. The DISN provides RTS via its router networks (NIPRNET, SIPRNET and the DISN Service Delivery Nodes) and via DSN, DRSN and DVS. DSN and DRSN are worldwide private-line telephone sub-networks of the DISN that provide long-haul secure and non-secure telecommunications services to DOD component authorized users. They are the integral components of the Global Information Grid (GIG) that provide End-to-End services to critical users at the highest levels of Government. Connection approval shall follow the instructions and processes in CJCSI 6211.02B (reference hh). Both DSN and DRSN are under the management control of the Director, Defense Information Systems Agency (DISA). As the single system manager (SSM) (reference oo), on behalf of USSTRATCOM, for both networks and the executive agent (EA) of the DRSN, the Director, DISA, will be responsive to the needs and requirements of the Chairman of the Joint Chiefs of Staff (CJCS) and DOD components. This policy supersedes CJCS messages dtg 171649Z Dec 2002 Interim Voice over IP (VoIP), dtg 221621Z Oct 2004 Voice over Secure IP (VoSIP) Requirements. Enclosures A, D, and E, provide policy for the DSN. Enclosures B, D, and E, provide policy for the DRSN. Enclosure C, D, and E provide policy for RTS. Specific responsibilities are outlined in Enclosure E.

5. Definitions

a. The DSN is an inter-base, non-secure 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 (IAW) national security directives. Non-secure dial-up voice (telephone) service is the system's principal service. (See references a and b)

b. The DRSN is a secure C2 system and is a key component of the DOD global secure voice services. The DRSN supports secure voice and secure conferencing requirements of the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, DOD components, and select federal agencies in peacetime, crisis situations, and wartime. It is a separate, secure switched network that is considered part of the DISN. Three sub-services provide the foundation for the DOD secure voice services: the DRSN, the secure telephone unit-III/secure terminal equipment (STU-III/STE) and other secure communications interoperability protocol (SCIP) equipment that provide End-to-End encryption over the DSN, and other secure wireless products. (See references c and d)

c. The DISN is an integrated network, centrally managed and configured, to provide telecommunications services for all DOD activities. This information transfer service is designed to provide dedicated point-to-point; point-to-multipoint; and switched voice, data, imagery, and VTC services in support of national defense C3I decision support requirements (references e and oo). For GIG, Wide and Metropolitan Area Networking (WAN, MAN), use of the DISN is mandatory unless granted a waiver from the GIG Waiver Panel (reference hh). The DISN provides RTS via its circuit switched and IP router networks. These networks include, but are not limited to: the DSN, DRSN, DISN, and the DVS infrastructure, the DISN WAN to include the DISN SDN and access to those SDN, Teleport, SIPRNET, and NIPRNET. The DISN's underlying infrastructure is composed of three major segments or blocks IAW CJCSI 6211.02B (See reference hh):

(1) The sustaining base (i.e., base, post, camp or station and Service Enterprise Networks) command, control, communications, computers and intelligence (C4I) infrastructure will interface with the long-haul network to support the deployed warfighter. The sustaining base segment is primarily the responsibility of the Services.

(2) The long-haul telecommunications infrastructure, which includes the communication systems and services between the fixed environment and the deployed joint task force (JTF) and/or coalition task force (CTF) warfighter. The long-haul telecommunications infrastructure segment is primarily responsibility of DISA.

(3) The deployed warfighter and associated combatant commander telecommunications infrastructures supporting the JTF or CTF. The deployed warfighter and associated combatant command telecommunications infrastructure is primarily the responsibility of Services.

d. RTSs are a subset of the four categories of services contained in the GIG Net Centric Implementation Document (NCID) v2, Quality of Service (QoS) (T300): Signaling, Inelastic/RTS, Preferred Elastic and Elastic.

(1) Signaling includes Network Control for managing the network.

(2) Inelastic /RTS provide GIG users with live interactive telecommunications to include voice and video and the user signaling for setting up and taking down sessions over the network. They also include rapid delivery of critical C2 information involving weapons delivery capabilities. Inelastic RTS allows for the equivalent of "Face to Face" interactions in which both factual and emotional content of the interaction can be conveyed and the operation of surveillance and weapons systems that require rapid message delivery.

(3) Preferred Elastic services include services such as instant messaging, user authentication imagery, video, and audio streaming.

(4) Elastic services include services such as, e-mail, web browsing, and document transfers.

6. Responsibilities. See Enclosure E.

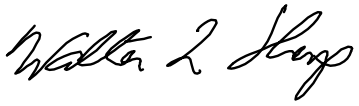
7. Administration. The DOD components must develop implementing policies and procedures for the provisions of this instructions policy. The policies and procedures must be coordinated with and provided to DISA to ensure that they do not adversely affect network operation. Combatant commands must validate DOD component policies.

8. Summary of Changes. The name of this instruction is changed from "Policy for Department of Defense Voice Networks" to "Policy for Department of Defense (DOD) Voice Networks with Real Time Services (RTS)". This includes the use of (Internet Protocol) IP networks to transmit voice or video services whether wired or wireless, tactical or strategic, Sensitive But Unclassified (SBU) or Classified (reference oo). It also applies the emerging policies of the GIG Mission Area Initial Capabilities Document JROCOM 095-04, 14 June 2004, Key Performance Parameters to DISN RTS to support migration to a Net Centric NetOps environment. Additionally, this revision updates DSN and DRSN network performance parameters, cost recovery procedures, usage and security policy, and enhancements to switches and terminal equipment. It updates the definition of C2 users. It also incorporates guidance for the use of Enhanced Mobile Satellite Service (EMSS) in conjunction with the DSN, as well as numerous administrative and procedural changes.

9. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components, other federal agencies, and the public may

obtain copies of this instruction through the Internet from the CJCS Directives Home Page -- http://www.dtic.mil/cjcs_directives.

10. Effective Date. This Instruction is effective immediately upon receipt.



WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Enclosure(s):

A--Policy for the DSN
B--Policy for the Defense RED Switch Network
C--Policy for DISN Real Time Services
D--Precedence Approval Authorities
E--Responsibilities
F--References
GL--Glossary

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Assistant Secretary of Defense/NII (Networks & Information Integration)/DOD CIO	2
US Delegation, Inter-American Defense Board	2
US Delegation, United Nations Military Staff Committee	2
Military Communications-Electronics Board	2
Commandant, US Coast Guard	2
Federal Emergency Management Agency	2

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSI 6215. 01. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 6	O	F-1 thru F-4	O
i thru xii	O		
A-1 thru A-8	O		
B-1 thru B-6	O		
C-1 thru C-4	O		
D-1 thru D-12	O		
E-1 thru E-16	O		

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE A

POLICY FOR THE DEFENSE SWITCHED NETWORK (DSN)

1. Purpose. This enclosure provides general guidance, usage, and performance objectives for the DSN. In addition, it describes functional requirements and military-unique features of the DSN.

2. General

a. The DSN is a rapid, reliable, survivable, telecommunications network serving DOD authorized users. The DSN is a sub network of the DISN and GIG. The basic DSN is a worldwide hierarchal network of telecommunication switches to which end instruments are connected. It provides rapid, reliable, survivable, non-secure, secure, and economical C2 telecommunications to selected users. To take advantage of economies of scale, the DSN also provides service to non-C2 users as long as the primary mission supporting C2 users is not impacted.

b. The USSTRATCOM/JTF-GNO Global NetOps Center (GNC), DISA Global NetOps Support Center (GNSC) thru the Theater NetOps Centers (TNC) provide high-level monitoring and situational awareness of the core DSN infrastructure 24 hours a day, 7 days a week. These centers implement the DSN service manager's authority and responsibility to take immediate and necessary action to perform network-level fault isolation or restoral actions in the event of outages, network compromise, or critical world situation. GNC, GNSC and TNC roles in monitoring and situational awareness of connectivity to allies will be limited to the terms agreed upon in the memorandum of agreement/memorandum (MOA/MOU) of understanding that governs the allied connections to the DRSN. This will be determined on a case-by-case basis.

c. The integral components of the DSN and connections to the Deployable Voice Exchange (DVX) are under the DISA SSM, on behalf of USSTRATCOM, and have direct management control for day-to-day peace time and crisis operation of the DSN long haul terminations. Configuration Management (CM) and Information Assurance (IA) are shared responsibilities. Integral components are the stand alone(SA), Multifunction, end office (EO), and Small End Office (SMEO) switches including versions of these switches with Time Division Multiplexing (TDM) trunks and VoIP on the line side, as well as the End-to-End IP-based RTS addressed in Enclosure C.

d. The user equipment (PBXs, DVXs, and end instruments) connects to the DSN at an EO switch in order to reach the worldwide DSN backbone. All DSN on-net equipment, to include elements controlled and managed by the Military Departments such as PBXs, DVXs, deployable/tactical switches, and user

terminal equipment, are considered part of the GIG and must meet End-to-End interoperability, functionality and IA requirements IAW DOD directives and CJCSIs. (See references e, f, hh, qq and rr)

e. The DSN is to be used only for official business or in the interest of the US Government and the first choice for all switched voice and dial-up video telecommunications between DOD user locations per DODI 8100.3. (See reference oo). All DOD long-haul communications requirements will be submitted to DISA IAW DODI 4640.14 (reference gg). DISA will use the appropriate DISN service to satisfy DOD long-haul and wide-area network information transfer requirements. Other systems *shall not* be used to "bypass" DSN unless the Joint Staff provides a waiver IAW reference z.

f. The primary function of the DSN is to provide non-secure dial-up voice service. Enclosures A, B, and C outline policy and procedures for connection of specific equipment to the DSN and procedures to obtain switched voice non-secure service for DSN users.

g. The DSN provides, via STU, STE, and other SCIP terminal equipment, an additional source of secure communications for DRSN users. A direct interface between DSN to DRSN allows DRSN communications to be extended to C2 users that are connected to DSN EOs.

3. Cost Recovery under DISN Subscription Services (DSS). The Office of the Secretary of Defense (OSD) directed a cost recovery program based on site subscription fees for DISN services. This program, part of a DSS, began implementation in FY06.

(1) The DISN subscription charge is based on bandwidth and actual DISN services provided from the DISN Subscription locations to the users' infrastructure. The customer (host, tenant, or remote user) is responsible for the costs of getting to the DISN meet-me-point (i.e., the DISN or commercial demarcation point) from the user's infrastructure. Validated requirements must be provided to the DISN Customer Forum (DCF) to ensure they are incorporated in the DOD components DSS provided for their specific locations. All questions regarding this process should be directed to the DOD component representative on the DCF.

(2) Customer requirements (Subscription Bandwidth Allocation plus a term of services), including DSN services, are aggregated at each DISN Subscription location and represented by a single weight factor. Currently, there are four DISN Subscription Bandwidth Allocation choices and five DSS Packages. The current combination of Subscription Bandwidth Allocation and DSS Packages results in a matrix of twenty service options. Weight factors are based on both increasing bandwidth allocation and services provided.

4. Usage Policy. General DOD components use of the DSN is restricted to the official business of the US Government or in the interest of the US Government. Local commanders have the approval authority for long distance services on the DSN. (See reference oo)

a. DSN is the official DOD components switched voice network and will be the first choice communications means for all Special C2, C2, and non-C2 users. It is the primary means of secure (STU-III STE/SCIP family) communications for non-tactical C2 users. DSN must be the user's first choice; however, if DSN is not immediately available, or if the called party does not have access to DSN service, other long-distance calling methods may be used. DOD components shall not install or otherwise implement other long haul voice networks to permanently "BY PASS" primary DSN telecommunications in accordance with (IAW) reference z.

b. The DOD may grant non-DOD activities access to DSN when necessary for national security; when not in conflict with US Government rules and regulations or OCONUS local post, telephone and telegraph (PTT) ordinances; when those activities and individuals have critical National Security or Emergency Preparedness (NS/EP) needs; and access is in the best interest of the US Government IAW reference oo. If access is approved, DSN services are provided on a cost-reimbursable basis (normally charged to the non-DOD requester through OSD; however, reimbursement may be made through the sponsoring DOD Component). In CONUS, requests for telephone service by non-DOD users should be satisfied by available commercial service and US General Service Administration (GSA), Federal Telecommunications Services (FTS) 2001 (or the successor services, Networx Universal) if the use is clearly not associated with the military mission of the Department of Defense. When in the best interest of the US Government, access to the DSN can be provided on a not-to-interfere basis (i.e., does not affect the DOD mission). Requirements to support non-DOD or non governmental activities or agencies, such as the Department of Justice, state government organizations, DOD contractors, labor unions, and foreign embassies, will be validated by the Joint Staff and referred to OSD for approval, except as provided in Paragraph 3e below.

c. Health, Morale and Welfare (HMW). IAW reference mm, when approved by theater commanders in the interest of HMW, DSN may be used by military members and other DOD employees who are deployed outside CONUS for extended periods on official DOD business. DSN may be authorized, within and outside CONUS, by military members who, although are no longer directly supporting a contingency operation, are hospitalized as a result of wounds or other injuries incurred while serving in direct support of a contingency operation. (See reference xx) combatant commands will establish policy for

authorization, management control, frequency, and duration of HMW calls to be compatible with operational requirements, local restrictions, and host-nation laws or agreements. The following conditions apply to HMW use of DSN:

(1) Calls will have management controls that prevent unauthorized use of the DSN and other public networks (PSTN, PTT etc.), or through the DISA-managed interface to the PSTN as described in Enclosure A, Appendix A., 7.f.(2) (c). To ensure compliance with reference mm, technical means will be implemented to prevent completion of CONUS-originated calls.

(2) Calls should be placed only during normal non-duty hours at the originating location and, where possible, timed to avoid the normal duty period at the terminating location.

(3) Calls must be placed only at the ROUTINE precedence and normally should not exceed 15 minutes in duration. No off-net HMW call will incur a toll charge to the US Government, even if the intent is to reimburse the US Government. An off-net HMW call that would incur a commercial toll charge may be placed if the called party agrees to accept the charges on a collect call basis or some other means of assured payment such as a credit card.

d. Netting. Interconnection of long-distance (originating at another switch) DSN calls with a local or long-distance commercial network (on or off-netting) are only allowed for the following purposes:

(1) Operations support. A combatant command (Command Authority), also known as COCOM, Service Chief, or director of a Defense agency may authorize automatic or manual official long-distance telephone traffic for personnel to maintain contact with their office and carry out their responsibilities.

(2) Emergencies, Special Circumstances. On and off-netting of official long-distance telephone traffic by automatic or manual interfaces is authorized for crisis or national emergency conditions. Additionally, off-netting is authorized to support DOD operational requirements via the PSTN to authorized wired or wireless terminals.

(3) Control. OCONUS combatant commands must establish procedures to positively control all on and off-net access within their area of responsibility (AOR). DOD components will establish procedures for positive control of all on and off-net access in CONUS.

e. Non-DOD Agencies

(1) American Red Cross (ARC). Access to the DSN is provided to the ARC in support of cases involving military members, DOD civilians, and their families. Global access at ROUTINE precedence is authorized.

(2) Contractors.

(a) US civilian contractor personnel in overseas areas may use the DSN when they are performing duties normally performed by DOD civilian or military personnel. Foreign national contractors may be authorized DSN access when validated by the appropriate DOD component and approved by the Joint Staff. Only DSN calls directly related to and necessary for the accomplishment of contracted duties are permitted between an overseas location and CONUS or within an overseas theater.

(b) US Contractor personnel within CONUS may use the DSN when performing a mission normally performed by DOD civilian or military personnel, subject to the following:

1 The contractor's function is supporting a C2 mission.

2 DSN access provided to the contractor is equivalent to that access previously provided to the military organization originally performing the function. Study, analysis, design engineering, and other similar support functions are not missions requiring C2 access. Requests for ROUTINE access must be validated at the local level and approved by an agent with written delegation from the appropriate DOD component. Precedence access above ROUTINE must be approved by the DOD.

3 Contractors located in CONUS requiring new or increased DSN access must have each specific request approved by the appropriate DOD component. Blanket approvals are not authorized.

(c) The requesting DOD component must validate the requirement and certify that contract documents contain guidance and restrictions, certified by the contracting officer, ensuring contractor use of DSN complies with established Network Management (NM) procedures. Requests for approvals must identify the contract termination date.

(d) Procedures for reviewing, monitoring, and controlling contractor access to DSN have been published in DOD component or command regulations. As a minimum, contractor access to DSN is reviewed every 3 years and in conjunction with every renewal or period of performance extension of the contract.

(e) Copies of all contractor access requests, approvals, and terminations are provided through the contracting officer to DISA, DSN SSM.

(f) Approvals and contracts must state that the DOD has the right to terminate the DSN service at any time and DOD does not guarantee the quality or quantity of service to be supplied and cannot be held liable for any discontinuance or failure of the service.

f. DSN Service for personnel supporting Non- US functions. The use of DSN IMMEDIATE, PRIORITY AND ROUTINE precedence by DOD personnel assigned to non-US (foreign government adviser, UN, NATO, etc.) organizations must be approved by the appropriate DOD component. Requests for FLASH or FLASH OVERRIDE must be validated by the appropriate DOD component and approved by the Joint Staff.

g. DSN Service to Canada. Use of the DSN by Canadian Defense Forces is authorized as an extension of the Canadian Switch Network (CSN) for combined cross-border C2 communications in support of their worldwide mission.

h. Foreign Governments and Treaty Organizations. Foreign government activities may be granted access to the network by the DOD for purposes of national security and when not in conflict with existing agreements or local PTT ordinances. This access must be initiated by, and processed through, the appropriate DOD sponsor IAW reference n. Combatant commands may authorize the use of DSN in his/her AOR, at ROUTINE precedence, by personnel of friendly foreign governments or treaty organizations for discussion of official US Government business with US personnel, if such use will not reduce the grade of service (GOS) objectives outlined in this instruction. Combatant commands must ensure effective control of this use and may authorize the service only when other telecommunications systems are unavailable or unsatisfactory. If the DSN access required by personnel of friendly foreign governments or treaty organizations becomes routine or becomes a formal requirement, the arrangement must be formalized by an international agreement. (See reference n)

i. Foreign Military Sales (FMS). Use of DSN service may be approved as part of an FMS arrangement. Requests for DSN service for non-US or non-DOD users must be submitted through the Joint Staff to OSD (NII). (See reference t).

j. Labor Unions. Access to DSN is not normally provided to labor unions and is not routinely authorized in contract documents. The basis for supporting a request to OSD must be a clearly operational, military-related

function. The Joint Staff, DOD components, and DISA will be notified of command support for a request to OSD for labor union access to DSN.

k. Non-appropriated Fund (NAF) Activities. NAF activities may be authorized to use the DSN to conduct command management functions dealing with appropriated funds matters. Local commanders are responsible for approval and control of NAF access and requirements, ensuring DSN use is on a cost-reimbursable basis. The DOD components must institute procedures to revalidate requirements periodically.

l. Residential Services. When normal commercial service is either unavailable or unreasonably expensive, DOD employees (excluding contractors) may be provided DSN access/lines at overseas locations only on a cost-reimbursable basis. Local commanders may request this service, for geographic location(s) within his or her command. Requests must be forwarded to the combatant command for approval/disapproval and to the DISA DSN program management office (PMO) for information. Approved Class B service must be revalidated by the combatant command biennially. Local commanders are responsible for determining appropriate cost reimbursement rates (reference u). In addition, DSN service may be provided in residences of key personnel for official calls.

m. Commercial Leased Transmission. The DSN may use commercial leased transmission facilities when cost-effective or mission-essential requirements dictate. Commercial leased transmission facilities in overseas areas are negotiated country-by-country by the DISA, IAW the appropriate combatant commands and operations and maintenance (O&M) commanders.

5. Objective Technical Parameters and Special Functions

a. Network Performance Objectives. Network performance objectives aimed at providing DSN services to satisfy the system requirements and reduce costs are recommended by DISA in coordination with the DOD components. They must be validated by the Joint Staff and approved by ASD (NII)/DOD (CIO). Performance objectives employ commercial standards and practices, when practical, to satisfy mission requirements. The objective for ROUTINE precedence calls traversing the network from an EO instrument is a peacetime theater GOS of P.07 (P.07= probability of seven calls out of 100 will be "blocked" during the "busy hour") or better, and an inter-theater GOS of P.09 or better, as measured during normal business hours of the theaters. DOD component O&M commands will ensure the GOS between the EO and any PBX users do not exceed an additional blockage of P.02. DOD component O&M commands are responsible for supporting DISA's data collection requirements on all DSN switches. DOD component O&M commands will report, to DISA, any user locations where GOS objectives cannot be achieved behind the EO

due to economic or operational limitations. DISA then compiles the data into monthly reports showing GOS across the DSN.

(1) DISA will report to the Joint Staff and respective combatant commands, those network access points (EOs and multifunction switch (MFS)) that do not meet the following performance standards:

(a) GOS criteria for inter-theater of P.09.

(b) Theater objective of P.07 as measured during the normal business hours between the DSN locations. (combatant commands may waive specific theater EO ROUTINE GOS implementations after coordination and consideration of DISA's network impact assessment.) The Joint Staff must be notified of all waivers of the theater GOS objective by the combatant command, and these waivers must be revalidated every 2 years.

(c) Any EO not meeting the special C2 user (DSN multilevel precedence and preemption (MLPP) FLASH OVERRIDE and FLASH) non-blocking criteria.

(2) Combatant commands report shortfalls in achieving the above target-GOS criteria because of economic or operational reasons to include shortfalls behind EOs.

b. Voice Quality. Because intelligibility of voice communications is critical to C2, the DSN voice service quality rating on at least 95 percent of the voice calls will have a mean opinion score (MOS) IAW the DOD Information Technology Standards Registry (DISR) (reference nn) shown in Table 1.

Configuration	Objective MOS
Fixed to Fixed	4.0
Fixed to Tactical	3.6*
Tactical to Tactical	3.2

Table 1. Voice Quality Objective Mean Opinion Score
* As is specified in Appendix 2 of the Generic Switching Center requirements (GSCR)

c. Voice Technology Migration. The DSN SSM is designated as 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. As such, all DOD component installation (base, post, camp, or station) voice transport and processing initiatives shall be coordinated with the DSN SSM. The DSN SSM will provide an annual assessment of the impact of emerging voice processing/transport technologies on global End-to-End voice performance and C2 services to the Joint Staff and the DSN CCB.

ENCLOSURE A -- APPENDIX A

PROCEDURES FOR REQUESTING DSN REQUIREMENTS

1. Purpose. This appendix provides an overview of DSN requirements.

2. General. DSN requests must be defined, validated, coordinated, and approved through DISA SSM for all mission and traffic requirements for DSN services. Requests must first be validated by the appropriate CC/S/A IAW (reference oo). Forward approved DSN requirements and priorities to DISA SSM for coordination or implementation. Provide the appropriate planning requirements to DISA for incorporation into the DSN program plans. Comply with references (f and pp) requirements for interoperability and supportability. Validated requests for a waiver to DSN policy and requests for an Interim Certificate to Operate (ICTO) are to be forwarded thru the chain of command to the Chairman of the Joint Chiefs of Staff for consideration.

3. Military Unique Features. The DSN achieves Assured Services through implementation of military unique features (MUF) to support military C2 functions. (See references e through j.)

a. Survivable Service. DSN supports C2 user traffic during peacetime, crisis, conflict, natural disaster, and network disruptions and possesses the robustness to provide a surge capability when needed. The following objectives contribute to the survivability of the DSN:

(1) No single point of vulnerability for the entire network, to include the NM facilities.

(2) No more than 15 percent of the bases, posts, camps, or stations impacted by an outage in the network.

(3) System robustness through maximum use of alternative routing, backup.

(4) To the maximum extent possible, transport supporting major installations (base, post, camp, and station, leased or commercial sites/locations) will use physically diverse DISN routes.

(5) The National Military Command Center (NMCC) (and Alternate), combatant commanders, or DOD component headquarters will not be isolated longer than 30 minutes because of an outage in the backbone (long-haul) portion of the network.

(6) DSN priorities, in order, by stress levels are:

(a) Crisis, Pre-attack, and Theater Non-nuclear War. DSN network capabilities must support all peacetime readiness (Priority 3) users, plus surge requirements for non-nuclear war. These capabilities are handled according to established precedence levels (reference tt).

(b) Post-attack. In the CONUS, DSN possesses the capability to reconstitute itself, from segments of the DSN surviving a conventional or nuclear war, to support the NCS in reconstituting national communications. Overseas, DSN possesses the same capabilities to support the NCS after a non-nuclear war.

(c) Peacetime Readiness. DSN supports both C2 and non-C2 users.

(d) Early Trans-attack (few weapons, possible High-Altitude Electromagnetic Pulse (HEMP)). DSN will support C2 user traffic as able. HEMP protection will be consistent with reference h.

(e) Massive Nuclear Attack. DSN will support special C2 user traffic as able.

b. Assured Connectivity.

(1) Assured service capability ensures the connectivity from user-instrument-to-user-instrument across the DSN, including US Government-controlled PBXs, EOs, the overseas DSN and tactical networks that incorporate MLPP features.

(2) DSN is required to provide assured voice communications to C2 users. Assured service or connectivity is defined as the ability of the DSN to optimize call completion rates for all C2 users IAW the guidelines in this instruction, despite degradation because of network disruptions, natural disasters, or surges during crisis or war. The DSN was designed with the MLPP capability to permit higher precedence users to preempt lower precedence calls. Special C2 users (FLASH and FLASH OVERRIDE within the current DSN MLPP framework) are provided with non-blocking service (P.00 threshold) from user to user. (P.00 = out of every 100 calls, the probability is that zero calls will be blocked.)

c. Responsive Service. DSN service must be responsive to the needs of C2 users. Special C2 users under the current DSN MLPP scheme -- FLASH and FLASH OVERRIDE -- are provided non-blocking service.

d. Surge Capacity

(1) Mitigation of short-term traffic surges is inherent in the MLPP capabilities of the DSN. DISA will ensure that PRIORITY and IMMEDIATE traffic will encounter, at a minimum, GOS of P.02 (two calls out of 100 will be "blocked" during the "busy hour") and P.01 respectively during a 100 percent increase above normal precedence usage.

(2) The DSN design provides, at a minimum, a 25 percent increase in spare trunking port capacity above the current employed network trunking at all tandem switches, MFSs, and critical dual-homed EO switches. DISA, in coordination with DOD components, annually identifies and re-validates critical DSN switches.

(3) During times of surge or crisis, the CJCS can direct implementation of certain traffic controls, such as selected blocking, directionalization, and usage or availability control (i.e. MINIMIZE) to ensure usage for critical users. In addition, affected combatant commands, Services, and agencies should utilize all means available to reduce (i.e. MINIMIZE) and/or remove nonessential voice traffic.

(4) The long-haul portion of the network must be able to support a regional crisis in one theater, yet retain the surge capability to respond to a regional crisis occurring nearly simultaneously in another theater.

e. Secure Service. DSN permits, through the use of secure instruments, protection of classified and sensitive information being passed, to ensure its confidentiality, integrity, and authentication. Where possible, the DSN is configured to minimize attacks on the system that could result in denial or disruption of service.

f. Interoperable Service. DSN is designed with the capability to permit interconnection and interoperation with similar tactical, US Government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable and IA Accredited as specified. (See references f, w, y, and oo).

4. National Security and Emergency Preparedness (NS/EP) Compliant Service. DSN complies with the requirements, priorities, and procedures established by the NCS regarding NS/EP (reference i). In the United States and its territories, NS/EP support is provided IAW FCC rules and regulations through the commercial telecommunications industry and the TSP system (reference j). For example, access to the Government Emergency Telephone System (GETS) is available via the DSN. The DSN must comply with the NS/EP's TSP system for service restoration. Within the United States of America and its territories, NS/EP Telecommunications Service Priority (TSP)-approved requirements will

be provisioned within 72 hours. In other OCONUS areas not under the control of the US Government, the DOD components will provide NS/EP support where feasible and available through agreements with host governments and IAW TSP. OCONUS requirements will be provisioned as quickly as possible.

5. Integrated Services Digital Network (ISDN) Services. VTC, data, and other switched system applications performance objectives must use DSN performance objectives as their minimum standard.

6. Network and Applications. In addition to standard dial-up service, DSN provides and supports a variety of other data and video systems, programs and applications:

a. Data Network Augmentation. The primary means of passing data over the DISN are the packet-switched networks. However, DSN augments the DISN packet-switched data networks, e.g., NIPRNET, SIPRNET, as required, by providing supplementary backbone transmission access where there are no DISN data services. These data services must conform to the guidelines outlined in Enclosure B for connection to the DSN.

b. Switched Data.

(1) DISA provides network standards, NM, transmission, and switching services. Users are responsible for procurement, operation and maintenance of their customer premise equipment (CPE) using the DSN.

(2) DSN provides both 64 Kb Integrated Services Digital Network (ISDN) and switched 56 kb digital services (restricted mode ISDN). These services provide the improved capability for the DSN to support STE, dial-up video services, bulk data transfer, and other switched data transmission requirements. The objective is for the DSN to implement ISDN services from EO to EO as Service switch upgrade projects and programs are completed. The components are responsible for ensuring ISDN capabilities are provided in the EOs at the base, post, camp, or stations for all DOD organizations that will require the use of STEs or other ISDN interfaces. DISA is responsible for system designs, configurations, and equipment required for the interconnection of EOs to ubiquitously implement ISDN services across the DSN. The DSN provides switched services connectivity for the DOD common-user video teleconferencing system. The DSN also provides switched data circuit connectivity in support of user VTC long-haul transmission requirements. VTC programs and requirements are outlined in references k and l. See Enclosure B for specific procedures for connecting VTC equipment to the DSN.

7. Network Interfaces. Interfaces to the DSN must comply with the DSN interface criteria in DODD 5105.19 and DOD Voice Networks, GSCR. (See

references m and y) Use of network interfaces that do not conform to the DSN interface criteria must be coordinated with DISA and approved by the Chairman of the Joint Chiefs of Staff. Network interfaces not conforming to DSN or DRSN interface criteria shall be permitted only after DISA SSM technical review and approval, on a site-specific basis, by the Chairman of the Joint Chiefs of Staff. (See reference oo)
In each of these interfaces, a method for controlling the flow of traffic across the interface must be established and monitored by DISA. DSN supports the following network interfaces:

a. Canadian Switch Network (CSN). The DSN will support the combined US/Canadian North American Aerospace Defense Command (NORAD), Tactical Autovon System (NTAS) and general-purpose requirements for communications. As such, the CSN interfaces and functions as an integral part of the DSN to combine the networks utilizing the DSN numbering plan for C2 communications worldwide.

b. Enhanced Mobile Satellite Service (EMSS). The EMSS facility provides connectivity between the DSN and the wireless, satellite-based IRIDIUM Satellite network. EMSS users are authorized direct access to place precedence calls from the IRIDIUM system. DSN users may place precedence calls destined for EMSS users in the IRIDIUM system. EMSS direct precedence access and egress must meet the following standards:

(1) Direct DSN precedence access.

(a) Access to DSN must be via the authorized gateway switch.

(b) Precedence access to the DSN must be controlled by the DSN Precedence Access Threshold (PAT) function on all access trunks.

(c) Precedence calls receive standard precedence call processing upon entering the DSN.

(d) Precedence calls blocked within the DSN receive standard DSN-blocked precedence treatments.

(e) Precedence calls blocked in the IRIDIUM system receive standard IRIDIUM blocked-call treatment.

(2) Direct DSN precedence egress to IRIDIUM.

(a) Precedence calls receive standard precedence call processing while in the DSN.

(b) Egress to IRIDIUM must be via the authorized gateway switch.

(c) The originating user must receive an announcement upon leaving the DSN infrastructure prior to entering the IRIDIUM gateway that DSN precedence is not supported.

(d) The precedence call must then be released to the IRIDIUM network.

(e) Precedence calls blocked in the IRIDIUM system receive standard IRIDIUM blocked-call treatment.

c. National Communications System (NCS). In the United States, the NCS will use the DSN and other switched systems to carry the traffic of NS/EP users. Post attack recovery and reconstitution of federal agencies in CONUS will center on support provided by the NCS. Following attack, surviving DSN network capabilities will be incorporated into the NCS. DISA is responsible for developing interoperability between the DSN and the NCS. (See references i, j, q, r, s, and t.)

d. National Defense Network (NDN) Interconnects. The Defense Switched Network (DSN) Interconnects with the following allies to provide bi-directional direct dialing services. These services are provided under international agreements to share voice services between the national systems. DISA is responsible for processing the required agreements with the affected countries.

(1) Australian Telecommunications Network.

(2) British Defense Fixed Telecommunications Service (DFTS).

e. NATO Core Network (NCN). DSN interoperates with the NCN to provide users access to both networks. The NCN-DSN interfaces have been developed and implemented at locations as agreed among NATO, the affected commands, and the Joint Staff. NDN's of NATO members can be accessed via the NCN-DSN interface. DISA is responsible for processing the required agreements with NATO. (See references n and o.)

f. Public Switched Telephone Networks (PSTNs).

(1) Automatic Interfaces Automatic off-netting interconnections (i.e., not requiring operator intervention) to allow DSN users to reach local private or PSTN subscribers (users) may be authorized by the authority controlling the EO or PBX:

(a) Automatic Interconnection is only allowed between an incoming long-distance DSN call and the local commercial system (off-netting)

when proper controls ensure authorized use. Likewise, automatic interconnection is only allowed between an incoming call from a commercial system and the DSN (on-netting) when proper controls ensure authorized use. See Enclosure A, 3 c for proper controls to be used.

(b) "Call Fowarding" is an authorized form of off-netting a DSN call to a single PSTN number or instrument. This off-netting is authorized in order for an official call to be connected at another location (e.g., residence) or provide a mobile capability, for mission accomplishment. Authority to provide such service shall be within the guidelines of reference oo and mm. All precedence calls must be routed to an operator. Sensitive calls received on a non-DOD instrument must be terminated immediately by the users or local authority. DOD components are responsible for connection and usage charges on public networks.

(c) Local calls (often identified as "dial 9" service) are allowed, including enhanced call completion features (e.g., forwarding and call waiting) if deemed appropriate by local DOD component in the local area for local calls. These features must in no way diminish the DSN assured service connectivity from user to user. The DOD components are responsible for any connection and usage charges to public networks.

(2) Managed Interfaces. DISA and the DOD components will manage controlled interfaces between the DSN and the PSTN to fulfill communications requirements between DOD and non-DOD networks/systems and to provide alternative communications in the event of DSN disruptions. All requests for implementing automatic on netting interfaces to the DSN will be submitted to DISA GS23 for review and to Joint Staff J-6C for final approval. Requests will include and identify the organizational process and an IA and Interoperability technical solution to ensure compliance with requirements of Enclosure A, 3.d. (See reference y)

(a) If interface usage will incur additional call-by-call charges for the commercial segment of the call, a bill payer arrangement must be included in the planning, agreements and implementation of the interface.

(b) These interfaces may only be used for health morale and welfare (HMW) calls and charges will be IAW Enclosure A, 3 c. At a minimum, these interfaces will meet the criteria in paragraph 7.f. (1) (c).

(c) The primary interface from the DSN to the PSTN shall be DISA's managed interface to the PSTN's "toll free" numbers (area codes 800, 888, 866, and 877). This interface is accessed with the DSN telephone number 809-4-OFF-DSN (809-463-3376) and then dialing 1+ the 10-digit number after the second dial tone. Authorized uses of this interface are for calling: Government contractors' toll free numbers for official business/support; Help Desk

numbers for hardware/software support; Non-toll free PSTN number with Government provided calling cards for official calling requirements or with an individuals' calling card, if the call is for HMW purposes. Reverse billing to call recipient via "1-800 Call Collect" Services for either official or HMW calls is also an option. Local Commanders may limit/restrict access to this service by Class of Service tables and classmarking user lines to manage resources and/or meet other mission requirements.

(d) Protection of Administrative Telephone System: Voice firewalls are required for administrative voice traffic to protect against internet attacks via modem interfaces to the PSTN or to the FTS. Voice firewalls will ONLY be allowed on the DSN Network in a non-interfering, passive listening mode for inter-switch trunks of the MFS/SA/EO/SMEO/PBX1/PBX2 and RSUs.

(3) Other automatic interconnections, on or off-netting, may be permitted on a case-by-case basis. HMW calls must be IAW reference mm and Enclosure A, 3.c. All automatic on-netting interfaces to the DSN must have as a minimum the following controls:

(a) Positive identification of all users and access control through some means, such as PINs. If PINs are used, only one individual is permitted to use an assigned PIN. Blanket issuance of access means or PINs to a class of users is not allowed. However, organizational accounts may be used to meet mobility or deployment requirements.

(b) An identification system that is secure enough to rapidly detect and prevent fraud, abuse, or compromise. PINs or identification schemes must be operated with security features available IAW commercial practices and devised to prevent intuitive deduction or easy identification of the protection scheme by unauthorized users.

(c) A means of identifying all calls made through the automatic interconnection. All calls must be periodically verified by the user.

(d) A means of identifying costs of all calls for appropriate user or customer billing.

(4) Manual Interfaces. Manual off-netting connections between the DSN and PSTN for official calls by operator intervention at an EO switch or PBX may be authorized by the authority controlling the EO or PBX. DOD components are responsible for monitoring and preventing abuse of this capability.

g. Tactical Communications.

(1) DSN normally connects to tactical communications systems using Standardized Tactical Entry Point (STEP)/Teleport. The STEP/Teleport provides technical features to permit tactical communications systems to interoperate with the DSN. DISA maintains interface standards for the STEP/Teleport and will manage the configuration and provisioning of STEP/Teleport sites to interface with deployed networks, to include those of the JTF backbone and DOD components. (See references o and kk) Deployed voice systems, will comply with DSN specifications (see references m and y) to complete the needed interfacing with the DSN at STEP/Teleport sites.

(2) STEP/Teleport provides tactical voice switched networks two ways, either through the STEP/Teleport switch multiplexer unit (SMU), or directly through DSN compatible interswitch trunk (ISTs). The SMU operates in the DSN as a (SA) DSN switch and only provides tandem support. All tactical switches which connect to the DSN using DSN compatible ISTs must comply with reference y for technical interoperability, and comply with all applicable provisions of this instruction.

8. Network Management. DISA establishes DSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. The DSN is under the management control of the Director, DISA, on behalf of USSTRATCOM, and is responsive to the CJCS and the DOD components. DISA will attempt to coordinate with Service/Agency O&M personnel prior to implementation of any/all switch software changes. The DOD components will ensure switch systems are certified for interoperability and IA accreditation or obtain an ICTO or waiver and interim authority to operate (IATO) prior to connection to the network. (See references f and pp).

a. DISA must possess read-access and limited/controlled write- access capabilities for DSN switch database tables. DISA will coordinate with Service/Agency O&M personnel prior to implementation of any/all switch database changes consistent with local commander and combatant command needs and requirements. Database tables for the switch domains that are not controlled by DISA (PSTN, FTS, Local subscriber service) will continue to be the responsibility of the Service/Agency (DOD components) In OCONUS AORs, the theater combatant command or commander may direct that DISA (through O&M command personnel when they are present) be authorized access to non-DISA-controlled portions of switch database tables as required to meet theater operational needs. (See reference oo).

b. DISA must maintain a CM database of all switch configurations (CONUS and OCONUS) and provide access to DOD components as authorized by ASD (NII)/DOD CIO; the Director, Joint Staff, and DISA. (See reference oo).

c. DISA will have sufficient read/write access to implement network control commands to all DSN switches either through direct intervention by DISA personnel at the CONUS GNSC or the OCONUS TNC. Consistent with Local Commander and combatant command needs and requirements, DISA will use onsite O&M activities to implement network controls except as outlined in Para 8d. (See reference oo).

d. During emergencies the GNSC or a TNC has the authority to direct and implement switch database revisions required for operation and management of the DSN consistent with paragraphs 8a and 8c above. (See reference oo).

e. DOD O&M commands/organizations must maintain DISA's intra- and inter-switch routing, numbering and dialing plans to ensure End-to-End interoperability and standardization across the Global DSN. Standardization of the dialing plans in DOD switches has historically been DISA's objective, but resource limitations and priorities have prevented closure with a documented requirement. The objective of DISA and the O&Ms is to work together to transition non compliant dialing plans. DOD components must implement DSN access codes, as defined in the DSN GSCR document, (reference v) and use the DSN standardized dialing plan that as a minimum which includes:

(1) 7-digits intra-theater (includes intra-base calls on a base/camp/post/station.

(2) 10-digits inter-theater.

(3) 10-digits including special services (e.g. ISDN) and Tactical access.

(4) Standard access codes.
90 DSN, FLASH OVERRIDE Precedence.
91 DSN, FLASH Precedence.
92 DSN, IMMEDIATE Precedence.
93 DSN, PRIORITY Precedence.
94 DSN access Routine dialing (default)
95 Off-net 700 services
96 Not Assigned
97 FTS access.
98 FTS access.
99 Commercial (PSTN) access.

9. Network Security. The DSN will implement appropriate IA controls as identified in DODI 8500.2 (reference rr) and conform to the Security Certification & Accreditation (C&A) process outlined in reference v. The objective of this requirement is to establish a DOD-standardized approach to

protect and secure the entities that comprise the Defense Information Infrastructure.

10. Network Survivability Features.

a. Network Design. DISA must design the topology (nodal, MFS, and EO) of the DSN (where to connect switches in the DSN) and publish a plan and update annually. The DOD components must coordinate recommendations with DISA (and the combatant command concerned if OCONUS) for designation or re-designation of an EO or MFS. DISA evaluates and engineers all changes or redesign issues as appropriate for tactical switches and JCS J-6C Staff adjudicates any disagreements.

b. Vulnerability Analysis. DISA is responsible for initiating and providing technical analysis and IA assessment of the network for survivability, to include risk analysis. DISA will forward results of the analysis to the Joint Staff for review.

11. DSN Switches, Network Elements, Appliances, and End Instruments. The DSN configuration of switches and equipment is constructed to meet DOD user requirements to support the warfighter. Specific interoperability certification requirements of each category of switch and appliance (e.g., SA, MFS, EO/SMEO, PBX, RSU, DVX, and VTC) are published in the current DSN GSCR, reference y. The DSN GSCR includes VoIP line side services. All future IP based RTS will be addressed in the RTS Generic System Requirements document required in Enclosure C. SAs, MFSs, EOs/SMEOs are under DISA's NM responsibilities. PBXs and RSUs are secondary voice switching facilities on users' installations that derive DSN service through the local DSN EO. The combination of all the switches makes up the Strategic DSN for the purposes of this instruction. DOD components must not directly interconnect switches (MFSs, EOs/SMEOs, PBX) in a manner which circumvents or bypasses the long-distance DSN network. (See reference oo.)

a. The following switching and transmission elements of the DSN fall directly under DISA's management responsibilities as the SSM:

(1) The SA nodal switch (tandem).
(2) The nodal switch function of the MFS.
(3) All connectivity between the following switch types:
    (a) SA nodal to SA nodal.
    (b) SA nodal to MFS and/or EO switch.
    (c) MFS to MFS and/or EO switch.
    (d) EO switch to EO switch.

b. The following switching and transmission elements of the DSN fall directly under DOD components' management responsibilities:

(1) PBXs
(2) DVXs
(3) User Terminal Equipment
(4) Access Transmission from PBX/Terminal Equip to the EO
(5) COI trunks
(6) User Lines
(7) RSU's

c. Combatant commands may designate tactical assets and engineer the tactical voice architecture IAW Enclosure E, Para 5.a. (5). DISA will assign tactical area codes for these assets IAW DODI 8100.3, Para 5.4.2.3 and CJCSM 6231.07D, Enclosure E, Para 8.b. (2).

d. DSN Backbone Switches.

(1) Two switch types provide the switching subsystems for the DSN backbone. These backbone switch types are the SA nodal switch (tandem switch) and the MFS. The nodal switch connects multiple MFS's, provides access to a variety of transmission media, routes calls to other nodal switches.

(a) Stand Alone (SA) Switch. A nodal switch that only provides tandem functions in the DSN backbone (CONUS)

(b) Multifunction Switch (MFS). A switch that combines the tandem function of the SA switch with the EO function of connecting the user's lines to the backbone trunks. Logically the SA and EO are separate, but within the same physical configuration.

e. Installation Switches at base, post, camp, and station (b/p/c/s). EO is used generically for the primary switch for one or more installations in geographic proximity to each other whether it is technically an EO or SMEO. In unique cases, due to costs or technical considerations, an EO or SMEO may be configured behind another EO, but each must still meet JITC Certification and IA Accreditation requirements. The EO is an integral part of the GIG and achieves worldwide long distance communications networking via the DSN nodes (either SA or MFS). EOs are normally connected directly to DSN nodes.

f. End Office (EO). A switch which is integral to the DSN and serves as a primary switch for long distance services for either an installation or group of installations in a geographic area by interconnecting users to the DSN nodal switches.

g. Small End Office (SMEO). A switch that serves as the primary switch, functions as an EO, but at smaller DOD installations. A SMEO does not have full DSN Network Traffic Management capabilities. It offers limited performance reporting and may not support SS7 signaling. Therefore, SMEOs will not serve installations that are critical to combatant command missions where NM control and network visibility for situational awareness is required.

h. Private Branch Exchanges (PBX). Secondary voice switching facilities on users' installations that derive DSN service through the local DSN EO are considered customer premise equipment. PBXs are primarily concentrators to distribute voice services to enclaves of installation end users. PBXs, on a case-by-case basis, may be connected and served by a DSN tandem switch for critical C2 missions approved by the Joint Staff. Although PBXs are not considered elements of the DSN and are owned, operated and managed by the components, they are still part of the GIG and therefore must meet all IA and interoperability requirements of the GIG. (See references e, f and oo.) Special C2 users are not authorized to be served by either a PBX1 or PBX2, since these switches cannot provide the appropriate level of availability with a single computer processor. There are two types of PBXs used in the DSN - PBX1 and PBX2.

(1) PBX1 switches have MLPP capabilities to serve C2 users that have a military mission to either originate or receive C2 calls for orders and direction at precedence levels above ROUTINE. At all PBX1 locations capable of implementing MLPP access line interfaces, at least one access line must be conditioned for incoming preemption or an EO operator must intercept all precedence calls. PBX switches with precedence terminating service through an EO attendant must not have executive override, preemption call waiting, or other features enabled that will inhibit preemption or a precedence call.

(2) PBX2 switches have no MLPP capabilities and only serve DOD non-C2, non-DOD, non-US Governmental and foreign government users that have no missions or requirements for C2 communications under existing military scenarios to support the Warfighter, as an adjunct site or to augment communications of other installations. Users are provided PBX2 services for economic or policy benefits of the DOD when not in conflict with local public telephone ordinances. PBXs without precedence terminating service through an EO attendant may have executive override to enhance completion of essential/emergency services IAW DOD 8100.3. PBX2 switches can only be procured or implemented after being granted a waiver for MUF requirements by the Joint Staff.

i. Remote Switch Unit (RSU). The RSU is a switching capability that is connected to a host as a remote via an umbilical, dependent upon the host switch for software control, some or all centralized OA&M, and is integral to the

DSN. RSU is the generic term for a number of switching concentrators Remote Line Concentrating Module, Meridian Cabinet Remote Module -SONET, EPN MISC etc.) that depends upon a host switch.

(1) The RSU can best be described or envisioned as an installation of the host switch's internal "line and trunk cabinets" at a location within the confines of the Installation, b/p/c/s authorized boundaries, or at a related adjacent site, normally with in few miles of the host switch." During degraded operating conditions, only partial service may be available from the RSU. The RSUs line and trunk cabinets are of the same basic type and originally certified by the JITC during the "host switch's" MFS, EO or SMEO certification process.

(2) RSUs are cost effective ways to improve "reach" and extension of voice communications capabilities and services to users located in buildings that are some distance from the host switch. An RSU is an extension for the voice switch's previously certified DOD components. For this reason:

(a) RSUs retain legacy status even if the host switch is upgraded.

(b) RSUs can be capacity upgraded, expanded and moved within the authorized boundaries (within a reasonable distance of the Installation, Base Post, Camp or Station).

(c) RSUs used to extend the host switches' capability do not require stand-alone (MUF) capability.

(d) Stand-alone capability is only required if an RSU is utilized in EO/SMEO applications not within a reasonable distance of the host switch.

(e) Line and trunk sizing does not trigger APL requirements.

(f) CAS to PRI transitions do not trigger APL requirements.

j. Switch Multiplex Unit (SMU). The SMU is a tactical voice trunk switch which provides an interface to the DSN for current TRI-services tactical (TRI-TAC) compatible digital transmission groups and trunk group clusters. The SMU operates in the DSN as an SA DSN switch and provides only tandem support. The SMU is capable of providing direct user access when equipped with the required communication security (COMSEC) equipment, but its primary purpose is to service as a tandem gateway between TRI-TAC switched voice networks and the DSN. A SMU is installed at every STEP/Teleport site .

k. Secure Voice Terminals. The STU-III/STE/SCIP family provides a secure voice capability over the non-secure switched voice network. Secure voice terminals are managed as CPE similar to the non-secure telephone instruments, but IAW national, CC/S/A procedures.

l. Customer Premises Equipment (CPE). Non-secure and secure telephones, STU-III/STE/SCIP family telephone instruments, data terminals, video conferencing facilities and equipment, facsimile machines, and other user

terminal equipment are the responsibility of the user to manage as CPE. This responsibility includes the acquisition, operation, maintenance, security, and funding of specified equipment. DISA is responsible for establishing interface standards, ensuring interoperability, and establishing procedures to minimize the impact of the terminal equipment on the network. (See references m and y) CPE must meet GOS objectives for the GIG. The DOD component O&M command is responsible for monitoring the performance of CPE equipment and must report all substandard performance to DISA and take all necessary actions to ensure DSN GOS objectives are met.

m. Two (2)-Wire Analog Telephones

(1) Any 2-Wire analog telephone that bears a label confirming compliance with FCC Rules and Regulations, Parts 15 and 68 will be considered approved for connection to DSN and the PSTN and requires no further testing for interoperability certification and information assurance accreditation. Such telephones can be purchased, connected and operated without the manufacturer or device name(s) appearing on the APL. 2-Wire analog telephones, digital (e.g., ISDN, digital proprietary phones) and cordless and wireless devices are excluded and must be tested, certified, accredited and added to the APL before connecting to the DSN.

12. Command and Control (C2)

a. The DSN SA nodal, MFS, and EO switches must contain the necessary MLPP features to satisfy user C2 requirements and interconnected to DISA NM subsystem; Advanced DSN Integrated Management Support System (ADIMSS). DISA has the complete responsibility to supervise and manage ADMISS. The user terminal end of DSN is currently the long-distance termination in the EO for DISA's NM purposes. DISA DSN NM responsibilities extend throughout the enterprise network to the EO switch. DISA, as the DSN Single-System Manager (SSM), is responsible for ensuring special C2 user services and establishes the criteria for handling special C2 calls end-to-end. The O&M command is responsible for providing switch maintenance to ensure service to all C2 users from the EO switch to the instrument is IAW DSN performance objectives (Enclosure A, para 4) and will periodically review user authorization for DSN access and precedence capabilities.

b. Executive override, preemption call waiting, or any similar EO or PBX special feature must not be enabled to interrupt a precedence DSN call or deny DSN precedence access unless the precedence call is forwarded to an alternate number or attendant position. If a precedence call is forwarded to an attendant position, the call in progress must be interrupted if the attendant determines the precedence of the incoming call is higher than the one in

progress. If a precedence call is forwarded to an alternate number, that number must be pre-emptable.

13. DSN Support. DSN supports four categories of users:

a. Special C2 Users. A special class of user who has access to the DSN for origination and reception of essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness. This user also requires communications among all DOD components. Specifically, these special C2 users are identified through one or more; Chairman of the Joint Chiefs of Staff, combatant commanders, Service, or DOD agency validation processes. The following are required capabilities of special C2 users:

(1) Chairman of the Joint Staff-approved FLASH, FLASH OVERRIDE, or IMMEDIATE precedence origination.

(2) Combatant command-validated minimum-essential circuits.

(3) Combatant command or Service-approved IMMEDIATE and PRIORITY precedence origination.

b. C2 Users. Users who have a requirement to originate and/or receive C2 communications but do not meet the criteria for class of Special C2 user. C2 users can exercise authority and direction as a Joint Staff (Joint Staff)/CC/S/A properly designated commander over assigned and attached forces in accomplishment of the mission. These Joint Staff/CC/S/A designated users can originate IMMEDIATE and/or PRIORITY precedence calls to issue or receive guidance or orders that direct, control, or coordinate military forces, whether said guidance or order is issued, received or effected during peacetime or wartime. Any Joint Staff/CC/S/A user that can originate ONLY Routine calls does not need to meet the availability or redundancy requirements of the Special C2 users or C2 users capable of originating PRIORITY precedence. All C2 users are capable of receiving FO/F/I/P calls. C2 users can be re-designated by Joint Staff to originate FO/F calls or designated by the combatant command of the AOR to originate IMMEDIATE and PRIORITY calls if situation warrants. There are four (4) types of DSN C2 users:

(1) Users approved by the Joint Staff or DOD component for PRIORITY and ROUTINE precedence origination.

(2) DOD users with a military mission that may receive C2 calls for orders or direction at precedence above ROUTINE, even though they do not

have a C2 mission for issuing guidance or orders. Therefore, these users must be served by DSN switches that provide the MUFs of the DSN or DRSN.

(3) Any Joint Staff/CC/S/A user that is authorized to originate ONLY Routine calls does not need to meet the availability or redundancy requirements of Special C2 users or C2 users capable of originating I/P precedence.

(4) Any non DOD US Government organization supporting Homeland Defense that requires assured services with DSN MUFs and the requirement has been validated by Joint Staff and approved by ASD (NII)/DOD CIO.

(a) The exercise of authority and direction by a properly designated commander over assigned and attached forces in accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

c. Non-C2 Users. Those users, DOD, non-DOD, non-US Government and foreign government users that have no missions or communications (equipment) requirements to originate or receive C2 communications under existing military scenarios. These users are provided access to the DSN for the economic benefit of the DOD and to meet the first choice requirement of paragraph 2.d and 3.a when it is not in conflict with local PTT ordinances. During a crisis or contingency, these users may be denied access to the DSN.

d. Administrative Users. Users at DOD locations who have both local and long distance telephone requirement for communications with industry or the public. These requirements are met by having connections from DSN switches to administrative telephone networks called PSTN or FTS which is provided by GSA. DOD users originating calls over the DSN may access these administrative telephone networks only IAW DSN on/off-net policies of this document.

14. Assignment and Control of Precedence Levels

a. Precedence Levels. Access to a level of precedence must be determined only by mission requirements and must not be used as a means of improving a GOS above that provided to ROUTINE users. Appropriate restoration priority or TSP should be considered with all special C2 precedence requirements. Any change in the assignment of precedence levels must be reviewed by DISA to ascertain the network impact and to size the DSN architecture to accommodate the change. All precedence requirements must be validated by the appropriate combatant command, Service Chief, or director of Defense agency, who also

approves requirements for IMMEDIATE and PRIORITY service. Requests for precedence are not restricted by Maximum Calling Area (MCA). The Joint Staff is the approval authority for FLASH and FLASH OVERRIDE calling capabilities. With the exception of new missions, requests for FLASH and FLASH OVERRIDE should normally be accompanied by a tradeoff of equal precedence.

b. Precedence Service. The DOD components must establish and maintain policy to control access and use of DSN precedence service through operator-assisted calls. EO switch users/subscribers are authorized precedence and long-distance DSN service only when a means is provided to positively control the number of simultaneous outgoing calls for each precedence level entering the DSN; e.g., instrument classmarks. DISA provides criteria for the EO switch processing of precedence calls to and from DSN to achieve the stated GOS and will determine the appropriate trunk sizing and switch configuration based on DOD component requirements and traffic-engineering analysis. Traffic-engineering and trunk-sizing requirements are based on business hours between DSN locations.

c. Control of Calling Areas for Precedence Levels. Local commanders are responsible for both the control and approval of the calling area capabilities available to their DSN users.

d. Control of Precedence Access. When NM capabilities, per paragraph 9, are available, classmarking of the user lines is employed to technically activate, manage, and control calling capabilities. When NM capabilities are not available, PATs or access line classmarking are employed to control access to the DSN.

e. Temporary Precedence Upgrades. Temporary DSN service upgrading to support DOD components or other equivalent personnel during travel is authorized for all precedence levels for up to 30 days. Temporary upgrading is also authorized for emergencies and exercises. Requests should follow the procedures in Enclosure A, Appendix C and must be coordinated with DISA and approved by the combatant command. Approvals of FLASH OVERRIDE and FLASH access must be provided to DISA and the Joint Staff. The DOD component must identify source of funding to cover additional costs prior to approval.

ENCLOSURE A -- APPENDIX B

POLICY AND PROCEDURES FOR CONNECTION OF SPECIFIC EQUIPMENT TO THE DSN

1. Purpose. Establish policy and procedures to support connection of specific types of equipment to the DSN.

2. General. All equipment must be procured from the Approved Products List (APL), that is JITC Interoperability Certified/IA Accredited, local site-accredited via an Authority to Operate (ATO) and must have an Authority to Connect (ATC) from the DSN Single System Manager (SSM). APL contains all current interoperability certification and IA accreditation for all equipment hardware and software. New services or equipment cannot negatively impact or degrade the overall end-to-end network performance. APL can be accessed via the web at: http://jitc.fhu.disa.mil/tssi/apl.html. ATC submissions may be placed at: http://www.disa.mil/gs/dsn/jic/atcsubmittal.html.

a. DISA provides the technical interface standards for equipment connected to the DSN. (See reference y.)

b. DOD components are responsible for ensuring JITC Interoperability Certification (JIC) and IA Accreditation of all upgraded or new hardware and software on DOD and sponsored Non-DOD installations prior to cutover. (See references e and f) To support implementation of DSN equipment in specific configurations, local commanders must:

(1) Ensure certification and accreditation IAW reference v.
(2) Ensure the Information Assurance Manager (IAM) validate configuration compliance IAW w/STIGs.
(3) Ensure the ATO memo is signed by the DAA prior to implementation.
(4) Obtain ATC from DSN SSM.
(5) Ensure equipment re-certification and re-accreditation at the end of 3 year certification/accreditation period or sooner when changes affect the security posture of the system identified.

3. Secure Transmission with a STU-III/STE/SCIP

a. The STU-III/STE/SCIP is the primary device for enabling secure communications over the DSN. It may be used for secure voice, data, video, or facsimile.

b. Approval under provisions of this instruction is not required for conversion of a non-secure telephone instrument to a STU-III/STE/SCIP on DSN.

c. For a STU-III/STE/SCIP to be connected to the DSN it must have the preempt feature enabled at all times.

d. When a STU-III/STE/SCIP is used to transmit secure data or facsimile, the instrument must meet the following requirements:

(1) National guidance for use of STU-III/STE/SCIP in secure data transmission, including access control TEMPEST, must be implemented (See reference s.)

4. Switched Data/Imagery

a. The DISN packet-switched networks are the primary means for transmitting data. However, the DSN switched voice (dial-up) circuits may be used to supplement the packet-switched networks where packet-switch connectivity is not available or where dial-up data connectivity is more operationally advantageous.

b. Data processing equipment using DSN switched dial-up voice or data must be capable of automatically disconnecting from the access line or IST when the transmission is complete or the circuit is preempted.

c. DSN users needing to use the DSN for large volumes of data, for extended holding times (in excess of 1 hour), or for dedicated operational systems requiring switched-data connectivity must coordinate with DISA for technical evaluation of the requirements. This process is necessary to determine the impact and to reconfigure the network as needed.

d. DISA provides technical assistance, interface standards, and connection approval for the types of devices in use over the DSN.

5. Dial-Up Facsimile. DSN may be used to transmit non-secure facsimile traffic without a STU-III/STE/SCIP only if the facsimile machine (or transmitting computer) automatically disconnects from the DSN access line or IST within 1 minute after the facsimile transmission ends or if the circuit is preempted. Dial-up secure facsimile transmission with a STU-III/STE/SCIP will follow procedures outlined in paragraph 3d.

6. Video Teleconference (VTC).

a. The DSN provides connectivity to the DOD common-user teleconferencing system by providing a dial-up switched digital capability at the 56/64 Kbps rate and multiples thereof.

b. DSN users with requirements for frequent VTCs with extended holding times (in excess of 1 hour) or for dedicated VTC circuits must coordinate with DISA for a technical evaluation to determine the impact and required network reconfigurations.

c. DSN VTCs must be pre-emptable if using the common-user DSN trunking. Dial-up VTC calls should be placed at a precedence level appropriate for mission requirements of each conference, not at a predetermined precedence to avoid disruption of the video conference.

7. DSN Control, Data Collection, and Orderwire Circuits. A/NM circuits and telemetry are critical assets to ensure the C2 operational capabilities of the DSN are maintained. All circuits that support the A/NM of the DSN will be maintained as high interest circuits with the TSP of 1.

(INTENTIONALLY BLANK)

ENCLOSURE A -- APPENDIX C

PROCEDURES FOR REQUESTING DSN SERVICE

1. Purpose. This enclosure provides procedures for requesting DSN service via Telecommunications Service Requests (TSRs) through the DISA Direct Order Entry (DDOE) process or in the case of Hawaiian Island Telecommunications System (HITS)/JHITS via Communications Information Tool (COMIT). The message format contained in paragraph 4 is for precedence requests for DSN services to the Joint Staff however, the DMS message format is not required. Submission via email is preferred.

2. General

a. All DSN service requests will be routed through DDOE system for the appropriate DOD component. Non–DOD Agency requests must be sponsored by a DOD component and forwarded through the Joint Staff to ASD (NII)/DOD CIO for final approval. Requests for DSN service must be submitted via DDOE procedures or in the case of HITS/JHITS via COMIT. Forecasts of future requirements (those appropriate for the DSN program plan) should be provided to DISA DSN SSM and the appropriate DOD components.

b. DOD component organizations with validation or approval authority must ensure requirements comply with this instruction. Specifically:

(1) Mission requirements are the drivers behind all requests for DSN access.

(2) Precedence requirements are justified in terms of explicit mission need, to include an explanation of negative mission impact if the request is not approved.

(3) Requirements affecting other DOD components have been coordinated with those affected.

(4) Appropriate telecommunication service priorities are identified. (See reference dd.)

(a) Originating requests from DOD components for Flash Override and Flash precedence must be forwarded through the JS for approval. Requests must be validated at the level immediately below the approval level.

(b) Requests from activities outside the Department of Defense must be sponsored by a DOD component and must be forwarded through the Joint Staff to ASD (NII)/DOD CIO for approval.

(c) Requests for DSN STEP/Teleport access will be requested IAW this instruction using the Gateway Access Request (GAR). (See reference ll)

3. Approval Authority. DSN Telecommunications Services Requests (TSR's) must be validated at the level immediately below the approval level (e.g., Joint Staff is the approval authority for FO/F/Non DOD services), the sponsoring DOD component must validate the request prior to submission to the Joint Staff. The level of the approval authority for DSN service requests is determined by the precedence requirement. (See Enclosure D and reference oo).

4. Request Format. TSR's will be created via DDOE or in the case of HITS/JHITS via COMIT for DSN. DDOE is the DISA approved order entry system and is mandated for all DOD customer use except in the case of HITS/JHITS which uses COMIT. The primary format to request a new or upgraded service is via e-mail below. DMS is acceptable, but not required.

a. The DSN customer Authorized Requesting Official (ARO) requests DSS (either the Meet Me Service or the Meet Me Plus option) and submits the TSR.

b. Once submitted, the TSR will automatically be routed to the Applicable DISA Theater Engineer Office for a technical assessment of the impact to the DSN and validation of solution.

c. Upon approval of the TSR by the Applicable DISA Theater Engineer Office, the applicable Defense Information Technology Contracting Office with estimates of the costs or defers until it goes through the provisioning process.

d. Upon approval of the TSR by the Applicable DISA (Theater Estimate Office) the TSR is routed IAW Program Designator Code (PDC) Routing Matrix. Source of updates: disadirect.disa.mil/products/ASP/sbscrpt_desc.asp

Example format:

FROM: (Originating Activity)
TO:JOINT STAFF J6C C4 SYSTEMS SUPPORT DIVISION(UC)//*
(*or activity with requisite approval authority)
INFO: SA WASHINGTON DC//G6//
CNO WASHINGTON DC//N61//
SAF WASHINGTON DC//XCD//
CMC WASHINGTON DC//CCT//
DISA WASHINGTON DC/GS23/GS233//
Validating authority, others (as required)

(If approval authority is below the Joint Staff level, information addressees will consist of affected DOD components and Joint Staff/J-6C. DISA will be an information addressee on all requests.)
UNCLAS or appropriate classification
MSGIC/GENADMIN/as appropriate per message text format (MTF)//
REF/as appropriate per MTF//
AMPN/as appropriate per MTF//
NARR/as appropriate per MTF//
REPLY/as appropriate per MTF//
RMKS/SUBJECT: CJCSI 6215.01 DSN REQUEST FOR (identify location or activity requesting service)//

1. Description of required capability (concise narrative description).

a. Complete identification of the requirement; (e.g., type of change, deletion, or addition including circuit or equipment quantities, configurations, sequence numbers).

b. Unit, title, and geographic location of requesting agency.

c. Precedence requested.

d. Start date (if short notice, give justification and mission impact of delay).

e. Restoration priority or TSP.

f. Servicing switch (EO, MFS).

g. Terminating equipment; e.g., type, brand, model of PBX, facsimile, data terminal/modem, VTC studio terminal equipment, emergency action console, STU-III/STE/SCIP.

h. Number of extensions required. Indicate if extensions are to be located in geographically separate locations that will require long-haul connectivity to servicing switch.

i. Location of the user requested DSN service (geographic and physical location of the DSN phone instrument).

j. Trade-off (identify by sequence number, command communications service designator (CCSD), precedence, Joint Staff approval number, or other pertinent data) or explanation if none provided.

k. DISA or Joint Staff waivers in effect (DMS/DDN, etc.).

l. Identification of the destination and expected frequency and duration of calls, data transmissions, or facsimile transmission. Information may also be expressed in terms of Erlangs of traffic.

m. If service request is for a new switch, switch upgrade or switch software upgrade it must have a validated interoperability certification and IA accreditation (listed on the current APL) or have a validated ICTO or waiver issuance by ASD (NII)/DOD CIO.

2. Justification

a. Present capabilities for DSN and why they are inadequate.

b. Detailed description of the mission directly supported by the requirement or the mission change that generated the requirement and mission impact if disapproved.

c. CC/S/A's validation authority and approval point of contact.

d. Identify source of funds. If available, identification of expected yearly costs to include:

(1) Identification of implementation costs and source of funds.

(2) Identification of annual depot support costs and source of funds.

(3) Identification of annual O&M costs and source of funds.

(4) Identification of increase in the DOD components annual site subscription price and source of funds. If cost figures are unavailable, DISA will calculate as part of its technical evaluation prior to approval. However, sources of funding must be identified as part of the validation process prior to approval.

e. Identification of DISA point of contact or DISA area representative (office code and phone number) who provided coordination and network impact assessment, or reason DISA was not contacted.

f. Other considerations or remarks as appropriate.

3. DOD components point of contact (name, office symbol, DSN and commercial phone numbers).

(NOTE: Only 1A, B, D, F, H, I, 2A, B, and 3 are required for requests for deactivation or cancellation of DSN service.)

(INTENTIONALLY BLANK)

ENCLOSURE B
POLICY FOR THE DEFENSE RED SWITCH NETWORK

1. Purpose. This enclosure provides general guidance, usage and performance objectives for the DRSN. In addition, it describes required functional requirements and MUFs of the DRSN.

2. General. The DOD and select federal agencies have a continuing operational requirement for a separate, controlled, and interoperable secure communications and conferencing network to support command, control, and crisis management activities. The DRSN provides the capability to satisfy that requirement. The DRSN is the secure circuit-switched element of the DISN. It is a Joint Staff-directed network of circuit switches interconnected by DISN backbone and commercial transmission links. DISA provides program and operational management of the DRSN. The DRSN provides high-quality, secure-voice services, voice conferencing, and the ability to provide other value-added services to senior decision makers. These additional services include, but are not limited to, red gateway functions for wireless, VoSIP, and strategic-to-tactical secure-voice interoperability. (See reference ee.)

a. The DRSN provides high-quality, secure telecommunications for C2 and crisis management. Through the use of cryptographically secured backbone trunks and access interfaces, the DRSN provides user-dialed secure connections among senior DOD, civil, and allied decision makers within the following user communities:

(1) The President, Secretary of Defense, Chairman of the Joint Chiefs of Staff.

(2) NMCC.

(3) NMCC Site R.

(4) Airborne Command Post community.

(5) Combatant commands.

(6) Military Departments and subordinate organizations (military and civilian).

(7) US Government departments and agencies (e.g.; Department of State) specifically approved by ASD (NII)/DOD CIO.

(8) Allies of the United States specifically approved by ASD (NII)/DOD CIO.

b. The DRSN is the primary network for secure conferencing and is the host network for the World Wide Secure Voice Conferencing System (WWSVCS) conferees, Defense Satellite Communications System (DSCS) based Enhanced Pentagon Capability (EPC) conferences, and the Military Strategic and Tactical Relay Satellite (MILSTAR) based Survivable Emergency Conferencing Network (SECN). Other conferencing requirements are accommodated by the DRSN on a not-to-interfere basis. (See reference ff.)

c. The USSTRATCOM/JTF-GNO GNC, DISA GNSC thru the TNC provide high-level monitoring and situational awareness of the core DRSN infrastructure 24 hours a day, 7 days a week. These centers implement the DRSN service manager's authority and responsibility to take immediate and necessary action to perform network-level fault isolation, restoral, or provisioning actions in the event of outages, network compromise, or critical world situation. GNC, GNSC and TNC roles in monitoring and situational awareness of connectivity to allies will be limited to the terms agreed upon in the MOA/MOU that governs the allied connections to the DRSN. This will be determined on a case-by-case basis.

d. The DRSN is the designated DOD strategic secure voice network serving peacetime, pre-attack, and, to the maximum extent practical, trans-attack and post-attack secure voice requirements. During nuclear attack, trans-attack and post-attack, the system will merge with other national assets to provide required service to users. The SECN integrates the DRSN with MILSTAR for just such contingencies providing direct support to the President and Secretary of Defense. The DRSN will be used as the primary network for satisfying DOD C2 secure-voice requirements, providing strategic-tactical secure-voice interoperability and conferencing for terminal equipment such as STU-IIIs, STEs, other SCIP devices and terminals, and evolving wireless secure-voice devices, and, where feasible, accommodating survivable mission requirements. No automatic or dedicated secure-voice trunking by and between RED voice switches and/or multimedia platforms and/or enclaves other than by the DRSN is authorized, except as waived by the DOD GIG CIO Executive Board. (See references x, z, gg, and hh)

e. Under authority of this instruction, DISA will promulgate operation and maintenance, security, performance, interface and interoperability, and Joint logistic support planning guidance for the DRSN. All DOD components supporting, using, or interfacing the DRSN must comply with DISA-promulgated guidance and performance, interoperability, security, and capability requirements listed in this instruction. (See reference oo)

3. Cost Recovery.

(1) Cost recovery for the network side of the DRSN is now included in the DSS, per OSD/PA&E Memorandum of the Three-Star Programmers, Subject: Results of the Three-Star Programmers Meeting of Defense

Information System Network Funding and C4 Governance Enhanced Planning Process, dated Aug 13, 2004.

(2) For the benefit of Service and Agency financial planning for the improvements and equipment replacements for which they are responsible at the b/p/c/s level, DISA will include financial planning information in the bi-annually updated and submitted DRSN program plan. The DRSN program plan will be staffed with the Services and forwarding to ASD (NII)/DOD CIO, and are the final approval/disapproval. ASD (NII)/DOD CIO is the final approval/disapproval authority for the DRSN program plan.

4. Usage Policy. General DOD use of the DRSN is restricted to the official business of the US Government or in the interest of the US Government.

5. Objective Technical Parameters and Special Functions.

a. Network Performance Objectives. The DRSN is designed to ensure that FLASH OVERRIDE OVERRIDE, FLASH OVERRIDE, and FLASH precedence call attempts by "directly connected" special C2 users will be completed on a non-blocking basis. This objective will be maintained as the initial network configuration is augmented and expanded as necessary to extend service to additional Service and/or agency RED switches. RED switches must comply with the DRSN interface criteria and only connect to the DRSN with the approval of the Joint Staff. Internally, DRSN RED switches must provide non-blocking service from an inlet (line or trunk) to an idle outlet (line or trunk). (See reference ee)

b. Voice Quality. The end instrument-to-end instrument voice quality of a telephone connection is subjective and is determined from the complex interaction of multiple switching, speech encoding, voice compression techniques, and transmission parameters. The objective of the DRSN is to provide toll quality secure-voice service on a DRSN-user-to-DRSN-user basis, and to ensure the highest practical voice quality when DRSN users are interfaced to external systems and equipment. This is defined as receiving a score of at least 90 on the diagnostic rhyme test (DRT) and a score of at least 60 on the diagnostic acceptability measure (DAM). The DRT measures intelligibility, and the DAM measures quality. These objective intelligibility and quality scores are achieved by adhering to the DOD, national, vocoding, and international transmission design and operational standards. DRSN voice quality is addressed in the development of new vocoders- for DRSN interfaces and voice compression algorithms for the network. Routine day-to-day assessment of voice quality occurs at the user level with problem reporting to the site DRSN operations and maintenance support activity for resolution.

c. Call Set-Up Time. Call set-up time is the elapsed time from the end of an originator's signaling until ringing of the called party begins. It is determined by switch processing delay, inter-switch signaling speed, and the total number of links involved in establishing the connection. The call set-up time from the originator completing dialing until ringing is applied has a design objective of 5 seconds maximum for direct calls (calls made without attendant assistance) and an objective of 15 seconds maximum for indirect (attendant-assisted) calls. Also, dial tone delay, which is measured from the time the user goes off-hook until the provision of the dial tone, must not be over 3 seconds for more than 1.5 percent of the calls during the busy hour. In addition, the postdialing delay, which is the time elapsed from the last digit dialed to switch through, is 1 second or less, on average, for an intra-switch call, including circuit operation and translation time. For tandem calls, the following trunk seizure, switch processing, and signaling delay parameters must not be exceeded in 90 percent of calls during the busy hour. Trunk-seizure delay is the time elapsed between a connected switch trunk seizure and the switch acknowledgment of the seizure that allows signaling to proceed. For each call the trunk-seizure delay must not exceed 0.1 second. Switch-processing delay, which is the time for the switch to select an idle path and send a trunk seizure to the distant switch, must not exceed 0.1 second. Once the distant switch acknowledges the trunk seizure, signaling must begin within 0.1 second. Calls connected to other secure voice systems through other than protected wireline or full-period COMSEC equipment may experience up to an additional 12-second delay for cryptographic synchronization.

d. Security Features.

(1) DRSN RED switches must operate with physical security and TEMPEST compliance to allow users within a RED enclave to conduct unencrypted and classified telephone conversations at the level commensurate with the facility, system, and user clearances (up to the TS/SCI level). As a minimum, DRSN switching nodes must operate at the TS security level. However, individual directly connected users may be configured at the SECRET level.

(2) Telephone instruments installed outside the RED enclave, but within a limited exclusion area in the same facility, may be connected to the switching subsystem through an approved Protective Distribution System (PDS) or link encryption between the RED enclave and the "exclusion" area. (See reference s.)

(3) All other connectivity into and out of the DRSN RED enclave must be secured with NSA-approved Type I encryption equipment. DRSN RED switches must interconnect with other RED switches and/or peripheral devices (to include, but not limited to, tactical secure-voice switches/enclaves, radio

interfaces, audio systems, voice announcers, and multimedia and/or secure-voice over data capabilities) through encrypted ISTs or by means of a PDS. Other secure systems must interconnect to the DRSN using DISA-established interface criteria and encryption devices or PDS.

(4) Special DRSN security features include:

(a) Automatic Number Identification (ANI). During intra-switch and inter-switch call processing, DRSN switches exchange classmark information that includes the calling and called-station identity and call security access level (SAL) assignments. The ANI information (of the calling party) is displayed on the called party's DRSN user telephone display prior to the call being answered by the called party. When the called party answers, the ANI information of the called party is displayed on the calling party's DRSN user instrument as well as the security level (SECRET, TS, or TS/SCI) of the established connection being displayed on both the calling and called parties' DRSN user instrument. User ANI identity information is defined in the database of the DRSN switch to which a user is directly connected. All equipment connected to the DRSN must be capable of providing ANI to the DRSN switch to which it is or will be connected.

(b) Security Access Levels. The SAL is a user classmark assigned to each instrument, line key, and trunk and provides security authentication of the calling and called party. SALs are assigned to each instrument, line key, and trunk based upon the classification and access level authorized for the user. The DISA DRSN service manager will develop and publish a standardized set of SALs, which must be implemented at all DRSN nodes. In addition to a standardized set of SALs, the DISA DRSN service manager may implement special SALs on a case-by-case basis to meet specific mission requirements. Alteration of SALs and/or implementation of SALs without specific direction and/or approval of the DISA DRSN service manager is not permitted and constitute a reportable security infraction.

(c) Automatic Security Authentication (ASA). ASA ensures DRSN calls are set up in accordance with security and access authorization criteria defined for each user and/or DRSN switch interface. ASA uses a combination of fixed and variable SAL assignments to reconcile and establish, or deny establishment of, connections between users and between users and DRSN switch interfaces based upon a highest common denominator scheme. For example, a connection between a user classmarked with a VSAL (see paragraph 2 below) of SECRET calling a user classmarked with a VSAL of TS will be permitted at the SECRET level. As another example, a connection between a user classmarked with a VSAL of SECRET calling a user classmarked with a Fixed Security Access Level (FSAL)) (see paragraph 1 below) of TS/SCI will NOT be permitted because there is no highest common denominator. This

highest common denominator ASA scheme is analogous to that implemented in the STU-III/STE/SCIP family of equipment.

1. Fixed security access level (FSAL). FSAL emphasizes call security over call completion. A user selects an FSAL-classmarked line when he or she must ensure the call is established at the desired security level. Under FSAL, a call's SAL is "fixed" at the user-selected level and cannot be downgraded as the call progresses through the network. If the called and calling parties and interconnecting trunks are classmarked with the same SAL (e.g., TS), the RED switches will establish the call and display the common security level. If a trunk group with a SAL equal to that of the originating station is not available for call routing, the originating RED switch will not complete the call, but instead will route the call to a security code violation-recorded announcement. If the called party has a different SAL assignment than the calling party (e.g., the called line is assigned SECRET and the calling line is assigned TS/SCI), the call will not be completed, and the originator will be routed to a security code violation-recorded announcement.

2. Variable Security Access Level (VSAL). VSAL emphasizes call completion over call security level. With VSAL, a call is established if network resources are available; however, the call may be established at a security level less than that selected by the calling party. The VSAL feature allows calls to be set up when SAL codes among calling and called stations and trunk groups are not equal. Calls are automatically established at the highest common security level of the users and trunk facilities. The highest common security level, as determined by the switching system, is displayed on the called and calling instruments. Users must read the displayed security level and ensure the security level of conversations does not exceed the displayed security level.

(d) Push-to-Talk Handset. The push-to-talk handset is an integral part of the physical protection afforded classified DRSN voice traffic. Removal of the push-to-talk feature may be justified only by legitimate operational requirements and will be approved on a case-by-case basis of the DAA, through the DISA DRSN information systems security manager. Prior to removal, the user must justify the action, develop procedures for maintaining the secure integrity of the instrument, and have written approval IAW DRSN security guidelines.

ENCLOSURE B -- APPENDIX A
PROCEDURES FOR REQUESTING MAJOR DRSN REQUIREMENTS

1. Purpose. This appendix provides an overview of major DRSN requirements.

2. General. DRSN requests must be defined, validated, coordinated, and approved through DISA SSM for all mission and traffic requirements for DRSN services. Requests must first be validated by the appropriate CC\S\A (See Enclosure D). Forward approved DRSN requirements and priorities to DISA for coordination or implementation. Provide the appropriate planning requirements to DISA for incorporation into the DSN program plans. Comply with references (f and pp) requirements for interoperability and supportability. Validate requests for a waiver to DRSN policy and requests for an interim certificate to operate (ICTO) are to be forwarded to the CJCS for consideration. (See reference oo)

3. Military-Unique Requirements. The DRSN must adhere to the following capability objectives to ensure its ability to support effective military C2 functions. (See reference ee.)

a. Survivable Service. The DRSN supports secure C2 user traffic during peacetime, crisis, conflict, natural disaster, and network disruptions, and possesses the robustness to provide a surge capability when needed. DRSN priorities, in order, by stress levels are:

(1) Crisis, Pre-attack, and Theater Non-nuclear War. DRSN network capabilities must support all peacetime readiness (priority 3) users, plus surge requirements for non-nuclear war. These capabilities are handled according to established precedence levels.

(2) Post-attack. In the CONUS, DRSN possesses the capability to reconstitute itself from segments of the DRSN surviving a conventional or nuclear war to support the NCS in reconstituting national communications. Overseas, DRSN possesses the same capabilities to support the NCS after a non-nuclear war.

(3) Peacetime Readiness. DRSN supports C2 and other users.

(4) Early Trans-attack (few weapons, possible HEMP). DRSN will support C2 user traffic as able. HEMP protection will be consistent with reference h for the DRSN as a whole except as may be required on a site-by-site basis to support specific mission requirements.

(5) Massive Nuclear Attack. DRSN will support special C2 user traffic as able.

b. Assured Connectivity. The DRSN is required to provide assured secure voice communications to C2 users. Assured service or connectivity is defined as the ability of the DRSN to optimize call completion rates for all C2 users IAW the guidelines in this instruction, despite degradation because of network disruptions, natural disasters, or surges during crisis or war. To meet military-unique requirements, the DRSN is designed, and will be sustained, with a particular MUF, namely MLPP. MLPP permits higher-precedence users to preempt lower-precedence calls. Special C2 users (FLASH and FLASH OVERRIDE within the current DRSN MLPP framework) will be provided with non-blocking service (P0.00) from user to user. Assured service capability ensures the connectivity from DRSN user instrument to DRSN user instrument across the DRSN infrastructure. To the maximum extent practical, the design and deployment of the DRSN will provide assured connectivity to and through peripheral interfaces to other systems and networks. FLASH OVERRIDE OVERRIDE (FOO) is a network feature that allows WWSVCS and selected other national level conferences to be completed.

c. Responsive Service. DRSN service must be responsive to the needs of C2 users. Under the current DRSN scheme, FLASH and FLASH OVERRIDE users are provided non-blocking service.

d. Surge Capability. The DISA DRSN service manager will ensure the design of the DRSN backbone infrastructure can accommodate increased demands for service in response to unforeseen mission requirements responsively. The DISA DRSN service manager, in conjunction with the DOD components, will periodically evaluate potential "surge scenarios" and, as appropriate, initiate actions to mitigate adverse impacts of "surge" on critical DRSN nodal switches. During times of surge or crisis, affected DOD components will utilize all means available to reduce (e.g., MINIMIZE) and/or remove nonessential voice traffic.

e. Secure Service. DRSN design and implementation must permit, through the use of physical security, cryptographic equipment and information assurance techniques, the protection of classified and sensitive information being passed. This design and implementation will ensure the information's confidentiality, integrity, availability, authentication, as well as protection from attacks on the system that would result in denial or disruption of service. The DRSN supports multiple levels of security ranging from Secret to Top Secret/SCI.

f. Interoperable Service. Although the DRSN is designed with the technical capability to permit interconnection and interoperation with similar networks, interconnection and/or interface to the DRSN by other DOD networks must be

approved by the Joint Staff after technical evaluation by the DISA DRSN service manager. Interconnection and interface by non-DOD US Government or allied networks must be approved by OSD. For each interface to the DRSN, all hardware, software, and subtending interfaces of the network/equipment to be interfaced must be certified as interoperable as specified in reference f.

4. NS/EP Compliant Service. DRSN complies with the requirements, priorities, and procedures established by the NCS regarding NS/EP (reference j). In the United States and its territories, NS/EP support is provided IAW FCC rules and regulations through the commercial telecommunications industry and the TSP (reference i). In OCONUS areas not under the control of the US Government, the DOD components will provide NS/EP support where feasible and available through agreements with host governments and IAW TSP.

a. The DRSN provides today's senior leaders and warfighters rapid, high-quality, secure communications and conferencing capabilities. It is a circuit-switched network that provides three unique capabilities:

(1) Integrated RED/BLACK (secure/non-secure) call origination/termination and switching (not implemented at all locations).

(2) Interoperable secure-voice conferencing with both the tactical and the strategic communities through approved interfaces.

(3) Direct interoperability with other secure-voice networks through approved secure interfaces.

b. MLPP

(1) The DRSN supports MLPP and is capable of processing traffic at six progressively higher levels of precedence: R, P, I, F, FO and FOO. The DRSN MLPP feature allows users with higher-precedence capabilities to rapidly traverse MLPP-supporting networks when high traffic loads or other network degradations limit the number of network calls that can be completed.

(2) Each station with authorized DRSN access is classmarked with a maximum precedence authorized and has the capability to use any precedence up to and including the highest precedence authorized for that station. The actual maximum precedence level assigned to a user is determined as part of the validation and approval process discussed in Enclosure E of this instruction. Assignment of the F and FO precedence levels must be approved by the Joint Staff. During call initiation, the precedence level of a call, up to the user's maximum authorization, is established by the caller as part of the "dialing" process. Calls are automatically established with an "R" precedence unless a higher precedence is dialed by the caller. If a station attempts a

higher precedence than authorized, the call is routed to an unauthorized precedence announcement.

(3) FOO is a special precedence implemented to support WWSVCS. Use of FOO ensures that WWSVCS conference calls can be completed through the DRSN even if the network is flooded with FO calls. (See reference ff.)

5. Network Services and Applications. In addition to providing user-to-user dial-up service, the DRSN provides and supports a variety of secure services. For secure conferencing, the DRSN supports an integral, digital, secure, conferencing capability and supports PCM summing; LPC-10 speaker broadcast conferencing, and mixed excitation linear predictive-encoded conferencing. Conferences may be established among DRSN users and other users served by a wide range of dissimilar systems interfacing the DRSN, including the STU-III, Advanced Narrowband Digital-Voice Terminal (ANDVT), STE, and evolving secure wireless voice (NSA secure wireless initiative) products. (See reference ee.)

a. The DRSN supports both network and local-level ad hoc and preset conferences.

(1) Ad hoc Conference. The DRSN permits three-party and progressive ad hoc conferences. Three-party conferences (three conferees) and progressive conferences (four or more conferees) are initiated by the user by dialing the desired parties sequentially and using the telephone conference feature key (or dialing a feature code).

(2) Preset Conference. DRSN preset conferences have predefined conference members (assigned in the switch database). All conferees are dialed simultaneously when the conference is activated. Preset conference records can only be created or changed from a switch console position. The system operator may activate preset conferences. Properly classmarked users may also activate preset conferences by dialing the preset conference feature code followed by the assigned two-digit conference number.

b. WWSVCS. The WWSVCS is a set of special-purpose C2 conferences that uses DRSN preset conferencing capabilities and user-managed switch interfaces. It provides secure-voice conferencing for the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, combatant commands, and other users designated by the Joint Staff.

c. SECN and EPC. The SECN and EPC are special-purpose C2 conferencing networks that use DRSN conferencing capabilities and user-managed switch interfaces over the MILSTAR and DSCS transmission media respectively. They provide survivable secure-voice conferencing for the

President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, combatant commands, and other users designated by the Joint Staff.

d. Multi-Node. Combatant commander sponsored conferences. Many combatant commands sponsored conferences use resources that include DRSN nodes in many different AORs and Federal Agency's. These conferences are critical C2 conferences involving many participants at different combatant commands and agency staffs. Combatant commands may request DISA assistance in the engineering and technical management of these conferences.

6. Network Interfaces. A key feature of the DRSN is its ability to interface and interoperate with a variety of DOD and commercial networks. All interfaces to the DRSN must be approved in writing on a case-by-case basis by the DISA DRSN service manager. JITC certification letters documenting a technical interoperability with the DRSN do not constitute connection approval. Such certification letters only serve as a technical basis for requesting approval for connection to the DRSN in support of a Joint Staff-validated mission requirement. DISA DRSN service manager's approval for an interface may be in the form of a permanent, conditional, or temporary interface. Use of interfaces not conforming to DRSN interface criteria or as stipulated in the DISA DRSN service manager's approval letter, can have adverse technical and security impacts on all DRSN users and constitute an unauthorized use of the DRSN. Any such interfaces can result in the switch supporting such interfaces being denied network-level access to the DRSN infrastructure. All connectivity from a DRSN switch to users outside the RED enclave (i.e., to another building, facility, location, or system) must be provided through an approved interface. The DRSN supports, but is not limited to, supporting the following interfaces:

(a) DRSN Switch Internal Interfaces. An internal interface provides intra-DRSN access (i.e., user-to-host DRSN switch or DRSN switch-to-DRSN switch).

(1) DRSN IST Interfaces. The DRSN IST interface provides secure (encrypted) connectivity to other DRSN RED switches through ISTs linking the RED switches.

(2) DRSN Remote Subscriber Interfaces. Secure service between remote users and the host DRSN RED switch is provided through remote subscriber interfaces.

(b) DRSN External Interfaces. External interfaces on DRSN RED switches provide connectivity to secure users on non-DRSN networks and may be of an automatic or manual type. To the maximum extent practical, secure external interfaces to a network other than the DRSN are to be configured to provide and exchange user and security information (i.e., ANI) (see paragraph

4b (2) (a) above) on a user-to-user basis across the interface. Calls made over an interface from a network other than the DRSN cannot tandem the DRSN to reach either a third network or another portion of the calling network (except through command center intervention) without case-by-case approval from the DISA DRSN service manager. To support optimum interoperability, connection between appropriately equipped interface trunks is possible on a digital or analog basis, depending on interface type. DRSN switch external interfaces are provided to, but not limited to, the following equipment or systems:

(1) STU-III. The DRSN will interoperate with STU-III users on the DSN, PSTN, and FTS-2001 (and successors) through the DRSN STU-III/R interface. Both incoming and outgoing STU-III direct-dialing capability is supported. STU-III users must use a STU-III that is keyed at the SECRET or higher level to complete a call through the STU-III/R interface to a DRSN RED switch. Connectivity can be provided between the DRSN RED switches and collocated BLACK switches through STU-III/Rs to provide DRSN users access to STU-III users on the DSN, FTS-2001 (and successors), and PSTN. In some locations, connectivity is provided from the RED switches through STU-III/Rs directly to the DSN, FTS-2001 (and successors), and PSTN. STU-III users may not traverse the DRSN to call other STU-III users.

(2) STU-IIB/SY-71e. A limited number of DRSN RED switches interface with NATO and other allied systems. The pre-dominate nature of these interfaces is that they are "manual/operator"-controlled. These interfaces are provided to permit US-allied interoperability only and are not to be used for allied or allied-system tandem calling.

(3) STE/SCIP. The DRSN interoperates with STE/SCIP users on the DSN, PSTN, and FTS-2001 (and successors) through the DRSN single-channel STE interface or the multi-channel CEU and will serve as the host for the "formal" conferencing bridge capability for STEs/SCIP Terminals supporting the Department of Defense. Both incoming and outgoing STE/SCIP Terminal direct-dialing capability is supported. STE/SCIP users must use a STE/SCIP Terminal that is keyed at the SECRET or higher level to complete a call through the single-channel or CEU interfaces to a DRSN RED switch. Connectivity can be provided between the DRSN RED switches and collocated BLACK switches through single-channel or CEU interfaces to provide DRSN users access to STE/SCIP users on the DSN, FTS-2001 (and successors), and PSTN. In some locations, connectivity is provided from the RED switches through single-channel interfaces or the CEU directly to the DSN, FTS-2001 (and successors), and PSTN. STE/SCIP users may not traverse the DRSN to call other STU-III or STE/SCIP users.

(4) Secure Wireless. The DRSN interoperates with secure wireless users on the DSN, PSTN, and FTS-2001 (and successors) through the DRSN

single-channel STE interface or the multi-channel CEU when future narrowband digital terminal signaling is supported. Both incoming and outgoing secure wireless direct-dialing capability is supported. Secure wireless users must use secure wireless equipment that is keyed at the SECRET or higher level to complete a call through the single-channel or CEU interfaces to a DRSN RED switch. Connectivity can be provided between the DRSN RED switches and collocated BLACK switches through single-channel or CEU interfaces to provide DRSN users access to secure wireless users on the DSN, FTS-2001 (and successors), and PSTN. In some locations, connectivity is provided from the RED switches through single-channel interfaces or the CEU directly to the DSN, FTS-2001 (and successors), and PSTN. Secure wireless users may not traverse the DRSN to call other secure wireless, STU-III or STE/SCIP users.

(5) ANDVT . The DRSN interfaces the ANDVT through either an analog or a digital interface. The ANDVT is employed with high frequency (HF) radio and narrowband satellite communications (SATCOM) systems. Calls incoming to the DRSN from the ANDVT interface must be answered by a designated DRSN attendant, who then forwards the call to the desired party. DRSN users may place calls directly to a platform (a single ship or aircraft) or into a net, where the caller can talk to multiple listeners. The ANDVT interface requires the caller to use radio procedures (e.g., use of push-to-talk and delay of speech until cryptographic synchronization).

(6) TRI-TAC. Selected RED switches interface TRI-TAC systems. RED switch subscriber calls or calls tandeming the RED switch to a deployed TRI-TAC or mobile subscriber equipment unit.

(7) UHF TACSAT. The PSC-5D interface provides connectivity to UHF TACSAT radios.

(8) VHF/UHF/SATCOM. Interface with VHF/UHF radio and SATCOM systems are provided through the KY-57/58 interface. Properly classmarked DRSN subscribers may dial directly to encrypted radio circuits. In the net monitor mode, an external speaker is monitored by an attendant or user, who transfers calls to and from the radio network as required. This interface requires the caller to use radio procedures.

(9) HF/SATCOM Radios/Tactical Wireline Systems. The KY-65/75 interface provides connectivity to HF and SATCOM radios and tactical wireline systems.

(10) EHF/SATCOM Radios. The KY-68 interface provides connectivity to EHF and SATCOM radios.

(11) EPC. The EPC is an identifiable system-level capability derived from the DRSN and other interfaced systems, which satisfies an operational requirement HEMP-hardened, secure-voice warning and decision conferences. The EPC uses dedicated equipment over military satellite transmission paths and hardened landlines. This system provides conferencing capability to a relatively small, but high-level, group of federal and DOD users.

(12) SECN. The ANDVT digital interface provides the DRSN interface to the SECN and other MILSTAR connectivity for simulated full- or half-duplex operation. The DRSN provides feature keys that include the MILSTAR call box functionality allowing the nets to be controlled and operated from the telephone. There is also a backup capability to ensure SECN availability whenever the DRSN switches are taken down for maintenance or upgrade.

(13) National Airborne Operations Center (NAOC). The NAOC is one member of the Worldwide Airborne Command Post fleet of airborne command posts. Each airborne platform provides several secure-voice systems to support a variety of communications requirements. On-board user telephones are connected through external circuits that are protected using a variety of encryption devices. The RED side of the encryption devices collocated with the DRSN RED switch interface node is the demarcation point between the NAOC and the DRSN. Service is currently provided via STU-IIIR interfaces; STE/Secure wireless and MILSTAR/SECN.

(14) Joint Communications Support Element (JCSE). Deployable RED Switch. The JCSE provides communications support for JTF operations and smaller communications packages for worldwide crisis, contingency, and war-time operations. DRSN support is provided to the JCSE through the deployable RED switch. The deployable RED switch is a switching platform fully compatible with the DRSN, enabling calls to be passed between the DRSN and deployed RED switch networks. The deployable RED switch also has the capability to use VoSIP gateways to DRSN. DISA is responsible for VoSIP IP addressing scheme and numbering plan. The STEP/teleport uses gateway or long-local RED switches that provide stand-by DRSN-deployed access by installing operational circuits among multiple RED switches and STEP/teleport sites throughout the world. These DRSN gateway nodes are preconfigured with appropriate interface equipment to connect to JCSE-deployable RED switches or long-local DRSN equipment through encrypted channels. STEP/teleport sites are the approved method for tactical-to-strategic DRSN secure-voice connectivity.

(15) Non-DRSN RED Switches. Some non-DRSN RED switches have been granted limited access to the DRSN. Presently, all such switches access the DRSN through encrypted ISTs. Authority for approving such

terminations resides with the Joint Staff after all security and interoperability concerns are resolved. (See reference oo)

(16) Interfaces to Future and Evolving External Voice Systems. DISA, as the single systems manager and EA for the DRSN will ensure that DRSN is maintained and sustained as a viable secure C2 network and that appropriate interoperable interfaces and capabilities are incorporated into DRSN infrastructure to support evolving operational requirements and technical capabilities.

(17) DRSN STEP/Teleport Interfaces. STEP/Teleport provides access to DRSN for deployed users through use of Dual Terminal Adaptors (DTAs) and Multifunction Digital Adaptors (MDAs) at specified DRSN sites that support a specific STEP/Teleport ground entry point. The DTA/MDA interface is capable of support trunk or subscriber configurations. At least three DRSN DTA/MDA interfaces are pre-positioned at each DRSN switch that supports a STEP/Teleport site.

(18) Performance, Security, and Interoperability of External Interfaces. Due to potential differences in technical and performance characteristics of interfaced external systems and the DRSN itself, DRSN performance criteria cannot be assured beyond boundary of the DRSN. To the maximum extent practical, preservation of DRSN technical performance and security integrity will be the predominant factor in the design and implementation of any interface to the DRSN.

7. Network Management (NM). DISA establishes DRSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. DRSN is under the management control of the Director, DISA SSM, on behalf of USSTRATCOM, and is responsive to the Chairman of the Joint Chiefs of Staff, the combatant commands, the Military Departments, and Defense agencies and activities.

a. DISA must possess read-access and limited/controlled write-access capabilities to all DRSN nodal switch network-related database tables, RED bandwidth managers, and other network-level infrastructure data.

b. DISA must maintain a CM database of all switch configurations (CONUS and OCONUS) and provide access to agencies, activities, and Military Departments as authorized by OSD; the Director; DISA; and the Joint Staff.

c. DISA must have the ability to implement network-level database changes and/or network control commands to all DRSN nodal switch network-related database tables, RED bandwidth managers, and other network-level infrastructure data. To the maximum extent practical, the DISA DRSN service

manager must attempt to notify O&M activities before implementing DRSN nodal switch network-level database changes and/or network controls.

d. During emergencies, DISA has the authority to use direct write capabilities to implement switch database revisions required for operation and management of the DRSN.

e. DISA will take necessary action to establish capabilities and procedures necessary to sustain the DRSN in the event of a failure of the TNCs and to reconstitute a major DRSN nodal element in the event of a catastrophic failure.

8. Network Security

a. DRSN RED switches must be located in RED enclaves. DRSN RED switches at the NMCC, the NMCC Site R, and combatant command headquarters, as well as those locations that have subscriber terminals authorized to process TS/SCI, must be located in an sensitive compartmented information facility (SCIF). DRSN RED switches provide:

(1) In-the-clear calling within each RED enclave by means of PDSs.

(2) Cryptographically protected calling between RED enclaves supported by DRSN RED switches.

(3) DRSN RED switches interface to external cryptographic equipment for all other calling.

b. DRSN RED switches support up to TS/SCI communications and must not connect to CONFIDENTIAL or UNCLASSIFIED end instruments. However, the DRSN BLACK switches may connect NSA-approved end instruments to unclassified networks. DRSN BLACK switches are programmed to provide subscriber instruments with identification and security displays similar to those associated with the operation of STU-III/STE/SCIP cryptographic equipment.

c. NSA-approved encryption equipment provides COMSEC to the DRSN. The encryption equipment or PDSs secure all DRSN ISTs and protect links to remote enclaves to include remote locations and quarters. The TSEC/KG-84 family of equipment (including KIV-7) provides TRANSEC to ISTs to locations (including quarters) receiving DRSN service via Dual Phone Adapters (DPA), DTA/MDAs, and KG-84 telephone interfaces. The TSEC/KG-81 family of trunk equipment (including KIV-19s, TSEC/KG-81s, TSEC/KG-94s, and TSEC/KG-194s) bulk encrypts the digital streams between geographically separated DRSN RED switch nodes and affords similar functionality to local users served by digital phone multiplexers (DPM) or universal multiplexer (UMUX). KIV-

7HS's are sometimes used in lieu of the KG-81 family, but are not preferred because of re-key function limitations. Pairs of encryption equipment use unique traffic encryption keys to ensure both confidentiality and authenticity.

d. DRSN switch nodes may be configured to interface with NATO KY-71A (STU-II) and allied KY/SY-71A (STU-II) nets and/or circuits and with tactical voice networks secured by KY-57/58, KYV-5/KY-99, KY-65A/75A, or KY-68 cryptographic equipment. DRSN interfaces with NATO or allied networks and/or circuits must be approved by ASD (NII)/DOD CIO. DRSN cryptographic interface configurations must be approved by DISA.

e. DRSN instruments and service capability may be installed in senior officer quarters on a case-by-case basis. Such facilities constitute the establishment of a RED enclave/limited exclusion area within the quarters and must comply with physical and technical security criteria applicable to the use and storage of COMSEC equipment. Use of DRSN equipment in quarters must comply with DRSN operating and security procedures applicable to a RED enclave office environment.

(1) Any DRSN phone instrument installed in a quarters must be DISABLED at all times when not under the physical control of the authorized user.

(2) Where the RED signal path (digital or analog) between COMSEC and the DRSN RED equipment (i.e., DRSN instrument and other DRSN terminal equipment) is greater than 3 meters from the COMSEC device, the RED signal path will be routed in an approved PDS.

(3) Prior to installing DRSN service in quarters, the DISA DRSN service manager must be contacted for approval and confirmation of current applicable operating and security criteria.

9. Network Survivability Features.

a. Network Design. Survivability features, such as dual and split homing, diverse and avoidance routing, automatic and semi-automatic restoral and physical protection must be limited to high-priority functions and facilities with an established mission requirement for survivability, as determined by the combatant command concerned, with validation by the Joint Staff. The DISA DRSN service manager must ensure the survivability features are incorporated into the design and configuration of the DRSN.

b. Vulnerability Analysis. The DISA DRSN service manager, in coordination with DIA and NSA, must provide technical analysis of network survivability, to include a risk analysis, when proposing major changes in the

network topology. A report resulting from the analysis of the survivability and vulnerability of the DRSN must be forwarded to the Joint Staff for review.

10. DRSN Support. DRSN supports three categories of users:

a. Special C2 Users. A special class of users who has access to the DRSN for essential secure communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war secure telecommunications service for intelligence, alert, and strategic readiness. The user also requires secure communications among the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other members of the Joint Chiefs of Staff, Service Chiefs, and the combatant commands. Specifically, these special C2 users are identified through one or more Joint Staff, combatant command, Service, or DOD agency validation processes. The following are required capabilities of special C2 users:

(1) Joint Staff-approved FO, or F precedence origination.

(2) Combatant command -validated minimum-essential circuits.

(3) Combatant command or Service-approved I and P precedence origination.

b. C2 Users. Users who have a requirement to originate and/or receive secure C2 communications but do not meet the criteria for the class of Special C2 user. C2 users can exercise authority and direction as a Joint Staff/CC/S/A properly designated commander over assigned and attached forces in the accomplishment of the mission. These Joint Staff/CC/S/A designated users can originate IMMEDIATE and/or PRIORITY precedence calls to issue or receive guidance or orders that direct, control, or coordinate military forces, whether said guidance or order is issued, received or effected during peacetime or wartime. Any Joint Staff/CC/S/A user that can originate ONLY Routine calls does not need to meet the availability or redundancy requirements of the Special C2 users or the C2 users capable of originating PRIORITY precedence. All C2 users are capable of receiving FO/F/I/P calls. C2 users can be re-designated by the Joint Staff to originate FO/F calls or designated by the combatant command of the AOR to originate IMMEDIATE and PRIORITY calls if situation warrants.

c. Other Users. Users who have a requirement to use the DRSN for national security purposes but who do not meet the criteria for the classes of “special C2 users” or “C2 users.”

11. Assignment and Control of Precedence Levels.

a. Assignment of Precedence Levels. Access to a level of precedence must be determined only by mission requirements and must not be used as a means of improving a GOS above that provided to ROUTINE users. Any change in the assignment of precedence levels must be reviewed by the DISA DRSN service manager to ascertain the network impact and to size the DRSN infrastructure to accommodate the change. All precedence requirements must be validated by the appropriate combatant command, Service or Agency who also approves requirements for IMMEDIATE and PRECEDENCE service. The Joint Staff is the approval authority for F, FO, and FOO (applicable only to WWSVCS) calling capabilities. Combatant commands, Service Chiefs, and directors of Defense agencies must review and revalidate F and FO calling capabilities annually.

b. Control of Precedence. The combatant commands, Service Chiefs, and directors of Defense agencies must establish and maintain policy to control use of precedence access through operator-assisted calls.

c. Control of Precedence Access. Classmarking of the user instrument is employed to technically activate, manage, and control calling capabilities.

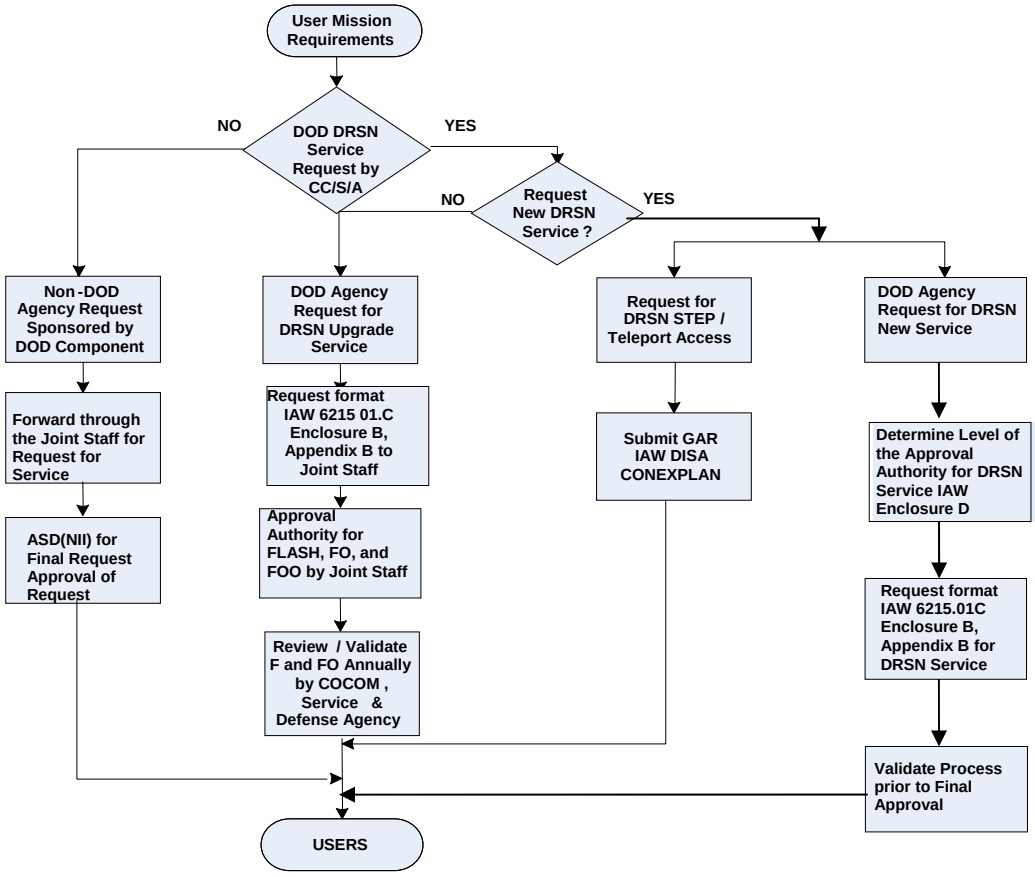
d. Enclosure D. identifies approval authority for DRSN service requests.

(INTENTIONALLY BLANK)

ENCLOSURE B – APPENDIX B
PROCEDURES FOR REQUESTING DRSN SERVICE

1. Purpose. This enclosure provides procedures for requesting DRSN service.

2. General. These procedures apply to the Joint Staff, combatant commands, Services, and Defense agencies. All DRSN service requests must be forwarded through the requestor's chain of command to the appropriate approval authority see Enclosure D. Non-DOD agency requests must be sponsored by a DOD component and forwarded through the Joint Staff to the ASD (NII)/DOD CIO for final approval.



a. DRSN requests for service must be submitted in the format provided in paragraph 4. The message format contained in paragraph 4 is for precedence requests for DRSN services to the Joint Staff however, the DMS message format is not required. Submission via e-mail is preferred. Requests must include a thorough discussion of operational requirements. Combatant commands, Services and Agencies may tailor the format for requests for which they are the

approval authority. Forecasts of future requirements (those appropriate for the DRSN program plan) should be provided to DISA and the Services.

b. Activities with validation or approval authority will ensure requirements comply with this instruction. Specifically:

(1) Mission requirements are the drivers behind all requests for DRSN access.

(2) Precedence requirements are justified in terms of explicit mission need, to include an explanation of negative mission impact if the request is not approved.

(3) Requirements affecting other combatant commands, Services, or Defense agencies have been coordinated with those affected.

c. Requests from non-DOD activities must be sponsored by a DOD component and must be forwarded through the Joint Staff to OSD for approval.

d. Requests for DRSN STEP/Teleport access will be requested IAW this instruction using the GAR in reference ll.

e. Combatant commands should request DISA provide engineering assistance and technical configuration management of multi-switch conferences. The combatant commander maintains operational control of their conferences and approves all members for inclusion in the conference. DISA will design and direct database changes necessary to implement the conference when requested. DISA will assist combatant commanders in technical aspects of configuration control. Combatant commander J-6 staff must send a request for DISA (ATTN: GS24) to assist in engineering and implementing a conference. The request shall be sent to the same address as request for DRSN service. The name of the conference, purpose of conference, number of users in each geographic area or agency, precedence of the conference and any unique operational requirements should be included. The request should include the classification of the conference. The combatant commander J-6 staff is responsible for tasking the O&M Command to provide DISA with the necessary data field information to engineer the conference to include the Subscriber Directory Number (SDN), security level, instrument type and precedence.

3. Approval Authority. The level of the approval authority for DRSN service requests is determined by the precedence requirement IAW Enclosure D. Requests must be validated at the level immediately below the approval level.

4. Request Format. Requests for TSRs will be submitted for DRSN IAW the above flow chart in the provided format below. The primary format to request new or upgraded service is via e-mail. DMS is acceptable, but not required.

Example format:

FROM: (Originating Activity)
TO:JOINT STAFF J6C C4 SYSTEMS SUPPORT DIVISION (UC)//*
(*or activity with requisite approval authority)
INFO: SA WASHINGTON DC//G6//
CNO WASHINGTON DC//N61//
SAF WASHINGTON DC//XCD//
CMC WASHINGTON DC//CCT//
DISA WASHINGTON DC/GS24/GS234//
Validating authority, others (as required)

(If approval authority is below the Joint Staff level, information addressees will consist of affected DOD Components and Joint Staff/J6C. DISA will be an information addressee on all requests.)

UNCLAS or appropriate classification
MSGIC/GENADMIN/as appropriate per message text format (MTF)//
REF/as appropriate per MTF//
AMPN/as appropriate per MTF//
NARR/as appropriate per MTF//
REPLY/as appropriate per MTF//
RMKS/SUBJECT: CJCSI 6215.01C DRSN REQUEST FOR (identify location or activity requesting service//

1. Description of required capability (concise narrative description).

A. Complete identification of the requirement; e.g., type of change, deletion, or addition including circuit or equipment quantities, configurations, and sequence numbers.

B. Unit, title, and geographic location of requesting agency.

C. Precedence requested.

D. Start date (if short notice, give justification and mission impact of delay).

E. Location of servicing switch.

F. Number of extensions required. Indicate if extensions are to be located in geographically separate locations that will require long-haul connectivity to servicing switch.

G. Location of the user requested DRSN service (geographic and physical location of the DRSN phone instrument).

H. Identification of the destination and expected frequency and duration of calls.

I. Operational mission security requirement. Collateral SECRET/TS, or TS/SCI.

2. Justification

A. Present capabilities for secure voice (e.g., STU-III STE/SCIP) and why they are inadequate.

B. Detailed description of the mission directly supported by the requirement or the mission change that generated the requirement and mission impact if disapproved.

C. Theater commander's approval and point of contact.

D. Identification of source of funds. If available, identification of expected yearly costs to include:

(1) Identification of implementation costs and source of funds.

(2) Identification of annual depot support costs and source of funds.

(3) Identification of annual O&M costs and source of funds.

(4) Identification of increase in Service's annual DWCF bill and source of funds.

(5) If desired by the requester, DISA can estimate cost prior to submission of request. Sources of funding must be identified as part of the validation process prior to final approval.

E. Identification of DISA point of contact or DISA area representative (office code and phone number) who provided coordination and network impact assessment, or reason DISA was not contacted.

F. Other considerations or remarks as appropriate.

3. Combatant command, Service, or agency point of contact (name, office symbol, DSN, and commercial phone numbers).//

(NOTE: Only 1A, B, D, E, F, G, I, 2B, C, and 3 are required for requests for deactivation or cancellation of DRSN service.)

ENCLOSURE C
POLICY FOR DISN REAL TIME SERVICES

1. Purpose. This enclosure provides general guidance, usage, and performance objectives for the RTS. In addition, Appendix A describes functional requirements and military-unique features for Assured Services of the RTS.

2. General. RTS will be operated and defended IAW CDRUSSTRATCOM's concept of operations. (See reference vv) The DISN provides End to End RTS via its IP router networks (NIPRnet, SIPRnet and the DISN Service Delivery Nodes), via its circuit switch networks (DSN and DRSN), via the DVS II VTC services, via the MILDEP access circuits, Local Area Network (LAN) and end instrument infrastructures on their facilities all via the RTS signaling systems. The Director, DISA, as the RTS SSM of the DISN network, will be responsive to the needs and requirements of the DOD components. All the policies/requirements for DSN apply to the DISN SBU RTS. All policies/requirements of DRSN apply to VoSIP/SIPRNET (single security level] and DISN Classified RTS. The policy for use of IP based RTS to include VoIP, Video over IP (to include VTC), and VoSIP over the DISN is as follows:

a. DOD components will ensure that their current and future IP based RTS implementations are compliant with RTS Generic System Requirements (GSR) and use the products listed on the APL. Deployment of IP based RTS requires that all equipment is listed on the APL or as approved via the ISP/T-ISP process. (See reference oo). As the scope of DOD information technology policy expands to include non-RTS, ASD (NII)/DOD CIO will develop and approve Unified Communications Requirements (UCR) based on the RTS GSR. Once available, DOD components will ensure their future IP based implementations are compliant with UCR and use products listed on the APL.

b. RTS Pilots are permitted as limited deployments (one (1) year)as long as it's directed by ASD (NII)/DOD CIO or an approved waiver is obtained from ASD(NII)/DOD CIO. (See reference oo). The Pilot shall not be the only RTS communication capability available for Special C2 and C2 users. Special C2 and C2 users must be provided assured services via DSN or DRSN connectivity until the IP based RTS equipment is listed on the APL.

c. IP based RTS cannot replace the DSN or DRSN until it can provide equal or better assured services that meet Joint Staff requirements.

d. Sensitive But Unclassified (SBU) Services Equipment and software that are leased, procured, or operated (systems or services) by a DOD component to provide SBU RTS, shall be Joint Staff interoperability certified and type IA accreditation. Based on achieving both interoperability and IA type

accreditation the equipment and software shall be placed on the APL or shall be approved via the ISP/T-ISP process of CJCSI 6212.01D. Prior to connection, the DOD component's DAA must accredit and validate the configuration and installation before the DSN SSM provides connection approval to DISN SBU RTS. (See reference oo)

e. Classified Services. Equipment and software that are leased, procured, or operated (whether systems or services) by a DOD component to provide classified RTS, shall be Joint Staff interoperability certified and type accredited by their classified system DAAs. Based on achieving both interoperability and IA type accreditation the equipment and software shall be placed on the APL (DRSN)or shall be approved via the ISP/T-ISP process of CJCSI 6212.01D. Prior to connection, the DOD component's DAA must accredit the configuration and installation before the DRSN SSM provides connection approval to DISN Classified RTS IAW reference oo.

f. All equipment and software that provide RTS shall comply with DOD memorandums and policies for IPv6.

g. Risk assessment and mitigation shall be managed by the local DAA accreditation of installed APL equipment and software that provide RTS.

h. The GIG IA Architectural requirements shall be met.

i. Wireless RTS. RTS wireless services to include cellular, LANs, strategic SATCOM tactical extensions, Land Mobile Radio and their associated end instruments shall meet the RTS GSR or be approved via the ISP/T-ISP process IAW reference x.

j. The DOD may grant non-DOD activities access to DOD networks that provide RTS when necessary for national security; when those activities and individuals have critical NS/EP needs or when access is in the best interest of the US Government. (See reference oo) Access may only be provided to non-DOD activities or agencies on a not-to-interfere basis. Requests for access by non-DOD or agencies shall be forwarded to the Joint Staff for validation and the ASD (NII)/DOD CIO for approval. (See reference hh) Non-DOD or non-C2 users (e.g., combined or coalition partners and US Government Departments and Agencies) interfaces to the DOD networks that provide RTS:

(1) Shall comply with interface criteria established by the RTS SSM, and approved by appropriate accrediting authorities.

(2) Network interfaces not conforming to RTS interface criteria shall be permitted only after RTS SSM technical review and approval, on a site-specific basis, by the Joint Staff. (See reference oo) In each of these interfaces, a

method for controlling the flow of traffic across the interface must be established and monitored by DISA.

3. Usage. The RTS policy is not applicable to all GIG Networks however; it is applicable to GIG End-to- End networks that provide RTS. These networks consist of: DISN networks, Tactical Networks and MILDEP networks. The DISN RTS networks are; DSN, DRSN, VoSIP, DVS, DISN Transport, DISN Service Delivery Nodes (SDN's) and Teleports. Tactical Networks are those that have ISP/TISPS which, require RTS services that interoperate with the DISN RTS networks. MILDEP networks are those which are regional or strategic facilities to include their LANs and End Instruments that inter-operate with the DISN RTS networks. DISN RTS networks also provide voice or video services, whether wired or wireless, tactical or strategic, Sensitive But Unclassified (SBU) or Classified.

4. Objective Technical Parameters and Special Function.

a. The DISN provides RTS via its router networks (NIPRNET, SIPRNET and the DISN Service Delivery Nodes) and via DSN, DVS, DRSN, DISN Video Services (DVS) infrastructure, the DISN Wide Area Network (WAN) to include the DISN Service Delivery Nodes (SDN) and access to those SDN, Teleport SIPRNET, and NIPRNET services. DSN and DRSN are worldwide private-line telephone sub-networks of the DISN that provide long-haul secure and non-secure telecommunications services to DOD authorized users. They are the integral components of the GIG that provide End-to-End services to critical users at the highest levels of government.

b. RTS consist of a subset of the following four categories of services: Signaling, Inelastic/Real Time, Preferred Elastic and Elastic.

(1) Signaling includes both Network Control and User Signaling for managing the network and setting up and taking down sessions over the network.

(2) Inelastic RTS are delay intolerant and provide GIG users with primarily live interactive telecommunications to include multimedia communications or rapid delivery of critical command and control information involving weapons delivery capabilities that clearly allow for:

(a) The equivalent of "Face to Face" interactions in which both factual and emotional content of the interaction can be conveyed.

(b) Operation of surveillance and weapons systems that require rapid message delivery.

(3) Preferred Elastic services include services such as instant messaging, user authentication imagery, video and audio streaming.

(4) Elastic services include services such as, e-mail, web browsing, and document transfers.

5. Applicability. This instruction identifies RTS policy and responsibilities to DOD components in peacetime, crisis situations, and wartime. This instruction is applicable to non-DOD governmental, foreign government and civilian organizational requests for DISN Assured RTS support (DARTS). Requests for waivers to this instruction will be forwarded through the DOD component chain of command to the Joint Staff, stating the reason compliance is not possible.

a. The equipment and software that provide RTS services including voice, video, interactive video conferencing, command and sensor data, short time and critical messaging across a network. All equipment and software leased, procured (whether systems or services), or operated by any DOD component or by authorized non-DOD users (e.g., Combined or Coalition partners).

b. End-to-End network equipment and software that may provide both strategic and tactical RTS include the WANs/MANs/LANs, SATCOM, enterprise and NM, intrusion detection systems, firewalls, multiplexers, routers, conferencing bridges and end instruments (e.g. PC to PC, phone-to-phone, video-to-video compression-decompression algorithm (CODEC) unit, fax-to-fax; STE (e.g. STE-to-STE, SCIP-to-SCIP).

c. All technologies and equipment that support RTS, to include; IP routers, IP hubs, circuit switch, Time Division Multiplexers, optical, wired, wireless, ATM, Voice and Video over IP, web applications, computers, encryption, CODECs and all directory services (e.g. email addressing, web addressing, phone numbers).

d. Signaling includes both network control messages for managing and controlling the network and user signaling messages to request for sessions and/or bandwidth reservation over the network. Inelastic services are sensitive to delay jitter and packet loss and provide users with live interactive voice and video services to include multimedia communications or rapid delivery of critical command and control information. RTS does not include preferred elastic and elastic services that are tolerant of delays as IM, collaboration, imagery, email, target list management, and web browsing.

e. The DOD component's planning, investment, development, operations, and management of their IT infrastructure that use or are a part of networks and include all programs that are required to prepare Information Support

Plans (ISP) and Tailored Information Support Plans [T-ISP] per CJCSI 6212.01D.

f. All authorized non-DOD or non-C2 users (e.g., combined or coalition partners and US Government Departments and Agencies) that use DISN RTS. For authorized non-DOD users, only the interfaces to the DOD networks and services are subject to this instruction.

ENCLOSURE C - APPENDIX A

PROCEDURES FOR REQUESTING DISN RTS REQUIREMENTS

1. Purpose. This appendix provides procedures for requesting RTS services and an overview of RTS requirements.

2. General. RTS requests must be defined, validated, coordinated, and approved through DISA SSM for all mission and traffic requirements for all DISN services. Requests must first be validated by the appropriate CC/S/A. (See reference oo). Forward all approved RTS requirements and priorities to DISA SSM for coordination or implementation. Provide the appropriate planning requirements to DISA for incorporation into their DISN program plans. Comply with references (f, pp, and tt) requirements for interoperability and supportability. All validated requests for a waiver (APL testing) and requests for an ICTO are to be forwarded to the Joint Staff (J-6I) for consideration. Requests for all other waivers to this instruction will be forwarded through the DOD component chain of command to the Joint Staff, stating the reason compliance is not possible.

3. Military Unique Features. The RTS achieves assured service through implementation of MUF (reference oo) to support military C2 functions. The MUFs and Objective Technical Parameters and Special Functions defined in both Enclosure A and B apply as well as the SBU DISN RTS and Classified DISN RTS respectively. The reliability, availability, survivability, and maintainability features of GIG Mission Area Initial Capabilities Document (MA-ICD) JROCOM 095-04 14 June 2004 is designed to support all functions necessary to meet the RTS requirements that is defined in Chapter IV including the ability to recover from critical failures. (See references uu and vv) The requirements MA-ICD, Key Performance Parameters apply to all DISN RTS. However, certain sections of the MA-ICD are directly applicable to RTS and are repeated herein as an overview.

a. Technology Change Management. Synchronization information technology is evolving at a rapid rate. Local Commanders or Program Managers implementing GIG-enabled systems should plan to take advantage of technology changes. This is, sometimes, easier said than done. The rate of change in information technology is two-to-three times faster than the multi-year acquisition cycle. This means that many information technology programs deliver products/systems that are often a generation behind what is available in the commercial sector, before they get fielded they are “legacy” systems.

b. Standards and Proprietary Technology. A large percentage of information technology solutions are commercial products that are available in the market place before the industry has settled on a “standard.” A current

example would be the evolving standards development for extensible mark-up language (XML). Also, some companies seek to maintain a competitive economic advantage through proprietary technologies. While these solutions may satisfy an operational requirement, they most always create interoperability problems. Program Managers need to consider commercial standards when implementing GIG solutions with a view toward understanding that standards are necessary but not sufficient to ensure interoperability among systems.

c. Configuration Management. Introducing new technology into operational environments requires rigorous configuration control. Commanders and decision makers at all levels of command must have complete confidence in the information technology they use to maintain situational awareness or commit forces. Often, backward compatibility to legacy systems will be required and should be considered as part of the new system design. Conversely, the infusion of new technology may involve process re-engineering. GIG-enabled systems should be flexible enough to accommodate such change.

d. In the final analysis, successful implementation of GIG depends in large part on how well technology change is managed to allow us to take advantage of current and future innovations in information technology.

e. Operational Suitability and Infrastructure Support

(1) Operational suitability is the degree to which GIG-enabled systems can be satisfactorily developed, fielded, deployed, operated, and sustained while meeting performance parameters and the users' needs. The following guidelines are provided to help in implementing the GIG:

(2) The reliability, availability, survivability, and maintainability features of GIG-enabled systems should be designed to support all functions necessary to meet the requirements documented in Chapter IV of the GIG MA ICD, including the ability to recover from critical failures.

f. Communications: Transport

(1) General. Transport is the movement of information and/or knowledge among users, producers, and intermediate entities. The capabilities detailed in the following paragraphs will work to alleviate transport shortfalls identified in Chapter III of the GIG MA ICD, by improving QoS through the implementation of DOD transport standards, and reducing duplication of transport functions. While these improvements may not totally offset the shortage of available bandwidth in face of expanding information transport

requirements, these enhancements should go far to improve the current situation.

(2) Switching/Routing/Transmission. To ensure the unimpeded exchange of information that is necessary to meet user requirements, systems providing switching, routing, and transmission control capabilities/mechanisms shall be fully interoperable and work seamlessly across the entire GIG, in accordance with the DISR (Threshold).

(3) Quality of Service (QoS). Emphasis on superior QoS commensurate with each user's requirements must be an overarching GIG operating principle. Required Q0S factors include:

(a) Prioritization. End users shall be able to assign priority to information targeted for transport (Threshold).

(b) Response Time. All transport capabilities shall be designed to meet or exceed customer stated expectations for response times (Threshold).

(c) Precedence. Data shall receive expedited handling during transport IAW the commander's policy and user assigned priority (Threshold).

(d) Reliability. Delivery of information shall be guaranteed in IAW assigned service level (Threshold).

(e) Latency. It shall be possible to deliver information in real and/or near real time (Threshold).

(4) Information Integrity. Systems shall maintain and guarantee during transport the integrity of all information elements exchanged throughout the GIG to enable user confidence; information integrity shall be 99.99 percent (Threshold, KPP) and 99.999 percent (Objective, KPP).

(5) Standards. To ensure system interoperability across the GIG and to support assured uninterrupted service, all transport capabilities shall be standards-based using DISR, unless waived IAW the waiver process described in DOD 5000.2-R (latest version) (Threshold). It is only through the rigid enforcement of and compliance with such standards that fully GIG-wide information exchange will be possible.

(6) Connectivity. Transport systems shall provide connectivity on demand to all fixed and deployed locations/users (Threshold). This on-demand, seamless connectivity is essential to satisfy the rapidly changing requirements of warfighters at all levels engaged in operations throughout the world. Unimpeded mobility, while maintaining uninterrupted connectivity both

laterally and vertically, is a basic requirement of the 21st century warfighter. This is essential given the combination of a shrinking force structure and ever-increasing missions locations where our military forces are required to operate. Transport systems shall have the ability to maintain network connectivity on-the-move to meet both Service and JTF requirements in all warfighting environments (afloat, sub-surface, airborne, in space, and on the ground) (Objective).

(7) Capacity. With minimal exceptions, GIG transport capacity shall be viewed as an open system that is available to transport information from all domains utilizing unicast, multicast, and/or broadcast techniques wherever necessary to provide information on demand to the warfighter/decision maker (Threshold). Transport systems shall have the reserve capacity to accommodate surge loading and support multiple military operations as described in Defense Planning Guidance (Objective).

(8) Technology Insertion. To effectively keep pace with advances in technology that have the potential to render existing systems obsolete shortly following acquisition, the GIG shall enable and support the seamless and efficient insertion and incorporation of emerging (future) technologies into the transport domain (Threshold). Such a technology insertion provision is essential to maintain the operational effectiveness of the GIG.

(9) Security. Systems shall provide link and transmission security based on the level of risk acceptable to the user, and the GIG security architecture shall support use of clear headers if and when necessary (Threshold).

(10) Robustness. Transport system reliability is a fundamental requirement for ensuring necessary information exchanges to support military operations. Single points of failure are a primary concern in any transport architecture. To avoid any single point of failure, the GIG shall use multiple connectivity paths (not susceptible to the same threats) and media (Threshold).

(11) Scalability. Modern military force deployment scenarios require varying force levels depending on the particular mission and associated operational requirements. Therefore, transport capability shall be scalable and adaptable to meet the dynamic needs of users (Threshold)

(12) Survivability. Transport systems shall be protected against all potential threats commensurate with the operating environment and the criticality of information being transported, and shall also ensure connectivity through total threat environment (i.e., conventional and nuclear) (Threshold).

(13) Availability/Reliability. To be effective, transport capabilities shall be available to provide reliable information exchange services to the warfighter/decision maker on demand and shall be responsive to the criticality of the information to be exchanged (Threshold).

(14) Tactical Deployability. Military tactical forces require maximum mobility and ease of deployment. This requires that their supporting systems also be easily transportable. Therefore, transport systems supporting tactical forces shall minimize lift requirements and be transportable using existing JTF/Service lift capabilities (Threshold).

(15) Transport Element Status. All transport elements (e.g. switches, routers, etc.) shall be capable of providing status changes to NM devices by means of an automated capability in near real time 99 percent (Threshold, KPP) and 99.9 percent (Objective, KPP) of the time.

(16) Secure Voice Interoperability. Strategic and tactical secure voice systems shall be interoperable, with a 99 percent (Threshold, KPP) and 99.9 percent (Objective, KPP) call throughput success rate. Throughput success/failure is defined as a call completion rate when both secure voice systems are operational and available.

(17) Secure Voice with Allied and Coalition Forces. Secure voice cryptography shall be provided to or developed with allied forces to enable interoperability (Threshold). Secure voice systems shall be interoperable with coalition forces (Objective). A secure voice system shall be able to be provided to coalition forces which is interoperable with the US version using coalition releasable technology (Threshold).

(18) Information Over Tactical Data Links. Systems transporting/exchanging information over tactical data links (TDLs) shall use one or more members of the J-Series Family of Tactical Data Links IAW DOD Joint Tactical Data Link Management Plan (JTDLMP) and DOD Joint Technical Architecture (JTA/DISR) (Threshold).

g. Network Operations. (NetOps)

(1) General: CDRUSSTRATCOM will coordinate and direct the operations and defense of GIG within DOD component-operated domains. Assign responsibilities and establish procedures for implementing and executing NetOps for the Department of Defense. NetOps is the DOD-wide construct used to operate and defend the GIG.

(2) Network Operations is the organizational and procedural structure used to monitor, manage, and control GIG by means of the GIG functions of

NM, Information Dissemination Management (IDM), and IA. To effectively support network-centric warfare (including collaborative planning) key parts of these functions must be integrated. Commanders (e.g., at the theater and enterprise level) must have situational awareness of network IT assets and information flow across echelons. Separate management of some NM, IDM, and IA functions is also necessary.

h. Network Management (NM)

(1) NM is the set of activities that establishes and maintains GIG network switching, transmission, information services, and computing resources available to fulfill users' telecommunications and connectivity needs and demands. NM services are fault, configuration, account, performance, and planning management. The capabilities detailed in the following paragraphs will alleviate shortfalls described in Chapter III of the GIG MA ICD by enabling and supporting distributed and partitioned network control, the implementation of standards, and enhanced asset visibility. These enhancements will result in greatly improved overall NM.

(2) GIG End-to-End Situational Awareness. Network managers, on behalf of commanders, must have real time knowledge of the network. This knowledge must encompass awareness of all aspects of the network, including all network assets, their physical location, and their logical relationship within the network. To accomplish GIG End-to-End situational awareness, systems shall have the NM capability of automatically generating and providing an integrated/correlated presentation of networks and all associated network assets (Threshold).

(3) Dynamic, Predictive Planning. Systems. Shall have the NM capability to perform dynamic, predictive planning by gathering, storing and using knowledge about GIG assets/resources, so as to optimize their utilization (Threshold). Knowing equipment types and quantities available to support an operation is imperative for GIG utilization planners. Initially, a database must be defined and populated with organizations and their known GIG assets/resources. Once defined and populated, the database should have capability to be modified, as required, to support changing mission requirements to include activation/deactivation. The NM system should include network design and engineering functions that account for all voice, video, and data networks that could comprise a proposed system, including commercial technology. These functions should include automated mapping of network topology; measurement and recording of traffic flow data; trend analysis; spectrum planning and management; propagation analysis; electromagnetic resolution; and electronic key management. A modeling and simulation capability should be provided to allow a planner to assess the impact of changes to a system or network, without interrupting operational

network. Systems shall have the NM capability to create/modify/distribute GIG network plans and orders IAW user requirements (Threshold).

(4) Distributed and Partitioned Network Control. Systems shall have the NM capability to transfer control rapidly of one or more objects or groups of varying size, and reestablish control when relinquished without hindering End-to-End visibility by the senior network manager, while maintaining continuous control (Threshold). Only one designated active manager for a network object should be permitted at any given time. However, oversight of managers of network objects may shift as forces/assets are apportioned, allocated, or assigned without requiring a change of the active manager.

(5) Remote Object and Network Control and Configuration. Network managers must be able to monitor, configure, and control all aspects of the network and observe changes in network status. Networks comprising the GIG are evolutionary in nature and generally are comprised of both legacy and emerging systems, some with their own management systems. Systems shall have a NM capability that leverages existing and evolving technologies and has the ability to perform remote network device configuration/reconfiguration of objects that have existing DOD JTA/DISR management capabilities (Threshold).

(6) Network Status. components of the GIG provide metrics to network managers to allow them to make decisions on managing the network. Systems shall have an automated NM capability to obtain the status of networks and associated assets in near real time 99 percent (Threshold, KPP) and 99.9 percent (Objective, KPP) of the time.

(7) Automated Fault Management. Systems shall have the NM capability to perform automated fault management of the network, to include problem detection, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving (Threshold). This capability allows network managers automatically to monitor and maintain situational awareness of the network's manageable devices, and to become aware of network problems as they occur based on the trouble tickets generated automatically by affected object or network. Alarms will be correlated to eliminate those that are duplicated or false, initiate test, and perform diagnostics to isolate faults to a replaceable component.

i. Information Assurance (IA)

(1) IA are measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and

response capabilities. Information systems will implement IA requirements identified IAW references v, x, hh, qq, rr.

(2) Ensure application of IA controls based on the system mission assurance category and confidentiality level IAW reference rr. IA controls provide an objective condition achieved through the application of specific safeguards or through the regulation of specific activities in specific areas including:

(a) Security Design and Configuration.

(b) Identification and Authentication.

(c) Enclave and computing Environment.

(d) Enclave Boundary Defense.

(e) Physical and Environment.

(f) Personnel

(g) Continuity.

(h) Vulnerability and Incident Management.

j. Interoperability.

(1) General: Interoperability is the ability of two or more systems, units, or forces to provide services to and accept services from other systems, units or forces to enable them to operate effectively together. This condition is achieved between communication-electronics systems or equipment when information or services can be exchanged directly and satisfactorily between users. The degree of interoperability that can be achieved will be determined primarily by the accomplishment of the In Effect Report (IER).

(2) Based on the GIG MA ICD requirements associated with availability and reliability, the following requirements shall be met by IP based RTS.

(a) Availability requirement for equipment/software serving Special C2 users as defined in Appendix A is Threshold 0.99999 with eight hours uninterrupted power supply.

(b) Availability requirement for equipment/software serving C2 users as defined in Appendix A is Threshold 0.99997 with two hours uninterrupted power supply.

(c) Availability requirement for equipment/software serving C2 users that are authorized to originate Routine ONLY and non C2 users as defined in Appendix A is Threshold 0.999 with no uninterrupted power supply.

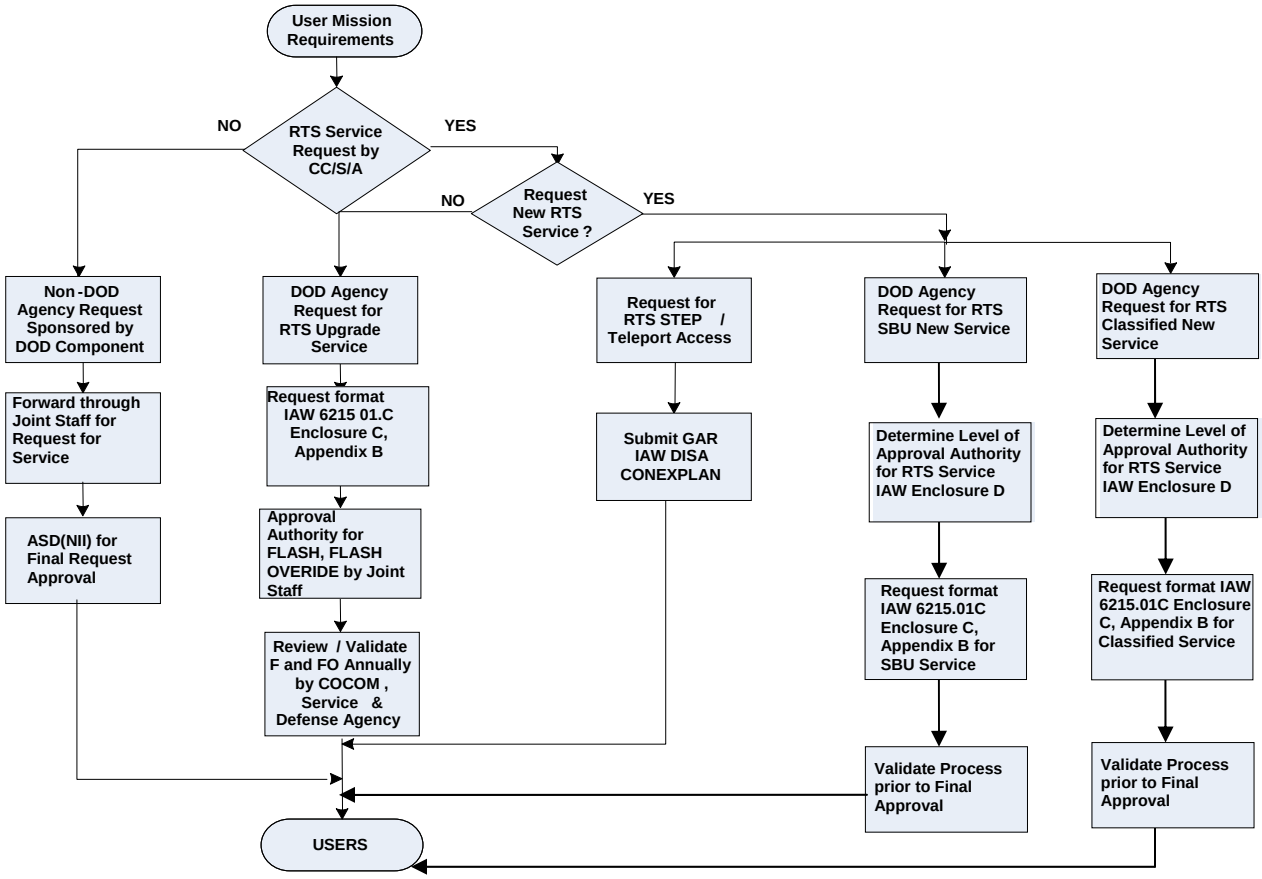
(INTENTIONALLY BLANK)

ENCLOSURE C - APPENDIX B

PROCEDURES FOR REQUESTING DISN IP BASED RTS SERVICE

1. Purpose. This enclosure provides procedures for requesting DISN RTS service.

2. Applicability. These procedures apply to the DOD components and the Joint Staff. All DISN SBU RTS requests and DISN Classified RTS requests must be forwarded through the requestor's chain of command to the appropriate combatant command\Service\Agency IAW DSN formal procedures identified herein. Non-DOD agency requests must be sponsored by a DOD component and forwarded through the Joint Staff to the ASD (NII)/DOD CIO for final approval.



a. RTS requests for service must be submitted in the format provided in paragraph 4. The message format contained in paragraph 4 is for precedence

requests for RTS services to the Joint Staff however, the DMS message format is not required. Submission via e-mail is preferred. Requests must include a thorough discussion of operational requirements. Combatant commands and Services may tailor the format for requests for which they are the approval authority. Forecasts of future requirements (those appropriate for the RTS program plan) should be provided to DISA and the Services.

b. Activities with validation or approval authority will ensure requirements comply with this instruction. Specifically:

(1) Mission requirements are the drivers behind all requests for RTS access.

(2) Precedence requirements are justified in terms of explicit mission need, to include an explanation of negative mission impact if the request is not approved.

(3) Requirements affecting other combatant commands, Services, or Defense agencies have been coordinated with those affected.

c. Requests from non-DOD activities must be sponsored by a DOD component and must be forwarded through the Joint Staff to OSD for approval.

d. Requests for RTS STEP/Teleport access will be requested IAW this instruction using the GAR. (See reference ll.)

e. Combatant commands should request DISA provide engineering assistance and technical configuration management of multi-switch conferences. The Combatant commander maintains operational control of their conferences and approves all members for inclusion in the conference. DISA will design and direct database changes necessary to implement the conference when requested. DISA will assist combatant commanders in technical aspects of configuration control. Combatant commander J-6 staff must send a request for DISA (ATTN: GS24) to assist in engineering and implementing a conference. The request shall be sent to the same address as request for RTS service. The name of the conference, purpose of conference, number of users in each geographic area or agency, precedence of the conference and any unique operational requirements should be included. The request should include the classification of the conference. The combatant commander J-6 staff is responsible for tasking their O&M Command to provide DISA with the necessary data field information to engineer the conference to include the IP address, Subscriber Directory Number (SDN), security level, instrument type and precedence.

3. Approval Authority. The level of the approval authority for RTS service requests is determined by the precedence requirement IAW Enclosure D. Requests must be validated at the level immediately below the approval level.

4. Request Format. Request for RTS service will be submitted via e-mail IAW the above flow chart and provided in the format below for all new or upgraded RTS service. DMS is acceptable, but not required.

Example format:

FROM: (Originating Activity)
TO: JOINT STAFF J6C C4 SYSTEMS SUPPORT DIVISION (UC)//*
(*or activity with requisite approval authority)
INFO: SA WASHINGTON DC//G6//
CNO WASHINGTON DC//N61//
SAF WASHINGTON DC//XCD//
CMC WASHINGTON DC//CCT//
DISA WASHINGTON DC/NS54/NS542/NS543//
Validating authority, others (as required)

(If approval authority is below the Joint Staff level, information addressees will consist of affected DOD components and Joint Staff/J-6C. DISA will be an information addressee on all requests.)

UNCLAS or appropriate classification
MSGIC/GENADMIN/as appropriate per message text format (MTF)//
REF/as appropriate per MTF//
AMPN/as appropriate per MTF//
NARR/as appropriate per MTF//
REPLY/as appropriate per MTF//
RMKS/SUBJECT: CJCSI 6215.01C RTS REQUEST FOR (identify location or activity requesting service//

1. Description of required capability and equipment/hardware that is compliant and listed on the APL (concise narrative description for VoIP/VoSIP/Video over IP).

a. Complete identification of the requirement; e.g., type of change, deletion, or addition including circuit or equipment quantities, configurations, and sequence numbers.

b. Unit, title, and geographic location of requesting agency.

b. Precedence requested.

d. Start date (if short notice, give justification and mission impact of delay).

e. Location of servicing switch.

f. Number of extensions required. Indicate if extensions are to be located in geographically separate locations that will require long-haul connectivity to servicing switch.

g. Location of the user requested RTS service (geographic and physical location of the RTS instrument).

h. Identification of the destination and expected frequency and duration of calls.

i. Operational mission security requirement. SBU, Collateral SECRET/TS, or TS/SCI.

2. Justification

a. Present capabilities for secure voice (e.g., STU-III STE/SCIP) and why they are inadequate.

b. Detailed description of the mission directly supported by the requirement or the mission change that generated the requirement and mission impact if disapproved.

c. CC/S/A's validation authority and approval point of contact.

d. Identification of source of funds. If available, identification of expected yearly costs to include:

(1) Identification of implementation costs and source of funds.

(2) Identification of annual depot support costs and source of funds.

(3) Identification of annual O&M costs and source of funds.

(4) Identification of increase in Service's annual DWCF bill and source of funds.

(5) If desired by the requester, DISA can estimate cost prior to submission of request. Sources of funding must be identified as part of the validation process prior to final approval.

e. Identification of DISA point of contact or DISA area representative (office code and phone number) who provided coordination and network impact assessment, or reason DISA was not contacted.

f. Other considerations or remarks as appropriate.

3. Combatant command, Service, or agency point of contact (name, office symbol, DSN, and commercial phone numbers).//

(NOTE: Only 1A, B, D, E, F, G, I, 2B, C, and 3 are required for requests for deactivation or cancellation of RTS service.)

(INTENTIONALLY BLANK)

ENCLOSURE D

PRECEDENCE APPROVAL AUTHORITIES

Purpose: This enclosure identifies the approval authorities for DSN, DRSN and RTS precedence.

Approval Authorities:

REQUEST ORIGINATOR

TYPE OF REQUEST	**MIL SVS**	**U/S CMD**	**DOD AGENCY**	**NMCS J-STAFF**	**NON-DOD AGENCY or ORGANIZATION**
FLASH OVERRIDE OVERRIDE	JS(J6)	JS(J6)	JS(J6)	JS(J6)	ASD (NII)/DOD CIO
FLASH OVERRIDE	JS(J6)	JS(J6)	JS(J6)	JS(J6)	ASD (NII)/DOD CIO
FLASH	JS(J6)	JS(J6)	JS(J6)	JS(J6)	ASD (NII)/DOD CIO
IMMEDIATE	Serv.Ch.#	CC	Agency#	JS(J6)	ASD (NII)/DOD CIO
PRIORITY	Serv.Ch.#	CC	Agency#	JS(J6)	ASD (NII)/DOD CIO
ROUTINE	Local	Local	Local	Local	Local

Note:
1. Request approval may be granted only with identification of funding source and coordination with DISA.
2. DODI 8100.3, Para 5.2.12 (DOD components) "Approve users with Immediate, Priority and Routine precedence origination capability."

LEGEND

JS - Joint Staff J-6C
CC - Combatant Command
Serv.Ch. - Service Chief
Agency - Director of Defense Agency

ASD (NII) - Office of the Assistant Secretary of Defense for Networks and Information.
Local - Local installation commander (see Enclosure A, 3. for more specific guidance)
- OCONUS CC approves requests in AOR

ENCLOSURE E
RESPONSIBILITIES

1. Purpose. This enclosure lists the responsibilities for the operation of DOD voice networks.

2. Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer.

a. DSN

(1) Approves the biennial DSN program plan after recommendation and consultation with the Chairman of the Joint Chiefs of Staff.

(2) Approves access by non-DOD agencies, organizations, activities, or entities upon consultation with the Joint Staff.

(3) Enforce policy and provide oversight, with the DOD components, for telecommunications switches, signaling appliances and services operating on the DSN.

(4) Develop a process, with the Chairman of the Joint Chiefs of Staff, the DISA, and other DOD components, to conduct annual risk assessments (technical, IA, and mission) and develop associated mitigation plans for non-certified telecommunications voice appliances and switches connected or planned for connection to the DSN.

(5) Approve technical requirements documentation for certification of telecommunication switches to ensure consistent and uniform application of certification policy for the GSCR and GSR.

b. DRSN

(1) Approves the biennial DRSN program plan after recommendation and consultation with the Chairman of the Joint Chiefs of Staff and after staffing by the DRMC (DISN Rate Management Council).

(2) Approves access by non-DOD agencies, organizations, activities, or entities upon consultation with the Joint Staff.

3. Chairman of the Joint Chiefs of Staff.

a. DSN

(1) Reviews the operational effectiveness of the DSN. The Joint Staff will report to ASD (NII)/DOD CIO those matters having a major effect on the network.

(2) Validates the biennial DSN program plan and submits to OSD for approval.

(3) Reviews and approves or disapproves all requests for FLASH and FLASH OVERRIDE DSN service after validation by the combatant command, Service Chief, or director of Defense agency.

(4) Ensures users granted FLASH and FLASH OVERRIDE access have a continuing mission need for those levels of service and will initiate action to discontinue such access when the mission need changes. These capabilities will be revalidated on a biennial basis.

(5) Approves or disapproves special telecommunications survivability requirements for DSN.

(6) Review and approve DISA-recommended, DOD component-coordinated performance objectives and interface criteria for the DSN to satisfy system requirements.

(7) Ensures DSN meets applicable requirements of the NCS.

(8) Participates in and acts as final arbiter of the DSN CCB.

(9) Reviews and approves or disapproves proposed schemes for automatic interconnection onto the DSN from public switched networks after technical evaluation by DISA.

(10) Reviews and approves/disapproves all combatant command validated requests from OCONUS local commanders for Class B service.

(11) Reviews and approves or disapproves DISA-recommended, Service-coordinated performance objectives and interface criteria.

(12) Resolves requests for service identified by DISA as having the potential to harm the DSN network.

(13) Process JIC ICTO requests for all uncertified telecommunications switches connected or being considered for connection to the DSN. Forward

recommendation for approval of JIC ICTO requests to the ASD (NII)/DOD CIO for decision, via the GIG Waiver Panel.

(14) Define DISN processes and procedures for telecommunications switch accreditation and connection to the DSN.

(15) Direct implementation of traffic controls (e.g., selected blocking, directionalization) and usage or availability control (e.g., minimize) to ensure assured service for critical users during times of surge due to war or crisis.

b. DRSN

(1) Reviews the operational effectiveness of the DRSN. The Joint Staff will report to OSD those matters having a major effect on the network.

(2) Validates the biennial DRSN program plan and submits to OSD for approval.

(3) Reviews and approves or disapproves all requests for FLASH, FLASH OVERRIDE and FLASH OVERRIDE OVERRIDE DRSN service after validation by the combatant command, Service Chief, or director of Defense agency.

(4) Ensures users granted FLASH and FLASH OVERRIDE access have a continuing mission need for those levels of service and will initiate action to discontinue such access when the mission need changes. These capabilities will be revalidated on a biennial basis.

(5) Reviews and approves all requests for network access to the DRSN and connections between DRSN and non-DRSN secure voice equipment.

(6) Participates in and acts as final arbiter of the DRSN CCB.

(7) Reviews and approves or disapproves DISA recommendations for modifications to the DRSN topology.

(8) Reviews and approves or disapproves DISA-recommended, Service-coordinated performance objectives and interface criteria.

(9) Resolves requests for service identified by DISA as having the potential to harm the DRSN network.

4. Director, Defense Information Systems Agency

a. DSN

(1) Serves as the SSM, on behalf of USSTRATCOM, for the DSN to provide management control of DSN.

(a) On behalf of USSTRATCOM provides management control and technical guidance for the DSN.

(b) Provide an annual assessment to the Chairman of the Joint Chiefs of Staff and the DSN CCB on the impact of emerging voice processing and transport technologies for global End-to-End voice performance and C2 services.

(c) Initiate and provide technical analysis of network survivability, including risk analysis, when proposing major changes in the DSN network technology or architecture. The Director, DISA shall forward the results of the analysis to the Chairman of the Joint Chiefs of Staff for review.

(2) Chairs and manages the DSN CCB. Implements approved and funded DSN CCB actions. The DSN CCB will collect and maintain configuration management information, to include (see reference hh):

(a) Network connectivity (switches signaling appliances, bandwidth and trunking), performance specification, and excess capacity data.

(b) Network routing, dialing, and numbering scheme.

(c) Switch and signaling appliance databases.

(d) Interface and control criteria.

(e) FLASH and FLASH OVERRIDE users' line assignment and location.

(f) Interoperability certification data on all DSN switching software and hardware.

(3) Produces and updates, on a biennial basis, the following DSN documents to be submitted through the Joint Staff for validation and to OSD for approval.

(a) DSN program plan (to include the worldwide DSN topology).

(b) Certification test plan.

(c) Network configuration management plan.

(d) DSN security guide.

(e) DSN classification guide.

(f) DSN system interface criteria.

(g) GSCR, JIEO 8249.

(h) Worldwide numbering and dialing plan.

(4) Provides systems engineering program management of DSN in response to DSN program plan validated, approved, and funded requirements.

(5) Ensures End-to-End interoperability by providing all DOD dialing and numbering plans for telephony services for the Department of Defense.

(6) Manages the effectiveness of the DSN on a 24-hour-per-day, 7-days-per-week basis and evaluates O&M practices and procedures to ensure C2 requirements are being met.

(7) Reports the status and operational effectiveness of DSN to the Joint Staff quarterly. This report may be required more frequently if issues exist that may have a major effect on the network.

(8) Publishes implementing documents for approved DSN objectives in coordination with DOD components.

(9) Reviews, processes, and implements approved requests for DSN telecommunications service. If any request for service has the potential to harm the network, DISA will forward the request to the Joint Staff for resolution regardless of approval level shown in Enclosure D.

(10) Uses exercises to verify the readiness of DSN and its ability to support user missions over the full range of stress scenarios.

(11) Issues an annual DSN Policy Letter that describes the multifunction switch operation and maintenance (MFS O&M) reimbursement policy and the allowable percentage of reimbursement, beginning in FY07. The MFS site is responsible for providing sufficient detail to support the costs and or changes (e.g., salary, job description, prior approvals, parts list, repair invoices, statement of work, contract, task orders etc) in their annual submissions for reimbursement as described in the DSN policy letter in order to be reimbursed. Funds expended for items other than those described below, is at the component's risk.

(a). DISA will reimburse 100 percent of a civilian salary (Max GS-11, step 10) if the site elects to dedicate a single position to support of the MFS.

(b). DISA will reimburse 100percent of travel for one government person to attend DISA DSN related functions. Neither training nor military technical schools are included.

(c). DISA may reimburse MFS sites for equipment training to meet DISA requirements if the site coordinates the training with the DSN SSM prior to scheduling the training.

(d). DISA will reimburse 30 percent of the repair, parts, and supply costs of MFS sites. Subscriber items are excluded.

(e). DISA will reimburse 30 percent of the total DSN switch O&M contract costs for MFS sites.

(f). DISA will reimburse 30 percent of the utilities, custodial services, fuel for emergency generators and maintenance of US Government owned heating, air conditioners and generators.

(12) Coordinates and reviews combatant command, Service, and agency policies and procedures on DSN use when requested.

(13) Processes and implements approved DSN service agreements with foreign governments.

(14) Provides technical evaluation for proposed schemes for automatic interconnection onto the DSN from public switched networks and forwards to Joint Staff for approval/disapproval.

(15) Implements applicable NCS requirements and standards in the DSN.

(16) Implements NM procedures as specified in Enclosure A, paragraph 8.

(17) Produces, updates, and distributes the DSN directory annually.

(18) Recommends consolidation and modification of the DSN to improve network effectiveness or reduce costs.

(19) Conduct along with DOD components an annual inventory, assess technical risks of DSN switches, recommend possible mitigations and submit to the JS and ASD (NII)/DOD CIO.

(20) Operates a DSN testing facility and maintains documentation pertaining to connection approval and interface standards.

(21) Ensures only those switches and software loads that have been certified as interoperable by JITC and IA Certified and Accredited are introduced into the DSN. (Reference v)

(22) Disseminates specific instructions for operation of switching centers to the Services.

(23) Maintains a database of all contractor DSN access requests, approvals, and terminations.

(24) Approves or disapproves metropolitan calling areas as proposed by the combatant commands/Services. Maintains a list of approved metropolitan calling areas and notifies combatant commands/Services when biennial revalidation is required.

(25) Implement controls necessary to limit DSN network usage of Special C2, C2 and non-C2 services to those users authorized in this instruction.

(26) Maintains a database of all combatant command approvals for OCONUS Class B service. Notifies combatant commands of biennial revalidation requirement.

(27) Provides an annual assessment of the impact of emerging voice processing/transport technologies on global End-to-End voice performance and C2 services to the Joint Staff and the DSN CCB.

(28) Develops and maintains intra and interswitch dialing plans in the DSN GSCR document and reference y, to ensure standardization across the network.

b. DRSN

(1) Acts as the SSM, on behalf of USSTRATCOM, of the DRSN by providing management control of DRSN.

(2) Chairs and manages the DRSN CCB. Implements approved and funded DRSN CCB actions. The DRSN CCB will review configuration management information as collected and maintained by the DRSN Service Manager, to include (see reference ee):

(a) Network connectivity (switches and trunking), performance specification, and excess capacity.

(b) Network routing, dialing, and numbering scheme.

(c) Switch databases.

(d) Timing and synchronization scheme.

(e) Interface and control criteria.

(f) FLASH, FLASH OVERRIDE and FLASH OVERRIDE OVERRIDE users' line assignment and location.

(g) Standardized SAL list to be implemented at all DRSN nodes.

(3) Produces and updates the following DRSN documents.

(a) DRSN program plan (to include the worldwide DRSN topology) to be produced biannually and submitted through the Joint Staff for validation and to OSD for approval.

(b) Network configuration management plan.

(c) DRSN system description.

(d) DRSN security guide.

(e) DRSN classification guide.

(f) Worldwide numbering and dialing plan.

(4) Provides systems engineering program management of DRSN in response to DRSN program plan validated, approved, and funded requirements.

(5) Manages the effectiveness of the DRSN on a 24-hour-per-day, 7-days-per-week basis and evaluates O&M practices and procedures to ensure C2 requirements are being met.

(6) Takes immediate action to isolate, restore, or provide additional circuits in the event of outages, network compromise, or critical world situation when necessary.

(7) Reports the status and operational effectiveness of DRSN to the Joint Staff quarterly. This report may be required more frequently if issues exist which may have a major effect on the network.

(8) Publishes implementing documents for approved DRSN objectives in coordination with DOD components.

(9) Reviews, processes, and implements approved requests for DRSN service. If any request for service has a potential to harm the network, DISA will forward the request to the Joint Staff for resolution regardless of approval level shown in Enclosure D.

(10) Uses exercises to verify the readiness of DRSN and its ability to support user missions over the full range of stress scenarios.

(11) Produces, updates, and distributes the DRSN directory semi-annually located on the DRSN secure webpage.

(12) Operates a DRSN testing facility and maintains documentation pertaining to connection approval and interface standards.

(13) Budgets and centrally managed funds for DRSN via the DSS.

(14) On behalf of USSTRATCOM produces and updates the DRSN concept of operations and provides management control for all DRSN switching centers.

(15) Recommends and, upon approval of the Joint Staff, implements consolidations and modifications to the DRSN topology to improve network effectiveness or reduce costs.

(16) Provides DRSN logistics information to the EA for logistics support.

(17) Accredits all DOD DRSN RED switches that handle collateral information.

c. RTS

(1) Designate an RTS SSM, on behalf of USSTRATCOM, to be responsible for architecture, system engineering, program management, operational direction, and management control of the End-to-End performance of DOD networks that provide assured RTS.

(2) Serve, respectively, as the RTS SBU and classified RTS technology migration coordinator to ensure End-to-End global assured services. The

combatant commands, the Military Services, the Defense Agencies, bases, camps, posts, and stations shall coordinate RTS initiatives with the RTS SSM.

(3) Provide a risk assessment for emerging technologies associated with equipment and software that provide RTS which impact on global, End-to-End assured services to the Chairman of the Joint Chiefs of Staff and the RTS CCB.

(4) Ensure End-to-End interoperability, by providing all DOD dialing and numbering plans for RTS for the Department of Defense.

(5) Provide a RTS Master Plan biannually that consolidates the global migration plan, schedules and funding required across the DOD to transition the DSN and DRSN from circuit switched technology to IP based RTS. The RTS Master Plan shall be published in time to support C/S/A POM submissions.

(6) Provide RTS GSRs that define the standards and specification for use in placing IP based RTS systems on the APL.

(7) Provide End-to-End Enterprise Management and RTS NM for RTS.

(8) Serve as the Secretariat to the RTS CCB and working group.

(9) Migration of the DSN GSCR to a DISN SBU RTS GSR document.

(10) Migration of the DSN Program Plan to a DISN RTS Master Plan.

(11) Migration of the DRSN/VoSIP specifications and standards to a DISN Classified RTS GSR document.

(12) Migration of the DRSN Program Plan to a DISN RTS Master Plan.

5. The Combatant Commands.

a. DSN

(1) Define, validate, coordinate, and approve requirements for DSN service within their purview according to Enclosure D.

(2) Forward approved DSN requirements, priorities, and precedence service to DISA and the supporting Service for implementation. The combatant commands will provide planning requirements for incorporation into the DSN program plan.

(3) Provide policy guidance and procedures in conformance with this policy and in coordination with the Services and DISA for use of DSN within their AORs.

(4) Provide acquisition, operation, maintenance, and logistic requirements for DSN CPE within facilities for which the combatant command is operationally responsible.

(5) Engineer the tactical voice architecture in support of combat operations within the combatant command area of operations. Coordinate with DISA before approval to determine if a DSN service request would degrade network performance.

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

(7) Support DISA in contingencies, crises, and exercises involving operational elements of the DSN as required. (See references mm and nn.)

(8) Review and validate operational requirements for DSN to meet requirements of OPLANs, CONPLANs, and CONEXPLANs.

(9) Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability after DISA technical evaluation to determine potential network performance degradation. Revalidate these requirements biennially.

(10) Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval in accordance with Enclosure D.

(11) Participate as voting members of the DSN CCB.

(12) Provide copies of all contractor DSN access requests, approvals, and terminations to DISA.

(13) Forward proposals for metropolitan calling areas to DISA for approval/disapproval. Revalidate OCONUS metropolitan calling areas biennially.

(14) Approve or disapprove OCONUS local commander requests for Class B service. Notify DISA DSN PMO of approvals.

(15) Develop and implement policies and procedures to limit DSN use to that authorized in this instruction.

(16) Coordinate all emerging technology base, post, camp, and station voice transport and processing initiatives with the DSN PM.

(17) Implement policies and procedures to limit DSN network usage of Special C2, C2 and non-C2 services to those users authorized in this instruction.

(18) Register all unclassified voice switches and update the DISA System/Network Approval Process (SNAP) (https://nap.DOD.mil) database tool with all switches leased, owned connected to, or scheduled to be connected to the Defense Switched network (DSN) or the Public Switched Telephone Network (PSTN). This includes all fixed, Tactical and Afloat switches that are able to make or receive DSN or PSTN calls and is technology independent (TDM, VoIP, VoATM, ect). (References oo and hh)

b. DRSN

(1) Define, validate, coordinate, and approve requirements for DRSN service within their purview according to Enclosure D.

(2) Forward approved DRSN requirements, priorities, and precedence service to DISA and the support Service for implementation. The combatant commands will provide planning requirements for incorporation into the DRSN program plan.

(3) Provide acquisition, operation, maintenance, and logistic requirements for CPE, including secure-voice instruments within facilities for which the combatant command is operationally responsible.

(4) Review and validate operational requirements for DRSN switches to meet requirements of OPLANs, CONPLANs, and CONEXPLANs.

(5) Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability after DISA technical evaluation to determine potential network performance degradation. Revalidate these requirements biennially.

(6) Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval in accordance with Enclosure D.

(7) Combatant command J-3 and J-6 staffs will review and revalidate conference requirements annually.

(8) Participate as voting members of the DRSN CCB.

c. RTS

(1) Implement policies and procedures to migrate the DSN GSCR to a DISN SBU RTS GSR document.

(2) Review and validate operational requirements to the DSN Program Plan for consolidation to a DISN RTS Master Plan.

(3) Implement policies and procedures to migrate to the DRSN/VoSIP specifications and standards to a DISN Classified RTS GSR document.

(4) Provide input to the migration of the DRSN Program Plan to a DISN RTS Master Plan.

(5) Provide acquisition, operation, maintenance, and logistic requirements for CPE, including secure-voice instruments within facilities for which the combatant command is operationally responsible.

(6) Forward approved RTS requirements, priorities, and precedence service to DISA and support Service for implementation. The combatant commands will provide planning requirements for incorporation into the RTS program plan.

6. Service Chiefs and Directors of Defense Agencies.

a. DSN

(1) Define, validate, coordinate, and approve requirements for DSN services IAW Enclosure D.

(2) Participate in the DSN CCB as a voting member.

(3) Forward approved DSN requirements and priorities to DISA for coordination or implementation and provide planning requirements for incorporation into the DSN program plan.

(4) Program, budget, acquire, operate, maintain, and fund for assigned portions of the DSN and for telecommunications services provided by DSN.

(5) Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability after DISA technical evaluation to determine potential network performance degradation. Revalidate these requirements biennially.

(6) Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval IAW Enclosure D.

(7) Provide acquisition, operation, maintenance, logistic, and funding support for CPE and terminal equipment.

(8) Provide training and periodic technical evaluations to ensure that facilities, equipment, and personnel meet DSN performance, objectives and interface requirements.

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

(10) Support DISA in exercises involving operational elements of the DSN.

(11) Comply with references (e and pp) requirements for interoperability and supportability. Ensure telecommunication switches connected to, or planned for connection to the DSN are tested for joint interoperability certification by the DISA JITC.

(12) Comply with references (rr, ss, v and w) requirements for IA certification and accreditation for all telecommunications equipment.

(13) Use only equipment listed on the DSN telecommunications switch APL, published by DSN SSM, for connection to the DSN. An unapproved switch may not be leased or procured unless and until a waiver is approved.

(14) Maintain equipment hardware/software within three versions of the approved hardware/software on the APL.

(15) Review and validate operational requirements for DSN switches under their operational control.

(16) Operate respective switching centers per directions disseminated by DISA.

(17) Provide copies of all contractor DSN access requests, approvals, and terminations to DISA.

(18) Forward proposals for metropolitan calling areas to DISA for approval/disapproval. Revalidate CONUS metropolitan calling areas biennially.

(19) Implement policies and procedures to limit DSN network usage of Special C2, C2 and non-C2 services to those users authorized in this instruction.

(20) Coordinate all emerging technology post, camp, or station voice transport and processing initiatives with the DSN PM.

(21) Maintain DISA's intra- and interswitch dialing plans for end users and implement DSN access codes as defined in the DSN GSCR document, reference y, to ensure standardization across the network.

b. DRSN

(1) Define, validate, coordinate, and approve requirements for DRSN services IAW Enclosure D.

(2) Participate in the DRSN CCB as a voting member.

(3) Forward approved DRSN requirements and priorities to DISA for coordination or implementation and provide planning requirements for incorporation into the DRSN program plan.

(4) Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability after DISA technical evaluation to determine potential network performance degradation. Revalidate these requirements biennially.

(5) Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval IAW D.

(6) Provide acquisition, operation, maintenance, logistic, and funding support for CPE and terminal equipment, including secure-voice instruments.

(7) Review and validate operational requirements for DRSN switches under their operational control.

c. RTS

(1) Implement policies and procedures to migrate the DSN GSCR to a DISN SBU RTS GSR document.

(2) Review and validate operational requirements to the DSN Program Plan for consolidation to a DISN RTS Master Plan.

(3) Implement policies and procedures to migrate to the DRSN/VoSIP specifications and standards to a DISN Classified RTS GSR document.

(4) Provide input to the migration of the DRSN Program Plan to a DISN RTS Master Plan.

(5) Provide acquisition, operation, maintenance, and logistic requirements for CPE, including secure-voice instruments within facilities for which the combatant command is operationally responsible.

(6) Forward approved RTS requirements, priorities, and precedence service to DISA and the support Service for implementation. The combatant commands will provide planning requirements for incorporation into the RTS program plan.

7. EA, DRSN (US Air Force)

a. Provides DRSN logistics support, to include contract management, engineering, training, and vendor services.

b. Coordinates specific DRSN logistics requirements with the DISA, combatant commands, Services, and agencies.

8. Director, DIA. In addition to responsibilities in paragraph 6:

a. Provides guidance for DRSN security issues.

b. Accredits all DOD Top Secret DRSN facilities and switches that handle SCI.

9. Director, NSA. In addition to responsibilities in paragraph 6:

a. Serves as security and INFOSEC adviser for the DSN, DRSN and RTS networks.

b. Recommends countermeasures based on DIA threat analysis in conjunction with DSN, DRSN and RTS security designs.

c. Advises DISA on security technical parameters of DRSN switches and STU-IIISTE/SCIP interfaces.

ENCLOSURE F
REFERENCES

a. USDRE memorandum, 9 September 1982, "Defense Switched Network"

b. OSD (C3I) memorandum, 11 December 1992, "Defense-Wide Secure Voice Program"

c. J-6A 01665-92, 17 November 1992, "Operational Requirement Document for Secure Voice Requirements"

d. J-6A 01137-93, 27 September 1993, "Defense red Switch Network Defense-Wide Resources"

e. DODD 4630.05, 5 May 2004, "Interoperability and supportability of Information Technology (IT) and National Security Systems (NSS)

f. CJCSI 6212.01 Series, "Interoperability and Supportability of National Security Systems and Information Technology Systems"

g. J-6A 00062-93, 9 March 1993, "Defense Switched Network Operational Improvements"

h. CJCSI 3222.01 Series, "CJCS Prioritization of C3 Nodes and Systems for High Altitude Electromagnetic Pulse Protection"

i. NCS Directive 3-10, 10 February 2001, "Telecommunications Operations Government Emergency Telecommunications Service (GETS)"

j. NCS Directive 3-1, 10 August 2000, "Telecommunications Service Priority (TSP) System for National Security and Emergency Preparedness (NS/EP)"

k. DASD (C3) memorandum, 26 October 1993, "Department of Defense (DOD) Policy for Video teleconferencing (VTC) Management, Acquisition, and Standards"

l. DASD (C3) memorandum, 31 October 1994, "Video Teleconferencing (VTC) Standards Guidance"

m. DODD 5105.19, 25 July 2006, "Defense Information Systems Agency (DISA)"

n. CJCSI 6740.01 Series, "Military Telecommunications Agreements and Arrangements between the United States and Regional Defense Organization or Friendly Foreign Nations"

o. CJCSM 6231.07 Series, "Manual for Employment of Joint Tactical Communications Joint Network Management and Control"

p. Executive Order 12472, 3 April 1984, "Assignment of National Security and Emergency Preparedness Telecommunications Functions"

q. Executive Order 12656, 18 November 1988, "Assignment of Emergency Preparedness Responsibilities"

r. Title 47, CFR, Part 64, Appendix A, "Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP)"

s. NSTISSP 101, 14 September 1999, "National Policy on Securing Voice Communications"

t. DODD 2040.2, 17 January 1984, "International Transfers of Technology, Goods, Services, and Munitions"

u. United States Code, Title 10 – Armed Forces

v. DOD CIO Memorandum, 6 July 2006, Interim Department of Defense (DOD) Information Assurance (IA) and Certification and Accreditation (C&A) Guidance.

w. DOD CIO G&PM No. 4-8460, 24 August 2000, "DOD GIG Networks"

x. DODD 8100.02, 14 April 2004, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG) "

y. DOD Voice Networks Generic Switching Center Requirements, (GSCR), 8 Sept 2003

z. DODD 4640.13, 5 December 1991, "Management of Base and Long-Haul Telecommunications Equipment and Services"

aa. DepSecDef memorandum, 19 October 1999, "FY 2000 Implementation of Commercial Pricing for Telecommunications Services"

bb. Joint Pub 1-02, 12 April 2001, "Department of Defense Dictionary of Military and Associated Terms"

cc. CJCSI 5711.02 Series, "Policy on Action Processing"

dd. DISAC 310-130-4, 8 September 1997, "Defense User's Guide to the Telecommunications Service Priority (TSP) System"

ee. DISA, 16 May 1996, "Defense RED Switch Network (DRSN) System Description"

ff. CJCSI 3420.01B, 05 December 2006, "CJCS Conferencing Systems"

gg. DODI 4640.14, 6 December 1991, "Base and Long-Haul Telecommunications Equipment and Services"

hh. CJCSI 6211.02 Series, "Defense Information System Network (DISN): Policy, Responsibilities and Processes"

ii. DISAC 310-70-86, 1 February 1995, "Defense RED Switch Network (DRSN) Configuration Management (CM) Guide"

jj. Federal Standard 1037C, 28 February 2001, "Telecom Glossary 2000"

kk. DISA Defense Satellite Communications System (DSCS) Standardized Tactical Entry Point (STEP) Concept of Operations (CONOPS), 12 May 1998

ll. DISA Global Contingency and Exercise Plan (CONEXPLAN) 05-2000, Annex H and Appendix 1 to Annex N

mm. Joint Ethics Regulation, DOD 5500.7-R, Chapter 2, Second Amendment, Change 6 23 March 2006.

nn. DOD Information Technology Standards Registry (DISR), (https: disronline.disa.mil)

oo. DODI 8100.3, 16 January 2004, Department of Defense Voice Networks

pp. DODI 4630.8, 30 June 2004, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security systems (NSS)

qq. DODD 8500.1, 24 October 2002, Information Assurance (IA)

rr. DODI 8500.2, 6 February 2003, Information Assurance (IA) Implementation

ss. DISAC 310-130-1, 04 April 2000, Communications Requirement Submissions of Telecommunications Service Requests

tt. GIG Net Centric Implementation Document (NCID) T300 v3, 1 September 2006.

uu. JROCOM 095-04, 14 June 2004, GIG Mission Area Initial Capabilities Document

vv. Joint Concept of Operations for Global Information Grid NetOps, Version 3 dated 04 Aug 2006.

ww. E-Government Act, (Public Law 107-347), Title III, Federal Information Security Management Act (FISMA)

xx. National Defense Authorization Act for Fiscal Year 2004 (Public Law 108-136) 24 November 2003, section 355.

yy. DOD CIO Memorandum, 6 July 2006, Interim Department of Defense (DOD) Information Assurance (IA) Certification and Accreditation (C&A) Guidance.

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

ADIMSS	Advanced DSN Integrated Management Support System
A/NM	Administration/Network Management
ANDVT	Advanced Narrowband Digital-Voice Terminal
ANI	Automatic Number Identification
AOR	Area of Responsibility
APC	Adaptive Protective Coding
APL	Approved Product List
ARC	American Red Cross
ARO	Authorized Requesting Official
ASA	Automatic Security Authentication
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
ASD (NII)/DOD CIO	Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer.
ATC	Authority to Connect
ATO	Authority to Operate
ATM	Asynchronous Transfer Mode
AUTOVON	Automatic Voice Network
C&A	Certification and Accreditation
CCB	Configuration Control Board
C2	command and control
C3	command, control, and communications
C3I	command, control, communications and intelligence
C4I	command, control, communications; computers and intelligence
CCSD	command communications service designator
CEU	channel encryption unit
CIO	Corporate Information Officer
CM	configuration management
COCOM	Combatant Command (Command Authority)
COMSEC	communications security
COMPUSEC	computer security
CONEXPLAN	contingency and exercise plan
CONPLAN	operation plan in concept format
CONUS	continental United States
CPE	customer premises equipment
CTF	coalition task force
DAA	Designated Approval Authority
DAM	diagnostic acceptability measure
DCF	DISN Customer Forum

DDOE	DISA Direct Order Entry
DFTS	Defense Fixed Telecommunications Service
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISAC	Defense Information Systems Agency Circular
DISN	Defense Information System Network
DITCO	Defense Information Technology Contracting Office
DMS	Defense Messaging Service
DOD	Department of Defense
DPA	Dual Phone Adapter
DPM	digital phone multiplexers
DRSN	Defense Red Switch Network
DRT	diagnostic rhyme test
DSCS	Defense Satellite Communications System
DSN	Defense Switched Network
DTA	Dual Trunk Adaptor
DVS	Defense Video Services
DVX	Deployable Voice Switch
DWCF	Defense Working Capital Fund
EC	Echo Canceller
EMSS	Enhanced Mobile Satellite Service
EO	End Office
EPC	Enhanced Pentagon Capability
EPP	Enhanced Planning Process
F	Flash
FCC	Federal Communications Commission
FMS	foreign military sales
FO	Flash Override
FOO	Flash Override Override
FSAL	Fixed Security Access Level
FTS	Federal Telecommunications System
GAR	Gateway Access Request
GETS	Government Emergency Telecommunications Service
GIG	Global Information Grid
GNC	Global NetOps Center
GNOSC	Global NetOps and Security Center
GNSC	Global NetOps Support Center
GOS	Grade of Service
GPS	General Purpose Segment
GSCR	Generic Switching Center Requirements
GSR	Generic System Requirement
HEMP	High-Altitude Electromagnetic Pulse

HF	high frequency
HMW	health, morale, and welfare
I	Immediate
IA	Information Assurance
IAS	Integrated access Switch/System
IATO	interim authority to operate
IAW	in accordance with
IER	In Effect Report
IP	Internet Protocol
ISP	Information Support Plans
ISDN	Integrated Services Digital Network
IST	interswitch trunk
JCSE	Joint Communications Support Element
JIEO	Joint Information and Engineering Organization
JITC	Joint Interoperability Test Command
JTA	Joint Technical Architecture
JTDLMP	Joint Tactical Data Link Management Plan
JTF	Joint Task Force
JTF-GNO	Joint Task Force Global Network Operations
JWICS	Joint Worldwide Intelligence Communications Systems
Kb	Kilobits
KPP	Key Performance Parameters
LAN	Local Area Network
LPC	linear predictive coding
MCA	maximum calling area
MDA	Multifunction Digital Adaptor
MFS	multifunction switch
MILSTAR	Military Strategic and Tactical Relay Satellite
MLPP	Multilevel Precedence and Preemption
MOA	memorandum of agreement
MOS	mean opinion score
MOU	memorandum of understanding
MTF	message text format
MUF	military-unique feature
NAF	non-appropriated fund
NAOC	National Airborne Operations Center
NATO	North Atlantic Treaty Organization
NCA	National Command Authorities
NCID	Net Centric Implementation Document
NCN	NATO Core Network

NCS	National Communications System
NDN	National Defense Network
NE	Network Element
NIPRNET	Sensitive, but unclassified Internet Protocol Router network
NMCC	National Military Command Center
NM	network management
NMCC	National Military Command Center
NMCS	National Military Command System
NORAD	North American Aerospace Defense Command
NSA	National Security Agency
NS/EP	National Security and Emergency Preparedness
NTAS	NORAD Tactical AUTOVON System
OA&M	Operation, Administration and Maintenance
OCONUS	outside continental United States (CONUS)
O&M	operations and maintenance
OPLAN	operation plan
OSD	Office of the Secretary of Defense
P	PRIORITY
PAT	Precedence Access Threshold
PBD	Program Budget Decision
PBX	Private Branch Exchange
PBX1	Private Branch Exchange Type 1
PBX2	Private Branch Exchange Type 2
PCM	Pulse-code Modulation
PDC	Program Designator Code
PDS	protected distribution system
PIN	personal identification number
PMO	Program Management Office
POM	Program Objective Memorandum
PSTN	Public Switched Telephone Network
PTT	Public Telephone and Telegraph
QoS	Quality of Service
R	Routine
RMC	Resource Management Committee
RSU	Remote Switching Unit
RTS	Real Time Services
SA	stand-alone
SAL	security access level
SATCOM	satellite communications
SBU	Sensitive But Classified

SCI	sensitive compartmented information
SCIF	SCI facility
SCIP	Secure Communications Interoperability Protocol
SDN	Subscriber Directory Number
SECN	Survivable Emergency Conferencing Network
SIPRNET	Secret Internet Protocol Router Network
SMEO	Small End Office
SMU	Switch Multiplexer Unit
SSM	Single System Manager
STE	Secure Terminal Equipment
STEP	Standardized Tactical Entry Point
STU-III	Secure Telephone Unit third generation/low-cost terminal
SVS	Secure Voice System
TDL	Tactical Data Links
TDM	Time Division Multiplexing
T-ISP	Tailored Information Support Plans
TNC	Theater NetOps Center
TRI-TAC	Tri-Services Tactical Communications
TSEC	Telecommunications Security
TSP	Telecommunications Service Priority
TR	Telecom Request
TS	TOP SECRET
TSRS	Telecommunications Service Requests
UCR	Unified Communications Requirements
UHF	ultrahigh frequency
UMUX	universal multiplexer
UN	United Nations
VHF	very high frequency
VOIP	Voice Over Internet Protocol
VOSIP	Voice Over Secure IP
VSAL	variable security access level
VTC	video teleconferencing
WWSVCS	Worldwide Secure Voice Conferencing System

PART II -- DEFINITIONS

Entries here with caption (JP 1-02) are from the Department of Defense Dictionary of Military and Associated terms (short title: Joint Publication 1-02). JP 1-02 terminology is approved for DOD wide general use. The other terminology is specialized and limited to the scope of this instruction.

area of responsibility (AOR). The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. Also called AOR. (See reference bb)

automatic number Identification (ANI). A service feature in which the directory number or equipment number of a calling station is automatically obtained. ANI is used in message accounting. (See reference jj.)

avoidance routing. The assignment of a circuit path to avoid certain critical or trouble-prone circuit nodes. (See reference jj.)

backbone

a. The high-traffic-density connectivity portion of any communications network.

b. In packet-switched networks, a primary forward-direction path traced sequentially through two or more major relay or switching stations. Note: In packet-switched networks, a backbone consists primarily of switches and interswitch trunks. (See reference jj.)

combatant commander (CCDR). A commander of one of the unified or specified combatant commands established by the President. (See reference bb)

classmark. Designator used to describe the service privileges and restrictions for lines accessing a switch (e.g., precedence level, conference privilege, security level, or zone restriction). (Telephony's Dictionary, Langley, Graham, Telephony Publishing Corp. Chicago, IL, June 1982)

command and control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (JP1-02).

communications security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to

mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. (See reference bb)

computer security (COMPUSEC). The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. Also called COMPUSEC. See also communications security (See reference bb)

Condor. NSA's program to secure wireless communications.

configuration management (CM). A discipline applying technical and administrative direction and surveillance to:

a. identify and document the functional and physical characteristics of a configuration item
b. control changes to those characteristics
c. record and report changes to processing and implementation status. (See reference bb.) (See reference kk.)

continental United States (CONUS). United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico. Also called CONUS. (See reference bb.)

cryptosecurity. The component of communications security that results from the provision of technically sound cryptosystems and their proper use. (See also communications security). (See reference bb.) (See reference kk.)

Defense Information Systems Network (DISN). An integrated network centrally managed and configured to provide long-haul information transfer services for all DOD activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services. (See reference bb.)

Defense Switched Network (DSN). A component of the Defense Information System Network (DISN) that handles DOD voice, data, and video communications. (See reference bb.)

directionalization. The temporary conversion of a portion or all of a two-way trunk group to one-way trunks favoring traffic flowing away from a congested switch. (See reference jj.)

DSS Terminology. a. Approval. The official sanctioning effort necessary to permit implementation of a requirement. The level at which approval must be obtained will vary based on the type of service required (See Enclosure D). Service approvals are not normally provided without identified funding. b. Coordination. Any request for service that affects the network within the geographic area of an overseas combatant command requires prior

coordination with concurrence of the affected combatant command. DISA coordination is required for all DSN requirements. New requirements for which funds have not been previously programmed require coordination with the DOD component designated to provide funding. These may include implementation costs, annual depot support costs, annual O&M costs, and a potential increase in a DOD component's annual DWCF bill. c. Resolution. Forward a requirement to the Joint Staff for resolution of the action when the view of an activity is not in accordance with current policy.d. Validation or Revalidation. The confirmation and declaration by competent higher authority that a requirement is justified. Requirements of a requesting agency are validated by the applicable combatant command, Service Chief, director of Defense agency, or head of other agency, or officials delegated this responsibility. Joint Staff validation or revalidation, when required. Validation or revalidation of a requirement by itself does not guarantee funding unless the funding profile is included in the validation or revalidation process.

dual homing. The connection of a terminal so that it is served by either of two switching centers. Note: In dual homing, a single directory number or a single routing indicator is used. (See reference kk.)

emission security. Protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment, AIS, and telecommunications systems. (See reference kk.)

end office (EO). A central office at which user lines and trunks are interconnected-providing long-distance service by interconnecting with DSN nodal switches. [FS1037] EO switches provide users with switched call connections and all DSN service features, including MLPP.

End-to-End. All DSN services beginning at the initiating users facilities until it reaches the receiving user (e.g., phone-to-to phone, video unit-to-video unit, fax-to-fax, STE-to-STE [Secure Terminal Equipment] and deployed applications).

Federal Communications Commission (FCC). The US Government board of five presidential appointees that has the authority to regulate all nonfederal government interstate telecommunications (including radio and television broadcasting) as well as all international communications that originates or terminates in the United States. Note: Similar authority for regulation of federal government telecommunications is vested in the National Telecommunications and Information Administration. (See reference kk.)

Federal Telecommunications System (FTS). A commercial switched long-distance telecommunications service provided for official federal government

use. Use of FTS contract services is mandatory for use by US Government agencies for all acquisitions subject to 40 USC 759.

foreign military sales (FMS). That portion of US security assistance authorized by the Foreign Assistance Act of 1961, as amended, and the Arms Export Control Act of 1976, as amended. This assistance differs from the Military Assistance Program and the International Military Education and Training Program in that the recipient provides reimbursement for defense articles and services transferred. (See reference bb.)

global integrated grid (GIG). A DODD 8100.1, dated 19 September 2002, established the definition of the GIG, which by agreement among DOD CIO, the Under Secretary of Defense (USD) for Acquisition, Technology and Logistics (AT&L), and the Joint Staff/J-6. The GIG is defined as follows:

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, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, National Security, and related Intelligence Community (IC) 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.

b. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

(1) Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

(2) Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

(3) Processes data or information for use by other equipment, software, and services.

c. Non-GIG Information Technology (IT) – Stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

Global NetOps Center. The Global NetOps Center (GNC) is the JTF-GNO Command Center responsible for executing the daily operation and defense of the GIG. The GNC provides overall management, control, and technical direction for GIG NetOps and oversees collaborative coordination process involving all CC/S/As, supporting the needs of the President, SECDEF, NetOps Community, and the warfighting, business, and intelligence domains. (See reference vv.)

Global NetOps Support Center (GNSC). The Global NetOps Support Center (GNSC) provides the day-to-day technical operation, control, and management of the portions of the GIG that support Global Operations but are not assigned to a combatant command. The GNSC conducts GIG backbone NetOps, tactical DISN extension via Standard Tactical Entry Point (STEP) and Teleport mission support, provisioning of provided services, network engineering, circuit implementation, and inter-theater connectivity among USNORTHCOM, USPACOM, USEUCOM, USSOUTHCOM, and USCENTCOM areas of responsibility. The GNSC provides General Support (GS) to the TNCs, and provides DS to the GNCCs. (See reference vv.)

grade of service (GOS).

a. The probability of a call being blocked or delayed more than a specified interval, expressed as a decimal fraction, (e.g. P.09 means nine calls out of 100 will be blocked). GOS may be viewed independently from the perspective of incoming versus outgoing calls and is not necessarily equal in each direction. GOS may be applied to the busy hour or to some other specified period or set of traffic conditions.

b. In telephony the QoS for which a circuit is designed or conditioned to provide; e.g., voice grade or program grade. Criteria for different grades of service may include equalization for amplitude over a specified band of frequencies, or in the case of digital data transported via analog circuits, equalization for phase. (See reference jj.)

high-altitude electromagnetic pulse (HEMP). An electromagnetic pulse produced at an altitude effectively above the sensible atmosphere; i.e., above about 120 km. (See reference kk.)

Homeland Defense (HD). The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. (See reference bb).

installation. A grouping of facilities located in the same vicinity "which support particular functions". If a facility has a functions that is part of a DOD organization's mission, then it would be considered an installation. Example:

DISA HQ and the Navy Annex have functions that are required organizational functions and are considered installations.

Integrated Services Digital Network (ISDN). An integrated digital network in which the same time-division switches and digital transmission paths are used to establish connections for different services. ISDN services include telephone, data, electronic mail, and facsimile. The method used to accomplish a connection is often specified (e.g., switched connection, non-switched connection, exchange connection, or ISDN connection). (See reference jj.)

Joint Worldwide Intelligence Communications System (JWICS). The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing, also called JWICS (See reference bb.)

linear predictive coding (LPC). A method of digitally encoding analog signals, which uses a single-level or multilevel sampling system in which the value of the signal at each sample time is predicted to be a linear function of the past values of the quantized signal. Note: LPC is related to APC in that both use adaptive predictors. However, LPC uses more prediction coefficients to permit use of a lower information bit rate than APC, and thus requires a more complex processor. (See reference jj.)

maximum calling area (MCA). Geographic calling limits permitted to a particular access line based on requirements for the particular line. Note: MCA restrictions are imposed for network control purposes. (See reference jj.)

Multilevel Precedence and Preemption (MLPP). In military communications, a priority scheme: a. for assigning one of several precedence levels to specific calls or messages so that the system handles them in a predetermined order and timeframe

b. for gaining controlled access to network resources in which calls and messages can be preempted only by higher priority calls and messages

c. that is recognized only within a predefined domain

d. in which the precedence level of a call outside the predefined domain is usually not recognized. (See reference jj.)

National Command Authorities (NCA). The President and the Secretary of Defense or their duly deputized alternates or successors. (See reference bb.)

National Communications System (NCS). a. The organization established by section 1(a) of Executive Order No. 12472 to assist the President, the National

Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget, in the discharge of their national security emergency preparedness telecommunications functions. The NCS consists of both the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the EA, the NCS Committee of Principals, and the Manager. (See reference p) b. The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability. (See reference bb.)

National Security or Emergency Preparedness (NS/EP) telecommunications. Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States. (See reference jj.)

Network Management (NM). The execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a telecommunications network, including performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management. Note: NM does not include user terminal equipment. (See reference jj.)

nodal switch. A tandem switch in the DSN that connects multiple EOs, provides access to a variety of transmission media, routes calls to other nodal switches, and provides network features such as MLPP. Nodal switches are supervised by and interconnected to the DSN A/NM subsystem. The two types of nodal switches in the DSN are:

a. stand-alone switch (SA). The SA functions solely as a tandem switch in the DSN.

b. multifunction switch. This switch incorporates the combined functions of an SA switch and an EO switch. No physical division exists between the EO and SA functions within the MFS, but a logical division exists.

nonappropriated funds (NAF). Funds generated by DOD military and civilian personnel and their dependents and used to augment funds appropriated by the US Congress to provide a comprehensive, morale-building welfare, religious, educational, and recreational program designed to improve the well-being of military and civilian personnel and their dependents. (See reference bb.)

outside continental United States (OCONUS). World wide area outside the United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico.

off-hook.

a. In telephony, the condition that exists when an operational telephone instrument or other user instrument is in use; (i.e., during dialing or communicating). Note: Off-hook originally referred to the condition that prevailed when the separate ear piece (receiver) was removed from its switch hook, which extended from a vertical post that also supported the microphone and connected the instrument to the line when not depressed by the weight of the receiver. b. One of two possible signaling states, such as tone or no tone and ground connection versus battery connection. If off-hook pertains to one state, on-hook pertains to the other. c. The active state, i.e., closed loop, of a subscriber or PBX user loop.

d. An operating state of a communications link in which data transmission is enabled either for voice or data communications or network signaling. (See reference kk.)

off-net calling. The process by which telephone calls that originate or pass through private switching systems in transmission networks are extended to stations in a public switched telephone system.

physical security. The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (See reference bb.)

precedence. In communications, a designation assigned to a message by the originator to indicate to communications personnel the relative order of handling and to the addressee the order in which the message is to be noted. (See reference bb.) The ascending order of precedence for military messages is ROUTINE, PRIORITY, IMMEDIATE, FLASH and Flash Override.

a. ROUTINE. Precedence designation applied to official US Government communications that require rapid transmission by telephonic means but do not require preferential handling.

b. PRIORITY. Precedence reserved generally for telephone calls requiring expeditious action by called parties and/or furnishing essential information for the conduct of US Government operations.

c. IMMEDIATE. Precedence reserved generally for telephone calls pertaining to: (1) Situations that gravely affect the security of national and allied forces (2) Reconstitution of forces in a post attack period.

(3) Intelligence essential to national security. (4) Conduct of diplomatic negotiations to reduce or limit the threat of war. (5) Implementation of federal government actions essential to national survival.

(6) Situations that gravely affect the internal security of the United States.

(7) Civil Defense actions concerning US population. (8) Disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population. (9) Vital information having an immediate effect on aircraft, spacecraft, or missile operations.

d. FLASH. Precedence reserved generally for telephone calls pertaining to:

(1) Command and control of military forces essential to defense and retaliation.

(2) Critical intelligence essential to national survival.

(3) Conduct of diplomatic negotiations critical to the arresting or limiting of hostilities.

(4) Dissemination of critical civil alert information essential to national survival.

(5) Continuity of federal government functions essential to national survival.

(6) Fulfillment of critical US internal security functions essential to national survival.

(7) Catastrophic events of national or international significance.

e. FLASH OVERRIDE. A capability available to:

(1) The President of the United States, Secretary of Defense, and Joint Chiefs of Staff.

(2) Commanders of combatant commands when declaring Defense Condition One or Defense Emergency.

(3) USNORAD when declaring either Defense Condition One or Air Defense Emergency and other national authorities the President may authorize.

(4) FLASH OVERRIDE cannot be preempted in the DSN.

(5) FLASH OVERRIDE. A DRSN capability available to:

(a). The President of the United States, Secretary of Defense, and Joint Chiefs of Staff.

(b). Commanders of combatant commands when declaring Defense Condition One or Defense Emergency.

(c). USNORAD when declaring either Defense Condition One or Air Defense Emergency and other national authorities that the President may authorize in conjunction with Worldwide Secure Voice Conferencing System (WWSVCS) conferences.

FLASH OVERRIDE cannot be preempted.

preemption. The ruthless seizure -- usually automatic -- of a path through the military telephone system that is being used to serve lower precedence calls in order to immediately serve a higher precedence call. (See reference jj.)

Primary Switch. An installation switch (e.g., EO) that provides direct connections to user's terminals and the bulk of the installation's inter-DOD mission communications. Large installations may have multiple EOs that provides a significant amount of DOD communications for multiple missions of the whole installation or serve individual tenant organizations on an installation.

private branch exchange (PBX). 1. a. A telecommunications switch, owned by a DOD Component that usually includes access to the public switch network. b. A switch that serves a selected group of users and is subordinate to a switch at a higher level in the DSN hierarchy.

c. A private telephone switchboard that provides on-premises dial service and may provide connections to local and trunked communications networks. Note: A PBX operates with only a manual switchboard. A private automatic exchange PAX does not have a switchboard.(See reference jj.)

protected distribution system (PDS). A wireline or fiber-optics telecommunication system that includes terminals and adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information: A complete PDS includes the subscriber and terminal equipment and the interconnecting lines. (See reference jj.)

public switched telecommunications network (PSTN). Global collection of private and US Government interconnected public telephone networks providing voice and data communications via switched lines. Any common-carrier network that provides circuit switching among public users. Note: The term is usually applied to public switched telephone networks, but it could be applied more generally to other switched networks, such as packet-switched public data networks. (See reference jj.)

Real Time Services (RTS). A subset of the four categories of services contained in the GIG NCID, QoS (T300). The four categories of services are Signaling, Inelastic/Real Time, Preferred Elastic and Elastic. Signaling includes both Network Control and User Signaling for managing the network and setting up and taking down sessions over the network. Inelastic RTS provide GIG users with primarily live interactive services that are that are extremely sensitive to packet delay, jitter and loss to include voice, video, multimedia communications or rapid delivery of critical command and control information involving weapons delivery capabilities that clearly allow for (1) the equivalent

of “Face to Face” interactions in which both factual and emotional content of the interaction can be conveyed and (2) operation of surveillance and weapons systems that require rapid message delivery.

satellite communications (SATCOM). A telecommunications service provided via one or more satellite relays and their associated uplinks and downlinks. (reference jj.)

Secure Communications Interoperability Protocol (SCIP). SCIP is the US Government's standard for secure voice and data communication and was adopted to replace the FNBDT (Future Narrowband Digital Terminal) title in 2004. SCIP systems have been in use since 2001, beginning with the CONDOR secure cell phone. The standard is designed to cover wideband as well as narrowband voice and data security.

SECRET Internet Protocol Router Network (SIPRNET). Worldwide SECRET-level packet switch network that uses high-speed Protocol routers and high-capacity Defense Information Systems Network circuitry. (See reference bb.)

split homing. The connection of terminal equipment to more than one switching center by separate access lines, each of which has a separate directory number. (See reference jj.)

tactical communications. Communications in which information of any kind, especially orders and decisions, are conveyed from one command, person, or place to another within the tactical forces, usually by means of electronic equipment, including communications security equipment, organic to the tactical forces. Tactical communications do not include communications provided to tactical forces by the DISN, to non-tactical military commands and to tactical forces by civil organizations. (See reference jj.)

tandem. Pertaining to an arrangement or sequencing of networks, circuits, or links, in which the output terminals of one network, circuit, or link are connected directly to the input terminals of another network, circuit, or link. (See reference jj.)

tandem office. A central office that serves local subscriber loops and also is used as an intermediate switching point for traffic between central offices.(See reference jj)

Telecommunications Service Priority (TSP) service. A regulated service provided by a telecommunications provider, such as an operating telephone company or a carrier, for NS/EP telecommunications. Note: The TSP service replaced Restoration Priority service effective September 1990. (See reference jj.)

Theater NetOps Center (TNC). Each TNC provides direct support to its TNCC, ensuring the effective operation and defense of the GIG within the theater. The TNC is OPCON to JTF-GNO and offers onsite, theater support. Each TNC can issue technical directives to STNOSCs/Agency Theater Network Operations and Security Centers (ATNOSCs). The TNC develops, monitors and maintains a GIG SA view for the theater. The theater GIG Situational Awareness (SA) view is aggregated and segmented based on requirements provided by the TNCC as derived from the GIG common SA standards. The GIG SA view will include pertinent theater, operational, and tactical-level system and network, GND, and GCM status. Coordination with the TNCC is paramount especially with regards to reporting requirements and SA. (See reference vv.)

Theater NetOps Control Center (TNCC). The primary mission of the TNCC is to lead, prioritize, and direct theater GIG assets and resources to ensure they are optimized to support the GCC's assigned missions and operations, and to advise the combatant command of the GIG's ability to support current and future operations. The specific roles of the TNCC include monitoring of the GIG assets in their theater, determining operational impact of major degradations and outages, leading and directing responses to degradations and outages that affect joint operations, and directing GIG actions in support of changing operational priorities. The TNCC leads the combatant command response to NetOps events and responds to JTF-GNO direction when required to correct or mitigate a global NetOps issue. (See reference vv.)

transmission security. The component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than crypto-analysis. (See reference jj.)

TRI-TAC. Acronym for tri-services tactical. See tactical communications. (See reference jj.)

TRI-TAC equipment. Equipment that accommodates the transition from current manual and analog systems to fully automated digital systems and provides for message switching, voice communications circuit switching, and the use of secure voice terminals, digital facsimile systems, and user digital voice terminals. (See reference jj.)

ultrahigh frequency (UHF). Frequencies from 300 MHz to 3000 MHz. (See reference jj.)

user. A person, organization, or other entity (including a computer or computer system) that employs the services provided by a telecommunications system or an information processing system for transfer of information. (See reference jj.)