CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6	CJCSI 6215.01B
DISTRIBUTION: A, B, C, J, S	23 September 2001

POLICY FOR DEPARTMENT OF DEFENSE VOICE NETWORKS

References: See Enclosure H.

1. Purpose. This instruction establishes policy and prescribes responsibilities for use and operation of the DOD voice networks, specifically the DSN and the DRSN.

2. Cancellation. CJCSI 6215.01A, 1 February 1995, is canceled.

3. Applicability. This instruction applies to the Joint Staff, combatant commands, Military Services, and Defense agencies. This instruction also identifies policy and responsibilities concerning non-DOD governmental, foreign government, and civilian organizational requests for DSN and DRSN support. Requests for waivers to this instruction will be forwarded by chain of command, including the CINCs, Service Chiefs, or Defense agencies, to the Joint Staff, stating the reason compliance is not possible.

4. Policy. The DSN and DRSN are under operational direction and management control of the Director, DISA. As the SSM of both networks and the executive agent of the DRSN, the Director, DISA, will be responsive to the Chairman of the Joint Chiefs of Staff, CINCs, Military Services, and Defense agencies. Enclosures A, B, C, and F provide specific operational policy for the DSN. Enclosures D, E, and F provide specific operational policy for the DRSN.

5. Definitions

a. As approved by OSD, the DSN is an interbase, nonsecure or secure C2 telecommunications system that provides end-to-end command use and dedicated telephone service, voice-band data, and dial-up VTC for C2 and non-C2 DOD authorized users in accordance with national security directives. Nonsecure dial-up voice (telephone) service is the system's principal requirement. (See references a and b.)

b. The DRSN is the secure C2 system and is a key component of the DOD global secure voice services. The DRSN supports the secure voice and secure conferencing, requirements of the NCA, components, DOD, and select federal agencies in peacetime, crisis situations, and wartime. It is a separate, secure switched network that is considered part of the DISN. The DRSN, the STU-III/STE family of equipment that provides end-to-end encryption over the DSN, and Condor, the NSA's program to secure wireless communications, are the three subservices that together provide the foundation for the DOD secure voice services. (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 and switched voice, data, imagery, and VTC services in support of national defense C3I decision support requirements. For GIG, Wide and Metropolitan Area Networking (WAN, MAN), use of the DISN is mandatory unless granted a waiver through the DISN or GIG waiver board (reference v).

6. Responsibilities. See Enclosure G.

7. Summary of Changes. The name of this instruction is changed from "Policy for the Defense Switched Network" to "Policy for Department of Defense (DOD) Voice Networks" to recognize the unique nature of the DRSN, and includes more detailed guidance on the DRSN. Additionally, this revision updates network performance parameters, cost recovery procedures, usage and security policy, and discussion of switches and terminal equipment. It also incorporates guidance for the use of EMSS in conjunction with the DSN, as well as numerous administrative and procedural changes.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), 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/doctrine. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

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

S. A. FRY
Vice Admiral, U.S. Navy
Director, Joint Staff

Enclosures:
A--Policy for the DSN
B--Policy and Procedures for Connection of Specific Equipment to the
DSN
C--Procedures for Requesting DSN Service
D--Policy for the Defense RED Switch Network
E--Procedures for Requesting DRSN Service
F--Precedence Approval Authorities
G--Responsibilities
H--References
GL--Glossary

DISTRIBUTION

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

	Copies
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)	4
Director, Inter-American Defense Board	2
Director, National Communications System	2
US Delegation, United Nations Military Staff Committee	1
Military Communications-Electronics Board	1
Commandant, US Coast Guard	2
Federal Aviation Administration	1
Federal Emergency Management Agency	2
Director, Central Intelligence Agency	2
Director, National Security Agency	2
Director, General Services Administration	2

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 4	O	E-1 thru E-4	O
i thru viii	O	F-1 thru F-2	O
A-1 thru A-24	O	G-1 thru G-14	O
B-1 thru B-4	O	H-1 thru H-4	O
C-1 thru C-4	O	GL-1 thru GL-14	O
D-1 thru D-20	O		

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE Page

A POLICY FOR THE DSN A-1

Purpose A-1
General A-1
Commercial Leased Telecommunications A-1
General and Military-Unique Requirements A-2
Objective Technical Parameters and Special Functions A-4
Network and Applications A-6
Network Interfaces A-7
Usage Policy A-9
Network Management A-13
Network Security A-14
Network Survivability Features A-15
DSN Switches and Terminal Equipment A-15
Cost Recovery A-19
Approval Terminology A-20
DSN Support A-21
Assignment and Control of Precedence Levels A-22
Administration A-23

B POLICY AND PROCEDURES FOR CONNECTION OF SPECIFIC EQUIPMENT TO THE DSN B-1

Purpose B-1
General B-1
Secure Transmission with a STU-III/STE B-1
Switched Data/Imagery B-2
Dial-Up Facsimile B-2
Family of Off-line Cryptodevices (TSEC/KL-43) B-2
VTC B-3
DSN Control, Data Collection, and Orderwire Circuits B-3

C PROCEDURES FOR REQUESTING DSN SERVICE C-1

Purpose C-1
Applicability C-1
General C-1
Approval Authority C-2
Request Format C-2

D POLICY FOR THE DEFENSE RED SWITCH NETWORK D-1

Purpose D-1
General D-1
General and Military-Unique Requirements D-3
Objective Technical Parameters D-5
DRSN Services and Applications D-9
Network Management D-14
Network Security D-15
Network Survivability Features D-17
Cost Recovery D-17
Approval Terminology D-18
DRSN Support D-18
Assignment and Control of Precedence Levels D-18
Administration D-19

E PROCEDURES FOR REQUESTING DRSN SERVICE E-1

Purpose E-1
Applicability E-1
General E-1
Approval Authority E-2
Request Format E-2

F PRECEDENCE APPROVAL AUTHORITIES F-1

Purpose F-1
Approval Authorities F-1

G RESPONSIBILITIES G-1

Purpose G-1
Office of the Secretary of Defense G-1
Joint Staff G-1
Director, DISA G-3
The CINCs G-8
Service Chiefs and Directors of Defense Agencies G-10
Executive Agent, DRSN (US Air Force) G-12
Director, DIA G-12
Director, NSA G-12
Administration G-13

H REFERENCES H-1

GL GLOSSARY GL-1

Part I--Abbreviations and Acronyms GL-1
Part II--Definitions GL-4

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY FOR THE DEFENSE SWITCHED NETWORK (DSN)

1. Purpose. This enclosure provides general guidance, operational policy, and performance objectives for the DSN. In addition, it describes required functions and military-unique features of the DSN.

2. General

a. The DSN provides rapid, reliable, survivable, nonsecure/secure, and economical C2 telecommunications. To take advantage of economies of scale, the DSN also provides service to non-C2 users on a not-to-interfere basis.

b. The user terminal end of the DSN is the long-distance termination equipment of the EO switch. Those portions of MFSs and EO switches that are within the boundaries of the DSN will operate under DISA's operational management for the day-to-day operations and CM. However, all equipment connected to the DSN (to include SA switches, RSUs, PBXs, PABXs, and deployable/tactical switches) is considered to be part of the GIG and must be in compliance with all DOD directives and CJCSIs concerning interoperability and required functionality. See references e and f. (See Enclosure I and paragraph 12 below for definitions of switches.)

c. The DSN system is used only for official business or in the interest of the government and is the first choice for all switched voice and dial-up video telecommunications between DOD user locations.

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

3. Commercial Leased Telecommunications. DSN must use commercial leased telecommunications where cost-effective or when mission-essential requirements dictate. Use of commercial leased telecommunications in overseas areas is negotiated country-by-country by DISA, in coordination with the appropriate CINC and O&M commands.

4. General and Military-Unique Requirements. The DSN must adhere to the capability objectives below to ensure its ability to support effective military C2 functions. (See references e, f, g, h, i, and 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 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, etc.

(4) To the maximum extent possible, major installations routed to diverse facilities over separate paths.

(5) No major DOD installation, NMCC, combatant CINC, or component headquarters isolated longer than 2 hours because of an outage in the long-haul portion of the network.

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

(a) Crisis, Preattack, and Theater Nonnuclear War. DSN network capabilities must support all peacetime readiness (priority 3) users, plus surge requirements for nonnuclear war. These capabilities are handled according to established precedence.

(b) Postattack. 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 nonnuclear war.

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

(d) Early Transattack (few weapons, possible 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) 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 in accordance with 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 DSN was designed with a MUF, the MLPP capability. MLPP permits higher precedence users to preempt lower precedence calls. Special C2 users (FLASH and FLASH OVERRIDE within the current DSN MLPP framework) are provided with nonblocking service (P.00 threshold) from user to user. (P.00 = out of every 100 calls, the probability is that zero calls will be blocked.)

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

c. Responsive Service. DSN service must be responsive to the needs of C2 users. Special C2 users (see paragraph 15a) under current DSN MLPP scheme -- FLASH and FLASH OVERRIDE -- are provided nonblocking 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 CINCs and military departments, identify critical switches annually.

(3) During times of surge or crisis, the Chairman of the Joint Chiefs of Staff can direct implementation of certain traffic controls, such as selected blocking, directionalization, and usage or availability control (e.g., MINIMIZE) to ensure usage for critical users. In addition, affected

CINCs, Services, and agencies should utilize all means available to reduce (e.g., 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, federal government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable as specified in reference f.

g. 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 in accordance with Federal Communications Commission (FCC) rules and regulations through the commercial telecommunications industry and the TSP system (reference j). For example, access to the GETS is available via the DSN. The DSN must comply with the NS/EP's TSP system for service restoration. Within the CONUS, NS/EP TSP-approved requirements will be provisioned within 72 hours. In OCONUS areas not under the control of the US Government, the Military Services and CINCs will provide NS/EP support where feasible and available through agreements with host governments and in accordance with TSP. OCONUS requirements will be provisioned as quickly as possible.

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 CINCs and Chiefs of the Services. They must be validated by the Joint Staff and approved by OSD. 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 (seven calls out of 100 will be "blocked" during the "busy hour") or better, and an intertheater GOS of P.09 or better, as measured during normal business hours of the theaters. Service O&M commands will ensure the GOS between the EO and any PBX users do not exceed an additional blockage of P.02. Service O&M commands are responsible for supporting DISA's data collection requirements on all DSN switches. Service 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. DISA reports to the Joint Staff and respective CINCs those network access points (EOs and MFSs) not meeting the following performance standards:

(1) GOS service criteria for intertheater of P.09.

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

(3) Any EO not meeting the special C2 user (DSN MLPP FLASH OVERRIDE and FLASH) nonblocking criteria.

(4) Shortfalls in achieving the above target-GOS criteria because of economic or operational reasons to include shortfalls behind EOs as reported by Service O&M commands.

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 of 4.0 or better in accordance with "Telephone Transmission Quality Subjective Opinion Tests—Methods for Subjective Determination of Transmission Quality (ITU-T) Recommendation P.800."

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 CINC, Service, and agency post, camp, or station voice transport and processing initiatives should 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.

d. VTC, data, and other switched system application 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 systems, programs, and other applications:

a. Switched Data

(1) The DSN provides dial-up switched 56 kb digital services (restricted mode ISDN) and, where possible, 64 Kbs ISDN services. 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 FY 2002 objective is for the DSN to implement ISDN services from EO to EO as Service switch upgrade projects and programs are completed. The Services and agencies 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.

(2) DISA provides network standards, NM, transmission, and switching services. Users are responsible for procurement and operation and maintenance of their customer premises equipment using the DSN. Although DISA currently maintains special backbone trunking without echo cancelers to support data users, this inefficient use of common user facilities must be phased out. (As of 1 October 2002, user equipment for passing data over DSN must have “tone disabling” capabilities to disable echo cancellation. Tone disabling is the means of selectively disabling echo cancellation for transmission of digital traffic. The goal is to migrate to a fully digital architecture while maintaining military-unique capabilities.)

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

c. DMS. DSN provides a dial-up transmission restoral capability for DMS transition hubs.

d. VTC. 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 established by reference m. Use of network interfaces not conforming to the DSN interface criteria must be coordinated with DISA and approved by the Joint Staff. 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. NGCS. DSN interoperates with the NGCS. The NGCS-DSN interface has been developed and implemented at locations as agreed among NATO, the affected commands, and the Joint Staff. DISA is responsible for processing required agreements with NATO. (See references n and o.)

b. Commercial Telephone Networks or PSNs

(1) Manual connection of official calls by operator intervention at an EO switch or PBX may be authorized by the authority controlling the EO or PBX. Combatant commands, Military Services, and Defense agencies are responsible for monitoring and preventing abuse of this capability.

(2) Automatic Interfaces

(a) Automatic interconnections (those not requiring operator intervention) to the private or PSNs for local subscribers may be provided for local calls only by the controlling authority of an EO switch or PBX (often identified as “dial 9” service). Enhanced call completion features such as call forwarding and call waiting may be implemented if deemed appropriate in the local area for local calls, if mission essential. These features must in no way diminish the assured service connectivity from user to user. The Military Services and Defense agencies are responsible for any connection and usage charges to public networks. Particular care must be taken to ensure this capability does not allow automatic on or off-netting of long distance DSN or commercial calls.

(b) 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. Automatic interconnection of HMW calls must be in accordance with reference nn. See paragraph 8b(1) below.

(c) Managed Interfaces. DISA and the Services will manage controlled interfaces between the DSN and the PSN to fulfill communications requirements between DOD and non-DOD facilities and to provide alternative communications in the event of DSN disruptions. Interface usage will incur additional call-by-call charges for the commercial segment of the call if the interface incurs additional charges to the government. These interfaces may only be used for HMW calls in accordance with reference nn. See paragraph 8b(1) below. At a minimum, these interfaces will meet the criteria in paragraph 7d below.

(d) Other Automatic Interconnection. Other automatic interconnection, on or off-netting, may be permitted on a case-by-case basis. HMW calls must be in accordance with reference nn and paragraph 8b(1) below. All automatic interfaces to the DSN must have as a minimum:

1. 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.

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

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

4. A means of identifying costs of all calls for appropriate billing of users.

c. Tactical

(1) The DSN normally connects with tactical communications systems using Standardized Tactical Entry Points (STEP)/Teleport. The STEP/Teleport provides technical features to permit tactical communications systems to interoperate with the DSN. DISA maintains standards for STEP/Teleport facilities and will manage the configuration and provisioning of STEP/Teleport sites to interface with deployed networks, to include those of the JTF backbone and components (see references p and ll). Deployed voice systems, for their part, will comply

with DSN specifications (references m and y) to complete the needed interfacing with the DSN at STEP/Teleport sites.

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

(3) All tactical communications, planned exercises, contingencies, and tactical operations incur normal DSN usage charges for calls made through the DSN.

d. NCS. In the United States, the NCS will use the DSN and other switched systems to carry the traffic of NS/EP users. Postattack 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.)

8. Usage Policy

a. General

(1) Use of the DSN is restricted to the official business of the US Government or in the interest of the government.

(2) DSN is the official DOD switched voice network and will be the preferred communications means for special C2, C2, and non-C2 user. It is the primary means of secure (STU-III/STE family) communications for nontactical 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.

(3) The Department of Defense may grant non-DOD activities access when necessary for national security; when not in conflict with local PTT ordinances; when those activities and individuals have critical NS/EP needs; and access is in the best interest of the US Government. 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 the CONUS, requests by non-DOD users should be satisfied by available commercial service or (FTS-2000/2001 or their

successors) 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 of non-DOD or nongovernmental activities or agencies, such as the Department of Justice, state government organizations, DOD contractors, labor unions, and foreign embassies, are referred OSD for approval with a recommendation by the Joint Staff, except as provided in paragraph 8c below.

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

(1) HMW. In accordance with reference nn, 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. CINCs will establish policy for authorization, 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:

(a) Calls placed through the local installation switch are required to have management controls that prevent unauthorized use of the DSN and the PSN, or through the DISA-managed interface to the PSN as described in paragraph 7b(2)(c). To ensure compliance with reference nn, technical means will be implemented to prevent completion of CONUS-originated calls.

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

(c) 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 government, even if the intent is to reimburse the 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 credit card.

(2) Emergencies and Special Circumstances. On and off-netting of official long-distance telephone traffic by a manual interface is authorized for crisis or emergency conditions with national security implications. A CINC, Service Chief, or director of a Defense agency may

authorize manual on or off-netting of official long-distance telephone traffic for other special circumstances.

(3) Control. CINCs must establish procedures for the positive control of on and off-net access for EOs within their AOR. Service Chiefs and directors of Defense agencies will establish procedures for positive control of on and off-net access for EOs in CONUS that are not CINC responsibilities.

c. Contractors

(1) 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 CINC, Service Chief, or director of a Defense agency 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.

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

(a) The contractor's function is a C2 mission. Study, analysis, design engineering, and other similar support functions are not authorized missions.

(b) The DSN access provided to the contractor is equivalent to that access previously provided to the military organization originally performing the function. Requests for this access (ROUTINE only) must be validated at the local level and approved by an agent with written delegation from the appropriate CINC, Service, or Defense agency. Precedence access above ROUTINE must be approved by the CINC, Service, or Defense agency.

(c) Contractors located in CONUS requiring new or increased DSN access must have each specific request approved by the appropriate CINC, Service, or Defense agency. Blanket approvals are not authorized.

(3) The requesting CINC, Service Chief, or director of Defense agency 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 NM procedures. Requests for approvals must identify the contract termination date.

(4) Procedures for reviewing, monitoring, and controlling contractor access to DSN must be published in Service, command, or agency regulations. As a minimum, a review of contractor access to DSN must be conducted every 3 years and in conjunction with every renewal or period of performance extension of the contract.

(5) Copies of all contractor access requests, approvals, and terminations must be provided to DISA.

(6) Approvals and contracts must state that the Department of Defense has the right to terminate the service at any time and that the Department of Defense 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.

d. 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.

e. 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 CINCs, Service Chiefs, and directors of Defense agencies must institute procedures to revalidate requirements periodically.

f. 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, CINC, Military Service, Defense agency concerned, and DISA will be notified of command support for a request to OSD for labor union access to DSN.

g. Foreign Governments and Treaty Organizations. Foreign government activities may be granted access to the network by the Department of Defense 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 in accordance with reference o.

(1) CINCs may authorize the use of DSN, 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 GOS objectives outlined in this instruction.

CINCs must ensure effective control of this use and may authorize the service only when other telecommunications facilities 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, in accordance with reference o.

(2) DSN Service to Canada. As a continuation of the original NORAD requirements for the AUTOVON, the DSN will support the combined US/Canadian NORAD NTAS and general-purpose requirements for cross-border communications as an integral part of the DSN.

h. FMS of DSN Service. 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 to OSD in accordance with reference u.

i. DSN Service for DOD personnel assigned to non-US functions. The use of DSN by DOD personnel assigned to non-US (foreign government adviser, UN, NATO, etc.) organizations must be approved by the appropriate CINC, Service Chief, or director of Defense agency. Requests for FLASH or FLASH OVERRIDE must be validated by the appropriate CINC, Service Chief, or director of Defense agency and approved by the Joint Staff.

j. 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, formally known as “Class B” service, for geographic location(s) within his or her command. Requests must be forwarded to the CINC for approval/disapproval and to the DISA DSN program management office for information. Approved Class B service must be revalidated by the CINC biennially. Local commanders are responsible for determining appropriate cost reimbursement rates (see reference v). In addition, DSN service may be provided in key personnel residences for official calls.

9. Network Management. DISA establishes DSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. As specified in reference n, the DSN is under the operational direction and management control of the Director, DISA, and is responsive to the Chairman of the Joint Chiefs of Staff, the CINCs, the Military Departments, and Defense agencies and activities. The CINCs, the Military Departments, and Defense agencies and activities will ensure switch systems are certified for interoperability or obtain an IATO prior to connection to the network (see reference f).

a. DISA must possess read-access and limited/controlled write-access capabilities, unless Service/agency operational command personnel are available to make changes 24-hours a day, 7-days a week to all DSN switch database tables (excluding those tables associated with non-DISA-controlled portions of switch database tables).

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 the ASD(C3I); the Director, DISA; and the Joint Staff.

c. DISA must have the ability to implement network control commands to all DSN switches. DISA will use onsite O&M activities to implement network controls when they are present. In OCONUS AORs, the theater CINC 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.

d. During emergencies, DISA has the authority to implement switch database revisions required for operation and management of the DSN in accordance with paragraphs 9a and 9c above.

e. Service O&M commands must maintain DISA's intra- and interswitch dialing plans for end users and implement DSN access codes as defined in the DSN GSCR document, reference z, to ensure standardization across the network.

10. Network Security

a. The DSN will conform to the C&A procedures outlined in reference w. The objective of this requirement is to establish a DOD-standardized approach to protect and secure the entities that comprise the Defense information infrastructure. The systems security authorization agreement, Enclosure 6 of reference w, is the living document that represents agreement among the DAA, the certification authority, the user representative, and the system program manager on the approach for DSN C&A.

b. The design and operation of DSN must maximize protection of switches, transmission links, and NM facilities and provide protection against disruption, intrusion, compromise, and denial of service. Based on the mission, priority, and susceptibility of user and switch operations, security countermeasures must be applied to provide, COMSEC, and physical and personnel security protection.

c. The STU-III/STE family of instruments is self-authenticating to the level of classification displayed on the instrument. When STU-IIIR/STE users are connected to the distant end by a RED switch, the information shown on the message display is of the RED switch interface, not the distant end.

11. Network Survivability Features

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

b. Vulnerability Analysis. DISA is responsible for initiating and providing technical analysis of network survivability, to include a risk analysis, when proposing major changes in the network topology. DISA will forward the results of the analysis to the Joint Staff for review.

12. DSN Switches and Terminal Equipment

a. DSN Backbone Switches. Two switch types provide the switching subsystems for the DSN tandem backbone. These backbone switch types are the SA nodal switch (tandem switch) and the MFS.

b. Base, Post, Camp, or Station Functional Switch Types. Because the duration and rigor of switch certification testing is dependent upon the intended function of the switch, the following are functional definitions of switches residing on bases, posts, camps, or stations:

(1) EO. Switches integral to the DSN and which serve as the primary switching facilities for installations' long-distance voice services by interconnection with DSN nodal switches.

(2) PBX/PABX. Secondary voice switching facilities on the users' installations, derive their DSN service through the local DSN EOs, and are considered customer premise equipment. PBX/PABXs primarily function as concentrators for local base distribution.

(3) RSU. A technical rather than functional type of switch and categorized functionally as either an EO or PBX. If an RSU is employed as a "functional" EO switch; i.e., provides full command and control capabilities (MLPP), meets the requirements of paragraph 12d, and

serves as the primary DSN switch for that location, then that RSU is considered a DSN EO switch. However, if an RSU cannot satisfy the MLPP requirement or serves as a secondary switch behind the base EO, it is considered a PBX switch. RSUs will be tested in conjunction with the host switch for interoperability certification.

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

d. DISA must design the network topology (nodal, MFS, and EO) of the DSN (where to connect switches into the DSN) and publish the plan. This plan must be updated annually. The Services or Defense agencies must coordinate recommendations with DISA (and the CINC concerned if OCONUS) for switch designation or redesignation. DISA evaluates and engineers changes or redesign as appropriate. Inter-Service agreements are used to allocate PBX to EO support costs. The Joint Staff adjudicates any disagreements. DSN elements falling directly under DISA's management responsibilities include:

(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.

Although PBXs are not elements of the DSN, they are still part of the GIG and are therefore subject to all interoperability requirements of the GIG. (See references e and f.)

e. C2 and NM Capabilities. The DSN SA nodal switches, MFSs, and EO switches must contain the necessary features to satisfy C2 requirements and are supervised by and interconnected to the DISA NM subsystem. The user terminal end of DSN is currently the long-distance termination in the EO. DISA NM responsibilities extend throughout the network to the long-distance terminations in the EO switch. DISA, as the single-system manager of DSN, is responsible for ensuring special C2 user (see paragraph 15a) service and establishes criteria for handling special C2 calls down to the end instrument. The O&M command is responsible for providing switch maintenance activities and will ensure all C2 user service from the EO switch to the instrument in accordance with DSN performance objectives (paragraph 5a) and will periodically review authorizations for DSN access and precedence capabilities. 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 is forwarded to an alternate number, that number must be preemptable.

f. PBX, PABX, and RSU. Service changes or enhancements to DSN switches must be coordinated with DISA for network impact assessments. PBXs and PABXs are connected to, and served by, an EO or the EO portion of the MFS. In addition, PBXs and PABXs may be connected to and served by a DSN tandem switch, on a case-by-case basis, for critical C2 missions approved by the Joint Staff. PBXs, PABXs, and RSUs that are not employed as a “functional” EO switch are considered CPE. They are not part of the DSN, but they must meet DSN interface standards. Moreover, they are part of the GIG and must meet GIG interoperability standards as specified in references e and f. DSN interface standards include:

(1) The RSU must be software controlled by a serving MFS or EO switch providing DSN interconnection. RSU subscribers may have all features available to users of the supporting MFS or EO switch.

(2) PBX subscribers may not have direct precedence originating capability unless the PBX meets the EO criteria for interfacing with the DSN. PBX subscribers may be offered indirect precedence originating capability through an EO attendant position.

(a) Special C2 users are not normally provided network access by a PBX.

(b) PBXs 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.

(3) At all PBX 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.

(4) CPE must meet GOS objectives for the network. The O&M command is responsible for monitoring the performance of this equipment and must report all substandard performance to DISA and take all necessary actions to ensure GOS objectives are met.

(5) Services must not directly interconnect RSUs, PBXs, PABXs, MFSs, or EO switches in a manner which circumvents the long-distance DISN/DSN network. (See reference x.)

(6) Specific interoperability certification requirements of each category of switch (to include SA, MFS, EO, PBX, PABX, and RSU switches) is published in reference y. Interoperability certification or an IATO must be granted before connection to the DSN.

g. Secure Voice Terminals. The STU-III/STE family provides a secure voice capability over the nonsecure switched voice network. Secure voice terminals are managed as CPE similar to the nonsecure telephone instruments, but in accordance with national, CINC, and Service or agency procedures.

h. CPE. Nonsecure and secure telephones, STU-III/STE 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 reference m.)

i. EMSS. The EMSS program provides connectivity between the DSN and the wireless, satellite-based Iridium Satellite (IRIDIUM) network. EMSS users are authorized direct precedence 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 must be via authorized gateway switches only.

(b) Precedence access to the DISN must be controlled by the DSN 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 outside the DSN (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 authorized gateway switches only.

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

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

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

j. Network Access. DISA must implement the controls necessary to limit DSN network access to that authorized in this instruction. The CINCs, Services, and Defense agencies will implement policies and procedures to limit use to that authorized in this instruction.

13. Cost Recovery

a. Cost-Effective Service. In compliance with OSD direction (see references z and aa), DSN provides network flexibility to exploit new technology, tariffs, and commercially available resources. The DSN is funded by the Defense Working Capital Fund (DWCF). The DSN must evolve incrementally to meet objectives as opportunities occur to fund technological upgrading and service growth. Only those capabilities that are cost-effective for each DOD user or the DOD in general will be built into the DSN. DSN capital investment and recurring costs will be recovered through DWCF rates published based upon OSD direction. Military Departments, DOD components, and all other authorized users are responsible for budgeting and paying for DSN service.

b. Metropolitan Calling Areas. Metropolitan calling areas are calling areas created to provide a special DSN calling rate based on local commercial areas, practices, or tariffs (i.e., areas within which commercial point-to-point calls would be billed as local calls by commercial telecommunications service providers) for the purpose of maintaining competitive DWCF DSN rates. A metropolitan calling area may include interswitch calling between multiple DSN user locations served by two or more DSN switches. Specifically identified metropolitan calling areas may be established, if requested by the Services, to appropriately allocate telecommunications costs to the users. Specific metropolitan calling areas must be approved by the DSN PMO and must coincide with commercial local calling areas. DISA maintains a list of all approved metropolitan calling areas. Metropolitan calling areas must be revalidated every 2 years.

14. Approval Terminology. The following terminology is used for actions in accordance with this policy. (See reference bb.)

a. 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 CINC, Service Chief, director of Defense agency, or head of other agency, or officials delegated this responsibility. Joint Staff validation or revalidation, when required, will be in accordance with reference cc. Validation or revalidation of a requirement by itself does not guarantee funding unless the funding profile is included in the validation or revalidation process.

b. Coordination. Any request for service that affects the network within the geographic area of an overseas combatant command requires prior coordination with and concurrence of the affected CINC. DISA coordination is required for all DSN requirements. New requirements for which funds have not been previously programmed require coordination with the Service designated to provide funding. These may include implementation costs, annual depot support costs, annual O&M costs, and a potential increase in a Service’s annual DWCF bill.

c. Approval. The official sanctioning necessary to permit implementation of a requirement. The level at which approval must be obtained will vary based on type of service required (see Enclosure F). Service approvals are not normally provided without identified funding.

d. Resolution. Forwarding of a requirement to the Joint Staff for action when the views of an activity are not in accordance with current policy.

15. DSN Support. DSN supports three categories of users:

a. Special C2 Users. A special class of user who has access to the DSN for essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, preattack, and theater nonnuclear war telecommunications service for intelligence, alert, and strategic readiness. This user also requires 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 CINCs. Specifically, these special C2 users are identified through one or more Joint Staff, CINC, Service, or DOD agency validation processes. The following are required capabilities of special C2 users:

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

(2) CINC-validated minimum-essential circuits.

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

b. C2 Users. Users who have a requirement for C2 communications but do not meet the criteria for the class of “special C2 user.” C2 users include any person (regardless of the position in the chain-of-command) who issues guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration, and logistics), whether said guidance or order is issued or effected during peacetime or wartime. C2 users are identified as users of Joint Staff, CINC, Service-, and agency-approved PRIORITY and ROUTINE precedence origination.

c. Other Users. Users who have a requirement to use the DSN but who do not meet the criteria for the classes of “special C2 users” or “C2 users.” These users are granted only ROUTINE access when it is not in conflict with local PTT ordinances. They may be denied access during a contingency or crisis. Included in this class are non-DOD, nongovernmental, and foreign government users of OSD or Joint Staff-approved capability. (See paragraph 8.)

16. 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. 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 CINC, Service Chief, or director of Defense agency, who also approves requirements for IMMEDIATE and PRIORITY service. Requests for precedence are not restricted by 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. Control of Precedence. The CINCs, Service Chiefs and directors of Defense agencies must establish and maintain policy to control use of precedence access 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 CINC, Service, or agency 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 classmarking of access lines are employed to control access to the DSN.

e. Temporary Precedence Upgrades. Temporary DSN service upgrading to support the NCA, Chairman of the Joint Chiefs of Staff, CINCs, Service Chiefs, 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 C and must be coordinated with DISA and approved by the CINC or the Service Chief concerned. Approvals of FLASH OVERRIDE and FLASH access must be provided to DISA and the Joint Staff. The CINC or Service Chief must identify source of funding to cover additional costs prior to approval.

f. Enclosure F identifies approval authority for DSN service requests.

17. Administration. The CINCs, Service Chiefs, and directors of Defense agencies must develop implementing policies and procedures for the provisions of this policy. The policies and procedures must be coordinated with and provided to DISA to ensure that they do not adversely affect network operation.

(INTENTIONALLY BLANK)

ENCLOSURE B

POLICY AND PROCEDURES FOR CONNECTION OF SPECIFIC EQUIPMENT TO THE DSN

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

2. General

a. Ancillary equipment may be connected to the DSN only if it does not negatively impact DSN GOS. New services or equipment cannot degrade overall network performance.

b. DISA provides the technical interface standards for equipment connected to the DSN . (See references m and y.)

c. Local commanders must coordinate with DISA prior to connecting new equipment to the DSN. Further, the Services are responsible for obtaining interoperability certification for all new or upgrade hardware and software prior to cutover in accordance with references e and f.

3. Secure Transmission with a STU-III/STE

a. The STU-III/STE 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 nonsecure telephone instrument to a STU-III/STE on DSN.

c. A STU-III/STE connected to DSN must have the preempt feature enabled at all times.

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

(1) The STU-III/STE preempt feature must be enabled at all times.

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

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 nonsecure facsimile traffic without a STU-III/STE 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 will follow procedures outlined in paragraph 3d.

6. Family of Off-line Cryptodevices (TSEC/KL-43). Use of TSEC/KL-43 cryptographic devices is authorized on DSN with the following conditions:

a. The KL-43 must be disconnected from the line immediately after transmission of each message and must not be connected while composing a message.

b. Receiving and transmitting terminals must be monitored during transmission, and any transmission exceeding 90 seconds should be interrupted and reestablished. The maximum 2000-character message should take only 66 seconds for transmission. If the subscriber line at either end is preempted during a KL-43 transmission, only the receiving KL-43 will give an audible signal and display a message that synchronization has been lost. The sending KL-43 will continue transmitting without any indication that the circuit has been preempted.

Therefore, the person monitoring the receiving end should notify the person at the sending end of preemption as soon as he or she discovers it.

7. VTC

a. The DSN provides connectivity to the DOD common-user teleconferencing system by providing a dial-up switched capability at the 56/64 Kbps rate and multiples thereof. User terminal equipment must have "tone disabling" capabilities not later than 1 October 2002 to facilitate DISA's phasing out of the special dedicated trunking for 56/64 Kbps services.

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 preemptable 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.

8. 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 support the A/NM of the DSN will be maintained as high interest circuits with the TSP of 1.

(INTENTIONALLY BLANK)

ENCLOSURE C

PROCEDURES FOR REQUESTING DSN SERVICE

1. Purpose. This enclosure provides procedures for requesting DSN service. The format contained in paragraph 4 is for precedence requests for DSN service. Other requests, such as switching changes or non-DOD customers, may be processed with unformatted memorandums or messages.

2. Applicability. These procedures apply to the Joint Staff, combatant commands, Services, and Defense agencies. All DSN service requests must be forwarded through the requestor's chain-of-command to the appropriate CINC or Service. Non-DOD-agency requests must be sponsored by a DOD component and forwarded through the Joint Staff to OSD(C3I) for final approval.

3. General

a. Requests for DSN service must be submitted in the format shown in paragraph 5. 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 DSN 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 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 combatant commands, Services, or Defense agencies have been coordinated with those affected.

(4) Requests for FLASH or FLASH OVERRIDE should be accompanied by a trade-off of equal precedence.

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

c. Requests from activities outside the Department of Defense must be sponsored by a DOD component and must be forwarded through the Joint Staff to OSD(C3I) for approval.

d. Requests for DSN STEP/Teleport access will be requested in accordance with this instruction using the GAR in reference mm.

4. Approval Authority. The level of the approval authority for DSN service requests is determined by the precedence requirement. (See Enclosure F). Requests must be validated at the level immediately below the approval level.

5. Request Format. The following message format must be used when requesting new or upgrades in DSN service. AUTODIN or DMS message format is acceptable during transition to DMS.

FROM: (Originating Activity)
TO: JOINT STAFF WASHINGTON DC//J6T//*
(*or activity with requisite approval authority)
INFO: DA WASHINGTON DC//SAIS-PAC-C// (as appropriate)
CNO WASHINGTON DC//N6K// (as appropriate)
HQ AFCIC WASHINGTON DC//SY// (as appropriate)
CMC WASHINGTON DC//CCT// (as appropriate)
DISA WASHINGTON DC//NS53// (required)
Validating authority, others (as required)

(If approval authority is below the Joint Staff level, information addressees will consist of affected commands or Services and Joint Staff/J6T. 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.

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, 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 or upgrade to current switch, validate interoperability certification or IATO issuance.

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. 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. 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. Combatant command, Service, or agency 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.)

ENCLOSURE D

POLICY FOR THE DEFENSE RED SWITCH NETWORK

1. Purpose. This enclosure provides general guidance, operational policy, and performance objectives for the DRSN. In addition, it describes required functions and MUFs of the DRSN.

2. General. The Department of Defense 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 and is the foundation for Defense global secure-voice services. 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, data, voice conferencing, and the ability to provide other value-added services to senior decision makers. These additional services include, but are not limited to, secure VTC, RED gateway functions for wireless and voice-over-Internet Protocol, 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) NCA (White House, Secretary of Defense, Chairman of the Joint Chiefs of Staff).

(2) NMCC.

(3) NMCC Site R.

(4) Airborne Command Post community.

(5) CINCs.

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

(7) Specially approved government departments and agencies (e.g.; Department of State).

(8) Allies of the United States.

b. The DRSN is the primary network for secure conferencing and is the host network for the WWSVCS conferees and the MILSTAR NCA Conferencing Network (MNCN) implemented under the Joint Staff-directed NCA Conferencing Enhancement Program. Other conferencing requirements are accommodated by the DRSN on a not-to-interfere basis. (See reference ff.)

c. The DISA GNOSC and RNOSCs 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. GNOSC and RNOSC roles in monitoring and situational awareness of connectivity to allies will be limited to the terms agreed upon in the memorandum of agreement/memorandum of understanding 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, preattack, and, to the maximum extent practical, transattack and postattack secure voice requirements. 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, 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. The DRSN system is used only for official business.

f. 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 Service and agency components supporting, using, or interfacing the DRSN must comply with DISA-promulgated guidance and the performance, interoperability, security, and capability requirements listed in this instruction.

3. General and 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, Preattack, and Theater Nonnuclear War. DRSN network capabilities must support all peacetime readiness (priority 3) users, plus surge requirements for nonnuclear war. These capabilities are handled according to established precedence.

(2) Postattack. 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 nonnuclear war.

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

(4) Early Transattack (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 assure 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 in accordance with 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 nonblocking 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.

c. Responsive Service. DRSN service must be responsive to the needs of C2 users. Under the current DRSN scheme, Special C2 FLASH and FLASH OVERRIDE users are provided nonblocking 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 Services and agencies, 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 CINCs, Services, and agencies should 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.

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/or interface by non-DOD 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.

g. NS/EP Compliant Service. DRSN 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 in accordance with FCC rules and regulations through the commercial telecommunications industry and the TSP (reference j). In OCONUS areas not under the control of the US Government, the Military Services and CINCs will provide NS/EP support where feasible and available through agreements with host governments and in accordance with TSP.

h. 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/nonsecure) 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.

i. 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 that 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.)

4. Objective Technical Parameters

a. Performance Objectives. See reference ee.

(1) DRSN Performance Objectives. The DRSN is designed to ensure that FOO-, FO-, and F-precedence call attempts by "directly connected" special C2 users will be completed on a nonblocking 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 nonblocking service from an inlet (line or trunk) to an idle outlet (line or trunk).

(2) DRSN 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 DRT and a score of at least 60 on the 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.

(3) DRSN 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, interswitch 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 intraswitch 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.

b. Security Features

(1) General

(a) DRSN RED switches must operate with physical security and TEMPEST compliance to allow users within a RED enclave to conduct unencrypted, 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.

(b) 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 PDS or link encryption between the RED enclave and the "exclusion" area. (See reference t.)

(c) All other connectivity into and out of the DRSN RED enclave must be secured with NSA-approved 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.

(2) Special DRSN security features include:

(a) ANI. During intraswitch and interswitch 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 are not permitted and constitutes a reportable security infraction.

(c) 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 class-marked 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 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 family of equipment.

1. FSAL. FSAL emphasizes call security over call completion. A user selects an FSAL-class-marked 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 class-marked 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 SAL. 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 in accordance with DRSN security guidelines.

5. DRSN Services and Applications. In addition to providing user-to-user dial-up service, the DRSN provides and supports a variety of secure services.

a. 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, ANDVT, STE, and evolving Condor (NSA secure wireless initiative) products. (See reference ee.)

(1) The DRSN supports both network and local-level ad hoc and preset conferences.

(a) 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).

(b) 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 class-marked users may also activate preset conferences by dialing the preset conference feature code followed by the assigned two-digit conference number.

(2) 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 NCA, NMCC, CINCs, and other users designated by the Joint Staff.

(3) SECN. The SECN is a special-purpose C2 conferencing network that uses DRSN conferencing capabilities and user-managed switch interfaces over the MILSTAR transmission media. It provides survivable secure-voice conferencing for the NCA, NMCC, CINCs, and other users designated by the Joint Staff.

b. 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:

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

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

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

(2) 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:

(a) STU-III. The DRSN will interoperate with STU-III users on the DSN, PSN, and FTS-2000/2001 (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-2000/2001 (and successors), and PSN. In some locations, connectivity is provided from the RED switches through STU-IIIRs directly to the DSN, FTS-2000/2001 (and successors), and PSN. STU-III users may not traverse the DRSN to call other STU-III users.

(b) STU-IIB/SY-71e. A limited number of DRSN RED switches interface with NATO and other allied systems. The predominate 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.

(c) STE. The DRSN interoperates with STE users on the DSN, PSN, and FTS-2000/2001 (and successors) through the DRSN single-channel STE interface or the multichannel CEU and will serve as the host for the "formal" conferencing bridge capability for STEs supporting the Department of Defense. Both incoming and outgoing STE direct-dialing capability is supported. STE users must use a STE that is keyed at the SECRET or higher level to complete a call through the single-channel or CEU interface 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 users on the DSN, FTS-2000/2001 (and successors), and PSN. In some locations, connectivity is provided from the RED switches through single-channel interfaces or the CEU directly to the DSN, FTS-2000/2001 (and successors), and PSN. STE users may not traverse the DRSN to call other STU-III or STE users.

(d) Condor. The DRSN interoperates with Condor (an NSA secure wireless initiative) users on the DSN, PSN, and FTS-2000/2001 (and successors) through the DRSN single-channel STE interface or the multichannel CEU when future narrowband digital terminal signaling is supported. Both incoming and outgoing Condor direct-dialing capability is supported. Condor users must use Condor equipment that is keyed at the SECRET or higher level to complete a call through the single-channel or CEU interface 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 Condor users on the DSN, FTS-2000/2001 (and successors), and PSN. In some locations, connectivity is provided from the RED switches through single-channel interfaces or the CEU directly to the DSN, FTS-2000/2001 (and successors), and PSN. Condor users may not traverse the DRSN to call other Condor, STU-III or STE users.

(e) ANDVT. The DRSN interfaces the ANDVT through either an analog or a digital interface. The ANDVT is employed with HF radio and narrowband 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).

(f) 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 must be handled by a designated DRSN attendant.

(g) VHF/UHF/SATCOM. Interface with VHF/UHF radio and SATCOM systems is provided through the KY-57/58 interface. Properly class-marked 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.

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

(i) 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. This system provides conferencing capability to a relatively small, but high-level, group of federal and DOD users.

(j) MILSTAR. 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.

(k) 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/Condor and MILSTAR interfaces are being added.

(l) JCSE Deployable RED Switch. The JCSE provides communications support for joint task force 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 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.

(m) 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.

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

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

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

6. Network Management. DISA establishes DRSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. As specified in reference n, the DRSN is under the operational direction and management control of the Director, DISA, and is responsive to the Chairman of the Joint Chiefs of Staff, the CINCs, 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 RNOSCs and to reconstitute a major DRSN nodal element in the event of a catastrophic failure.

7. 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 SCIFs. 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 switch interfaces 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 and STE 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 DPA, DTAs, 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 DPM. KIV-7HS's are sometimes used in lieu of the KG-81 family, but are not preferred because of rekey 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 OSD. 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 installations 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 <u>DISABLED</u> 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 the installation of DRSN service in quarters, the DISA DRSN service manager should be contacted for approval and confirmation of current applicable operating and security criteria.

8. Network Survivability Features

a. Network Design. Survivability features, such as dual and split homing, diverse and avoidance routing, automatic and semiautomatic restoral, and physical protection must be limited to high-priority functions and facilities with an established mission requirement for survivability, as determined by the CINC 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.

9. Cost Recovery. The total costs to the DWCF for managing, maintaining, and operating the DISA-managed (common) network portion of the DRSN are recovered through equitable billing of the Services. The methodology for determining the fair share allocation of these costs to the Services has been approved by the DISA RMC, and any changes to that methodology require RMC approval. DISA will bi-annually develop a program plan that provides POM guidance for the base or execution year and the next 5 years. After review by the Joint Staff, the program plan will be staffed with the Services by the RMC and approved for forwarding to OSD. OSD is the final approval/disapproval authority for the program plan.

10. Approval Terminology. The following terminology is used for actions in accordance with this policy. (See reference bb.)

a. 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 CINC, Service Chief, director of Defense agency, or head of other agency, or officials delegated this responsibility. Joint Staff validation-revalidation, when required will be in accordance with reference cc. Validation or revalidation of a requirement by itself does not guarantee funding unless the funding profile is included in the validation or revalidation process.

b. Approval. The official sanctioning necessary to permit implementation of a requirement. The level at which approval must be obtained will vary based on type of service required (see Enclosure F). Service approvals are not normally provided without identified funding.

c. Resolution. Forwarding of a requirement to the Joint Staff for action when the views of an activity are not in accordance with current policy.

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

a. Special C2 Users. A special class of user 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, preattack, and theater nonnuclear war secure telecommunications service for intelligence, alert, and strategic readiness. This 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 CINCs. Specifically, these special C2 users are identified through one or more Joint Staff, CINC, 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) CINC-validated minimum-essential circuits.

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

b. C2 Users. Users who have a requirement for secure C2 communications but do not meet the criteria for the class of “special C2 user.” C2 users include any person (irrespective of the position in the chain-of-command) who issues guidance or orders that direct, control, or coordinate any military forces regardless of the nature of the military mission (including combat support, administration, and logistics), whether said guidance or order is issued or effected during peace or wartime. C2 users are those users approved by the Joint Staff, CINC, Service, or agency identified in Enclosure F for PRIORITY and ROUTINE precedence origination.

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.”

12. 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 CINC, Service Chief, or director of Defense agency, who also approves requirements for I and P service. The Joint Staff is the approval authority for F, FO, and FOO (applicable only to WWSVCS) calling capabilities. CINCs, Service Chiefs, and directors of Defense agencies must review and revalidate F and FO calling capabilities annually.

b. Control of Precedence. The CINCs, 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 F identifies approval authority for DRSN service requests.

13. Administration. The CINCs, Service Chiefs, and directors of Defense agencies must develop implementing policies and procedures for the provisions of this policy.

(INTENTIONALLY BLANK)

ENCLOSURE E

PROCEDURES FOR REQUESTING DRSN SERVICE

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

2. Applicability. 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 CINC or Service. Non-DOD agency requests must be sponsored by a DOD component and forwarded through the Joint Staff to the OSD(C3I) for final approval.

3. General

a. Requests for DRSN service must be submitted in the format shown in paragraph 4. 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 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 in accordance with this instruction using the GAR in reference mm.

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

5. Request Format. The following message format must be used when requesting new or upgrades in DRSN service. AUTODIN or DMS message format is acceptable during transition to DMS.

FROM: (Originating Activity)
TO: JOINT STAFF WASHINGTON DC//J6T//*
(*or activity with requisite approval authority)
INFO: DA WASHINGTON DC//SAIS-PAC-C//
CNO WASHINGTON DC//N6K//
HQ USAF WASHINGTON DC//SCMN//
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 commands or Services and Joint Staff/J6T. DISA will be an information addressee on all requests.)

UNCLAS or appropriate classification
MSGID/GENADMIN/as appropriate per 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 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) 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. <u>Sources of funding must be identified as part of the validation process prior to final approval</u>.

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 F

PRECEDENCE APPROVAL AUTHORITIES

1. Purpose. This enclosure identifies the approval authorities for DSN and DRSN precedence.

2. Approval Authorities

		REQUEST ORIGINATOR				
		MIL SVS	U/S CMD	DOD AGENCY	NMCS J-STAFF	NON-DOD AGENCY
TYPE OF REQUEST	FLASH OVERRIDE	JS	JS	JS	JS	OSD
	FLASH	JS	JS	JS	JS	OSD
	IMMEDIATE	Serv.Ch.#	CINC	Agency #	JS	OSD
	PRIORITY	Serv.Ch.#	CINC	Agency #	JS	OSD
	ROUTINE	Local	Local	Local	Local	Local

LEGEND

JS	-	Joint Staff
CINC	-	Commander of combatant command
Serv.Ch.	-	Service Chief
Agency	-	Director of Defense agency
OSD	-	Office of the Secretary of Defense
Local	-	Local installation commander (see Enclosure A, paragraph 8 for more specific guidance)
#	-	OCONUS CINC approves requests in AOR

Note: Request approval may be granted only with identification of funding source and coordination with DISA.

(INTENTIONALLY BLANK)

ENCLOSURE G

RESPONSIBILITIES

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

2. Office of the Secretary of Defense

a. DSN

(1) Approves the biennial DSN program plan upon 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.

b. DRSN

(1) Approves the biennial DRSN program plan upon recommendation and consultation with the Chairman of the Joint Chiefs of Staff and after staffing by the DISA RMC.

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

3. Joint Staff

a. DSN

(1) Reviews the operational effectiveness of the DSN. The Joint Staff will report to OSD 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 CINC, 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) Ensures DSN meets applicable requirements of the NCS.

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

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

(9) Reviews and approves/disapproves all CINC-validated requests from OCONUS local commanders for Class B service.

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

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

b. <u>DRSN</u>

(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 F and FO DRSN service after validation by the CINC, 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, DISA

a. DSN

(1) Acts as the single system manager of DSN by providing operational direction and management control of DSN.

(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 ii):

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

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

(c) Switch 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) 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.

(6) 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.

(7) Recommends DSN performance objectives and establishes interface criteria in coordination with DOD components. Forwards to the Joint Staff for approval.

(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 F.

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

(11) Budgets and funds for DSN through the DWCF and publishes rates to recoup the DSN investment. This includes funding 30 percent of the O&M and upgrade costs for both hardware and software for MFSs.

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

(13) Reviews CINC, Service, and agency DSN switch hardware and software requests for proposal and contracts for compliance with configuration management and interoperability policy.

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

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

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

(17) Implements NM procedures as specified in Enclosure A, paragraph 9.

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

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

(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 are introduced into the DSN.

(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 CINCs/Services. Maintains a list of approved metropolitan calling areas and notifies CINCs/Services when biennial revalidation is required.

(25) Implements the controls necessary to limit DSN network access to that authorized in this instruction.

(26) Maintains a database of all CINC approvals for OCONUS Class B service. Notifies CINCs 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, reference z, to ensure standardization across the network.

b. DRSN

(1) Acts as the single system manager of DRSN by providing operational direction and 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 ff):

(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 and FLASH 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) Recommends DRSN performance objectives and establishes interface criteria in coordination with DOD components. Forwards to the Joint Staff for approval.

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

(10) 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 F.

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

(12) Produces, updates, and distributes the DRSN directory annually.

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

(14) Budgets and centrally manages funds for DRSN through the DWCF.

(15) Produces and updates the DRSN concept of operations and provides operational direction for all DRSN switching centers.

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

(17) Provides DRSN logistics information to the executive agency for logistics support.

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

5. The CINCs

a. DSN

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

(2) Forward approved DSN requirements, priorities, and precedence service to DISA and the supporting Service for implementation. The CINCs 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 customer premises equipment within facilities for which the CINC is operationally responsible.

(5) 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 evaluate 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 F.

(11) Participate as nonvoting 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 program management office 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.

b. <u>DRSN</u>

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

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

(3) Provide acquisition, operation, maintenance, and logistic requirements for customer premises equipment, including secure-voice instruments within facilities for which the CINC 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 F.

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

6. Service Chiefs and Directors of Defense Agencies

a. DSN

(1) Define, validate, coordinate, and approve requirements for DSN services in accordance with Enclosure F.

(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. Maintain switch hardware/software within three versions of DISA interoperability certified release.

(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 F.

(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.

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

(12) Ensure only those switches and software loads that have been certified as interoperable by JITC are introduced into the DSN.

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

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

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

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

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

(18) 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 in accordance with enclosure F.

(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 in accordance with Enclosure F.

(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.

7. Executive Agent, 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, CINCs, Services, and agencies.

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

a. Provides guidance for DRSN security issues.

b. Accredits all DOD DRSN facilities and switches that handle special compartmented information.

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

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

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

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

10. Administration. CINCs, Service Chiefs, and directors of Defense agencies will develop implementing policies and procedures for the provisions of their assigned responsibilities. These procedures will be coordinated with DISA to ensure they comply with overall DSN and DRSN network operations.

(INTENTIONALLY BLANK)

ENCLOSURE H

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 4630.5, 11 December 1992, "Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems"

f. CJCSI 6212.01B, 8 May 2000, "Interoperability and Supportability of National Security SystemsS and Information Technology Systems"

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

h. CJCSI 3222.01, 8 October 1993, "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 Videoteleconferencing (VTC) Management, Acquisition, and Standards"

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

m. DCAC 370-175-13, 5 April 1988, "Defense Switched Network (DSN) System Interface Criteria"

n. DODD 5105.19, 25 June 1991, "Defense Information Systems Agency (DISA)"

o. CJCSI 6740.01, 18 September 1996, "Military Telecommunications Agreements between the United States and Regional Defense Organization or Friendly Foreign Nations"

p. CJCSM 6231.04A, 29 February 2000, "Manual for Employing Joint Tactical Communications"

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

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

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

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

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

v. United States Code, Title 10 – Armed Forces

w. DODI 5200.40, 30 December 1997, "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)

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

y. DISA JIEO Technical Report 8249, March 1997, "Defense Information System Network (DISN) Circuit Switch Subsystem Defense Switched Network (DSN) Generic Switching Center Requirements (GSCR)"

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, 23 March 1994, "Department of Defense Dictionary of Military and Associated Terms" cc. CJCSI 5711.01A, 1 March 1999, “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 3420.01, 8 July 1996, “CJCS Conferencing Systems”

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

hh. CJCSI 6211.02A, 22 May 1996, “Defense Information Systems Network and Connected Systems”

ii. DISAC 310-70-85, 12 July 1995, “Defense Switched Network (DSN) Network Configuration Management Plan (NCMP)”

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

kk. Federal Standard 1037C, 1996, “Glossary of Telecommunication Terms”

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

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

nn. Joint Ethics Regulation, DOD 5500.7-R, Chapter 2, Second Amendment, 25 March 1996.

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

A/NM	administration/network management
ANDVT	advanced narrowband digital-voice terminal
ANI	automatic number identification
AOR	area of responsibility
APC	adaptive protective codingS
ARC	American Red Cross
ASA	automatic security authentication
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
AUTODIN	Automatic Digital Network
AUTOVON	Automatic Voice Network

C&A	certification and accreditation
CCB	configuration control board
CINC	commander in chief
C2	command and control
C3	command, control, and communications
C3I	command, control, communications and intelligence
CCSD	command communications service designator
CEU	channel encryption unit
CIO	Corporate Information Officer
CM	configuration management
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

DAA	designated approval authority
DAM	diagnostic acceptability measure
DCS	Defense Communications System
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISAC	Defense Information Systems Agency Circular
DISN	Defense Information System Network
DMS	Defense Messaging Service
DOD	Department of Defense
DPA	dual phone adapters
DPM	digital phone multiplexers
DRSN	Defense RED Switch Network

DRT	diagnostic rhyme test
DSN	Defense Switched Network
DTA	dual truck adapter
DWCF	Defense Working Capital Fund
EMSS	Enhanced Mobile Satellite Service
EO	End Office
EPC	Enhanced Pentagon Capability
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
GNOSC	Global Network Operations and Security Center
GOS	grade of service
GPS	General Purpose Segment
GSCR	Generic Switching Center Requirements
HEMP	high-altitude electromagnetic pulse
HF	high frequency
HMW	health, morale, and welfare
I	immediate
IATO	interim authority to operate
ISDN	Integrated Services Digital Network
IST	interswitch trunk
JCSE	Joint Communications Support Element
JIEO	Joint Information and Engineering Organization
JITC	Joint Interoperability Test Command
JTF	joint task force
JWICS	Joint Worldwide Intelligence Communications Systems
Kb	kilobits
LPC	linear predictive coding
MCA	maximum calling area
MFS	multifunction switch

MILSTAR	Military Strategic and Tactical Relay Satellite
MLPP	multilevel precedence and preemption
MNCN	MILSTAR NCA Conferencing Network
MTF	message text format
MUF	military-unique feature
NAF	nonappropriated fund
NAOC	National Airborne Operations Center
NATO	North Atlantic Treaty Organization
NCA	National Command Authorities
NCS	National Communications System
NGCS	NATO GPS
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
OCONUS	outside continental United States (CONUS)
O&M	operations and maintenance
OPLAN	operation plan
OSD	Office of the Secretary of Defense
P	priority
PABX	private automatic branch exchange
PAT	precedence access threshold
PBX	private branch exchange
PCM	pulse-code modulation
PDS	protected distribution system
PIN	personal identification number
PMO	program management office
POM	Program Objective Memorandum
PSN	public switched network
PTT	public telephone and telegraph
R	routine
RMC	Resource Management Committee
RNOSC	Regional Network Operations and Security Center
RSU	remote switching unit

SA	stand-alone
SAL	security access level
SATCOM	satellite communications
SCI	sensitive compartmented information
SCIF	SCI facility
SECN	Survivable Emergency Conferencing Network
SIPRNet	secret Internet Protocol router network
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
TRI-TAC	Tri-Services Tactical Communications
TSEC	Telecommunications Security
TSP	Telecommunications Service Priority
TS	TOP SECRET
UHF	ultrahigh frequency
UN	United Nations
VHF	very high frequency
VSAL	variable security access level
VTC	video teleconferencing
WWSVCS	Worldwide Secure Voice Conferencing System

PART II -- DEFINITIONS

area of responsibility (AOR). 1. The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. 2. In naval usage, a predefined area of enemy terrain for which supporting ships are responsible for covering by fire on known targets or targets of opportunity and by observation. 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. Note: ANI is used in message accounting. (See reference kk.)

avoidance routing. The assignment of a circuit path to avoid certain critical or trouble-prone circuit nodes. (See reference kk.)

backbone. 1. The high-traffic-density connectivity portion of any communications network. 2. 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 kk.)

CINC. Commander or designated staff element of one of the following unified commands: US Central Command, US European Command, US Joint Forces Command, US Pacific Command, US Southern Command, US Space Command, US Special Operations Command, US Strategic Command, and US Transportation Command. (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. 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. Also called C2. (See reference bb.)

communications security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Note: Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (See reference kk.)

computer security (COMPUSEC). 1. Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer. [NIS] *Synonym* automated information systems security. 2. The application of hardware, firmware, and software security features to a computer system in order to protect against, or prevent, the unauthorized disclosure, manipulation, deletion of information, or denial of service. (See reference kk.)

Condor. NSA's program to secure wireless communications.

configuration management. 1. [The] management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation of an automated information system, throughout the development and operational life of a system. 2. The control of changes -- including the recording thereof -- that are made to the hardware, software, firmware, and documentation throughout the system lifecycle. (See reference kk.)

continental United States. 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 reference kk.)

Defense Information Systems Network. 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. Also called DISN. (See reference bb.)

Defense Switched Network (DSN). A component of the Defense Communications System 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 kk.)

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. [FS1037] End offices are an integral part of the DSN. EO switches provide users with switched call connections and all DSN service features, including MLPP. The EO provides long-distance service by interconnecting with DSN nodal switches. The EO does not service as a tandem in the DSN but may connect to other EOs where direct traffic volume requires, such as in a metropolitan calling area.

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 originate or terminate 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 switched long-distance telecommunications service formerly provided for official federal government use. Note: FTS has been replaced by Federal Telecommunications Service 2000 (FTS 2000) and Federal Telecommunications Service 2001 (FTS 2001).

Federal Telecommunications Service 2000 (FTS 2000). A long-distance telecommunications service, including services such as switched-voice service for voice or data up to 4.8 kb/s, switched data at 56 kb/s and 64 kb/s, switched digital integrated service for voice, data, image, and video up to 1.544 Mb/s, packet-switched service for data in packet form, video transmission for both compressed and wideband video, and dedicated point-to-point private line for voice and data. Note: Use of FTS 2000 contract services is mandatory for use by US Government agencies for all acquisitions subject to 40 USC 759. No US Government information processing equipment or customer premises equipment other than that required to provide an FTS 2000 service are furnished. FTS 2000 contractors will be required to provide service directly to an agency's terminal equipment interface. For example, the FTS 2000 contractor might provide a terminal adapter to an agency location in order to connect FTS 2000 ISDN services to the agency's terminal equipment. GSA awarded two 10-year, fixed-price contracts covering FTS 2000 services on 7 December 1988. The Warner Amendment excludes the mandatory use of FTS 2000 in instances related to maximum security. (See reference kk.)

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.)

grade of service (GOS). 1. The probability of a call being blocked or delayed more than a specified interval, expressed as a decimal fraction. Note: GOS may be applied to the busy hour or to some other specified period or set of traffic conditions. GOS may be viewed independently from the perspective of incoming versus outgoing calls and is not necessarily equal in each direction. 2. In telephony, the quality of service for which a circuit is designed or conditioned to provide; e.g., voice grade or program grade. Note: 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 also. (See reference kk.)

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.)

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. Note: ISDN services include telephone, data, electronic mail, and facsimile. The method used to accomplish a connection is often specified; for example, switched connection, nonswitched connection, exchange connection, and ISDN connection. (See reference kk.)

Joint Staff. 1. The staff under the Chairman of the Joint Chiefs of Staff as provided for in the National Security Act of 1947, as amended by the Goldwater-Nichols Department of Defense Reorganization Act of 1986.

The Joint Staff assists the Chairman and, subject to the authority, direction, and control of the Chairman, the other members of the Joint Chiefs of Staff and the Vice Chairman in carrying out their responsibilities. 2. The staff of a commander of a unified or specified command, subordinate unified command, joint task force, or subordinate functional component (when a functional component command will employ forces from more than one Military Department), which includes members from the several Services comprising the force. These members should be assigned in such a manner as to ensure that the commander understands the tactics, techniques, capabilities, needs, and limitations of the component parts of the force. Positions on the staff should be divided so that Service representation and influence generally reflect the Service composition of the force. (See reference bb.)

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. (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 kk.)

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 kk.)

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; and (d) in which the precedence level of a call outside the predefined domain is usually not recognized. (See reference kk.)

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). 1. 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 Executive Agent, the NCS Committee of Principals, and the Manager. 2. 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 kk.)

network management. 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: Network management does not include user terminal equipment. (See reference kk.)

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 interconnnected to the DSN A/NM subsystem. The two types of nodal switches in the DSN are:

1. stand-alone switch (SA). The SA functions solely as a tandem switch in the DSN.

2. 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.)

off-hook. 1. 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. 2. One of two possible signaling states, such as tone or no tone and ground connection versus battery connection. Note: If off-hook pertains to one state, on-hook pertains to the other. 3. The active state, i.e., closed loop, of a subscriber or PBX user loop. 4. 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, and FLASH.

1. ROUTINE. Precedence designation applied to those official government communications that require rapid transmission by telephonic means but do not require preferential handling.

2. PRIORITY. Precedence reserved generally for telephone calls requiring expeditious action by called parties and/or furnishing essential information for the conduct of government operations.

3. IMMEDIATE. Precedence reserved generally for telephone calls pertaining to: a. situations that gravely affect the security of national and allied forces; b. reconstitution of forces in a postattack period; c. intelligence essential to national security; d. conduct of diplomatic negotiations to reduce or limit the threat of war; e. implementation of federal government actions essential to national survival; f. situations that gravely affect the internal security of the United States; g. Civil Defense actions concerning US population and; h. disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population; and i. vital information having an immediate effect on aircraft, spacecraft, or missile operations.

4. FLASH. Precedence reserved generally for telephone calls pertaining to: a. command and control of military forces essential to defense and retaliation; b. critical intelligence essential to national survival; c. conduct of diplomatic negotiations critical to the arresting or limiting of hostilities; d. dissemination of critical civil alert information essential to national survival; e. continuity of federal government functions essential to national survival; f. fulfillment of critical US internal security functions essential to national survival; and g. catastrophic events of national or international significance.

5. FLASH OVERRIDE. A 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. USCINCNORAD when declaring either Defense Condition One or Air Defense Emergency and other national authorities the President may authorize. FLASH OVERRIDE cannot be preempted in the DSN.

6. FLASH OVERRIDE 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; and c. CINCNORAD 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 conferences. FLASH OVERRIDE OVERRIDE cannot be preempted.

preemption. The seizure -- usually automatic -- of military system facilities that are being used to serve a lower precedence call in order to serve immediately a higher precedence call. (See reference kk.)

private branch exchange (PBX). 1. A subscriber-owned telecommunications exchange that usually includes access to the public switched network. 2. A switch that serves a selected group of users and is subordinate to a switch at a higher level military establishment. 3. 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. A private automatic branch exchange (PABX) may or may not have a switchboard. Use of the term "PBX" is far more common than "PABX," regardless of automation. (See reference kk.)

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. Note: A complete PDS includes the subscriber and terminal equipment and the interconnecting lines. (See reference kk.)

public switched network (PSN). 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 kk.)

pulse-code modulation (PCM). Modulation in which a signal is sampled, and the magnitude (with respect to a fixed reference) of each sample is quantized and digitized for transmission over a common transmission medium. Note: In conventional PCM, before being digitized, the analog data may be processed (compressed), but once digitized, the PCM signal is not subject to further processing (digital compaction) before being multiplexed into the aggregate data stream. PCM pulse trains may be interleaved with pulse trains from other channels. (See reference kk.)

satellite communications (SATCOM). A telecommunications service provided via one or more satellite relays and their associated uplinks and downlinks. (See reference kk.)

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 a terminal facility to more than one switching center by separate access lines, each of which has a separate directory number. (See reference kk.)

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. Note: Tactical communications do not include communications provided to tactical forces by the DCS, to nontactical military commands and to tactical forces by civil organizations. (See reference kk.)

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 kk.)

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 kk.)

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 kk.)

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 crypt**o**-analysis. (See reference kk.)

TRI-TAC. Acronym for tri-services tactical. See tactical communications. (See reference kk.)

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 kk.)

ultrahigh frequency (UHF). Frequencies from 300 MHz to 3000 MHz. (See reference kk.)

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 kk.)