



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J6

DISTRIBUTION: A,B,C,J,S

CJCSI 6215.01
1 February 1995

POLICY FOR THE DEFENSE SWITCHED NETWORK

References: See Enclosure H

1. Purpose. This instruction establishes policy and prescribes responsibilities for use and operation of the Defense Switched Network (DSN)/Defense Red Switch Network (DRSN).
2. Cancellation. CJCS MOP 8, 13 February 1990, 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 governmental, and civilian organization requests for DSN support. Requests for waivers to this instruction will be forwarded by chain of command, including CINC, Service, or Defense agency, to the Joint Staff, stating the reason compliance is not possible.
4. Policy
 - a. As approved by OSD, the DSN is an interbase telecommunications system that provides end-to-end common user and dedicated telephone service, voice-band data, and dial-up VTC for the Department of Defense. The DSN is the switched circuit telecommunications system of the DISN. It provides switched dial-up secure and nonsecure voice, voice-band data, and video services to authorized users throughout the Department of Defense in accordance with national security directives. The principal requirement and reason for the system's design is the nonsecure dial-up voice (telephone) user.

b. The DISN is an integrated network, centrally managed and configured, to provide telecommunication services for all DOD activities. This information transfer service is designed to provide dedicated point-to-point and switched voice, data, imagery, and video teleconferencing services in support of national defense C3I decision support requirements and Corporate Information Management (CIM) functional business areas.

c. Although the DISN is in its formative stages, there are fully mature elements, such as the DSN and Joint Worldwide Intelligence Communications System, that are currently operational. Upon full operational capability, the DISN will provide the global long-haul information transfer infrastructure by integrating separate CINC, Service, and Defense agency networks into a DOD long-haul system to meet common-user and special-purpose information transfer requirements.

d. Secure voice service is provided by the Defense Red Switch Network, a separate secure switched network that is considered part of the DSN, and the STU-III/STE family of equipment that provides end-to-end encryption over nonsecure DSN circuits. The DSN incorporates and uses telecommunications equipment, software, and services acquired through telecommunications acquisition programs.

e. The DSN is under the operational direction and management control of the Director, DISA. As the single systems manager, the Director, DISA, will be responsive to the Chairman of the Joint Chiefs of Staff, CINCs, Military Departments, and Defense agencies.

5. Scope. This instruction outlines the military operational requirements for the DSN and provides operational policy and performance objectives. CJCSI 6215.01 also describes the DSN and its services and the procedures for requesting services, approvals, or waivers. Responsibilities for network management and DOD components are also described herein.

6. Responsibilities. See Enclosure D.

7. Procedures. Detailed procedures for the DSN are outlined in Enclosures A through H.

8. Summary of Changes. In addition to administrative changes, the instruction clarifies several areas related to network

management, network interfaces, and approval authority for telephone precedence.

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

For the Chairman of the Joint Chiefs of Staff:

\Signature\
CHARLES T. ROBERTSON, JR.
Major General, USAF
Vice Director, Joint Staff

Enclosures:

A-DSN Operational Policy
B-Policy for Nonsecure Voice Communications
C-Policy for the Defense Red Switch Network
D-Responsibilities
E-Policy and Procedures for Connection of Specific
Equipment to the DSN
F-Precedence Approval Authorities
G-Procedures for Requesting DSN Service
H-References

Glossary

(INTENTIONALLY BLANK)

DISTRIBUTION

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

	<u>Copies</u>
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

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for CJCSI 6215.01. Use this list to verify the currency and completeness of the document. An "0" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 4	0	E-1 thru E-4	0
i thru vi	0	F-1 thru F-2	0
A-1 thru A-18	0	G-1 thru G-4	0
B-1 thru B-4	0	H-1 thru H-2	0
C-1 thru C-2	0	GL-1 thru GL-8	0
D-1 thru D-8	0		

(INTENTIONALLY BLANK)

(INTENTIONALLY BLANK)

ENCLOSURE A

DSN OPERATIONAL POLICY

1. Purpose. This enclosure provides general guidance, operational policy, and performance objectives for the DSN.
2. General
 - a. The DSN will provide rapid, reliable, survivable, secure, and economic telecommunications for C2 users to ensure effective C2. For reasons of economy, the DSN will also provide service to lower priority users on a noninterference basis.
 - b. The user terminal end of the DSN is the long-distance termination equipment of the EO switch. The portions of MFSs and the portions of EO switches that are part of the DSN will operate under DISA's operational management for the day-to-day operations and configuration management (CM).
 - c. The DSN system will be used only for official business or in the interest of the government and will be the first choice for all new and existing switched voice telecommunications requirements.
3. Nonsecure Voice. DSN will primarily provide nonsecure dial-up voice service. Enclosures B, D, E, F, and G outline usage policy and procedures to obtain service for switched voice nonsecure DSN users.
4. Secure Voice System. The SVS elements of the DSN will provide secure voice to authorized users in accordance with national security directives. The SVS includes the DRSN, C2 conferencing, general purpose conferencing, and the STU-III/STE family of equipment. Red Switches for the NMCC, NMCC Site R, and the primary command centers at the combatant commands along with other locations are included in the DRSN. Enclosures C through G outline policy and procedures to be used for all Red Switch actions that affect the DRSN.
5. Commercial-Leased Telecommunications. DSN will use commercial-leased telecommunications services where C2 capable, cost-effective or mission-essential requirements dictate this means. Use of commercial-leased telecommunications in overseas areas will be negotiated country by country by DISA, in coordination with the appropriate CINC and O&M commands.

6. General and Military-Unique Requirements. The DSN will adhere to the following capability objectives to ensure its ability to support effective military C2 functions.

a. Survivable Service. DSN will support C2 user traffic during peacetime, crisis, conflict, natural disaster, network disruptions, and will possess the robustness to provide a surge capability when needed. DSN priorities, in order, by stress levels are:

(1) 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.

(2) Postattack. In CONUS, DSN will possess the capability to reconstitute itself from segments of the DSN surviving a conventional or a nuclear war to support the National Communications System in reconstituting national communications. Overseas, DSN will possess the same capabilities to support the NCS after a nonnuclear war.

(3) Peacetime Readiness. DSN will support C2 and other users.

(4) Early Transattack (few weapons, possibly HEMP). DSN will support C2 user traffic as able. HEMP protection will be consistent with reference j.

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

b. Assured Connectivity. DSN will provide rapid, reliable, and available service to C2 users. Assured service or connectivity is the ability for 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 military unique feature (MUF), the multilevel precedence and preemption (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) will be provided with nonblocking service (P0.00) from user to user.

Assured service capability will ensure the connectivity from user instrument to user instrument across the DSN, supporting government-controlled private branch exchanges, EOs, overseas DSN as well as integrating into tactical networks that incorporate MLPP features.

c. Responsive Service. The DSN will provide rapid, responsive, reliable, and assured service to C2 users. Special C2 users (under current DSN MLPP scheme--FLASH and FLASH OVERRIDE) will be provided nonblocking service.

d. Surge Capacity. The DSN design will be able to provide a 25-percent increase in capacity to respond to military operations or emergencies.

e. Secure Service. DSN will permit, by secure instruments or switches, protection of classified and sensitive information being passed to ensure its confidentiality, integrity, availability, authentication, as well as protection from attacks on the system that would result in denial of service. DSN will provide transmission support, switching support, and network management for SVSs.

f. Cost-Effective Service. In compliance with OSD direction, DSN will provide network flexibility to exploit new technology, tariffs, and commercially available resources. DSN will provide integrated voice, data, and video services to use resources effectively. DSN will evolve incrementally to meet objectives as opportunities occur to fund technological upgrading and service growth. DSN funding including investments, programmatic initiatives, and operating budget will be DBOF funded. DSN will include only those capabilities that are cost effective for each DOD user individually or to the Department of Defense in general. DSN will be programmatically and financially divided as required to accommodate necessary funding and management arrangements. DSN capital investment costs will be funded equitably. Recurring costs will be based on usage; the Military Departments, DOD components, and all other authorized users will budget and pay for service usage of the DSN. In addition, specifically identified metropolitan calling areas may be established, if requested by the Services, to appropriately allocate telecommunications costs to the users. The OCONUS CINCs may approve specific metropolitan calling areas. DISA assessment of impact will be considered and the Joint Staff notified. No blanket approvals will be made. All approvals will be revalidated at least every 2 years. The Joint Staff will be

the approval authority for all CONUS metropolitan calling areas.

g. Interoperable Service. DSN will be designed with the capability to permit interconnection and interoperation with similar tactical, Federal Government, allied, and commercial networks.

h. National Security and Emergency Preparedness Compliant Service. DSN will comply with the requirements, priorities, and procedures established by the NCS regarding NS/EP. In the United States and its territories, NS/EP support will be provided in accordance with FCC rules and regulations through the commercial telecommunications industry and the TSP. In OCONUS areas not under the control of the US Government, NS/EP support will be provided by the Military Services and CINCs where feasible and available through agreements with host governments and in accordance with TSP.

7. Objective Technical Parameters and Special Functions

a. Network Performance Objectives. Network performance objectives will be recommended by DISA in coordination with the CINCs and Chiefs of the Services, validated by the Joint Staff, and approved by OSD to provide DSN services to satisfy the DSN system objectives or reduce costs. These performance objectives will 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 P0.07 (7 calls out of 100 will be "blocked" during the "busy hour") or better and an intertheater GOS of P0.09 or better. DISA will report to the Joint Staff and respective CINCs those network access points (EOs and MFSS) that do not meet the following performance standards:

(1) GOS service criteria for intertheater of P0.09.

(2) Theater objective of P0.07. OCONUS CINCs may waive specific theater EO ROUTINE GOS implementations. DISA assessment of network impact will be considered and the Joint Staff notified. Concurrence is required from all affected components serviced by that EO switch. No blanket waivers will be approved. All waivers will be revalidated at least every 2 years.

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

(4) The inability to reach the above target grade of service criterion because of economic or operational reasons.

b. The DRSN, although measured separately, will meet the DSN performance standards above.

c. VTC, data, and other switched system application performance objectives, will be identified by their respective operational documents.

8. Network and Applications. In addition to secure and nonsecure dial-up service, DSN provides and supports a variety of systems, and programs and other applications:

a. Switched Data. The DSN will provide dial-up switched 56KBS digital transmission services and, when possible, 64KBS paths under the Narrowband ISDN protocol. This feature will provide the improved capability for the DSN to support video transmission, bulk data transfer, and other switched data transmission requirements. DISA will provide network standards, network management, transmission, and switching services. Users are responsible for procurement and operation and maintenance of their customer premise equipment using the DSN transmission facilities. Network transmission will provide full interoperability for all users.

b. Data. The primary means of passing data over the DISN are the packet-switched networks. However, DSN will augment DISN packet-switched data networks, as required, by providing supplementary transmission backbone access where there are no DISN data services. These data services will conform to the guidelines outlined in Enclosure E for connection to the DSN.

c. Defense Message System (DMS). The DMS consists of all hardware, software, procedures, facilities, and personnel used to exchange messages electronically between organizations and individuals of the Department of Defense. The current baseline of the DMS consists of AUTODIN as well as the DDN. The DISN systems, to include the DSN, provide transport services as part of the DISN. Reference i outlines policy and guidance for the DMS. DSN will provide a transmission restoral capability for DMS.

d. Video Teleconferencing. DSN will provide switched services connectivity for the DOD common user video

teleconferencing system. The DSN will also provide switched data circuit connectivity in support of user VTC long-haul transmission requirements. VTC programs and requirements are outlined in a separate CJCSI. Guidelines outlined in Enclosure E of this document also apply to the VTC services.

9. Network Interfaces. Interfaces to the DSN will comply with the DSN interface criteria established by DISA. 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 way to control the flow of traffic across the interface will be established and monitored by DISA. DSN will support the following network interfaces:

a. NATO's Initial Voice Switched Network. DSN will interoperate with the IVSN. The IVSN-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.

b. Commercial Telephone Networks or Public Switched Networks

(1) Automatic interconnection will not be allowed between either an incoming long-distance DSN call and the local commercial system (off-netting) or an incoming call from a commercial system and the DSN (on-netting) except as authorized in subparagraph 9b(4) below.

(2) 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. The combatant commands, Military Services, and Defense agencies are responsible for preventing abuse of this capability.

(3) Automatic interconnections to the private or public switched networks for local subscribers may be provided for local calls by the controlling authority by an EO switch or PBX (often identified as dial 9 service). Enhanced call completion features such as call-forwarding, call-waiting, etc., may be implemented if deemed appropriate in the local area for local calls if mission essential. These features will in no way diminish the assured service connectivity from user to user. Military Services and Defense agencies are responsible for any connection and usage charges to public networks. Particular care will be taken to make

sure that this capability does not allow automatic on- or off-netting of long-distance DSN or commercial calls.

(4) Automatic interconnection to the DSN may be permitted on a case by case basis, providing that the below listed criterion are met. Details of the scheme must be staffed with DISA for a technical evaluation and forwarded to the Joint Staff for approval. All automated interfaces to the DSN will have as a minimum:

(a) Positive identification of all users and access through some means such as personal identification numbers (PIN). If PINs are used, only one individual will be permitted to use an assigned PIN. There will be no blanket issuance of access means or PINs to a class of users.

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

(c) A means of identifying all calls made through the automated interconnection. All calls will be verified by the user on a periodic basis.

(d) A means of identifying costs of all calls for appropriate billing of users.

(e) No automatic interconnection is made for the purpose of using the DSN to conduct unofficial business.

c. Tactical. The DSN will connect with tactical communications systems by a standard tactical entry points (STEP). The STEP will provide technical features to permit tactical communications systems to interoperate with the DSN. DISA will maintain standards for STEP facilities.

d. National Communications System (NCS). In the United States, the NCS will use the DSN and other switched systems to carry the traffic of National Security and Emergency Preparedness (NS/EP) users. Postattack recovery and reconstitution of Federal agencies in CONUS will center

around 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.

10. 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:

a. Health, Morale, and Welfare (HMW). DSN may be used to place HMW calls from or to OCONUS isolated or remote geographic locations because of nonavailability of acceptable commercial services. CINCs will establish policy for authorization, control, and duration of HMW calls to be compatible with operational requirements, local restrictions, and host-nation laws or agreements. The following conditions apply to HMW use of DSN:

(1) Calls may be placed only through the local installation operator or, in the absence of an installation operator, from a telephone under a commander's supervision to ensure compliance with the controls described below.

(2) 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.

(3) Calls must be placed only at the ROUTINE precedence and normally should not exceed 15 minutes. Off-netting at the distant end is at the discretion of local commanders, who are encouraged to permit HMW calls. 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 toll charge may be placed if the called party agrees to accept the charges on a collect-call basis or some other arrangement (i.e., credit card).

b. 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 or for circumstances specifically authorized by a CINC, Chief of a Service, or director of a Defense agency.

c. Control. CINCs will establish procedures for the positive control of on- and off-net access for EOs within their AOR. Chiefs of the Services 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 responsibility.

11. Network Management. DISA will establish DSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. As specified in reference b, the DSN is under the operational direction and management control of the Director, DISA, and will be responsive to the Chairman of the Joint Chiefs of Staff, the CINCs, the Military Departments, and Defense agencies and activities.

a. DISA will possess read access capabilities to all switch data base tables excluding those tables associated with non-DISA controlled networks.

b. DISA will maintain a CM data base of all switch configurations and provide access to agencies, activities, and Military Departments as authorized by the ASD(C3I), the Director DISA, and the Joint Staff.

c. DISA will have the ability to implement network control commands to all DSN switches. DISA will attempt to notify O&M activities before implementing network controls. In OCONUS areas of operations, the theater CINC or commander may direct additional access as required to meet theater operational needs.

d. During emergencies, DISA will have the authority to implement switch data base revisions that are required for operation and management of the DSN.

e. DISA will review and update, as appropriate, biennially, the following DSN documents:

(1) DSN Program Plan (including the worldwide DSN Topology).

(2) Worldwide Operational Policy for Single System Management (SSM).

(3) Network Configuration Management Plan.

(4) DSN Security Guide.

- (5) DSN Classification Guide.
- (6) DSN System Interface Criteria.
- (7) Generic Switching Requirement (EO).
- (8) Generic Switching Requirement (MFS).
- (9) Test and Evaluation Master Plan.
- (10) Joint Integrated Logistic Support Plan.
- (11) Worldwide Numbering and Dialing Plan.

f. DISA will produce, update, and distribute the DSN Directory annually.

12. Network Security

a. The design and operation of DSN will maximize protection of switches, transmission links, and network management 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 will be applied to provide COMPUSEC, COMSEC, physical, and personnel security protection.

b. Physical security will be afforded secure voice terminals, keying material, switching facilities, and management control links in accordance with references c and i, and applicable Service publications. Special provisions applicable to facilities used for transmission of SCI are contained in reference a and applicable DISA and Service publications.

c. A DRSN telephone will be considered self-authenticating to the level of classification displayed on the instrument. It will not connect unclassified terminals.

d. The STU-III family of instruments is self-authenticating to the level of classification displayed on the instrument. When STU-III 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.

13. 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 will 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 will ensure the survivability features are incorporated into the design and configuration of the DSN.

b. Vulnerability Analysis. DISA, in coordination with DIA and NSA, will be responsible to initiate and provide technical analysis of network survivability to include a risk analysis every 2 years or when proposing major changes in the network topology. The analysis will report on the survivability and vulnerability of the DSN and will be forwarded to the Joint Staff for review.

14. DSN Switches and Terminal Equipment

a. DSN Nodal and EO Switches. These switch types are integral parts of the DSN and provide the switching subsystem for the DSN backbone. DISA's DSN management responsibilities include:

- (1) The stand-alone nodal switch.
- (2) The nodal switch function of the multifunction switch.
- (3) All connectivity between nodal switches, EO switches and nodal switches, and EO switches with other EO switches.

b. C2 and NM capabilities. The DSN nodal switch and the EO switch will contain the necessary features to satisfy C2 requirements and will be supervised by and interconnected to the DISA network management subsystem. The user terminal end of DSN is currently the long-distance termination in the EO switch. DISA system management responsibilities extend throughout the network to the long-distance terminations in the EO. DISA, as the single system manager of DSN, is responsible for ensuring special C2 user service and will establish criteria for handling special C2 calls down to the end instrument. The O&M command is responsible for

providing all C2 user service from the EO to the instrument in accordance with DSN performance objectives and abuse control procedures. Executive override, preemption call waiting, or any similar EO or PBX special feature will 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 will be interrupted if the attendant determines the precedence of the incoming call is higher than the one in progress. If a precedence call is forwarded to an alternate number, that number will be preemptable.

c. PBX, PABX, and RSU. Service changes or enhancements to DSN switches will be coordinated with DISA for network impact assessments. Any PBX and PABX will be connected to, and served by, an EO or the EO portion of the nodal switch. The PBX, PABX, and RSU are considered customer premise equipment and are not part of DSN; however, they must meet DSN interface standards.

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

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

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

(b) PBXs with precedence terminating service through an EO attendant will not have executive override, preemption call waiting, or other features enabled that will inhibit preemption or a precedence call.

(3) DISA will design the network topology (MFS, EO) of the DSN (i.e., where to connect PBXs into the DSN) and publish it in the DSN Transition Implementation Plan. The Services or Defense agencies will coordinate recommendations with DISA (and the CINC concerned if OCONUS) for switch designation or redesignation. DISA will evaluate and engineer changes or redesign. Inter-Service agreements will be used to allocate PBX to EO

support costs, and the Joint Staff will resolve differences.

(4) At all PBX locations that are capable of implementing MLPP access line interfaces, at least one access line will be conditioned to incoming preemption or must have EO operator intercept precedence calls.

(5) PBX will meet grade of service objectives for the network.

d. DRSN The Red Switches will provide high-quality, secure voice service and will interconnect other secure networks to critical command, control, and intelligence users within single secure perimeters (Red enclaves). Red Switches also will provide high quality conferencing capability for crisis management communications. The DRSN will contain the necessary features to satisfy C2 requirements. Connectivity, transmission, and network management for the DRSN will be supported by the DSN. DISA will provide an interface to the nonsecure DSN voice dial-up network for Red Switch to STU-III calls requiring that connectivity. The DRSN was not designed to tandem calls between STU-III instruments.

e. 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.

f. Customer Premises Equipment. Nonsecure and secure telephones, STU-III 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 will be responsible for establishing interface standards, ensuring interoperability, and establishing procedures to minimize the impact of the terminal equipment on the network.

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

15. Cost Recovery

a. DSN procurement, administration, operation and maintenance, and network management costs funded through the DBOF will be recovered by charging subscribers for the cost of providing service based on predetermined subscriber rates.

b. DISA will establish DSN subscriber rates for nonsecure services based on usage. In developing rates, DISA will consider such factors as calling distance or area, precedence level, type of service, usage, and special features.

16. Approval Terminology. The following terminology will be used for actions in accordance with this policy:

a. Validation. The confirmation and declaration by competent higher authority that a requirement is justified. Requirements of a requesting agency are validated by the applicable CINC, Chief of the Service, director of the Defense agency, or head of an agency, respectively, or officials delegated this responsibility. Joint Staff validation, when required, will be in accordance with reference h. Validation of a requirement by itself does not guarantee funding unless the funding profile is included in the validation 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 and SVS requirements. New requirements for which funds have not been previously programmed require coordination with the Chief of the Military Service designated to provide funding.

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. 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.

17. 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 crisis, 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 and other members of the Joint Chiefs of Staff, Chiefs of the Services, and the CINCs. Specifically, these special C2 users are identified through one or more Joint Staff, CINC, Service, or DOD agency validation processes. They are all DRSN subscribers as are the following identified subscribers of common user networks:

- (1) Joint Staff-approved FLASH, FLASH OVERRIDE, or, IMMEDIATE precedence origination capability.
- (2) CINC-validated minimum essential circuits.
- (3) CINC- or Service-approved IMMEDIATE and PRIORITY precedence origination capability.

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 peace or wartime. C2 users are identified as users of Joint Staff, CINC-, Service-, and agency-approved PRIORITY and ROUTINE precedence origination capability.

c. Other Users. Users who have a requirement to use the DSN for national security purposes but who do not meet the criteria for the classes of "Special C2 users" or "C2 users." These users will be granted only ROUTINE access when it is not in conflict with local PTT ordinances and they may be denied access during contingency or crisis. Included in this class are non-DOD, nongovernmental, and foreign government users of OSD- or Joint Staff-approved capability.

18. Precedence levels

a. Assignment of Precedence Levels. Access to a level of precedence will be determined only by mission requirements and will not be used as a means of improving a grade of service 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 will be validated by the appropriate CINC, Chief of the Service, or director of the Defense agency, who will also approve requirements for IMMEDIATE and PRIORITY service. Requests for precedence are not restricted by Maximum Calling Area (MCA). Connectivity is available to provide long-distance service if that service is requested (budgeted and funded). 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 will normally be accompanied by a tradeoff of equal precedence.

b. Control of Precedence. The CINCs, Chiefs of the Services, and directors of Defense agencies will establish policy to control use of precedence access through operator-assisted calls. EO users 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., Classmarks, or Precedence Access Threshold tables). DISA will provide criteria for the EO 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.

c. Temporary Precedence Upgrades. Temporary DSN service upgrading to support the NCA, Chairman of the Joint Chiefs of Staff, CINCs; Chiefs of the Services, or other equivalent personnel during travel is authorized for all precedence for up to 30 days. Temporary upgrading is also authorized for emergencies and exercises. Requests should follow the procedures in Enclosure G and will be coordinated with DISA and approved by the CINC or Chief of the Service concerned. Approvals of FLASH OVERRIDE and FLASH access will be provided to DISA and the Joint Staff. The approval will

indicate if a cost will be incurred for implementation and the source of funds.

d. Enclosure F identifies approval authority for DSN and DRSN service requests.

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

(INTENTIONALLY BLANK)

ENCLOSURE B

POLICY FOR NONSECURE VOICE COMMUNICATIONS

1. Purpose. This enclosure provides operational policy for the nonsecure voice.

2. General

a. Use of the DSN is restricted to the official business of the US Government.

b. DSN is the official DOD switched voice network and will be the preferred communications means for the special C2 and C2 user. It is the primary secure (STU-III family) communications means for nontactical C2 users. DSN must be the user's first choice; however, if DSN cannot be used in a timely manner or if the called party does not have access to DSN service, other long-distance calling means may be used.

c. Non-DOD activities may be granted access to the network by the Department of Defense when necessary for national security and when not in conflict with local PTT ordinances of those activities and individuals who have critical NS/EP needs and are unable to use a commercial system. If access is approved, DSN services will be 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). Requests by non-DOD users should be satisfied by available commercial service or FTS-2000 if the use is clearly not associated with the military mission of the Department of Defense. DOD policy is that under no circumstances will access to DSN be granted simply as a cost-effective measure to substitute for available commercial service. Requirements of non-DOD or nongovernmental activities or agencies (e.g., Department of Justice, State government organizations, DOD contractors, labor unions, foreign embassies) are referred to OSD for approval with a recommendation by the Joint Staff except as provided in paragraph 3 below.

3. Contractors

a. DSN may be used by US civilian contractor personnel in overseas areas when they are performing duties normally performed by DOD civilian or military personnel. DSN access may be given to contractors in CONUS if their mission supports deployed DOD forces. DSN access may be provided to

a foreign national contractor when validated by the appropriate CINC, Chief of a Service, 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.

b. DSN may be used by contractor personnel within CONUS when performing a mission normally performed by DOD civilian or military personnel, subject to the following:

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

(2) 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) will 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 will be approved by the CINC, Service, or Defense agency.

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

c. The requesting CINC, Chief of the Service, or director of Defense agency will validate the requirement and certify that contract documents contain guidance and restrictions, certified by the contracting officer, to ensure that contractor use of DSN complies with established network management procedures. Requests for approvals will identify the contract termination date.

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

e. DISA will be provided copies of all contractor access requests, approvals, and terminations.

f. Approvals and contracts will state that the Department of Defense will have the right to terminate the service at any time and that the Department of Defense will not guarantee the quality or quantity of service to be supplied or be held liable for any discontinuance or failure of the service.

4. Foreign Governments. Foreign government activities may be granted access to the network by the Department of Defense for national security and when not in conflict with existing agreements or local PTT ordinances. This access will be initiated by and processed through the appropriate DOD sponsor in accordance with reference g.

5. Nonappropriated Fund Activities. DSN use may be authorized for NAF activities to conduct command management functions dealing with appropriated funds matters. Requests should be forwarded to appropriate CINC or Service channels for approval and must be certified by the commander of the NAF activity as required for command management functions. Calls dealing with NAF business or functions other than command management will use the DSN on a cost reimbursable basis and if it does not impact the operational capabilities of the DSN. The CINCs and Chiefs of the Services will institute procedures to revalidate requirements periodically.

6. Labor Unions. Access to DSN will not be provided to labor unions and will not be routinely authorized in contract documents. The basis for supporting a request to OSD will be 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.

7. Foreign Military Sale of DSN Service. DSN Service may be approved as part of an FMS arrangement. The use of DSN by DOD personnel assigned to non-US (foreign government adviser, UN, NATO, etc.) organizations must be validated or approved by the appropriate CINC, Chief of the Service, or director of a Defense agency. If service is for non-US or non-DOD users, requirements should be submitted to OSD.

8. DSN Access by Friendly Foreign Governments and Treaty Organizations. 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 will ensure

CJCSI 6215.01
1 February 1995

effective control of this use and will 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 g.

ENCLOSURE C

POLICY FOR THE DEFENSE RED SWITCH NETWORK

1. Purpose. This enclosure provides operational policy for the Defense Red Switch Network (DRSN).

2. General

a. The operational requirements for the DRSN were validated per reference k, which specified DRSN service will be provided to the NMCC, NMCC Site R, CINC primary command centers, and component commands. Also, the DRSN will provide the means to access a variety of tactical secure voice systems (i.e., "long-local" KY-68 terminals and AN/TTC-39 series switches).

b. In September, 1993, existing and planned switching systems were categorized in their relationship with the DRSN. Per reference l, "Category I" switches (connected to the DRSN and under the operational management of DISA) pertain to this instruction. Category II and III switches are not under operational management of DISA and operate under separate policies and procedures. Additional category I switching systems can be established by submitting documentation in the format outlined in Enclosure G.

c. The DRSN is the primary network for secure conferencing and supports the majority of the Worldwide Secure Voice Conferencing System (WWSVCS) conferees. Other conferencing requirements will be accommodated by the DRSN on a non-interfering basis.

d. The DRSN is a dedicated secure network that is configured and managed by DISA. No automatic or dedicated trunking by other Red Switches is authorized.

e. The above requirements mandate dedicated 24-hour-a-day, 7-days-a-week, network management facilities to monitor the status of the DRSN and take necessary actions in the event of outages or world situation.

3. Non-DOD Activities. Non-DOD activities will not be connected to the DRSN without:

a. Recommendation of a DOD sponsor.

b. Concurrence of the Joint Staff.

c. Approval of OSD.

4. Cost Recovery. Those costs approved by the DBOF Manager for common (network) funding will be contained within the rate structure and interfaces in service.

5. Request for DRSN Service. Requests for DRSN service, authority, and allocation of precedence is the same as the DSN. The format for requesting service is listed in Enclosure G.

ENCLOSURE D

RESPONSIBILITIES

1. Purpose. This enclosure provides guidance on the responsibilities for the operation of the DSN. The responsibilities outlined below refer to both the DSN nonsecure and secure voice systems (DRSN network).
2. Responsibilities
 - a. Office of the Secretary of Defense
 - (1) Approves the DSN and DRSN Program Plans 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. Joint Staff
 - (1) Reviews the operational effectiveness of the DSN and DRSN. The Joint Staff will report to OSD those matters having a major effect on the network.
 - (2) Validates the DSN and DRSN Program Plans and submits to OSD for approval.
 - (3) Reviews and approves all requests for FLASH and FLASH OVERRIDE capability validated by the CINCs, Chiefs of the Services, and directors of Defense agencies. The Joint Staff will ensure that users granted FLASH OVERRIDE and FLASH 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.
 - (4) Reviews and approves all requests for network access to the DRSN and connections between DRSN and non-DRSN secure voice equipment.
 - (5) Approves special telecommunications survivability requirements for DSN.

(6) Reviews, validates, and approves service requirements where the desired capability adversely affects the network.

c. Director, DISA

(1) Acts as the Single System Manager of DSN by providing operational direction and management control of DSN.

(2) Provides systems engineering program management of DSN in response to DSN Program Plan validated, approved and funded requirements.

(3) Prepares and submits the DSN Program Plan to the Joint Staff for validation.

(4) Manages the effectiveness of the network on a continuing basis and evaluates O&M practices and procedures to ensure the C2 requirements are being met.

(5) Periodically reports the status and operational effectiveness of DSN to the Joint Staff.

(6) Recommends DSN performance objectives and establishes interface criteria in coordination with DOD components.

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

(8) Provides DRSN connectivity and network management within DSN.

(9) Reviews, processes, and implements approved requests for DSN telecommunications (data, secure and nonsecure voice, and video) service. If the potential exists to harm network service, the request will be forwarded to the Joint Staff for resolution.

(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 DBOF and publishes rates to recoup the DSN investment.

- (12) Coordinates and reviews CINC, Service, and agency policies and procedures when requested.
- (13) Produces and updates the DRSN Concept of Operations and provide operational direction for all DRSN switching centers.
- (14) Performs network management function identified in Enclosure A on a real-time basis.
- (15) Recommends and, upon approval of the Joint Staff, implements modifications to the DRSN.
- (16) Produces and updates, on a biennial basis, the following DSN documents to be submitted through to the Joint Staff, for validation, to OSD for approval.
 - (a) DSN Program Plan (to include the worldwide DSN Topology).
 - (b) Worldwide Operational Policy for Single System Management (SSM).
 - (c) Network Configuration Management Plan.
 - (d) DSN Security Guide.
 - (e) DSN Classification Guide.
 - (f) DSN System Interface Criteria.
 - (g) Generic Switching Requirement (EO).
 - (h) Generic Switching Requirement (MFS).
 - (i) Test and Evaluation Master Plan.
 - (j) Joint Integrated Logistic Support Plan.
 - (k) Worldwide Numbering and Dialing Plan.
- (17) Produces, updates, and distributes the DSN Directory on an annual basis.
- (18) Collects and maintains DRSN configuration management information, to include:

- (a) Network connectivity (switches and trunking), performance specification, and excess capacity data.
 - (b) Network routing, dialing, and numbering scheme.
 - (c) Switch data bases.
 - (d) Timing and synchronization scheme.
 - (e) Interface and control criteria.
 - (f) FLASH and FLASH OVERRIDE users' line assignment and location.
- (19) Produces and updates, on a biennial basis, the following DRSN documents:
- (a) Management Engineering Plan.
 - (b) Configuration Management Plan.
 - (c) Financial Management Plan.
 - (d) Integrated Logistics Support Plan.
 - (e) Security Guide.
 - (f) Test and Evaluation Master Plan.
 - (g) Network Vulnerability and Survivability Study.
- (20) Recommends consolidation and modification of the DSN and DRSN to improve networks effectiveness or reduce costs.
- (21) Operates a DRSN testing facility and maintain documentation pertaining to connection approval and interface standards.
- (22) Provides logistic information to the designated executive agency for logistic support.

d. The CINCs and the Joint Staff

(1) Define, validate, coordinate, and approve requirements for telecommunications services within their purview.

(2) Forward approved DSN requirements and priorities to DISA and the supporting Service for implementation. The CINCs will provide planning requirements for incorporation into the DSN Program Plan. Requirements for precedence service will be forwarded to DISA in accordance with established procedures.

(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 customer premise equipment, including secure voice instruments.

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

(6) Implement controls for 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 exercises involving operational elements of the DSN.

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

(9) Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability. Revalidate these requirements on a biennial basis.

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

e. Chiefs of the Services and Directors of Defense Agencies

- (1) Define, validate, coordinate, and approve requirements for telecommunications services within their purview.
- (2) Forward approved DSN requirements and priorities to DISA for coordination or implementation and provide planning requirements for incorporation into the DSN Program Plan.
- (3) Program, budget, acquire, operate, maintain, and fund for assigned portions of the DSN and for telecommunications services provided by DSN.
- (4) Exercise review and approval authority over requirements for IMMEDIATE and PRIORITY precedence capability. Revalidate these requirements on a biennial basis.
- (5) Validate and forward requirements for FLASH and FLASH OVERRIDE to the Joint Staff for approval in accordance with Enclosure G.
- (6) Provide acquisition, operation, maintenance, logistic, and funding support for CPE and terminal equipment, including secure voice instruments.
- (7) Provide training and periodic technical evaluations to ensure that facilities, equipment, and personnel meet DSN performance objectives and interface requirements.
- (8) Provide policy and implement controls for and monitor the use of precedence, on- and off-netting, and nonofficial use of DSN to prevent fraud, waste, or abuse.
- (9) Support DISA in exercises involving operational elements of the DSN.
- (10) Coordinate with DISA before approval to determine if a DSN service request would degrade network performance.
- (11) Review and validate operational requirements for DSN and DRSN switches under their operational control.

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

(13) Provide DISA with real-time access (at least "read only") to all elements of switch data bases.

(14) Program, budget, fund, and provide support for all switching centers under their direct operational control or executive agency.

(15) Provide logistic information to the designated executive agency for logistic support.

(16) Maintain required physical security and procedures on switching centers currently operating with Sensitive Compartmented Information subscribers and trunking.

f. The Air Force

(1) Performs executive agency duties for DRSN logistic support to include engineering, training, and vendor services.

(2) Coordinates specific DRSN logistic requirements with the network manager, CINCs, Military Department and agencies.

g. Director, DIA

(1) Provides guidance for security issues.

(2) Accredits all DOD DRSN switching centers less those under the operational control of the Director, NSA, that handle special compartmented information.

(3) Assists DISA in preparation of the DISN threat, survivability, and vulnerability analysis.

h. Director, NSA

(1) Serves as security and INFOSEC advisor for the DSN and DRSN networks.

(2) Recommends countermeasures based on DIA threat analysis in conjunction with DSN security designs.

(3) Coordinates technical parameters of secure voice and other secure terminals with DISA.

(4) Accredits those DRSN switching centers which handle special compartmented information and are under the operational control of the Director, NSA.

3. Administration. CINCs, Chiefs of Services, 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 that they are in sync with the overall DSN network operations.

ENCLOSURE E

POLICY AND PROCEDURES FOR CONNECTION OF SPECIFIC EQUIPMENT TO DSN

1. Purpose. To establish policy and procedures to support connection of specific types of equipment to the DSN.
2. General
 - a. Ancillary equipment connected to the DSN will be done in such a way to ensure that the DSN grade of service standards outlined in this document is not degraded. The overriding criterion is that adding new services or equipment will not be detrimental to overall network performance.
 - b. DISA will provide the technical interface standards for equipment to be connected to the DSN.
 - c. Users are responsible to coordinate with DISA on equipment being connected to the DSN.
3. Secure Transmission with a STU-III
 - a. The STU-III will be used as the primary device to enable secure communications over the DSN. It may be used for secure voice, data, or facsimile mode for voice communications.
 - b. Approval under provisions of this instruction is not required for conversion of a telephone instrument to a STU-III on DSN. A STU-III connected to DSN will have the preempt feature enabled at all times.
 - c. When the STU-III is used to transmit secure data or facsimile, the following criteria will be met:
 - (1) The STU-III at each end will be monitored during the complete transmission to ensure the circuit is maintained and the STU-III is in the secure mode.
 - (2) The STU-III preempt feature will be enabled at all times.
 - (3) National guidance for use of STU-III in secure data transmission, including access control TEMPEST, and computer security, be implemented.

4. Switched Data/Imagery

- a. The DISN packet switched networks are the primary means to transmit data. However, the DSN switched voice (dial-up) circuits may be used to supplement the packet switch 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 will be capable of automatically disconnecting from the access line or IST when the transmission is complete or the circuit is preempted.
- c. DSN users with requirements to use the DSN for large volume, extended holding times (in excess of one hour) or for dedicated operational system requiring switch data connectivity will coordinate with DISA for a technical evaluation of the requirements. This process is necessary to determine the impact and to reconfigure the network.
- d. DISA will provide technical assistance, interface standards, and connection approval for the types of device being used over the DSN.

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

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 will be disconnected from the line immediately after transmission of each message and will not be connected while composing a message.
- b. Receiving and transmitting terminals will 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.

7. Video Teleconferencing. The DSN will provide connectivity to the DOD common user teleconferencing system by providing a dial-up switched capability at the PX56KBS rate.
8. DSN Control and DCS Orderwire Circuits. DCS orderwire circuits, and DSN dedicated and dial-up A/NM data and voice circuits are exempt from the provisions of this instruction.

(INTENTIONALLY BLANK)

ENCLOSURE F

PRECEDENCE APPROVAL AUTHORITIES

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

2. Approval Authorities

<u>TYPE REQUEST</u>	<u>REQUEST ORIGINATOR</u>				
	MIL SVS	U/S CMD	DOD AGY	NMCS J-STAFF	NON-DOD AGY
FLASH OVERRIDE	J	J	J	J	O
FLASH	J	J	J	J	O
IMMEDIATE	S#	C	D#	J	O
PRIORITY	S#	C	D#	J	O
ROUTINE	L	L	L	L	L

LEGEND

- J - Joint Staff
- C - Commander of combatant command
- S - Chief of Service
- D - Director of Defense agency
- O - OSD
- L - Local level (see Enclosure B, paragraphs 2 through 8)
- # - OCONUS CINC approves requests in AOR.

Note: Requests should be based on availability of funds and coordination with DISA.

(INTENTIONALLY BLANK)

ENCLOSURE G

PROCEDURES FOR REQUESTING DSN SERVICE

1. Purpose. This enclosure provides procedures for requesting DSN service approval. The format contained in paragraph 4 will be used for precedence requests for DSN and DRSN service. Other requests (e.g., switching changes, 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 activities will request DSN service through their chain of command to appropriate CINC or Service, per local procedures. Non-DOD agency requests sponsored by DOD components will also comply with these procedures. Non-DOD requests to the Joint Staff will be forwarded to ASD(C3I) for consideration.
3. General
 - a. Requests for DSN service, DRSN service, or non-DRSN Red Switch connectivity will be submitted in the format shown below. Requirements must be fully documented and justified. Combatant commands and Services may tailor the format for requests that they approve. Future requirements (those appropriate for DSN Project Plan) should be provided to DISA and the Services.
 - b. Activities having validation or approval authority will ensure that requirements comply with this instruction specifically that:
 - (1) Requests for DSN access are motivated by legitimate mission requirements.
 - (2) Precedence capabilities are justified in terms of explicit mission need and negative impact if the request is disapproved. Network status provided by DISA will be reviewed to determine what capabilities currently exist, whether current access in service is fully used, and the impact of requested service on the grade of service for the requesting location.
 - (3) Requirements that affect other combatant commands, Services, or Defense agencies have been coordinated.
 - (4) Tradeoffs are provided for new or increased levels of service or capabilities as required.

(5) Appropriate restoration priorities are identified.

(6) Requirements for non-DRSN Red Switch connectivity or tandeming are justified and cannot be met by STU-III terminals.

c. Requests from activities outside the Department of Defense will be forwarded through the Joint Staff to ASD(C3I) for consideration.

4. Request Format. The following message format will be used when requesting upgrades in DSN service:

FROM: (Originating Activity)
TO: JOINT STAFF WASHINGTON DC//J6T//*
(* or activity with requisite approval authority)
INFO: DA WASHINGTON DC//SAIS-PPS//
CNO WASHINGTON DC//N61//
HQ USAF WASHINGTON DC//SCMM//
CMC WASHINGTON DC//CCT//
DISA WASHINGTON DC//WE33/WE339//
Validating authority, others as required.

(If approval authority is below the Joint Staff level, information addressees will consist of affected commands or Services. DISA will be an information addressee on all such 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 DSN (OR 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, 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. Serving switch (EO, MFS).
- G. Terminating Equipment; e.g., Type, Brand, Model of PBX, facsimile, data terminal/modem, VTC studio terminal equipment, EAC, STU-III.
- 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 (geographic and physical).
- J. Tradeoff (identify by sequence number, CCSD, precedence, Joint Staff approval number, or other pertinent data).
- K. DISA (DMS/DDN, etc.) or Joint Staff waivers in effect.
- L. Identification of the destination and expected frequency and duration of calls, data transmissions, or facsimile transmissions. Information may also be expressed in terms of Erlangs of traffic.

2. Justification

- A. Present capabilities for DSN calling 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. Whether theater commander(s) approves and point of contact.
- D. Identification of expected yearly cost and source of funds.
- E. Identification of DISA (or DISA area representative) who provided coordination and network impact assessment, office code, and phone number or why DISA was not contacted.

F. Explanation if no tradeoff is provided.

G. Other considerations or remarks as appropriate.

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

(NOTE: Streamlined procedures authorized for deactivation or cancellation of DSN/DRSN service)

ENCLOSURE H

REFERENCES

- a. DOD 5200.2-r, January 1987, "DOD Personnel Security Program."
- b. DODD 5105.19, 25 June 1991, "Defense Information Systems Agency (DISA)."
- c. DODD 5200.1, 7 January 1982, "DOD Information Security Program."
- d. DUSD(C3I) memorandum, 23 June 1982, "DSN Definition, Purpose and Scope."
- e. USDRE memorandum, 9 September 1982, "Defense Switched Network."
- f. OSD(C3I) memorandum, 11 December 1992, "Defense-Wide Secure Voice Program."
- g. CJCS MOP 43, 11 March 1992 (Rev 1), "Military Telecommunications Agreements Between the United States and Regional Defense Organizations or Friendly Foreign Nations."
- h. CJCSI 5711.01, 12 July 1993, "Policy on Action Processing."
- i. CJCSI 5721.01, 28 June 1993, "Defense Message System Network and Connected Systems."
- j. CJCSI 3222.01, 8 October 1993, "CJSC Prioritization of C3 Nodes and Systems for High Altitude Electromagnetic Pulse Protection."
- k. J-6A 01665-92, 17 November 1992, "Operational Requirement Document for Secure Voice Requirements."
- l. J-6A 01137-93, 27 September 1993, "Defense Red Switch Network Defense-Wide Resources."
- m. NACSI 4008, 4 March 1983, "Safeguarding COMSEC Facilities."

CJCSI 6215.01
1 February 1995

(INTENTIONALLY BLANK)

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

A/NM	administration/network management
AOR	area of responsibility
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
AUTODIN	Automatic Digital Network
AUTOSEVOCOM	Automatic Secure Voice Communications Network
AUTOVON	Automatic Voice Network
CINC	commander of a unified command
C2	command and control
C3	command, control, and communications
C3I	command, control, communications, and intelligence
CCSD	command communications service designator
COMSEC	communications security
COMPUSEC	computer security
CONUS	continental United States
CPE	customer premise equipment
CSIA	Communications Service Industrial Activity
DBOF	Defense Business Operating Fund
DCS	Defense Communications System
DDN	Defense Data Network
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
EAC	emergency action console
EO	end office
FCC	Federal Communications Commission
FMS	foreign military sales
FTS	Federal Telecommunications System
GOS	grade of service
HEMP	high-altitude electromagnetic pulse
HMW	health, morale, and welfare
ISDN	Integrated Service Digital Network
IST	interswitch trunks
IVSN	Initial Voice Switched Network

MCA maximum calling area
MFS multifunction switch
MLPP multilevel precedence and preemption
MTF message text format

NACSI National Communications Security Instructions
NAF nonappropriated fund
NATO North Atlantic Treaty Organization
NCS National Communications System
NM Network management
NMCC National Military Command Center
NMCS National Military Command System
NSA National Security Agency
NS/EP National Security and Emergency Preparedness

OCONUS outside CONUS
O&M Operation and Maintenance

PABX private automatic branch exchange
PBX private branch exchange
PTT public telephone and telegraph

RMC (CSIA) Resource Management Committee
RSU remote switching unit

SA stand-alone switch
SCI sensitive compartmented information
SMEO small end office
STU-III secure telephone unit three/low-cost terminal
SVS secure voice system

TSP Telecommunications Service Priority System

USACOM US Atlantic Command
USCENTCOM US Central Command
USEUCOM US Europe Command
USPACOM US Pacific Command
USSOUTHCOM US Southern Command
USSPACECOM US Space Command
USSOCOM US Special Operations Command
USSTRATCOM US Strategic Command
USTRANSCOM US Transportation Command

VTC video teleconferencing

WWSVCS Worldwide Secure Voice Conferencing System

PART II--DEFINITIONS

Automatic Voice Network. Previously, the principal long-haul, nonsecure voice communications within the Defense Communications System. Also called AUTOVON. (JCS Pub 1-02)

avoidance routing. Circuits routed so as to avoid critical junctions and known target areas.

backbone. The DSN backbone consists of nodal switches, connectivity among nodals, long-distance termination at DSN EOs, connectivity between EOs and nodal switches, and connectivity between EOs.

CINC. Commander or designated staff element of one of the following unified commands: US Atlantic command, US Central Command, US European Command, US Pacific Command, US Southern Command, US Space Command, US Special Operations Command, US Strategic Command, US Transportation Command.

command and control. The exercise of authority and direction by a properly designated commander over assigned 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. (JCS Pub 1-02)

C4 systems operational direction. The authority necessary to ensure effective operation of a C4 system or activity. It includes the authority to direct and assign tasks to C4 operating elements and supervise the execution of those tasks; allocate and reallocate C4 systems or activity to accomplish the mission; and develop C4 technical standards, practices, methods, and procedures for performance and operations.

communications security. The protection resulting from all measures designed to deny an unauthorized person information of value that might be derived from the possession and study of telecommunications or to mislead unauthorized persons to their interpretations of the results of such possession and study. Also called COMSEC. Communications security includes: (a) cryptosecurity, (b) transmission security, (c) emission security, and (d) physical security of communications security materials and information.

1. cryptosecurity - The component of communications security that results from the provision of technically sound crypto-systems and their proper use.

2. transmission security - The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

3. emission security - The component of communications security that results 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 and telecommunications systems.

4. 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. (JCS Pub 1-02)

computer security. The protection resulting from all measures designed to prevent either deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, or modification of information in the computer system. COMSEC measures may be among those applied in achieving computer security.

continental United States. United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico. (JCS Pub 1-02)

diverse routing. Connectivity servicing the same facility but routed over geographically separate circuits.

dual homing. The connection of a terminal so that it is served by either of two separate switching centers. This service uses a single directory number.

end office. An integral part of the DSN. Any EO switch provides to the users switched call connections and all DSN service features, including MLPP. The EO will provide long distance service by interconnection with DSN nodal switches. The EO will not serve as a tandem in the DSN but may connect to other EOs where direct traffic volume requires (Metro Calling Area).

grade of service. The probability of call blockage expressed as a percentage of calls blocked. Grade P.05, for example, denotes

that five calls of every 100 offered will probably fail to complete.

Joint Staff. The staff of the Chairman, Joint Chiefs of Staff, as provided for under the National Security Act of 1947, as amended by the DOD Reorganization Act of 1986.

Joint Worldwide Intelligence Communications System (JWICS). The sensitive compartmented information component of the DISN. The primary mission of JWICS is to support the production and dissemination of intelligence to the entire intelligence community.

management control. The review, evaluation, coordination, and management actions necessary to fulfill the responsibilities of operational direction for a system or an activity.

maximum calling area. A description of user calling privileges based on the destination of the call.

multilevel precedence and preemption. The capability to originate calls based on precedence and to preempt calls of lower precedence in the network.

nodal switch. A tandem switch in the DSN that will connect multiple EOs, provide access to a variety of transmission media, route calls to other nodal switches, and provide network features such as MLPP. Nodal switches will be supervised by and interconnected to the DSN A/NM subsystem. The two types of nodal switches in the DSN are:

a. stand alone switch. The SA switch functions solely as a tandem switch in the DSN.

b. multifunction switch. This switch incorporates the combined functions of an SA switch and an EO switch. No physical division exists between the EO and SA functions within the MFS, but a logical division exists.

metropolitan calling area. A community of interest having operational telecommunications needs in the local area.

off-net calling. Calls placed over DSN extended to commercial telephone numbers.

on-net calling. Calls from commercial telephone numbers to the DSN network.

precedence. Calling capability assigned to a DSN or DRSN user terminal. The five levels of precedence in ascending order are:

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

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

IMMEDIATE--Precedence reserved generally for telephone calls pertaining to: (1) Situations which gravely affect the security of national and allied forces; (2) Reconstitution of forces in a post-attack period; (3) Intelligence essential to national security; (4) Conduct of diplomatic negotiations to reduce or limit the threat of war; (5) Implementation of Federal Government actions essential to national survival; (6) Situations which gravely affect the internal security of the United States; (7) Civil Defense actions concerning our population and their survival; (8) Disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population; (9) Vital information having an immediate effect on aircraft, spacecraft, or missile operations.

FLASH--Precedence reserved generally for telephone calls pertaining to: (1) Command and control of military forces essential to defense and retaliation; (2) Critical intelligence essential to national survival; (3) Conduct of diplomatic negotiations critical to the arresting or limiting of hostilities; (4) Dissemination of critical civil alert information essential to national survival; (5) Continuity of Federal Government functions essential to national survival; (6) Fulfillment of critical United States internal security functions essential to national survival; (7) Catastrophic events of national or international significance.

FLASH OVERRIDE--Same as FLASH, capability available to (1) The President of the United States, Secretary of Defense and Joint Chiefs of Staff; (2) Commanders of combatant commands when declaring Defense Condition One or Defense Emergency; (3) CINCNORAD when declaring either Defense Condition One or Air Defense Emergency and other national authorities the President may authorize. FLASH OVERRIDE cannot be preempted.

preemption. The act of seizing telecommunications connectivity from a call of lower precedence to support calls of higher precedence.

private branch exchange. A telephone exchange servicing a single organization or area where service requires connection to another telephone exchange for long-distance capabilities. A PBX, either manual or automatic (PABX), is customer premise equipment and is not an integral part of DSN. PBX and PABX are used interchangeably.

remote switching unit. An out-stationed part of the parent switch, controlled by the parent software. The RSU concentrates originating traffic from a number of local lines and then sends it to its parent switching unit. Similarly, the RSU deconcentrates terminating traffic. A subscriber of an RSU can enjoy all of the features available to a direct subscriber of the parent switch.

Secure Voice System. The title given to the collective secure voice capabilities that replaced AUTOSEVOCOM and substantially expands and improves the DOD secure voice posture. The SVS will significantly increase the number of secure voice users through extensive fielding of the STU-III family of equipment.

small end office. An EO switch terminating 1000 or less subscribers and meeting the DISA SMEO specifications. As used herein EO includes SMEO unless specifically excluded.

split homing. The connection of a DSN terminal to two switching centers with the assignment of two DSN telephone numbers.

stress level. The military operating conditions under which DSN must function based on scenarios ranging from peacetime to massive nuclear attack.

STU-III family. One or more of the various models of the STU-III terminal (STU-III, STU-IIIA, STU-III cellular, STU-IIIR, etc).

tandeming. Use of the DRSN Red Switch network to extend a secure call that should have been extended via other networks. The two cases are: (1) a STU-III user interconnects with the Red Switch network at a point other than the destination Red Switch and uses the network to extend the call to the destination (prohibited). (2) a non-DRSN Red Switch subscriber extends a call via the DRSN to another non-DRSN Red Switch (limited).

tandem switch. A switch or portion of a Multifunction switch that processes trunk group routing and connects only to other switches.

user. An individual who is authorized to access DSN and uses a specified set of services and features.