



Draft
**Department of Defense
INSTRUCTION**

Number 8100.XX
Date

ASD(NII)/DoD CIO

SUBJECT: Department of Defense (DoD) Voice Networks

- References:
- (a) Public Law 107-314: Bob Stump National Defense Authorization Act for Fiscal Year 2003, SEC 353, Installation And Connection Policy And Procedures Regarding Defense Switch Network
 - (b) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
 - (c) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," January 11, 2002
 - (d) DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002
 - (e) through (j), see enclosure 1

1. PURPOSE

This Instruction:

- 1.1. Implements the provisions of references (a) and (b).
- 1.2. Provides policy, procedures and assigns responsibilities for test, certification, accreditation, lease or procurement, installation, connection, and operation of telecommunications switches and services on DoD voice networks, specifically the Defense Switched Network (DSN) and Defense RED Switch Network (DRSN).

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies (see paragraph E2.8., below) the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively as "the DoD Components").

2.2. All telecommunication switches leased, procured (systems or services), or operated by any Component of the Department of Defense or by authorized non-DoD users (e.g., Combined or Coalition partners and U.S. Government Departments and Agencies that are designated as Special C2 or C2 users) that are or will be installed or connected to the DSN, DRSN or Public Switched Telecommunications Network (PSTN) to include:

2.2.1. The hardware or software to send and receive voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the DSN, DRSN or PSTN. For authorized non-DoD DSN users, only the telecommunications switch interfaces to the DSN are subject to the provisions of this instruction.

2.2.2. End-to-end (e.g., phone to phone; video to video unit, fax to fax; Secure Terminal Equipment (STE) to STE) and tactical applications.

2.2.3. All technologies (i.e., circuit switch, Voice over Asynchronous Transfer Mode (VoATM) and Voice over Internet Protocol (VoIP)) that use DSN or DRSN phone numbers and provide dial tone for origination and reception of voice, dial up video and dial up data for routine and precedence subscribers; or are otherwise incorporated into the DSN or DRSN numbering and routing plan by means of area code, access code, address resolution scheme (e.g., ENUM) for origination and reception of voice, dial up video and dial up data for routine and precedence subscribers.

2.2.4. DoD Component's planning, investment, development, operations and management of telecommunications switches connected to the DSN or DRSN for processing and transport of voice, dial up video and dial up data.

2.3. All authorized non-DoD or non-C2 users (e.g., combined or coalition partners and U.S. Government Departments and Agencies), that are or will be connected to the DSN or DRSN.

2.4. Requests for waivers to the provisions of this instruction shall be forwarded via chain of command, through the Chairman of the Joint Chiefs of Staff, to Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)/DoD Chief Information Officer (CIO), stating the reason compliance is not possible. Only the ASD(NII)/DoD CIO is authorized to

approve waivers to DSN policy and Interim Authority to Operate (IATO) requests. IATO requests shall be submitted via the GIG waiver process for consideration.

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. DSN is the preferred non-secure DoD inter-installation telephony service (i.e., voice, dialup data and dialup video) network and shall be the primary communications means for special Command and Control (C2), C2, and non-C2 users. It shall be the primary means of secure (i.e., point-to-point dial-up to include the STU-III/STE family of secure voice terminal devices) communications for non-tactical C2 users.

4.2. DRSN is the preferred DoD secure telephony service network and shall be the primary secure voice communications means for Special C2 and C2 users in peacetime, crisis situations, and wartime. The DRSN shall be the primary secure command and control communications system that supports the secure voice and secure conferencing requirements of the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, the National Military Command System (NMCS), DoD Components and subordinate organizations, Combatant Commanders, and specially approved government departments and agencies (e.g., Department of State, Department of Justice), and U.S. allies.

4.3. The DSN and DRSN shall be used for only official business, or in the best interest of the Government, and is the first choice for all switched non-secure and secure voice and dial-up data, video telecommunications between installations serving authorized users.

4.4. The DSN shall provide non-secure, end-to-end command and control capability and dedicated telephone service, voice-band data, and dial-up Video Teleconferencing (VTC). The DSN includes the end instruments, the switches on the installations, the backbone and tandem switches, the transmission connectivity between and among the installations, the network management system and the signaling system. Processing or transport technologies (to include VoIP and VoATM systems) shall also be considered as elements of the DSN.

4.5. The DRSN shall provide secure, end-to-end (e.g., phone to phone) command and control capability and dedicated telephone service. Processing or transport technologies used in a secure enclave environment (e.g., classified LAN, SIPRNet, etc.) and connected to DRSN to support voice service shall be considered as elements of the DRSN.

4.6. Telecommunications switches and services intended to connect to the DSN or DRSN shall comply with MUF requirements (e.g., Multi-Level Precedence and Preemption (MLPP), routing, special alternative routing, survivability, and security) unless granted a waiver by the Chairman of the Joint Chiefs of Staff.

4.7. The DSN and DRSN shall support C2 user traffic during peacetime, crisis, conflict, natural disaster, and network disruptions and possess the robustness to provide a surge capability when needed. Survivability objectives for the DSN and DRSN shall be specified by the Chairman of the Joint Chiefs of Staff.

4.8. The DSN and DRSN shall provide assured service or connectivity as follows:

4.8.1. Assured voice communications to Special C2 and C2 users. Assured service or connectivity is the ability of the DSN and DRSN to optimize call completion rates for all C2 users, despite degradation due to network disruptions, natural disasters, or surges during crisis or war. To meet MUF requirements, the DSN and DRSN shall employ an MLPP capability, which permits higher precedence users to preempt lower precedence calls. Special C2 users (Flash and Flash Override within the current DSN and DRSN MLPP framework) shall be provided with nonblocking service.

4.8.2. Assured service capability from user-instrument-to-user-instrument across the global DSN and DRSN, including government-controlled Private Branch Exchanges (PBXs), End Offices (EOs), and tactical networks that incorporate MLPP features.

4.8.3. Assured long-haul capability (long distance terminations on telecommunications switches at initiating installations to long distance terminations on telecommunications switches at distant installations) for supporting a regional crisis in one theater, yet retain the surge capacity to respond to a regional crisis occurring nearly simultaneously in another theater.

4.9. The DoD may grant non-DoD activities access to the DSN and DRSN when necessary for national security; when not in conflict with local Public Telephone and Telegraph (PTT) ordinances; when those activities and individuals have critical National Security (NS) and Emergency Preparedness (EP) needs; and access is in the best interest of the U.S. Government. Access can only be provided to non-DoD or nongovernmental activities or agencies (Department of Justice, state government organizations, DoD contractors, and foreign embassies) on a not-to-interfere basis. Requests for access by non-DoD or nongovernmental activities or agencies shall be forwarded to the Chairman of the Joint Chiefs of Staff for approval.

4.10. All authorized non-DoD or non-C2 users (e.g., combined or coalition partners and U.S. Government Departments and Agencies), with only Routine precedence service, that are or will be connected to the DSN or DRSN shall, respectively:

4.10.1. Comply with DSN system interface criteria at DSN controlled gateways.

4.10.2. Comply with DRSN interface criteria at controlled gateways or derive DRSN long-local service from a DRSN network switch.

4.11. Telecommunications switches (and associated software releases) procured or leased by DoD Components, and connected or planned for connection to the DSN, shall be joint interoperability certified by the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC) and granted information assurance certification and accreditation by the DISA Designated Approval Authority (DAA).

4.12. Telecommunications switches (and associated software releases) procured or leased by DoD Components, and connected or planned for connection to the DRSN, shall consist of a homogeneous set of DRSN specified equipment and/or functional features and capabilities (i.e., single vendor and/or transparency of features and capabilities) providing for full interoperability, Military Unique Feature (MUF) functionality, security, conferencing, and call processing. DRSN telecommunications switches (and associated software releases) shall be joint interoperability tested by DISA (JITC) in accordance with test plans, performance requirements and procedures established by the DRSN SSM; and IA certified and accredited by DISA and Defense Intelligence Agency (DIA) DAAs, as appropriate based on classification level of service provided.

4.13. DISA, as the DSN Single System Manager (SSM) and DRSN SSM, shall be responsible for operational direction and management control of the end-to-end performance of the DSN and DRSN. The DSN and DRSN SSMs shall:

4.13.1. Be designated, respectively, as the non-secure and secure telephony standards, processing, and transport technology migration coordinators to ensure end-to-end global voice quality, interoperability, and visibility for all non-secure and secure C2 voice services. Combatant Commands, Services, Agencies, posts, camps, and stations shall coordinate voice transport and processing initiatives with the DSN or DRSN SSM, as appropriate.

4.13.2. Provide an annual risk assessment of emerging voice processing and transport technology's impact on global, end-to-end voice performance and non-secure and secure C2 services to the Chairman of the Joint Chiefs of Staff and the DSN and DRSN Configuration Control Boards (CCB), respectively. All voice, video, data processing end instruments (e.g., Secure Telephone Unit (STU), fax, STE, Video Codecs, and Modems), and transport technologies (e.g., Circuit Switched, Time Division Multiplex (TDM) and Packet technologies) shall be included in the risk assessment.

4.13.3. Be responsible for DoD DSN and DRSN dialing and numbering plans for telephony services to ensure end-to-end interoperability.

4.13.4. Respectively initiate and provide technical analysis of network survivability, to include a risk analysis, when proposing major changes in the network technology or architecture

(geographic location of communications systems of the DSN or DRSN). DISA shall forward the results of the analysis to the Chairman of the Joint Chiefs of Staff for review.

4.14. The DSN and DRSN shall comply with the NS/EP Telecommunications Service Priority (TSP) system for service restoration.

4.15. 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 Combatant Commander, and Operations and Maintenance (O&M) commands.

4.16. Interfaces to the DSN and DRSN shall comply with interface criteria established, respectively, by the DSN or DRSN SSMs. Use of network interfaces not conforming to DSN or DRSN interface criteria, defined by the respective SSM, shall not be permitted without SSM technical review and approval, on a site-specific basis, by the Chairman of the Joint Chiefs of Staff. For these interfaces, a method for controlling the flow of traffic across the interface must be established and monitored by DISA.

4.16.1. All interfaces to the DRSN shall be approved, on a site-specific basis, by the DISA DRSN SSM. DISA DRSN SSM's approval for an interface may be in the form of a permanent, conditional, or temporary interface. Connectivity from a DRSN switch to users outside the RED enclave (i.e., to another building, facility, location, or system) shall be provided through an approved interface.

4.16.2. All interfaces to the DRSN must be through an encrypted inter-switch link/trunk, point-to-point cryptographically secured wireline or wireless path, protected wireline distribution system or other access/gateway configuration as prescribed and approved by the DRSN SSM. Authority for approving such terminations resides with the Chairman of the Joint Chiefs of Staff after all security and interoperability concerns are resolved.

4.17. DISA shall promulgate operation and maintenance, security, performance, interface and interoperability, and joint logistic support planning guidance for the DRSN. All DoD Components and federal agencies supporting, using, or interfacing with the DRSN must comply with DISA-promulgated guidance.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/ Department of Defense Chief Information Officer, shall:

5.1.1. Maintain this Directive, with the other DoD Components, to establish policy, procedures and responsibilities for test, certification, accreditation, lease or procurement, installation, connection, and operation of telecommunications switches and services on the DSN and DRSN.

5.1.2. Enforce policy and provide oversight, with the DoD Components, for telecommunications switches and services operating on the DSN and the DRSN.

5.1.2.1. Establish policy, process and responsibilities to enforce DSN and DRSN telecommunications switch compliance with references (c) and (d) requirements for interoperability and supportability.

5.1.2.2. Establish policy, process and responsibilities to enforce DSN and DRSN telecommunications switch compliance with references (e), (f), (g) and (h) requirements for IA certification and accreditation.

5.1.2.3. Approve all waivers to DSN and DRSN policy and IATO requests.

5.1.3. Develop a process, with the DoD Components, to annually evaluate DoD compliance with this instruction.

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

5.1.5. Approve network performance objectives for DSN and DRSN services to satisfy system requirements and reduce costs.

5.1.6. Approve the biennial DSN and DRSN program plans in consultation with the Chairman of the Joint Chiefs of Staff.

5.2. The Heads of the DoD Components shall:

5.2.1. Ensure the requirements of this Instruction are implemented. Establish Component policy and procedures and responsibilities for the test, certification, accreditation, lease or procurement, installation, connection, and operation of telecommunications switches and services on the DSN and DRSN.

5.2.2. Coordinate all DSN and DRSN, non-secure or secure voice transport and processing initiatives with the DSN SSM or DRSN SSM, as appropriate.

5.2.3. Define, validate, coordinate, and approve mission and traffic requirements for DSN and DRSN services. DRSN service requests shall be forwarded via the requesting agency's chain of command through the appropriate Combatant Commander or Service, to the Chairman of the Joint Chiefs of Staff for validation and final approval.

5.2.4. Validate all waivers to DSN and DRSN policy and IATO requests. Forward to the Chairman of the Joint Chiefs of Staff for consideration.

5.2.5. Validate DSN and DRSN minimum-essential circuits.

5.2.6. Forward approved DSN and DRSN requirements and priorities to DISA for coordination or implementation. Provide planning requirements to DISA for incorporation into the DSN and DRSN program plans.

5.2.7. Plan, program, and budget for telecommunications services provided by DSN and DRSN.

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

5.2.9. Comply with references (e), (f), (g) and (h) requirements for IA certification and accreditation.

5.2.9.1. Ensure telecommunication switches connected to, or planned for connection to the DSN are tested by DISA Center for IA Applications, and certified and accredited for IA by the DISA DAA. Conduct certification and accreditation of telecommunication switches operating at installed location per reference (h) and the DSN Security Technical Implementation Guide (STIG), and report status to the DSN SSM annually.

5.2.9.2. In coordination with the DISA DRSN SSM, ensure that telecommunication switches connected to, or planned for connection to the DRSN are evaluated by the NSA for security vulnerabilities, and accredited for IA by the DISA DAA for collateral telecommunications switches or the DIA for TS/SCI telecommunications switches.

5.2.10. Ensure test and evaluation plans are prepared for all telecommunication switches (acquired or procured) intended to operate on the DSN and DRSN.

5.2.11. Use DSN telecommunications switch Preferred Products List (PPL), published by the DSN SSM, for lease or procurement of telecommunications switches planned for connection to the DSN. Justification shall be provided to the DSN SSM for coordination, prior

to submission for ASD(NII)/DoD CIO waiver and contract award for lease or procurement of a switch that is not on the PPL.

5.2.12. Approve users with Immediate, Priority and Routine precedence origination capability.

5.2.13. Provide annual inventory to DISA on switches connected to, or planned for connection to the DSN or DRSN.

5.2.14. Collect and maintain installation Configuration Management (CM) data (e.g., telecommunication switches, phones, video units, fax, and STEs) to meet end-to-end requirements.

5.2.15. Provide Plan of Action and Milestones (PoA&M) for certifying or transitioning uncertified or unaccredited switches connected to the DSN.

5.2.16. Ensure standards-based Integrated Services Digital Network (ISDN) capabilities are provided in the DSN telecommunication switches at the installations for all DoD organizations that will require the use of STE or other ISDN interfaces.

5.2.17. Monitor and manage responsibility for connections and usage charges accruing for access to public networks. Ensure this capability does not allow automatic on or off-netting of long distance DSN or commercial calls except for DISA managed/approved interfaces.

5.2.18. Maintain DISA's intra- and inter-switch dialing plans for end users and implement DSN access codes to ensure standardization and interoperability across the network.

5.2.19. Report to the DSN SSM any user locations where Grade of Service (GoS) objectives cannot be achieved to the end instrument due to economic or operational limitations.

5.2.20. Participate in the DSN and DRSN CCBs.

5.3. The Chairman of the Joint Chiefs of Staff shall:

5.3.1. Ensure the requirements of this Instruction are implemented. Establish policy, procedures and responsibilities for the test, certification, accreditation, lease or procurement, installation, connection, and operation of telecommunications switches and services on the DSN and DRSN.

5.3.2. Ensure DSN and DRSN telecommunications switch compliance with references (c) and (d) requirements for interoperability and supportability.

5.3.2.1. Develop process, procedures and implementing instructions for Joint Interoperability Certification (JIC) of DSN and DRSN telecommunications switches.

5.3.2.2. Serve as the JIC validation authority for DSN and DRSN telecommunications switches.

5.3.3. Ensure DSN and DRSN telecommunications switch compliance with references (e), (f), (g) and (h) requirements for IA certification and accreditation.

5.3.3.1. Validate, with ASD(NII)/DoD CIO, IA requirements for DSN and DRSN telecommunication switches supporting joint and combined operations.

5.3.3.2. Develop, in collaboration with DISA, process, procedures and implementing instructions for IA certification and accreditation of DSN and DRSN telecommunications switches.

5.3.4. Validate requirements for telecommunications switches planned for connection to the DSN or DRSN.

5.3.5. Review and approve all requests for network access to the DRSN and connections between DRSN and non-DRSN secure voice equipment.

5.3.6. Approve DSN and DRSN access by non-DoD agencies, organizations, activities, or entities.

5.3.7. Approve:

5.3.7.1. DSN Flash and Flash Override precedence origination requests.

5.3.7.2. DRSN Flash, Flash Override, and Flash Override Override precedence origination requests.

5.3.8. Process JIC or IA IATO requests for all uncertified telecommunications switches connected or being considered for connection to the DSN. Forward recommendation for approval of JIC IATO requests to the ASD(NII)/DoD CIO for decision, via the GIG Waiver Panel.

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

5.3.10. Review and approve DISA-recommended, DoD Component coordinated performance objectives and interface criteria for the DSN and DRSN.

5.3.11. Review and approve DISA recommendations for modifications to the DSN and DRSN integrated architectures.

5.3.12. Review the operational effectiveness and assess the mission risks associated with the connection of telecommunication switches to the DSN, DRSN and the PSTN. Report to ASD(NII)/DoD CIO those matters having a major effect on the network.

5.3.13. Review and approve, with technical evaluation by DISA, proposed concepts for automatic interconnection to DSN from public switched networks.

5.3.14. Validate theater GoS objective waivers every two years.

5.3.15. Validate the biennial DSN and DRSN program plans and submit to ASD(NII)/DoD CIO/DoD CIO for approval.

5.3.16. Resolve requests for service identified by DISA as having the potential to harm the DSN or DRSN.

5.3.17. Participate in, and serve as final arbiter, for DSN and DRSN CCBs.

5.4. The Director, Defense Information Systems Agency shall:

5.4.1. Ensure the requirements of this Instruction are implemented. Establish procedures and technical requirements for the test, certification, accreditation, lease or procurement, installation, connection, and operation of telecommunications switches and services on the DSN and DRSN.

5.4.2. Serve as DSN and DRSN SSMs.

5.4.2.1. Provide operational direction, management control and technical guidance for the DSN and DRSN.

5.4.2.2. Provide an annual assessment to the Chairman of the Joint Chiefs of Staff and the DSN and DRSN CCBs, respectively, on impact of emerging voice processing and transport technologies for global end-to-end voice performance and C2 services.

5.4.2.3. Ensure end-to-end interoperability, by providing all DoD dialing and numbering plans for telephony services for DoD.

5.4.2.4. Initiate and provide technical analysis of network survivability, to include a risk analysis, when proposing major changes in the DSN or DRSN network technology or architecture. DISA shall forward the results of the analysis to the Joint Staff for review.

5.4.3. Review, approve and implement DoD Components' requests for DSN service. If any request for service has a potential to harm the networks, DISA shall forward the request to the Chairman of the Joint Chiefs of Staff for resolution.

5.4.4. Review and forward, with recommendation, to the Chairman of the Joint Chiefs of Staff for approval, all requests for network access to the DRSN and connections between DRSN and non-DRSN secure voice equipment.

5.4.5. Ensure DSN and DRSN telecommunications switch compliance with references (c) and (d) requirements for interoperability and supportability.

5.4.5.1. Develop process, procedures and technical standards for Joint Interoperability Certification (JIC) of DSN and DRSN telecommunications switches.

5.4.5.2. Serve as the JIC authority for DSN and DRSN telecommunications switches.

5.4.6. Ensure DSN and DRSN telecommunications switch compliance with references (e), (f), (g) and (h) requirements for IA certification and accreditation.

5.4.6.1. Develop process, procedures and technical standards for IA certification and accreditation of DSN telecommunications switches.

5.4.6.2. Serve as the IA certification and accreditation authority for DSN telecommunications switches, and for the operation of DSN backbone and tandem switches.

5.4.6.3. Serve as the IA certification and accreditation authority for collateral DRSN telecommunications switches. Ensure TS/SCI DRSN telecommunications switches are submitted to DIA for accreditation.

5.4.7. Approve DoD Components' requests to install and connect telecommunications switches to the DSN. Serve as issuer of DSN and DRSN Authority to Operate (ATOs).

5.4.8. Process JIC or IA IATO requests for all uncertified telecommunications switches connected to or planned for connection to the DSN. Provide recommendation to the Military Communications-Electronics Board (MCEB) for approval of JIC IATO requests.

5.4.9. Develop and maintain a PPL of certified and accredited DSN telecommunications switches for use by DoD Components in lease or procurement of switch or switch services.

5.4.10. Conduct, with DoD Components, an annual inventory of DSN and DRSN telecommunications switches. Consolidate the DoD Components' input into a single comprehensive DoD inventory of telecommunications switches connected to the DSN and DRSN and submit this inventory to ASD(NII)/DoD CIO and the Chairman of the Joint Chiefs of Staff.

5.4.11. Conduct technical and security interoperability risk assessments and mitigation plans for uncertified telecommunications switches connected to the DSN. Submit risk

assessments and mitigation plans for uncertified telecommunications switches to ASD(NII)/DoD CIO and the Chairman of the Joint Chiefs of Staff for review.

5.4.12. Provide end-to-end CM reports for the DSN and DRSN derived from DoD Component's installation CM data.

5.4.12.1. Maintain a database of all switch configurations (Continental United States (CONUS) and Outside Continental United States (OCONUS)) and provide access to authorized DoD Components.

5.4.12.2. Chair and manage the DSN and DRSN CCBs. Implement approved and funded DSN and DRSN CCB actions. The DSN and DRSN CCBs shall ensure that configuration management information is collected and maintained, to include:

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

5.4.12.2.2. Network routing, dialing, and numbering scheme.

5.4.12.2.3. Switch databases.

5.4.12.2.4. Interface and control criteria.

5.4.12.2.5. Interoperability certification data and security certification and accreditation data on software and hardware of all telecommunications switches connecting to the DSN and DRSN.

5.4.13. Recommend, in coordination with the DoD Components, performance objectives for providing DSN services to satisfy the system requirements and reduce costs.

5.4.14. Based on the mission and traffic requirements provided by the DoD Components, design, engineer, develop, publish and annually update the DSN architecture.

5.4.15. Provide technical interface standards for equipment and telecommunications switches connected to the DSN and DRSN.

5.4.16. Approve, with the Chairman of the Joint Chiefs of Staff, use of network interfaces not conforming to the DSN interface criteria. Establish a method for controlling and monitoring the flow of traffic across the non-conforming network interfaces.

5.4.17. Manage, with the DoD Components, controlled interfaces between the DSN and the PSTN to fulfill communications requirements between DoD and non-DoD facilities and to provide alternative communications in the event of DSN disruptions.

5.4.18. Maintain standards for Standardized Tactical Entry Point (STEP)/Teleport facilities and manage the configuration and provisioning of STEP/Teleport sites to interface with deployed networks, to include those of the Joint Task Force backbone and components.

5.4.19. Provide system designs, configurations, and equipment required for the interconnection of EOs to implement ISDN services across the DSN.

5.4.20. Provide monthly reports to the Chairman of the Joint Chiefs of Staff on GoS performance across the DSN.

5.4.21. DISA shall establish, in conjunction with DoD Components, DSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost-effective service. DISA shall possess:

5.4.21.1. Both read-access and write-access capabilities to the telecommunications switches as defined by Combatant Command mission needs.

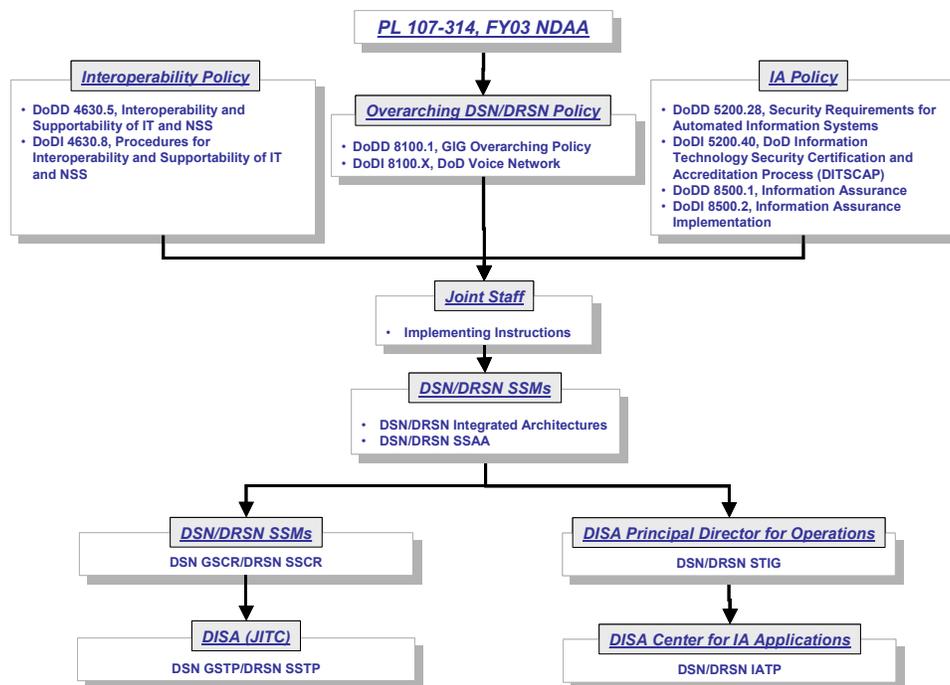
5.4.21.2. Ability to implement network control commands consistent with the mission needs of the Combatant Commands for all DSN switches.

5.4.21.3. Authority, during emergencies, to implement switch database revisions required for operation and management of the DSN.

6. Procedures

6.1. DoD DSN and DRSN Policy, Procedures and Technical Reference Documentation. PL 107-314 (reference (a)) establishes statutory requirements for installation and connection policy and procedures regarding DSN. The "GIG Overarching Policy" (reference (b)) establishes the basis for a common, or enterprise level, communications and computing architecture to provide a full range of information services for the Department. This Instruction is subordinate to reference (b) and provides policy, procedures and assigns responsibilities for test, certification, accreditation, lease or procurement, installation, connection, and operation of DSN and DRSN telecommunications switches and services on DoD voice networks. Figure F1. depicts the relationship between statutory requirements, DoD Directives and Instructions, implementing instructions of the Chairman of the Joint Chiefs of Staff and technical reference documents issued by DISA for the DSN and DRSN.

Figure F1. DSN and DRSN Policy, Procedures and Technical Reference Documentation



6.1.1. Interoperability Policy. Requirements for IT and NSS interoperability and supportability are contained in references (c) and (d). The Chairman of the Joint Chiefs of Staff shall ensure DSN and DRSN telecommunications switch compliance with requirements for interoperability; develop process, procedures and implementing instructions for JIC; and serve as the JIC validation authority. DISA shall develop process, procedures and technical standards for JIC; and serve as the JIC authority for DSN and DRSN telecommunications switches.

6.1.2. Information Assurance Policy. Requirements for IA certification and accreditation are contained in references (e), (f), (g) and (h). The Chairman of the Joint Chiefs of Staff shall ensure DSN and DRSN telecommunications switch compliance with requirements for IA certification and accreditation; validate IA requirements for DSN and DRSN telecommunication switches supporting joint and combined operations; and develop process, procedures and implementing instructions for IA certification and accreditation of DSN and DRSN telecommunications switches. DISA shall develop process, procedures and technical standards for IA certification and accreditation; and serve as the IA certification and accreditation authority for DSN and DRSN telecommunications switches. IA accreditation of DRSN switches providing TS/SCI service resides with DIA.

6.1.3. DSN and DRSN Technical Reference Documents. The DSN and DRSN SSMs shall develop and maintain the following DSN and DRSN telecommunications switch technical reference documents. These documents shall apply to all switches procured or leased and operated by DoD Components for installation and connection on the DSN and DRSN.

6.1.3.1. DSN and DRSN Integrated Architectures. The DSN and DRSN integrated architectures shall provide operational, systems, and technical views for the DSN and DRSN consistent with reference (j) architecture requirements. These architectures shall depict government-owned, DISA leased systems, and other DoD Component elements that provide long-haul communications and end-to-end voice, data and video services. These architecture products shall also include individual theater architectures, inter-theater connectivities, and intra-network interface specifications and end-to-end performance objectives such as GoS. The systems and technical view products shall describe network topologies, subsystems, interfaces and configurations, such as principal switch nodes, backbone and access transmission, network management systems, signaling systems, gateways to interfacing networks (including, tactical, NATO, Canadian and Pacific allies and other support components). The objective DSN and DRSN architectures and associated migration paths shall also be addressed in the DSN and DRSN integrated architectures.

6.1.3.2. DSN and DRSN System Security Authorization Agreements (SSAAs). The SSAAs shall document the operating agreements between the DAA, Certification Authority (CA), acquiring activity and users of the DSN and DRSN. The SSAAs shall contain a record of any changes made to the architecture, configuration, or security of the DSN and DRSN that may affect the accreditation status of the system. The SSAAs shall be used to verify the DSN and DRSN mission, environment, and architecture. It shall identify threats to the DSN and DRSN, and document compliance with certification and accreditation security requirements.

6.1.3.3. DSN Generic Switching Center Requirements (GSCR) and DRSN Secure Switching Center Requirements (SSCR). The GSCR/SSCR shall specify the technical requirements for a telecommunications switch and shall be used to support lease or procurement, and testing of DSN and DRSN telecommunications switches. The GSCR/SSCR shall identify the minimum switch requirements and features applicable to the overall DoD community for the

respective networks. The GSCR/SSCR shall also define and document interoperability requirements among telecommunications switches that are part of the DSN and DRSN. The DSN Generic Switch Test Plan (GSTP) and DRSN Secure Switching Test Plan (SSTP) shall be based on the requirements of the GSCR/SSCR.

6.1.3.4. DSN Generic Switching Test Plan (GSTP) and DRSN Secure Switching Test Plan (SSTP). The GSTP/SSTP shall specify interoperability test criteria for DSN and DRSN telecommunications switches connected or planned for connection to the DSN or DRSN. The GSTP/SSTP shall address interoperability requirements between new technologies; new technologies and the existing network; and the performance impact these new technologies on MUF.

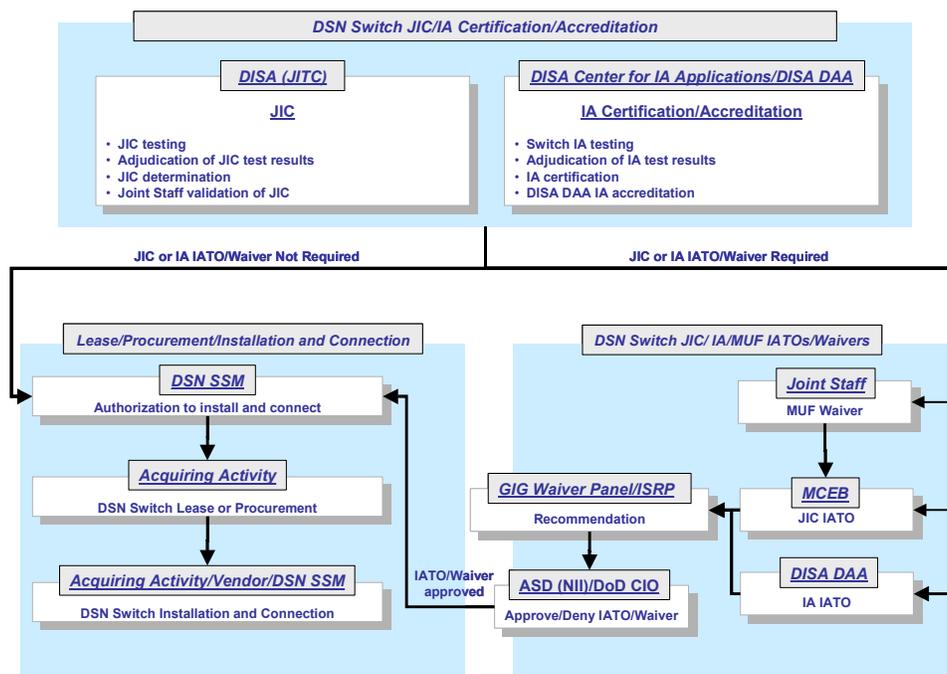
6.1.3.5. DSN and DRSN Security Technical Implementation Guides (STIGs). The DSN and DRSN STIGs shall provide the technical security policies, requirements, and implementation details for both the security features required for telecommunications switches, as well as the implementation guides for operating telecommunications switches by the DoD components. The STIGs shall support lease or procurement, testing and operational implementation procedures and assist DSN and DRSN sites in meeting the minimum requirements, standards, controls, and options for protecting telecommunications switch operations. The DSN and DRSN Information Assurance Test Plans (IATPs) shall be based on the DSN and DRSN STIGs.

6.1.3.6. DSN and DRSN Information Assurance Test Plans (IATPs). The IATPs shall provide security features test criteria for telecommunications switches connected or planned for connection to the DSN or DRSN. The IATPs shall evaluate security features within the existing network and critical areas involving MUF and new telecommunications technology. The IATPs shall also address security features between new technologies; new technologies and the existing network; and the performance impact of these new technologies on MUF. The IA testing shall be conducted, in accordance with the STIGs, prior to operation of telecommunications switches connected to the DSN or DRSN.

6.2. DSN Switch Certification and Accreditation Processes. Telecommunications switches (and associated software releases) procured or leased by DoD Components, and connected or planned for connection to the DSN, shall be both joint interoperability certified by DISA (JITC) and IA accredited by the DSN DAA. DISA (JITC) shall conduct JIC testing, adjudicate JIC test results, and provide JIC determination to the Chairman of the Joint Chiefs of Staff. The DISA Center for IA Applications shall conduct IA testing, adjudicate IA test results for the security features of the telecommunications switch. The DISA DAA may then issue an IA accreditation. Once a telecommunications switch has received both JIC and IA certification and accreditation, the acquiring activity may request authorization from the DSN SSM to install and connect to the DSN. When installed and connected, the telecommunications switch must be operated and maintained in accordance with the DSN STIG and the DISA (JITC) certified configuration. Telecommunications switch operation must be certified and accredited, on a site specific basis, by the DoD component as part of the overall DoD Information Technology Security Certification

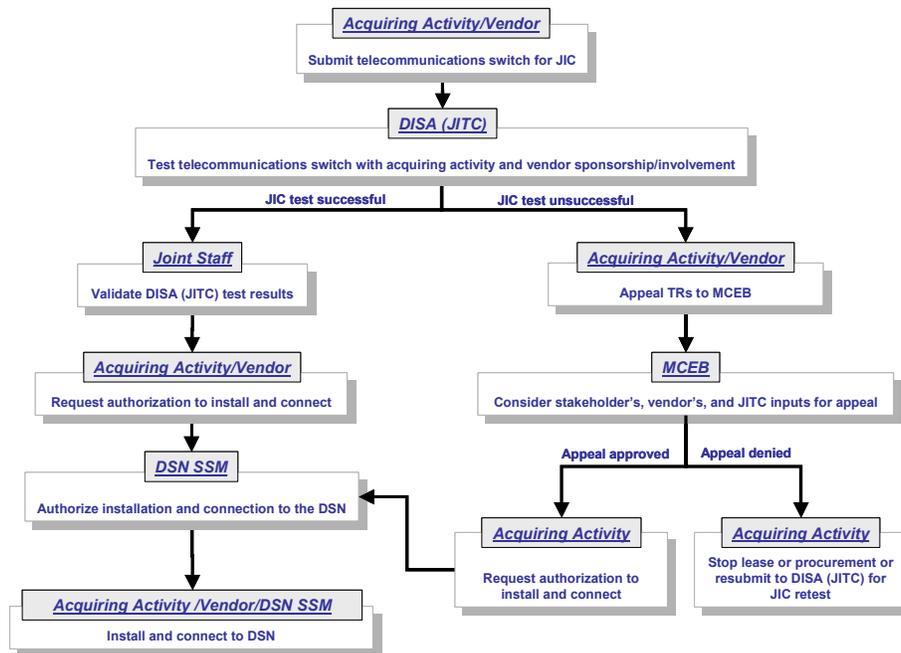
and Accreditation Process (DITSCAP) certification and accreditation process. This status shall be reported in the annual telecommunications switch inventory to the DSN SSM. If a telecommunications switch has not received a JIC and/or IA accreditation, and there is an urgent operational requirement for installation and connection, the acquiring activity may request a JIC or IA IATO, as appropriate. JIC and IA IATO requests shall be routed through the chain of command via the Chairman of the Joint Chiefs of Staff. The MCEB and DISA DAA shall provide a recommendation to ASD(NII)/DoD CIO for approval of the JIC or IA IATO, respectively, via the GIG waiver process. Only the ASD(NII)/DoD CIO may approve JIC and IA IATO requests. Figure F2. depicts an overview of the DSN switch JIC and IA certification and accreditation process.

Figure F2. DSN Switch JIC and IA Certification and Accreditation Process Overview



6.2.1. DSN Joint Interoperability Certification Process. The acquiring activity or vendor shall submit telecommunications switches to DISA (JITC) for JIC. DISA (JITC) will test the switch, with acquiring activity and vendor sponsorship and involvement. Figure F3. depicts the DSN JIC process.

Figure F3. DSN Joint Interoperability Certification Process

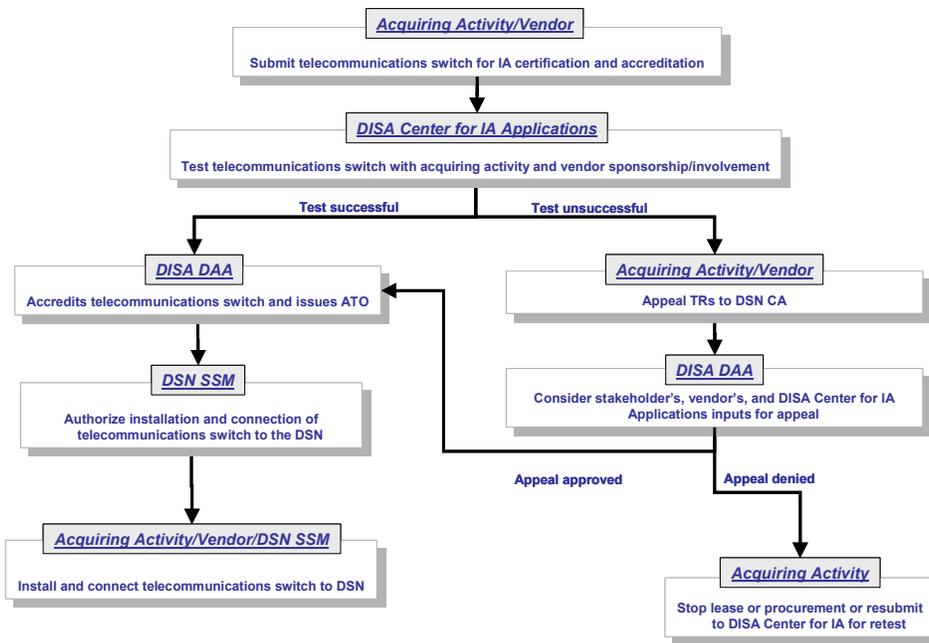


6.2.1.1. If the JIC test is successful, then the acquiring activity may request authorization to install and connect the switch to the DSN. Provided the switch has also received IA accreditation, the DSN SSM may issue an ATO. The acquiring activity may then install and connect the switch to the DSN. Once the telecommunications switch is installed and connected, the DoD component must ensure that the telecommunications switch is operated in the same configuration that was certified to preserve the integrity of the interoperability certification. Changes in configuration status shall be reported in the annual inventory to the DSN SSM.

6.2.1.2. If the JIC test is unsuccessful, then the acquiring activity or vendor may appeal the Test Results (TRs) to the MCEB. Provided the JIC test results are resolved during the appeal process, the acquiring activity may request authorization to install and connect the switch to the DSN and the DSN SSM may issue an ATO.

6.2.2. DSN Information Assurance Certification and Accreditation Process. The acquiring activity or vendor shall submit a request for IA test of telecommunications switches to the DISA Center for IA Applications. DISA Center for IA Applications will test the switch, with acquiring activity and vendor sponsorship and involvement. Figure F4. depicts the DSN IA certification and accreditation process.

Figure F4. DSN Information Assurance Certification and Accreditation Process



6.2.2.1. The test results will be provided to the DISA DAA for IA accreditation determination. If IA certification test is successful, the DISA DAA certifies and accredits the switch. The acquiring activity may then request authorization to install and connect the switch to the DSN. Provided the switch has also received JIC, the DISA DAA may issue an ATO. The acquiring activity may then install and connect the switch to the DSN.

6.2.2.2. If the IA certification test is unsuccessful, then the acquiring activity or vendor may appeal the Test Results (TRs) to the DISA DAA. Provided the IA test results are resolved during the appeal process, the acquiring activity may request authorization to install and connect the switch to the DSN and the DISA DAA may issue an ATO.

6.3. DRSN Switch Certification and Accreditation Processes. DRSN Telecommunications switches (and associated software releases) procured, leased, or operated by DoD Components, and connected or planned for connection to the DRSN, shall be both joint interoperability certified by DISA (JITC) and IA accredited by the DRSN DAA or DIA DAA, as appropriate based on classification level of service provided by the switch. Only DISA specified and approved (single vendor) DRSN telecommunications switches, authorized on a site-specific basis shall be installed and connected to the DRSN.

6.3.1. In coordination with the DRSN SSM, the DISA (JITC) shall conduct JIC testing and provide JIC determination to the DRSN SSM for review and forwarding to the Chairman of the Joint Chiefs of Staff.

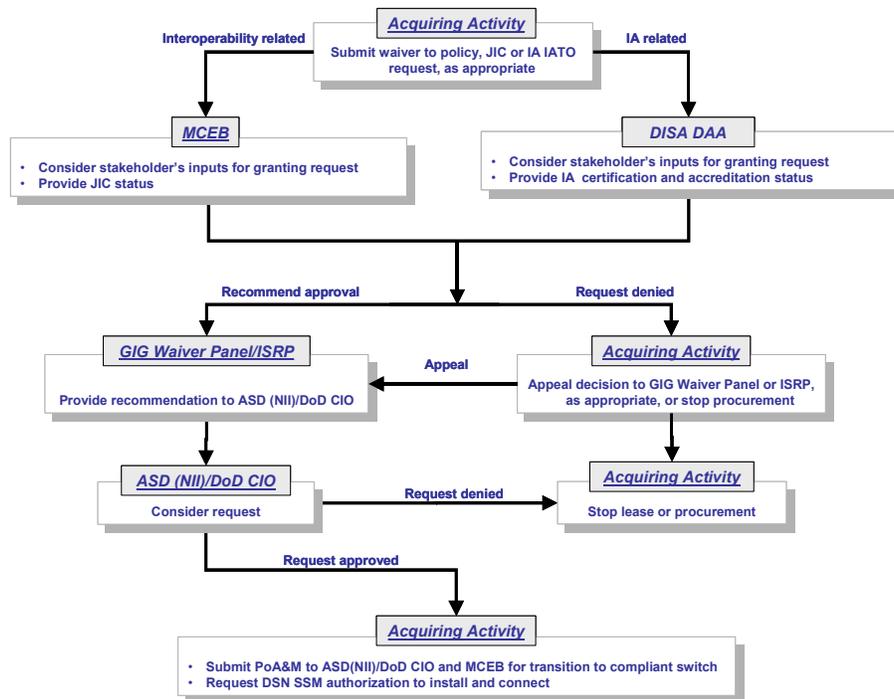
6.3.2. The DRSN SSM shall conduct IA testing and adjudicate IA test results for the security features of these DISA specified DRSN telecommunications switches. The DISA DAA or DIA DAA may then issue an IA accreditation, as appropriate.

6.3.3. Once a telecommunications switch has received both JIC and IA certification and accreditation, the acquiring activity may request authorization from the DRSN SSM to install and connect to the DRSN on a case by case basis. When installed and connected, the telecommunications switch must be operated and maintained in accordance with the DRSN interface criteria and the DISA (JITC) certified configuration. Telecommunications switch operation must be certified and accredited, on a site-specific basis, by the DoD component as part of the overall DITSCAP certification and accreditation process. This status shall be reported in the annual telecommunications switch inventory to the DRSN SSM.

6.3.4. If a telecommunications switch has not received a JIC and/or IA accreditation, and there is an urgent operational requirement for installation and connection, the acquiring activity may request a JIC or IA IATO, as appropriate. JIC and IA IATO requests shall be routed through the chain of command to the DRSN SSM for forwarding to the Chairman of the Joint Chiefs of Staff. The MCEB and DISA DAA or DIA DAA, as appropriate, shall provide a recommendation to ASD(NII)/DoD CIO for approval of the JIC or IA IATO, respectively, via the GIG waiver process. Only the ASD(NII)/DoD CIO may approve JIC and IA IATO requests.

6.4. Waivers to Policy and IATO Requests. It is DoD policy that all telecommunications switches (and associated software releases) procured or leased by DoD Components, and connected or planned for connection to the DSN or DRSN, shall be joint interoperability certified by DISA (JITC) and issued an IA accreditation by the DISA DAA. If a telecommunications switch has not received a JIC and/or IA certification and accreditation, and meets the conditions specified below, the acquiring activity may request a waiver to policy, or a JIC or IA IATO, as appropriate. Waivers to policy shall be submitted through chain of command to the ASD(NII)/DoD CIO, via the ISRP for approval. IATO requests shall be submitted through chain of command to the ASD(NII)/DoD CIO, via the GIG waiver process. Figure F5. depicts the waiver to policy, and JIC and IA IATO process.

Figure F5. Waivers to Policy and IATO Request Process



6.4.1. Waivers to provisions of this Instruction may be requested, in rare cases, under the following circumstances:

6.4.1.1. Urgent operational need, validated by the operational chain of command and the Chairman of the Joint Chiefs of Staff.

6.4.1.2. To accommodate introduction of new or emerging technology pilot programs that have been coordinated with, and recommended by the DSN or DRSN SSMs, and validated by the Chairman of the Joint Chiefs of Staff.

6.4.2. A JIC or IA IATO shall only be granted under the following conditions:

6.4.2.1. An urgent operational need, validated by the operational chain of command and the Chairman of the Joint Chiefs of Staff, requiring switch fielding prior to testing.

6.4.2.2. Telecommunications switches which are under test and DISA (JITC) is unable to assess all required interfaces.

6.4.2.3. A waiver to policy has been granted by ASD(NII)/DoD CIO.

6.4.3. To obtain a waiver to policy or IATO, the acquiring activity must prepare and submit a switch, configuration (end-to-end) and location specific request.

6.4.3.1. Interoperability related requests shall be submitted to the MCEB for consideration and adjudication. The MCEB may deny the acquiring activity's request, or forward a recommendation for approval to ASD(NII)/DoD CIO for decision, via the GIG waiver process or ISRP, as appropriate. If the MCEB denies the acquiring activity's request, the acquiring activity may appeal the MCEB's decision to the ASD(NII)/DoD CIO, via the GIG waiver process or the ISRP, as appropriate. Requests denied by the MCEB (unless appealed), or the ASD(NII)/DoD CIO, shall require the acquiring activity to stop lease or procurement of the telecommunications switch.

6.4.3.2. IA related requests shall be submitted to the DISA DAA or DIA DAA, as appropriate, for consideration and adjudication. The DISA DAA or DIA DAA may deny the acquiring activity's request, or forward a recommendation for approval to ASD(NII)/DoD CIO for decision, via the GIG waiver process or ISRP, as appropriate. If the DISA DAA or DIA DAA denies the acquiring activity's request, the acquiring activity may appeal the respective decision to the ASD(NII)/DoD CIO, via the GIG waiver process or ISRP, as appropriate. Requests denied by the DISA DAA or DIA DAA (unless appealed), or the ASD(NII)/DoD CIO, shall require the acquiring activity to stop lease or procurement of the telecommunications switch.

6.4.4. Waivers to policy or IATOs shall not be granted for a period of more than one year. Only in exceptional circumstances, and with ASD(NII)/DoD CIO approval, shall subsequent extensions of waivers or IATOs be granted. DISA shall maintain a database to track status of granted waivers and IATOs.

6.4.5. In cases where a waiver or IATO has been granted, the acquiring activity shall provide, within 30 days of receipt, a PoA&M for certifying or transitioning uncertified or unaccredited switches connected to the DSN or DRSN. DISA shall monitor acquiring activity's progress in achieving stated actions and milestones. Telecommunications switches that are not certified or accredited within the initial period of the waiver or IATO, shall be considered for disconnection from the DSN or DRSN.

6.4.6. In circumstances where a telecommunications switch does not meet DSN or DRSN MUF and/or other operational, functional or security requirements, a waiver must be first granted by the Chairman of the Joint Chiefs of Staff prior to requesting a JIC or IA IATO.

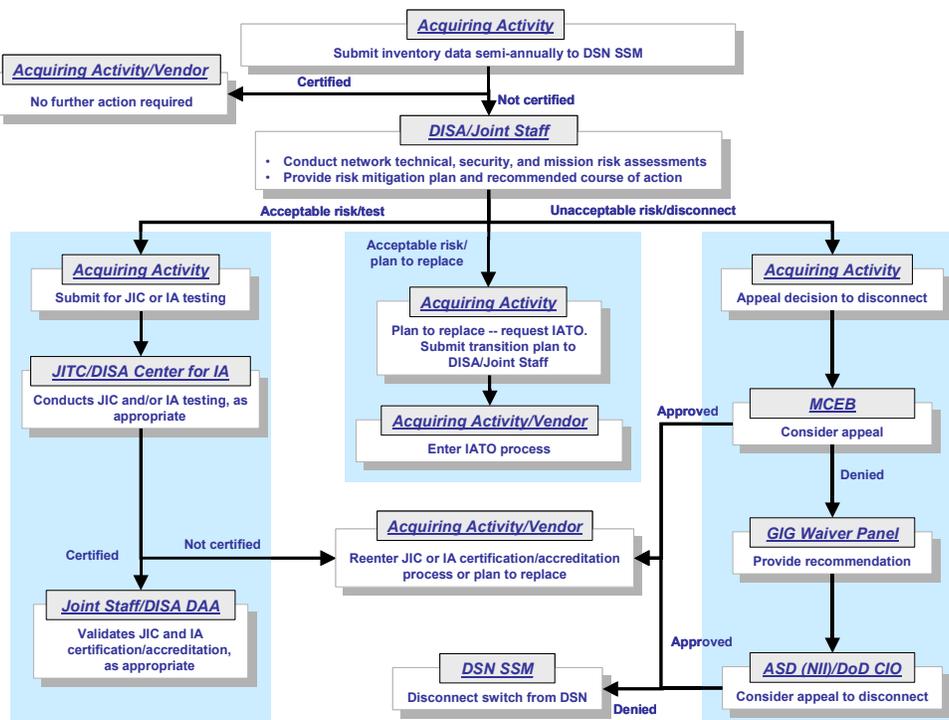
6.4.7. For non-DoD user installations, an IATO may be granted based on a satisfactory technical assessment of DSN or DRSN interface criteria shall be performed by the respective SSM.

6.5. DSN and DRSN Configuration Management (CM). The DSN and DRSN SSMs shall maintain configuration management over the DSN and DRSN to ensure software and hardware

remain joint interoperability certified and accredited; and are consistent with end-to-end performance requirements. To ensure CM of the DSN and DRSN is maintained, DoD Components shall coordinate all DSN and DRSN voice transport and processing initiatives with the DSN or DRSN SSMs, as appropriate. The DSN and DRSN CCBs, chaired by the DSN and DRSN SSM, respectively, shall review and approve changes to the DSN and DRSN that affect joint interoperability certification, accreditation and compliance with end-to-end performance requirements.

6.6. DSN Inventory, Risk Assessments and Mitigation Plans. To facilitate CM and risk management of the DSN, DoD Components shall compile and submit to DISA (on an annual basis) a complete inventory of all telecommunications switches that are connected, or planned for connection to the DSN (to include tactical switches) or public switched telecommunications networks. This inventory shall be used to assess risk associated with uncertified switches connected to the DSN and to develop course of action to mitigate these risks. The range of action, for uncertified or unaccredited switches operating on the DSN, may include submitting the switch for certification and or accreditation to disconnecting the switch from the DSN. Figure F6. depicts the process for conducting DSN inventory, risk assessments and developing associated mitigation plans.

Figure F6. DSN Inventory, Risk Assessments and Mitigation Plans



6.6.1. Inventory. DISA shall consolidate the DoD Components' input into a single comprehensive DoD inventory of telecommunications switches connected to the DSN and submit this inventory to ASD(NII)/DoD CIO and the Chairman of the Joint Chiefs of Staff.

6.6.2. Risk Assessments. DISA and the operating authorities shall use the compiled inventory to conduct technical and IA risk assessments and develop associated risk mitigation plans for uncertified telecommunications switches connected to the DSN. The Chairman of the Joint Chiefs of Staff shall conduct a mission risk assessment of uncertified switches; review DISA's technical and IA risk assessments and mitigation plans; and provide recommendations to the ASD(NII)/DoD CIO on the adequacy of these assessments and mitigation plans.

6.6.3. Mitigation Plans. For uncertified or unaccredited telecommunications switches operating on the DSN, DISA and the Chairman of the Joint Chiefs of Staff shall develop risk mitigation plans and provide recommended course of action to address uncertified or unaccredited switches.

6.6.3.1. Telecommunication switches determined to be an acceptable technical, IA and mission risk may be submitted to DISA for JIC or IA testing, as appropriate; or may be replaced with a certified and accredited switch from the PPL. In either case, the acquiring activity must obtain a JIC or IA IATO for the intervening period. If the telecommunications switch cannot be certified or accredited within the IATO period, then the acquiring activity shall plan to replace the switch with a certified and accredited switch from the PPL.

6.6.3.2. Telecommunication switches determined to be an unacceptable technical, IA or mission risk shall be considered for disconnection from the DSN based on DISA and Chairman of the Joint Chiefs of Staff recommendation. The acquiring activity may appeal the recommendation to disconnect to the MCEB. If the MCEB denies the acquiring activity's appeal, then the acquiring activity may appeal the MCEB's decision to the ASD(NII)/DoD CIO, via the GIG waiver process. If the ASD(NII)/DoD CIO denies the appeal, the acquiring activity shall replace the uncertified or unaccredited switch.

7. INFORMATION REQUIREMENTS

Reporting requirements identified in this Instruction are exempt from licensing according to paragraph C4.4.2 of DoD 8910.1-M (reference (i)).

8. EFFECTIVE DATE

This Instruction is effective immediately.

ASD(NII)/DoD CIO Signature Block

Enclosures - 3
E1. References, continued
E2. Definitions
E3. Acronyms

**E1. ENCLOSURE 1
REFERENCES, continued**

- (e) DoD Directive 8500.1 "Information Assurance (IA)," October 24, 2002
- (f) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (g) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988
- (h) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
- (i) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
- (j) "Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework," Version 2.0, December 18, 1997

E2. ENCLOSURE 2 DEFINITIONS

E2.1. Accreditation. Formal declaration by the DAA that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

E2.2. Assured Service or Connectivity. 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. 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.

E2.3. Backbone

E2.3.1. The high-traffic-density connectivity portion of any communications network.

E2.3.2. In packet-switched networks, a primary forward-direction path traced sequentially through two or more major relay or switching stations. In packet-switched networks, a backbone consists primarily of switches and inter-switch trunks.

E2.4. Certification. Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

E2.5. Certification Authority (CA). The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements.

E2.6. Configuration Management (CM)

E2.6.1. 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.

E2.6.2. The control of changes (including the recording thereof) that are made to the hardware, software, firmware, and documentation throughout the system lifecycle.

E2.7. Connection Approval. Formal authorization to interconnect information systems.

E2.8. Defense Agencies. All agencies and offices of the Department of Defense including the Ballistic Missile Defense Organization, Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Audit Agency, Defense Finance and Accounting Service, Defense Information Systems Agency, Defense Intelligence Agency, Defense Legal Services Agency, Defense Logistics Agency, Defense Threat Reduction Agency, Defense Security Cooperation Agency, Defense Security Service, National Imagery and Mapping Agency, National Reconnaissance Office, and National Security Agency.

E2.9. Defense Information Systems Network (DISN). 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.

E2.10. Defense RED Switch Network (DRSN). A secure C2 system which is a key component of DoD global secure voice services. The DRSN supports the secure voice and secure conferencing, requirements of the President, DoD Components, and select federal agencies in peacetime, crisis situations, and wartime. The DRSN is a separate, secure switched network that is considered part of the DISN.

E2.11. Defense Switched Network (DSN). 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 primary function.

E2.12. DSN and DRSN Users. 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.

E2.12.1. C2 Users. Users who have a requirement for Command and Control (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 or receives 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. There are two types of C2 users:

E2.12.1.1. Users approved by the Chairman of the Joint Chiefs of Staff, Combatant Commanders, Service, or agency for the Priority and ROUTINE precedence origination.

E2.12.1.2. DoD users having a military mission that might receive C2 calls for orders or direction at precedence above ROUTINE, even though they do not have a C2 mission for issuing guidance or orders. Therefore, these users must be served by switching facilities that provide the Military Unique Features (MUFs) of the DSN or DRSN.

E2.12.2. Special C2 Users. A special class of user who has access to the DSN or DRSN for essential communications for planning, directing, and controlling operations of assigned forces pursuant to assigned missions. This user requires capabilities that provide crises, pre-attack, and theater non-nuclear war telecommunications service for intelligence, alert, and strategic readiness. This user also requires communications among the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, and other members of the Joint Chiefs of Staff, Service Chiefs, and the Combatant Commanders. Specifically, these Special C2 users are identified through one or more Chairman of the Joint Chiefs of Staff, Combatant Commander, Service, or DoD agency validation processes. The following are required capabilities of Special C2 users:

E2.12.2.1. Chairman of the Joint Chiefs of Staff-approved Flash, Flash Override, or Immediate precedence origination.

E2.12.2.2. Combatant Commander validated minimum essential circuits.

E2.12.2.3. Combatant Commander or Service approved Immediate and Priority precedence origination.

E2.12.3. Non-C2 Users. DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirements to ever originate or receive C2 communications under the definitions for C2 and Special C2 Users. During a crisis or contingency, they may be denied access to the DSN or DRSN. These users are provided access to the DSN for the economic benefits to the DoD.

E2.13. Designated Approving Authority (DAA). Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk.

E2.14. 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.

E2.15. End Office (EO). A central office at which user lines and trunks are interconnected. 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.

E2.16. Grade of Service (GoS).

E2.16.1. The probability of a call being blocked or delayed more than a specified interval, expressed as a decimal fraction. 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.

E2.16.2. In telephony, the quality of service for which a circuit is designed or conditioned to provide; e.g., voice grade or program grade. Criteria for different grades of service may include equalization for amplitude over a specified band of frequencies, or in the case of digital data transported via analog circuits, equalization for phase also.

E2.17. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

E2.17.1. Includes any system, equipment, software, or service that meets one or more of the following criteria:

E2.17.1.1. Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

E2.17.1.2. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

E2.17.1.3. Processes data or information for use by other equipment, software, or services.

E2.17.2. Non-GIG IT. Stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network

E2.18. IA Certification and Accreditation (IA C&A). The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

E2.19. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.20. Information Technology (IT). Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT" includes National Security Systems (NSS).

E2.21. Installation. A grouping of facilities, located in the same vicinity, which support particular functions. If a facility has a particular function that is a part of a DOD organization's mission, then it would be considered an installation. Installations include all facilities on Military Department Forts, Posts, Camps and Stations as well as in Agency buildings and campuses.

E2.22. Integrated Services Digital Network (ISDN). An integrated digital network in which the same time-division switches and digital transmission paths are used to establish connections for different services. ISDN services include telephone, data, electronic mail, and facsimile. The method used to accomplish a connection is often specified; for example, switched connection, nonswitched connection, exchange connection, and ISDN connection.

E2.23. Military Communications-Electronics Board (MCEB). A decision making body chaired by the Chairman of the Joint Chiefs of Staff, and composed of the C4 heads of the Services, DIA, and NSA and the Director, DISA. This body deals with issues of interoperability and standardization between the Department of Defense and U.S. allies.

E2.24. Military Unique Features (MUFs). Those network and telecommunication switch features that are required to support C2 users and are above and beyond those supported by commercial carriers in telephony services to the general public. Military Unique Features include:

E2.24.1. Survivable Service. The guarantee that service is provided globally from peace, to crisis, to war.

E2.24.2. Assured Connectivity. The mission critical calls are completed end-to-end, despite degradation due to network disruptions, natural disasters, or surges during crisis or war using Multilevel Precedence and Preemption (MLPP) capability, if necessary.

E2.24.3. Responsive Service. The guarantee that C2 and Special C2 users always receive dial tone, never receive a busy signal and can interrupt a busy phone line to complete mission critical calls.

E2.24.4. Surge Capacity. The guarantee that C2 and Special C2 users always receive dial tone, never receive a busy signal and can interrupt a busy phone line to complete mission critical calls in spite of major traffic overloads due to global military actions.

E2.24.5. Secure Service. The guarantee that DSN and DRSN are configured to minimize attacks from enemies of the U.S. on the system that could result in denial or disruption of service.

E2.24.6. Interoperable Service. The guarantee that DSN and DRSN are designed with the capability to permit interconnection and interoperation with similar DoD, tactical, federal government, allied, and commercial networks.

E2.25. Multilevel Precedence And Preemption (MLPP). In military communications, a priority scheme:

E2.25.1. For assigning one of several precedence levels to specific calls or messages so that the system handles them in a predetermined order and timeframe;

E2.25.2. For gaining controlled access to network resources in which calls and messages can be preempted only by higher priority calls and messages;

E2.25.3. That is recognized only within a predefined domain; and

E2.25.2. In which the precedence level of a call outside the predefined domain is usually not recognized.

E2.26. 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.

E2.27. Nodal Switch. A tandem switch in the DSN that connects multiple EOs, provides access to a variety of transmission media, routes calls to other nodal switches, and provides network features such as MLPP. Nodal switches are supervised by and interconnected to the DSN A/NM subsystem. The two types of nodal switches in the DSN are:

E2.27.1. Stand-Alone (SA) Switch. The SA functions solely as a tandem switch in the DSN.

E2.27.2. Multifunction Switch (MFS). 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.

E2.28. 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. The ascending order of precedence for military messages is Routine, Priority, Immediate, and Flash.

E2.28.1. ROUTINE. Precedence designation applied to those official government communications that require rapid transmission by telephonic means but do not require preferential handling.

E2.28.2. PRIORITY. Precedence reserved generally for telephone calls requiring expeditious action by called parties and/or furnishing essential information for the conduct of government operations.

E2.28.3. IMMEDIATE. Precedence reserved generally for telephone calls pertaining to:

- E2.28.3.1. Situations that gravely affect the security of national and allied forces.
- E2.28.3.2. Reconstitution of forces in a postattack period.
- E2.28.3.3. Intelligence essential to national security.
- E2.28.3.4. Conduct of diplomatic negotiations to reduce or limit the threat of war.
- E2.28.3.5. Implementation of federal government actions essential to national survival.
- E2.28.3.6. Situations that gravely affect the internal security of the United States.
- E2.28.3.7. Civil Defense actions concerning U.S. population.
- E2.28.3.8. Disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population.
- E2.28.3.9. Vital information having an immediate effect on aircraft, spacecraft, or missile operations.

E2.28.4. FLASH. Precedence reserved generally for telephone calls pertaining to:

E2.28.4.1. Command and control of military forces essential to defense and retaliation.

E2.28.4.2. Critical intelligence essential to national survival.

E2.28.4.3. Conduct of diplomatic negotiations critical to the arresting or limiting of hostilities.

E2.28.4.4. Dissemination of critical civil alert information essential to national survival.

E2.28.4.5. Continuity of federal government functions essential to national survival.

E2.28.4.6. Fulfillment of critical U.S. internal security functions essential to national survival.

E2.28.4.7. Catastrophic events of national or international significance.

E2.28.5. FLASH OVERRIDE. A capability available to:

E2.28.5.1. The President of the United States, Secretary of Defense, and Joint Chiefs of Staff.

E2.28.5.2. Commanders of combatant commands when declaring Defense Condition One or Defense Emergency.

E2.28.5.3. Commander, U.S. Space Command 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.

E2.28.6. FLASH OVERRIDE OVERRIDE. A DRSN capability available to:

E2.28.6.1. The President of the United States, Secretary of Defense, and Joint Chiefs of Staff.

E2.28.6.2. Commanders of combatant commands when declaring Defense Condition One or Defense Emergency.

E2.28.6.3. Commander, U.S. Space Command 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.

E2.29. Private Branch Exchange (PBX).

E2.29.1. A subscriber-owned telecommunications exchange that usually includes access to the public switched network.

E2.29.2. A switch that serves a selected group of users and is subordinate to a switch at a higher level military establishment.

E2.29.3. A private telephone switchboard that provides on-premises dial service and may provide connections to local and trunked communications networks. 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.

E2.30. Public Switched Telecommunications Network (PSTN). Any common-carrier network that provides circuit switching among public users. 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.

E2.31. Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

E2.32. Risk Assessment. Process of analyzing threats to, and vulnerabilities of, an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures.

E2.33. Risk Management. Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected.

E2.34. Secure Terminal Equipment (STE). Telecommunications equipment providing 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, Combatant Commander, and Service or agency procedures.

E2.35. Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

E2.36. System Security Authorization Agreement (SSAA). A formal agreement among the DAA(s), the CA, the IT system user representative, and the acquiring activity. It is used throughout the entire DITSCAP to guide actions, document decisions, specify IT Security

(ITSEC) requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.

E2.37. 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.

E2.38. Validation. Determination of the correct implementation in the completed IT system with the security requirements and approach agreed on by the users, acquisition authority, and the DAA.

E2.39. Verification. The process of determining compliance of the evolving IT system specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and the DAA.

**E3. ENCLOSURE 3
ACRONYMS**

E3.1.1.	AIS	Automated Information System
E3.1.2.	ASD (NII)	Assistant Secretary of Defense for Networks and Information Integration
E3.1.3.	ATO	Authority to Operate
E3.1.4.	C2	Command and Control
E3.1.5.	C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
E3.1.6.	CA	Certifying Authority
E3.1.7.	CCB	Configuration Control Board
E3.1.8.	CIO	Chief Information Officer
E3.1.9.	CM	Configuration Management
E3.1.10.	CONUS	Continental United States
E3.1.11.	DAA	Designated Approval Authority
E3.1.12.	DIA	Defense Intelligence Agency
E3.1.13.	DISA	Defense Information Systems Agency
E3.1.14.	DISN	Defense Information Systems Network
E3.1.15.	DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
E3.1.16.	DoD	Department of Defense
E3.1.17.	DRSN	Defense Red Switch Network
E3.1.18.	DSN	Defense Switch Network
E3.1.19.	EO	End Office
E3.1.20.	GIG	Global Information Grid
E3.1.21.	GoS	Grade of Service
E3.1.22.	GSCR	Generic Switching Center Requirements
E3.1.23.	GSTP	Generic Switching Test Plan
E3.1.24.	IA	Information Assurance
E3.1.25.	IATO	Interim Authority to Operate
E3.1.26.	IATP	Information Assurance Test Plan
E3.1.27.	ISDN	Integrated Services Digital Network
E3.1.28.	IT	Information Technology
E3.1.29.	ITSEC	Information Technology Security
E3.1.30.	JIC	Joint Interoperability Certification
E3.1.31.	JITC	Joint Interoperability Test Command
E3.1.32.	MCEB	Military Communications Electronics Board
E3.1.33.	MFS	Multi-function Switch
E3.1.34.	MLPP	Multi-Level Precedence and Preemption
E3.1.35.	MUF	Military Unique Features
E3.1.36.	NMCS	National Military Command System
E3.1.37.	NS/EP	National Security and Emergency Preparedness
E3.1.38.	NSS	National Security System

E3.1.39.	OCONUS	Outside Continental United States
E3.1.40.	O&M	Operations and Maintenance
E3.1.41.	PABX	Private Automatic Branch Exchange
E3.1.42.	PAX	Private Automatic Exchange
E3.1.43.	PBX	Private Branch Exchange
E3.1.44.	PoA&M	Plan of Action and Milestones
E3.1.45.	PM	Program Manager
E3.1.46.	PPL	Preferred Product List
E3.1.47.	PSTN	Public Switched Telecommunications Network
E3.1.48.	PTT	Public Telephone and Telegraph
E3.1.49.	SA	Stand-Alone
E3.1.50.	SSAA	System Security Authorization Agreement
E3.1.51.	SSCR	Secure Switching Center Requirements
E3.1.52.	SSM	Single System Manager
E3.1.53.	SSTP	Secure Switching Test Plan
E3.1.54.	STE	Secure Terminal Equipment
E3.1.55.	STEP	Standardized Tactical Entry Point
E3.1.56.	STIG	Security Technical Implementation Guide
E3.1.57.	STU	Secure Telephone Unit
E3.1.58.	TDM	Time Division Multiplex
E3.1.59.	TR	Test Results
E3.1.60.	TSP	Telecommunications Service Priority
E3.1.61.	VoATM	Voice over Asynchronous Transfer Mode
E3.1.62.	VoIP	Voice over Internet Protocol
E3.1.63.	VTC	Video Conferencing