

# Memorandum for Record

## DEFENSE INFORMATION SYSTEMS AGENCY

P.O. BOX 4502  
ARLINGTON, VIRGINIA 22204-4502



IN REPLY

REFER TO: GS24

5 June 2008

### MEMORANDUM FOR RECORD

SUBJECT: Department of Defense's (DOD's) requirement for the Defense Information Systems Agency (DISA) to have read/write access to the telecommunications switches that make up the Defense Switched Network (DSN).

1. This memorandum for record provides clarification on the subject policy to ensure DISA has the required capabilities for Single System Management responsibilities, while ensuring the local Operations and Maintenance (O&M) organizations and commanders are allowed to maintain management control of their telecommunications switches for day-to-day operations.
2. Existing DOD policy, both DODI 8100.3 and CJCSI 6215.01C, stipulate requirements for DISA to be provided read/write access for DSN switches and acknowledges that the responsibility for switch database tables is shared between DISA and the Local Commanders. CJCSI 6215.01C states that "*DISA will attempt to coordinate with Service/Agency O&M personnel prior to implementation of any/all switch software changes.*" and "*DISA will coordinate with Service/Agency O&M personnel prior to implementation of any/all switch database changes consistent with local commander and combatant command needs and requirements.*" But, both of the instructions include the authority for DISA to make switch database changed in times of emergency.
3. The attached DSN Read/Write Access White Paper provides additional background, details, and clarification on these policies and provides point of contact information for the 24X7 DSN Controllers in the DISA's Global NetOps Support Center (GNSC) and Theater NetOps Centers (TNC).
4. All parties at the Apr 08 DSN Configuration Control Board (CCB) meeting understand the read/write policies and all members of the DSN CCB, including the JS and the ASD/NII representatives, supported the positions and clarifications provided in the DSN Read/Write Access White Paper, dated 25 April 2008, and concurred with the rationale supporting these positions.

  
Robert F McLaughlin  
Chief, Voice Services Division

Copy to:  
DSN CCB Chairman  
CCB Members

UNCLASSIFIED



---

---

**DEFENSE INFORMATION SYSTEMS AGENCY**

---

---

**DEFENSE SWITCHED NETWORK (DSN)  
READ/WRITE ACCESS  
WHITE PAPER**

**VERSION 1.0  
25 APRIL 2008**

**DEFENSE INFORMATION SYSTEMS AGENCY (DISA)  
NETWORK SERVICES  
VOICE SERVICES DIVISION, GS24**

UNCLASSIFIED

## 1 INTRODUCTION

This white paper is to provide clarification and outline the details to support the areas of responsibilities that are shared between the Defense Information Systems Agency (DISA) and the Department of Defense (DOD) Components that own and operate telecommunications switches in accordance with (IAW) DOD policies, DOD Instruction (DODI) 8100.3 and Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6215.01C. The specific focus for this white paper is in the requirement for DISA to access the DOD's telecommunication switches, hardware and software, that make up the Defense Switch Network (DSN). Additionally, it includes information to identify DISA access requirements to switching elements of the DSN for its Single System Manager (SSM) role.

Even though this white paper provides clarification and details for DISA's read/write access requirements, it is not intended to invalidate or necessitate the change for any existing agreements or relationships between the DISA and the DOD Component field organizations for the day-to-day operations of the DSN.

### 1.1 Background

DISA's network management (NM) responsibilities as the SSM for the DSN have included the requirement for read/write access to the switching elements for nearly twenty years. This was first documented by the SSM messages of 1988 as the DOD's voice network was transitioning from the Automatic Voice Network (AUTOVON) to the DSN and has been maintained in all versions of Joint Staff's policy for the DSN, since that time, to include Memorandum of Policy (MOP) 8 and the CJCSI 6215.01 series.

These requirements were revalidated and again formally documented in DODI 8100.3 by assigning DISA as the SSM for the DSN and specifically stating DISA shall "*Provide operational direction, management control, and technical guidance for the DSN*". Additionally, DODI 8100.3 also specifically addresses the requirement for DISA to have and be capable of using read/write switch access and network controls, in Paragraph 5.4.24, as follows:

*The DISA shall be granted:*

- *Both read- and write-access capabilities to the telecommunications switches as defined by the Combatant Command mission needs.*
- *Ability to implement network control commands consistent with the mission needs of the Combatant Commands for all DSN switches.*
- *Authority, during emergencies, for implementing switch database revisions required for operation and management of the DSN.*

CJCSI 6215.01C supports DISA SSM roles and provides further clarification on the network management requirements in Paragraph 8 of Enclosure A, Appendix A.

*8. Network Management. DISA establishes DSN management systems and procedures to ensure responsive, secure, interoperable, survivable, and cost effective service. The DSN is under the management control of the Director, DISA, on behalf of USSTRATCOM, and*

*is responsive to the CJCS and the DOD components. DISA will attempt to coordinate with Service/Agency O&M personnel prior to implementation of any/all switch software changes. The DOD components will ensure switch systems are certified for interoperability and IA accreditation or obtain an ICTO or waiver and interim authority to operate (IATO) prior to connection to the network. (See references f and pp).*

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

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

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

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

## **1.2 Scope**

IAW DODI 8100.3 and CJCSI 6215.01C, DISA has established management systems and procedures for the DSN to ensure responsive, secure, interoperable, survivable, and cost-effective service, as specified in DOD Directive (DoDD) 5105.19, DODI 8100.3, and CJCSI 6215.01C. DSN is under the operational direction and management control of the Director, DISA, and will be responsive to the CJCS, the Combatant Commanders, the MILDEPs, Defense Agencies, and DoD authorized activities. DISA will possess read/write access capabilities to all MFS and EO database tables, including those tables associated with non-DISA controlled networks, to support emergency requirements.

Although these requirements are understood to be global policy, it is further understood that in actual operations of the DSN, DISA's access to switches is currently limited to the OCONUS theaters and the six MFSs in CONUS, since connectivity of the ADIMSS to the CONUS EOs has yet to be funded and accomplished. The DSN SSM accepts the network management responsibilities and will work with the JS, Combatant Commanders (COCOMs), and O&M to identify and prioritize CONUS EOs for connection to the ADIMSS.

IAW DODI 8100.3 these policies are End-to-End and independent of technologies, to include Real Time Services (RTS) and existing Voice Over Internet Protocol (VoIP) systems.

It should also be noted that these policies are consistent with NETOPS and Global Information Grid (GIG) Enterprise Management (GEM) concepts (DISA NetOps Readiness Review Process, V2, 22 Feb 2007) to provide COCOMs support and situational awareness. NETOPS assured systems and network availability are achieved through visibility and control over the systems and network resources.

## **2 ACCESS REQUIREMENTS FOR DSN OPERATIONS**

The DSN is a dynamic network. Day-to-day operations include frequently adding or removing users, calling privileges, adding/changing trunks and trunk groups, and changing routing choices to support changes in traffic patterns/volume, military exercises or contingencies. Switch database tables must be updated to reflect and implement any of these changes. Although these areas are predominately responsibilities of the O&Ms, in practice, DISA is routinely requested to provide technical assistance in support of maintenance actions or the implementation and transition of new service activations.

However, DOD Policy acknowledges the potential for emergency requirements where DISA as the SSM would be required to assist. An emergency is considered to be any situations where the COCOMs might require DISA's crisis actions to support contingency operations or reconstitution efforts after a catastrophic event, be it a natural disaster or act of terrorism/war. Any situation where the DSN performance is deteriorated or deteriorating and immediate action is required to protect the health of the network and maintain C2 communications is also considered to be an Emergency.

In order to be pre-positioned for emergency support, DISA must have the capability to activate any/all system controls and the switch access privilege class for read/write access to all switch tables. But, IAW DOD and JS policy, DISA will not directly circumvent local O&Ms and Commands, if they are available and capable of implementing the database table changes or controls required. Additionally, if the requirement for table changes or network controls was not directed by the COCOM, DISA will notify the COCOM prior to directly accessing the switching systems. The theater Combatant Commander may direct additional access as required to meet theater operational needs.

Read/Write Access requirements can be generically categorized as being either NM Controls or Switch Database/Table changes.

### **2.1 NM Controls**

Although NM Controls may impact switch databases tables, these changes are temporary in nature and are necessitated by unusual changes/congestion in the network, either traffic surges or facility outages. These controls are implemented to modify call processing and/or routing in order to reduce traffic congestion, improve performance of the DSN, and maximize completion for Special C2 and C2 users.

DISA will have the ability to implement network control commands to all DSN MFS. DISA will attempt to coordinate with MILDEP Network Operations Security Centers (NOSC) for the

implementation of NM Controls IAW the table provided below in Paragraph 2.3. However, DISA, on behalf of USSTRATCOM, is authorized to implement these controls on a near real time basis during emergency situations to protect the global/theater network.

## 2.2 Switch Database Table Access

DSN uses digital Software Program Controlled (SPC) switches. The call processing software used by these switches includes an algorithm that executes a search of several database tables. Data fields in these tables are assigned certain values that determine how a switch processes a telephone call.

Although many of the switch database tables are nearly entirely the responsibility of the local O&M, many tables contain information where the responsibilities are shared between the O&M and DISA and others may be strictly in support of the DISA's backbone responsibilities, i.e. Common Channel Signaling.

While database tables contained in digital switches of other manufacturers may vary in content, all DSN switches, regardless of manufacturer, contain database tables with common data elements. These tables and the associated call processing parameters can be grouped into the following general functional categories:

- Telephone number assignment
- User class marking
- Signaling protocol
- Network call routing parameters
- Transmission system interface parameters

## 2.3 DISA Provided Technical Assistance

The local O&Ms and/or the NOSCs can get engineering support from DISA to augment the efforts of local technicians, to reduce dependency on the vendor provided Emergency Technical Assistance Support (ETAS), and to expedite the repair of critical services for the DSN users. As a normal practice the Service/Agencies should attempt to get assistance from the DSN Engineers stationed in DISA's Field Offices (GNSC and TNCs) first, but if more in-depth engineering assistance is needed DISA's JITC Hot line is always available as discussed below.

DISA has DSN Network Controllers on duty 24x7 and additional engineering resources on stand-by in each theater for NM of the DSN. These resources are available to assist in the restoral of systems or user services. The following contact information is provided for each of the DSN Theaters.

Table 2.3-1

DSN Theater	DSN Network Controller	
	DSN Number	Email Address
CENT	DSN: 318-439-3833	<a href="mailto:tnccentdsn@disa.mil">tnccentdsn@disa.mil</a>
CONUS	DSN: 312-770-9895	<a href="mailto:DSNOPS@disa.mil">DSNOPS@disa.mil</a>
EUR	DSN: 314-430-6373	<a href="mailto:Thomas.Dimock.ctr@disa.mil">Thomas.Dimock.ctr@disa.mil</a>
PAC	DSN: 315-456-0964/0965	<a href="mailto:Task9@disa.mil">Task9@disa.mil</a>

Additionally, DISA's JITC organization is set up to provide support for critical operational or contingency related interoperability problems that must be resolved as soon as possible and routine troubleshooting support requests. The following contact information is provided to facilitate acquisition of JITC's warfighter support.

### Critical Support

<http://jitc.fhu.disa.mil/critical.html>

Table 2.3-2

<b>Hotline Request Form:</b>	<a href="http://jitc.fhu.disa.mil/criticalsupport.html">http://jitc.fhu.disa.mil/criticalsupport.html</a>
<b>Toll-Free:</b>	<b>1-800-LET-JITC (538-5482)</b>
<b>Commercial:</b>	<b>1-520-LET-JITC (538-5482)</b>
<b>DSN:</b>	<b>TRY-JITC (879-5482)</b>
<b>Email:</b> (NIPRNet) <a href="mailto:hotline@disa.mil">hotline@disa.mil</a>	(SIPRNet) <a href="mailto:hotline@fhu.disa.smil.mil">hotline@fhu.disa.smil.mil</a>

JITC will contact you within one hour (24/7/365) at the provided contact number or email

### Routine Support

- **Unclassified Routine Request Form:**  
<http://jitc.fhu.disa.mil/support.html>
- **For Classified Support Requests:**
  - a. Fill out the Routine Request Form as above.
  - b. In the Request Information box - type, "please check classified email box".
  - c. Then please email: [hotline@fhu.disa.smil.mil](mailto:hotline@fhu.disa.smil.mil) to provide any classified details that may be required to explain the issues/problems.

## 3 DSN SWITCH ACCESS PROCEDURES

DISA field office personnel in all theaters will work separately with the O&Ms for specific processes and procedures to ensure consistency with local commander and combatant command needs and requirements are taken into consideration, but positive control of access and protection for Information Assurance is of utmost importance. Maintenance of passwords and logs will be determined by the local O&Ms and Commanders. This white paper only attempts to summarize requirements and establish top level guidance for Inter-Service/Agency procedures and the relationships with COCOMs.

The switch database change process involves both the switch O&M elements and DISA. The switch O&M element is the organization that normally actually implements the change to the switch database tables. However, the parameters required to perform database changes are determined by both the on-site MILDEP O&M element and the DISA engineers. In general, the MILDEP O&M Commands are responsible for the switch database tables and parameters that control on-base telephone service, while DISA is responsible for switch database tables and parameters that control network-related services. For routine business and day-to-day DSN operations, DISA will follow specific guidelines coordinated with the NOSCs and local O&M, as required, for any direct database table access that may be required to support information requirements or troubleshooting efforts. DISA's Switch Revision Message (SRM) process will

normally be used to provide the O&Ms with database table change requirements and the associated schedule/timetable for implementation.

The requirements that initiate the SRM process are normally received in a Telecommunications Service Order (TSO), and/or a Network Routing Order (NRO). DISA will determine if a switch database changes are required and if so, which switching systems are impacted. If schedules are critical, DISA will immediately work directly with the local O&M and Commands to coordinate implementation and follow-up with SRMs. As a norm, DISA will develop the appropriate table changes as a SRM. The SRM will then be uploaded onto disk in the appropriate switch/switches and an email notification forwarded to each impacted site. The SRM will contain all information necessary for implementation. A SRM will be prepared and transmitted to each MFS site or NOSC involved. In emergency or crisis conditions, DISA may implement database changes on line, as discussed above, but will follow-up with a SRM to the Site. Sites should ensure "Secret Logs" are enabled thereby providing a "track" of all switch database changes. Within 48 hours of implementation of the SRM, the MFS O&M Command will send a completion notice, by message to DISA (E-mail is acceptable for completion reporting).

Depending on the scenario, emergency conditions and requirements for network controls or switch database table changes to support routing changes, classes of service, or new service activations could be provided to DISA from the JTF/GNO or COCOM/TNCC. In these events, network controls may be immediately implemented, if the actions are required to protect global/theater communications network, DISA will first attempt to even work emergency requirements for network controls with the appropriate NOSC/O&M. On the other hand, for switch database table changes, DISA will always attempt to work through the NOSC/O&M, prior to remotely going directly into the switch for implementation of the required changes. In either case, if the situation dictates that DISA must directly implement either network controls or switch database table changes, follow-up coordination will be provided to notify the NOSC/O&M of the changes made and the requirement/circumstance/situation that necessitated the change be made immediately.

Since there are major differences between theaters with respect to the NETOPS command structures and the MILDEP organizational relationships for the O&Ms, detailed points of contact and procedures will vary by theater/region, but the tables below are provided here to show how direction for systems could flow from higher commands through DISA and down to the MILDEP O&Ms. Figure 1 reflects the relationships for direction from the JTF to each of the MILDEP's global operations centers and Figure 2 reflects the operations lineage from the COCOM to the O&M for theater requirements.

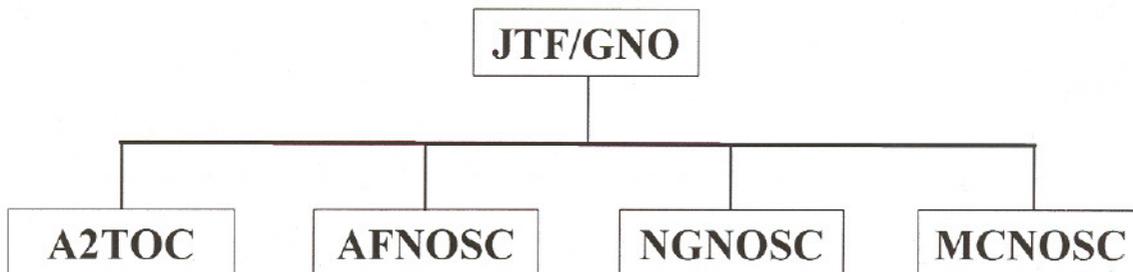


Figure 1 – JTF/GNO Operations contacts for the MILDEPs

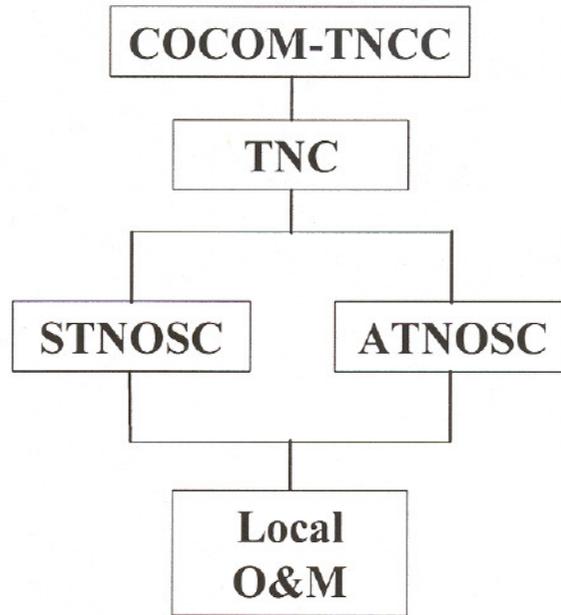


Figure 2 – COCOM Operations Direction

#### 4 SUMMARY

As discussed above, DOD and JS policies clearly require DISA to have access to DSN switches for both network controls and database table changes, but it is also clearly understood why the NOSC/O&Ms must be the first choice for implementing controls or database table changes. DISA will coordinate with the NOSCs and local O&M in each theater to establish theater/regional points of contact and the tactics, techniques, and procedures (TTP) (previously Standard Operating Procedures (SOP)) to ensure that DISA meets the needs and the requirements of the local commanders and the combatant commands.

**ACRONYMS**

A2TOC	ACERT ANOSC Theater Operations Center (Army's Global Ops Center)
ADIMSS	Advanced Defense Switched Network Integrated Management Support System
AFNOSC	Air Force Network Operations and Security Center
A/NM	Administration and Network Management
AO&M/NM	Administration, Operation and Management/Network Management
APL	Approved Products List
ATNOSC	Agency Theater Network Operations Security Center
AUTOVON	Automatic Voice Network
BPCS	Base/Post/Camp/Station
C2	Command and Control
CA	Certification Authority
C&A	Certification and Accreditation
CCB	Configuration Control Board
CCS	Common Channel Signaling
CCS7	Common Channel Signaling System No. 7
CJCSI	Chairman, Joint Chiefs of Staff Instruction
COCOM	Combatant Commander
CONUS	Continental/Contiguous United States
COS	Class of Service
DAA	Designated Approving Authority
DISA	Defense Information Systems Agency
DISAC	DISA Circular
DISAI	DISA Instruction
DISN	Defense Information Systems Network
DOD	Department of Defense
DODI	Department of Defense Instruction
DSN	Defense Switched Network
EO	End Office
ETAS	Emergency Technical Assistance Support
EUR	Europe
FOUO	For Official Use Only
FSO	Field Security Operations
GIG	Global Information Grid
GNSC	Global NetOps Support Center
GSCR	General Switching Center Requirements
GNO	Global Network Operations
I/O	Input / Output
IAW	In Accordance With
INFOSEC	Information Systems Security
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
JTF	Joint Task Force
JITC	Joint Interoperability Test Command
KBPS	Kilobits Per Second
LAN	Local Area Network
MCNOSC	Marine Corps Network Operations and Security Center
MFS	Multifunction Switch

UNCLASSIFIED

MILDEP	Military Department
MLPP	Multi-Level Precedence and Preemption
MOP	Memorandum of Policy
MUF	Military Unique Feature(s)
NAT	Network Address Translation
NCS	National Communications System
NGNOSC	Navy Global Network Operations Security Center
NM	Network Management
NMC	Network Management Center
NMS	Network Management System
NNM	Network Node Manager
NOC	Network Operations Center
NOSC	Network Operations Security Center
NRO	Network Routing Order
O&M	Operations and Maintenance
OCONUS	Outside CONUS
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
PAC	Pacific
PACOM	Pacific Command
PSTN	Public Switched Telephone Network
SOP	Standard Operating Procedure
SRM	Switch Revision Message
SPC	Software Program Controlled
SSM	Single System Manager/Management
STEP	Standardized Tactical Entry Point
STNOSC	Service Theater Network Operations Security Center
STP	Signaling Transfer Point (CCS7 device)
TNCC	Theater Network Control Center
TNC	Theater NetOps Center
TSO	Telecommunications Service Order
TTP	Tactics, Techniques, and Procedures

UNCLASSIFIED