DOD TELECOMMUNICATIONS AND DEFENSE SWITCHED NETWORK

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 3

30 April 2006

Developed by DISA for the DoD

This page is intentionally left blank.

TABLE OF CONTENTS

TABLE OF FIGURES

This page is intentionally left blank.

SUMMARY OF CHANGES from V2 R2

GENERAL CHANGES:

Updated Date, Version Number, and Release Number.

Corrected Table of Content import errors. Added STIGIDs throughout this document to replace the placeholders 'N/A'.

SECTION CHANGES:

SECTION 1. INTRODUCTION

Removed blank pages in Section 1.

Section 3.1.2 Information Assurance Vulnerability Management (IAVM)

Updated the second bullet by adding the STIGID DSN02.04.

Section 3.1.3 Vulnerability Management Systems

Updated the third bullet from DSN2.04 to DSN02.05.

Section 3.1.4 Compliance With Other STIGs

Added STIGID numbers to the bullets DSN03.01, DSN03.02, AND DSN03.03.

Section 3.1.5 System Procurement and DSN Connection Approval

Added the STIGID number to the bullets DSN03.04, DSN03.05, DSN03.06, DSN03.07.

Section 3.1.6 DSN APL Relationship to DITSCAP

Updated the second bullet by adding the STIGID DSN03.08.

Section 3.1.10 Configuration Management

Added the STIGID numbers to the *additional requirements* in this section: DSN17.04, DSN17.05, DSN17.06.

Section 3.1.11 Emergency Services

Updated the second bullet and added the STIGID DSN08.02.

Section 3.1.12 Speakerphones and Instruments In Classified Work Areas

Added the STIGID numbers DSN08.03, and DSN08.

Section 3.3.1.1 Authentication: User Accounts and Passwords

Updated the NOTE 2 under DSN13.03 and NOTE 3.

Section 3.3.2 Data Network Connectivity

Added the STIGID numbers to the bullets in this section, DSN04.07, DSN04.08, DSN04.09, and DSN04.10.

Section 3.3.3.3 Management Port Connectivity Via A Network

Added the STIGID numbers to the bullets in this section, DSN18.15, DSN18.16, and DSN18.17. Updated DSN18.17 to include “session”.

SECTION 5. SWITCH MULTIPLEX UNIT (SMU)

Added the STIGID numbers to all bullets in this section DSN20.01, DSN20.02, DSN20.03, DSN20.04.

SUMMARY OF CHANGES from V2 R1

GENERAL CHANGES:

Removed the system specific appendices from this document and made them separate individual appendices. These documents remain FOUO.

Replaced the FOUO designation of this document with UNCLASSIFIED. The purpose of this change is to allow more wide spread dissemination of the STIG while maintaining control over the distribution of the appendices to those who have the appropriate need to know.

SECTION CHANGES:

Section 1.3

Authority: Clarified the authority statement regarding the 8100.3.

Section 1.9 -

Configuration Guide Appendices: Added this section relating to the separate appendices.

Section 3.1.2 –

Information Assurance Vulnerability Management (IAVM) Program: Clarified this section

Section 3.1.3–

Vulnerability Management Systems: Clarified this section at the request of and in conjunction with the DSN PMO.

Section 3.3.4 –

Security Logon Banner: Clarified the verbiage of the requirement.

SUMMARY OF CHANGES from V1 R1

GENERAL CHANGES:

Changed Information Systems Security Officer and ISSO to Information Assurance Officer and IAO.
Changed Information Systems Security Manger and ISSM to Information Assurance manager and IAM.
Re-numbered figures throughout document.
Added DSN Potential Discrepancy Identifier (PDI) and Severity Code references to all requirements.
Globally changed “Services and Agency” and “MilDep” to “DoD component”.

SECTION CHANGES:

Sections 1, 1.2, 1.3: Introduction, Background, Scope, and Purpose

Rewrote section 1 to reflect the current DISA format for section 1 of all STIGS.
Removed the Purpose section and included appropriate verbiage in the Introduction.
Moved the bulk of the DSN description items to section 2.
Moved all requirement descriptions and bullets to other sections as appropriate.

Section 1: Introduction

Rewrote this section.
Removed “system failures” from the list of known threats. Added the words “operations and switching” to “DSN sites” in the first instance and “switch” to the second instance for clarity.

Section 1.1: Background

Rewrote this section.
Removed the first paragraph regarding authority and DITSCAP references. Removed the sentence “Although there is a wealth of information available regarding the potential risks associated with data networks, there is limited information regarding risks and countermeasures for voice networks.”

Section 1.2: Scope

Rewrote this section.

Section 1.3: Authority

Updated to the current FSO STIG authority verbiage and added verbiage to include the 8100.3. Defined the Mission Assurance Category acronym MAC as in MAC II

Section 1.4: Writing Conventions

Updated to the current FSO STIG writing convention verbiage.

-

Section 1.5: DISA Information Assurance Vulnerability Management (IAVM)

Updated to the current FSO STIG IVAM verbiage. Moved the VMS explanation and requirements to section 3.

Removed the section regarding extensions

Section 1.6: Vulnerability Severity Code Definitions

Added the section on severity codes.

Section 1.7: STIG Distribution

Updated to the current FSO STIG distribution verbiage.

Section 1.7.1: STIG Distribution to DSN Vendors

Added this section regarding distribution information for DSN vendors.

Section 1.8: Document Revisions and Support

Updated to the current FSO STIG document revision verbiage and added STIG support verbiage.

Section 2: DSN System Overview and Description

Created this section and collected all of the system descriptions here.

Section 2.1: DSN System Overview

Rewrote the system overview and description incorporating the generalized technical discussion items from all sections including those that were part of the introduction in section 1 including figures 1 and 2.

Clarified the description of the ADIMSS and switching sub-systems.

Delineated between the DSN “Backbone” and end user systems Added a description of what encompasses the end user systems.

Figure 1: This was Figure 4 from section 4.2 and revised the caption it.

Figure 2 : Was incorrectly numbered. Remained Figure 2

Figure 3; Was figure 2 in section 1, Clarified the PSTN and other government networks text box. Added “performance” to the DSN Concerns text box.

Section 2.2: DSN Backbone Devices And Sub-Systems

This section was section 2. Rewrote.

Section 2.2.1: Node switches

This section was section 2.1

Added (TS) following Tandem Switch, followed by “is a “backbone” device and is”; Added “(trunks)“ following “terminates circuits “.

Section 2.2.2: Signaling Network

This section was section 2.2
Second paragraph, replaced CCS-7 with CCS7 and replaced “such as the Global Positioning System (GPS)” with “as described in section 2.5.”

Section 2.2.3: Network Management

This section was section 2.3
Moved figure 3 up to section 2. Moved the discussion of the ADIMSS to section 4. Rewrote the section to describe general telecommunications network management, define OAM&P and the ADIMSS and delineate DISA and DoD component responsibilities.

Section 2.2.4: Transmission & Transport

This section was section 2.4

Section 2.2.5: Timing and Synchronization

This section was section 2.5
Added “Stratum 1” in front of “frequency reference” and replaced “Loran C” with “the Global Positioning System (GPS)”.

-

Section 2.3: DSN Topology

This section was part of section 4.2
Copied figure 4 to here. Revised the caption.

Section 2.4: DSN Switching System Descriptions

This section was section 4.1
Removed "but focuses on the DSN backbone switches" from the first sentence. Added a listing of switch types to define the acronyms. Added the "DoD Generic Switching Center Requirements (GSCR) document" to the first paragraph.

-

Section 2.4.1: DSN Backbone Switches

This section was section 4.1.1
Reworded for clarity. Clarified statements regarding the Tandem Switch. Moved vendor switch models to a sub bullet here and reworded.

Section 2.4.1.1: DSN Backbone Switch Vendor Models

This section was section 4.1.3

Section 2.4.2: Base, Post, Camp, or Station Functional Switch Types

This section was section 4.1.2
Reworded for clarity. Removed the reference to the rigor of certification testing. Removed references to PABX. Added PBX Type 1 and 2 description verbiage.

Section 2.5: Common Channel Signaling (CCS)

This section was section 5
Relocated the topic description cleaned up Figure 6 (was 5.1) SS7 network

Section 2.5.1: Signaling System 7 (SS7)

This section was section 5.1
Relocated the topic description
Section 2.6: Transmission & Transport
This section was part of section 7
Relocated the topic description

Section 2.7: ADIMSS

This section was sections 3 and 3.1
Added information moved from section 1 and rewrote for clarity. Incorporated additional information provided by the ADIMSS PM.

Section 2.7.1: ADIMSS Mission

This section was part of section 3.3

Section 2.7.2: ADIMSS Description

This section was section 3.3

Section 2.7.3: Network Management; DOD Components and Contracted Service

This section is new containing information provided by the ADIMSS PM.

Section 2.7.4: ADIMSS Topology

This section was section 3.4
Figure 7 was figure 3

Section 2.7.5: OAM&P / NM - OCONUS DSN

This section is new containing information provided by the ADIMSS PM.

Section 2.7.6: OAM&P / NM - CONUS DSN

This section is new containing information provided by the ADIMSS PM.

Section 2.7.7: OAM&P / NM Hawaii DSN (HITS)

This section is new containing information provided by the ADIMSS PM.

Section 3: DSN And DOD Telecommunications Security Concerns And Requirements

Collected all requirements and vulnerability discussions to this section and rewrote these sections for clarity as necessary.
Added verbiage defining a DSN site

Section 3.1: Administrative And General Requirements

Collected all general requirements into this section

Section 3.1.1: Information Assurance Officer

This section was under section 1.4 Scope
Clarified the verbiage concerning the establishment of a IAO position
DSN01.01, .02, .03 re wrote to proper PDI style and clarity

DSN01.03, rewrote for clarity. This had been written in to require the IAO to provide access without stating any limitation.
DSN16.01, moved this PDI from old section 8.5 in support of the requirement to assign an IAO. Rewrote for clarity.

Section 3.1.2: Information Assurance Vulnerability Management (IAVM)

This section was part of section 1.6 IVAM and DISA VMS
Rewrote for clarity.
DSN02.03, .05, moved this PDI from the section on VMS and Clarified the verbiage in this requirement regarding response to IVAM notices

Section 3.1.3: Vulnerability Management Systems

This section was part of section 1.6 IVAM and DISA VMS
Updated to the current FSO STIG VMS verbiage along with clarification regarding the tracking of Non DISA equipment. Also updated the VMS account / help contact information and location of the VMS CBT.
DSN02.01, Clarified the VMS requirement for DISA and added a caveat for non DISA owned equipment.
DSN02.02, Clarified the requirement for registration of SAs in VMS and other tracking systems and added a caveat for non DISA owned equipment.
Added PDI for systems and SAs not registered with VMS

Section 3.1.4: Compliance With Other STIGs

Added this section including a list of other applicable STIGS
Added PDI for DSN compliance with all applicable STIGs
Added PDI for compliance with all applicable STIGs
Added PDI for commercial systems compliance with all applicable STIGs

Section 3.1.5: System Procurement and DSN Connection Approval

Added this section relating to the DSN APL
Added PDIs for compliance with 8100.3 DSN APL requirements

Section 3.1.6: DSN APL Relationship to DITSCAP

Added this section relating to the DITSCAP
Added PDI for compliance with DITSCAP

Section 3.1.6.1: Site Security Baseline

This section was part of section 4.3

Section 3.1.7: Security Documentation

This section was section 8.1
Added reference to the DoDI 8100.3, other applicable STIGS, and DSN APL certification documentation.

Section 3.1.8: Physical Security

This section was section 8.3
Replaced “AN/M” with “OAP&P / NM”
Removed “Defense Communications Agency Circular (DCAC) 310-90-1, Physical Security Measures for Defense Communications System (DCS) Facilities, 10 November 1983” from second paragraph.
DSN14.01, generalized and clarified the requirement

Section 3.1.9: Personnel Security

This section was section 8.5
DSN16.01, moved this PDI to section 3.1.1

Section 3.1.9.1: Foreign National Personnel

This topic was part of section 4.4.1
Added this section and requirements as clarification of the subject
Added 3 PDIs

Section 3.1.10: Configuration Management

This section was section 8.6
Added “The IAO will ensure that” to the 3 requirement bullets.
DSN17.02, Added “off site” to the requirement for back-up storage.
Added PDIs relating to installation of patches and version releases.

Section 3.1.11: Emergency Services

This section was section 4.4.3
Clarified this paragraph and requirement regarding emergency services to include non-US systems.
DSN08.01, Replaced “Switch Administrator” with “IAO”
Added verbiage relating to emergency systems in response to public law following 9-11-2001.

Section 3.1.12: Speakerphones and Instruments In Classified Work Areas

Added this as a section and requirements.
Added PDIs to address this topic.

Section 3.2: System Specific Technical Security Requirements

Created this section from section 8 and others.

Section 3.2.1: Switch Security Concerns

This section was part of section 4.3
Moved descriptive verbiage to section 2
Distributed the PDIs appropriately through the subsequent sections. Rewrote for clarity.
Changed “Maintenance Access Port (MAP)” to “Man Machine Interface (MMI)” in second paragraph.
Removed “dedicated” and added “switch by a” in the 3rd paragraph.

Section 3.2.1.1: Switch Security Capabilities

Added this as a section. The information was part of section 4.4
DSN04.05, Clarified the topic and requirement verbiage regarding the attendant console.

Section 3.2.1.2: PBXs & Attendant Console

Added this as a section. The information was part of section 4.3
Added “Base” to “Base/Post/Camp/Station” in first paragraph and updated the acronym.

Section 3.2.1.3: Remote Switching Units (RSUs)

Added this as a section. The information was part of section 4.3

Section 3.2.1.4: Direct Inward System Access and Voice Mail Services

This section was section 4.4.2
DSN07.01 thru .04, removed “DISA” and “or” from “DISA or Voice Mail services” for clarity.
DSN07.01, Clarified for grammar
DSN07.04, Clarified for grammar
Section 3.2.2: OAM&P / NM and ADIMSS System Security Concerns
This section was section 3.5
Rewrote using information provided by the ADIMSS PM.
DSN03.01, 02, 03 Removed the PDIs from the requirements since they expand on the applicability of other STIGs and DSN02.10
Changed “Oracle” to “Database” in database review requirement

Section 3.2.3: SS7 Security Concerns and Requirements

This section was section 5.2
Rewrote the first and second paragraphs for grammar and clarity
Clarified the verbiage and requirements regarding labeling and diverse routing of redundant power cabling and A-links for SS7 equipment.
Added a paragraph and requirement SS7 link encryption.

Section 3.2.4: Transmission & Transport Security Concerns and Requirements

This section was section 7
DSN11.01, Added, “leaving the B/C/P/S” following “circuits”.

Section 3.3: Common Technical Security Requirements

Added this section.

Section 3.3.1: Authentication, Authorization, and Accountability (AAA)

Added this section.

Section 3.3.1.1: Authentication: User Accounts and Passwords

This section was section 8.2
DSN13.03, Clarified the requirement for shared user accounts
DSN13.03, Clarified the requirement on requiring usernames and passwords
DSN13.06, Rewrote the requirement to be in line with the password complexity requirements in the 8500.1.
DSN13.07, Changed password change interval from “180” to “90” days or less.
DSN13.13, Added “before or” to the expiration prompt requirement.
DSN13.14, Replaced the word “or” with “and” in “secure and controlled manner.”
Added PDI regarding remote authentication
DSN13.17, Added this requirement regarding strong two-factor authentication

Section 3.3.1.2: Authorization: Discretionary Access Control

This section was from section 4.4 and 4.4.1
Rewrote for clarity
Added “for its general use.” To the end of the first sentence.
Added “(i.e. the IAO).” following “security officer” in the second paragraph.
DSN06.03, rewrote for clarity and broadened the scope.
Removed the reference to foreign nationals from this section along with the requirement bullet.

Section 3.3.1.3: Accountability: Auditing and History

This section was section 8.4
DSN15.01 to 07, rewrote to proper PDI style
Added PDI “Record security relevant actions (e.g., the changing of security levels or categories of information)”.

Section 3.3.2: Data Network Connectivity

Added this section.
DSN04.01 is removed and superceded by DSN18.20

DSN04.03, .04, relocated these PDIs from another section, rewrote for clarity as needed.
Added PDIs to detail requirements for network connectivity.
Section 3.3.3: Remote And Local System Management Access
This section was section 8.7 reorganized into 3 subsections
Rewrote this section for clarity. Split it to detail the difference between local and network management vs. modem management, making 3 sections, general, modem, and network.

Section 3.3.3.1: General Requirements

This section was part of section 8.7
DSN18.07, .09, .10, .12, .13, Moved these PDI to here
DSN18.09, Changed "a link encryption mechanism" to "a FIPS140-2 compliant encryption mechanism". Also reworded for clarity.

Section 3.3.3.2: Serial Console Ports and Modem Access

This section was part of section 8.7
Moved "In addition, if an unauthorized person has physical access to a site's modems, the switch settings can be changed to affect the security of a system" from first bullet to first paragraph.
Replaced "modem phone lines" with "modems used to provided MMI to switching and signaling systems".
DSN18.03, Added "that appear on the DSN APL" to the requirement.
DSN18.11, .14, Changed these requirements to reflect applicability to serial connections.
Section 3.2.3.3: Management Port Connectivity Via A Network
This section was part of section 8.7
Added PDIs to detail requirements for management via network connectivity.
DSN04.02, relocated this PDI from another section, rewrote for clarity

Section 3.2.4: Security Logon Banner

This section was section 8.8
Rewrote for clarity and inclusion of minimum requirements. Included examples.

Section 4: Voice Over Internet Protocol (VoIP)

This section was section 6
Updated and clarified this section regarding VoIP using verbiage provided by the PMO.
Removed the requirement that VoIP not be the primary system for C2 users.
DSN10.01, Removed this PDI relating to the DSN APL. Superceded by requirements earlier in the document.
Added the PDI requirement to be in compliance with the VoIP, DSN and all other STIGS

Section 5: Switch Multiplex Unit (SMU)

This section was Appendix B
Corrected the responsible party in the first bullet. Reworded for clarity.
Added a requirement to not connect management ports to other networks.

Appendix A: Related Publications

Added “Department of Defense Instruction (DoDI) 8100.3, 16 JAN 03.” to list of Government Publications.
Added “Department of Defense Voice Network Generic Switching Center Requirements (GSCR) Document, 8 September 2003” to list of Government Publications.

Appendix B: Glossary of Terms
This section was Appendix H
Added the following terms to the glossary. AAA, ACD, APL, ADM, ANI, BPCS, BAN, CAN, CTI, DAC, DNS, DSAWG, DTSW, ESM, FTS, GETS, GPS, GSCR, HITS, I/O, IA, IAM, IAO, IS, ISUP, JITC, JWICS, MAC, MAN, MTP, MUF, NOC, NMS, OS, OMAP, PBX1, PBX2, PDI, PIN, PM, SIPRNet, SDID, SCP, SCCP, SMU, SMEO, SS7, SSP, TCAP, TOE, TS, TNM, UNIX, VCAO, and VOIP
Merged VoIP STIG glossary with this one also adding CAT, COS, CTIM, DC, DECC, DoS, HID, HTTP, IASE, IETF, IPSEC, ITU, LDAP, MAC, MCU MG, MGC, MGCP, MS, NAT, NTP, OSD, PC, PCM, PRI, QBE, QoS, RAS, RFC, SCCS, SG, SIP, SMB, SQL, SSL, TAPI, TDM, TFTP, UA, UAC, UAS, UDP, URL, VLAN, VPN, WLAN

Appendix C: Nortel Switch

Added “TABLE AND TUPLE SETTINGS” heading to section and changed PASSWORD_LIFETIME parameter setting from “180” to “90” in the same section.
Removed all references to default settings in all table configuration sections and added required setting parameters.

Former Appendix G. Interim Voice Over Internet Protocol (VoIP) Policy Message

Removed this section. Superceded by section 4

1. INTRODUCTION

This Security Technical Implementation Guide (STIG*)* provides the technical security policies, implementation details, and requirements for applying security concepts to the Department of Defense (DoD) telecommunications systems. While the focus of this STIG is the Defense Switched Network (DSN), the DSN is only one of the systems or programs providing telecommunications services to the DoD. The application of the requirements and concepts contained in this STIG pertain to all telecommunications systems and programs supporting the DoD.

The DSN encompasses inter-base and intra-base non-secure and/or secure C2 telecommunications systems that provide end-to-end common use and dedicated telephone service, voice-band data, and dial-up video teleconferencing (VTC) for authorized DoD C2 and non-C2 users in accordance with national security directives. Non-secure dial-up voice (telephone) service is the system's principal requirement. The span or scope of the DSN covers the Continental United States (CONUS) and a large portion of the world Outside CONUS (OCONUS).

The Defense Information Systems Agency (DISA) is the Single System Manager providing operational direction and management control of the DSN. DISA is responsible for establishing DSN policies and procedures and ensuring their enforcement. DoD Components and in some cases commercial providers are responsible for the implementation of these policies and procedures, along with the day-to-day operations and management of their portions of the system at a local level.

DISA has management responsibility for the portion of the DSN that includes inter-switch trunks (ISTs), terminating equipment for the ISTs, community-of-interest trunks, direct access circuitry, trunk and network functions, features and functions of the DSN switches, and Special C2 user equipment at the switches. Management, operations and maintenance for all other base, post, camp, and station functions, including local number assignments for users, is the responsibility of the various DoD Components and commercial service providers.

This STIG is intended to be used in conjunction with the other STIGs developed for the DoD by DISA. The Enclave, Network Infrastructure, and Voice over Internet Protocol (VoIP) STIGs provide crucial guidance for securing the networks that are part of DSN systems or to which DSN systems are connected. The operating system (OS) STIGs provide additional crucial guidance, where applicable, for securing the platforms (e.g. servers, management stations, and user workstations) on which some of the DSN systems run. The STIGs that cover database, web server products, and desktop applications provide guidance to ensure that those services, when used by DSN systems, also support a secure environment.

The purpose of the STIG is to make recommendations and assist DSN operations and switching sites with meeting the minimum requirements, standards, controls, and options for protecting telephone system operations. All DSN switch or system owners, operators, administrators, and maintenance personnel must strive to maintain the level of security as presented in the latest version of this document. Each site must strive to ensure its mission is carried out in support of its customer's requirements, especially when the customer is the warfighter. In the case of a DSN switch site, all measures must be taken to securely, effectively, and efficiently operate, administer, and maintain the critical devices that make up the DSN's infrastructure.

System security is an ever-changing requirement due to the fact that new threats are realized every day. For this reason, this document, along with its accompanying checklist, will be updated periodically to keep pace with the changing threats. Customarily, STIGs are revised annually while checklists and tools can be updated monthly.

The recommended audience for this STIG is the multitude of system owners, operators, and system administrators all across the DoD. This STIG applies to all telecommunications systems, as well as all peripheral systems and devices connected to the DSN whether owned by DISA, another DoD component, a DoD contractor, or other government agency that receives DSN service.

Because customer-driven requirements and site operating environments are so varied, a cookie-cutter approach to telecommunications network security is not practical. The telecommunications system owner in cooperation with customers and the following key individuals must weigh security with operational necessities.

The key individuals to be coordinated with are:

- Program Managers/Project Managers (PMs)
- DISA Field Security Operations (FSO)
- Information Assurance Managers (IAMs)
- Information Assurance Officers (IAOs)
- Network Security Officers (NSOs)
- Telecommunications Managers
- System Administrators (SAs)
- DoD component representatives

The telecommunications system owner is defined as "the person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the system," (per *DOD Instruction 5200.40* (DITSCAP) dated 30 December 1997).

The various applicable STIGs provide minimum baseline requirements for system security. Some STIGs overlap in some requirements, and they may conflict. The best approach is to apply the more stringent requirement if this occurs, while understanding the portion of the system that to which the requirement applies. Each site may implement additional or more stringent security measures as necessary to optimize the system's overall protection, but only with operational consideration and the prior approval of the site IAO.

As with all technology, security awareness and the posturing to counter intended and unintended disruptions are an evolving effort. Some of the threats are listed below; their protective measures will be the focus of this guide.

- Interception of communications
- Communications traffic analysis
- Modification of signaling or traffic
- Denial of service

1.1 Background

For DoD purposes, an Information System (IS) is a set of resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of national security information. This definition applies to all voice, data, and video systems employed by the DoD. The DSN and its components therefore fall into the IS category.

IA is defined as services that provide for system or data availability, integrity, and confidentiality, as well as user authentication, and/or non-repudiation. An IA device, product, or technology is one whose primary role is to provide any of the security or IA services. An IA-enabled product is a product or technology whose primary role is not security, but which provides security or IA services as an associated feature of its intended operating capabilities.

The Defense Information Systems Agency (DISA) Field Security Operations (FSO) Guidance and Processes Branch develops IA guidelines for the DoD. These guides are called Security Technical Implementation Guides or STIGs. Compliance with all applicable STIGs is mandatory for all DoD Information Systems (ISs).

The DSN is one of the sub-systems within the Defense Information Services Network (DISN). The DSN is a global network that provides telecommunications services to the entire DoD community including the warfighter, DoD contractors, and other government agencies.

Traditionally, telecommunications security has relied only on physical security (locks etc.) since one needed physical access to the switches, devices, and wires in order to become a threat to the system or the communications being transported. Personnel given physical access were usually trusted individuals. Those individuals with roles requiring system configuration access were given the common or group account and password since it could only be used with physical access to the device. The technical aspect of telecommunications security has traditionally focused on the prevention of surreptitious use of services. An example of this is toll fraud, which was the initial focus of the first hackers called phone phreaks.

Early hackers of data systems would focus on accessing individual computer systems via dial up connections. As data networks evolved, several computers would be connected together into Local Area Networks (LANs). Access to one computer on a LAN could give access to all others. LANs were subsequently connected to other LANs creating Wide Area Networks (WANs). Today, LANs and WANs have transitioned from isolated networks into enterprise wide intranets, which have been subsequently connected to the global Internet. This has allowed access to a computer from anywhere in the world thereby greatly expanding the number of threats being posed to any given computer or system.

There has been a lot of work done and there is a wealth of information available regarding the potential threats, risks, and mitigations associated with data systems and networks. Today, telecommunications systems are becoming computer and network based. As such they inherit all of the threats and risks associated with data networks. The physical aspect of traditional telecommunications security is no longer adequate.

This STIG is partially a result of the DISN Information Assurance Working Group's efforts to integrate information assurance (IA) activities across all DISN sub-systems.

1.2 Scope

The DSN and DoD telecommunications infrastructure is a mix of government owned and commercially leased switches, transmission facilities, and peripheral systems. While use of government-owned assets (and therefore applications of security procedures) is preferred, the infrastructure incorporates commercial leased telecommunications services where cost-effective or when mission-essential requirements dictate.

The requirements set forth in this document will assist security and switch support personnel with implementing and meeting the minimum-security requirements addressed in higher-level documents and as required to support final accreditation. For DSN services provided under contract by a commercial vendor, compliance of all requirements contained in this document is required. This document is to be used to assist in securing the DSN management, switching, signaling, and operations sub-systems by the following entities:

- DISA DSN
- DoD components
- Commercial contractors

Where applicable, a review of contract requirements and commercial best practices will be conducted to ensure security compliance with this STIG.

The requirements in this STIG are applicable to all systems that make up, support, and augment the DSN and other DoD telecommunications systems.

1.3 Authority

DoD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DoD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DoD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

Additionally, DoD Instruction 8100.3, which governs the DSN and connected systems, refers to the DoDD 8500.1 (IA policy) and DoDI 8500.2 (IA implementation), for IA requirements regarding system certification and accreditation. Some requirements in this document are derived directly from the 8100.3 such as those regarding the DSN Approved Products List (APL).

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**," indicate mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 DISA Information Assurance Vulnerability Management (IAVM)

The DoD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DoD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site, http://www.cert.mil.

1.6 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.

Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1. Vulnerability Severity Code Definitions

1.7 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.7.1 STIG Distribution to DSN Vendors

Most of the guidance and tools needed by vendors who are planning to, or are actively engaged in obtaining a DSN APL IA certification is available at IASE as noted above. STIGs, Checklists, and SRR Scripts are available for download to DSN Vendors originating from non .mil or .gov internet addresses. Certain resources and tools, such as the Windows Gold Disks, are not available for download by non .mil or .gov internet addresses at the present time. Non - Government Furnished Equipment (Non-GFE) versions of the Gold Disks may be made available for download in the future. The standard GFE Gold versions of the Disks cannot be distributed outside the DoD due to licensing issues related to some of the included software.

Once a sponsor and vendor has entered a Voice Connection Approval Office (VCAO) application for DSN APL testing, and a tracking number has been assigned, the vendor may request to be placed on mailing lists to receive all related STIGs, Checklists, SRR Scripts, and non-GFE Gold Disks. Contact FSO customer support at fso_spt@disa.mil to be placed on the mailing lists. The subject of all related correspondence with FSO_SPT must be formatted as follows: “DSN APL – Vendor_Name – TN” where TN is the solution’s VCAO Tracking Number. More information on this may be found in the *Guide to the STIGs for DSN Vendors* once finalized and published on the IASE web site.

1.8 Document Revisions and Support

Support is available for the application of the STIGs, Checklists, and Tools from FSO Customer Support at fso_spt@disa.mil. It must be noted however; that support is only available to DoD Customers and DoD sponsored vendors. Vendors contacting FSO for support will need to provide the VCAO tracking number for the product or system.

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

1.9 Configuration Guide Appendices

As a supplement to this document, separate DSN STIG Appendices have been produced that are Configuration Guides that can be used to assist in the configuration of specific DSN APL listed switches and systems. Since these documents contain specific system information and settings, they are considered to be “For Official Use Only” (FOUO). Each of these systems has it’s own separate document. It is our goal to produce a Configuration Guide Appendix for each system listed on the DSN APL with the assistance of the system’s vendors.

These appendices have been produced separate from this document so that this document may be more widely disseminated to vendors entering the DSN APL testing process. Each appendix is separate allowing for their individual distribution to only those DoD Components that have the specific system and therefore the need to know. The separate nature of this family of documents also allows for the production of additional Configuration Guide Appendices as systems are placed on the APL. It is also our intention that these guides will be restricted from access by competing vendors.

The distribution method for these appendices is un-determined. It may be controlled by the DSN VCAO or through the restricted area of IASE as mentioned above. The DSN VCAO can be contacted at NS534-web@disa.mil.

2. DSN SYSTEM OVERVIEW AND DESCRIPTION

This section will provide an overview and description of the DSN, its components, and sub-systems.

2.1 DSN System Overview

The DSN consists of two major parts. The first is what we will call (for the purposes of this document) the “backbone” which is the main transmission, switching, and signaling facilities. The second part is the end user interface (telephone instrument) and associated switching facilities.

The DSN “backbone” is comprised of three major sub-systems as depicted in *Figure 1*. They are as follows:

- The Network Sub-system witch consists of the DSN switching systems (Tandems/Stand Alones [SAs] and Multifunction Switches [MFSs]), the transmission/transport and Timing/Synchronization components. It also extends to the End Offices [EOs] or PBXs,
- The Common Channel Signaling (CCS7) sub-system.
- The Advanced DSN Integrated Management Support System (ADIMSS), which is the monitoring and control subsystem, its telemetry component, and portions of the support systems operated by the DoD components.

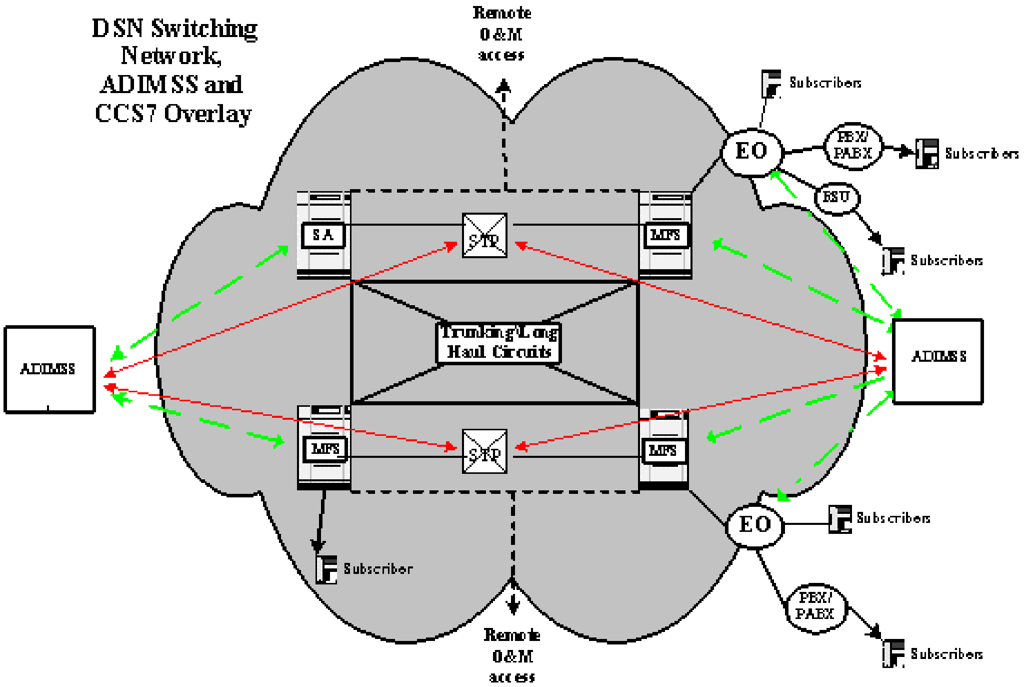


Figure 1. Three Major DSN Backbone Sub-systems

The user portion of the DSN as its name implies, serves the user community. It consists of large EOs and smaller PBXs along with their associated telephone instruments and peripheral systems. An EO can also be a MFS if it terminates trunks and CSS7 signaling circuits and performs the function of a Tandem switch. These switches, systems, and instruments are typically owned and operated by the various DoD components. These DoD components have management and security responsibility over the systems they own. DISA on the other hand has management and security responsibility over the backbone and also has performance responsibility over the end-to-end system, from user device to user device. See *Figure 2* for a depiction of this.

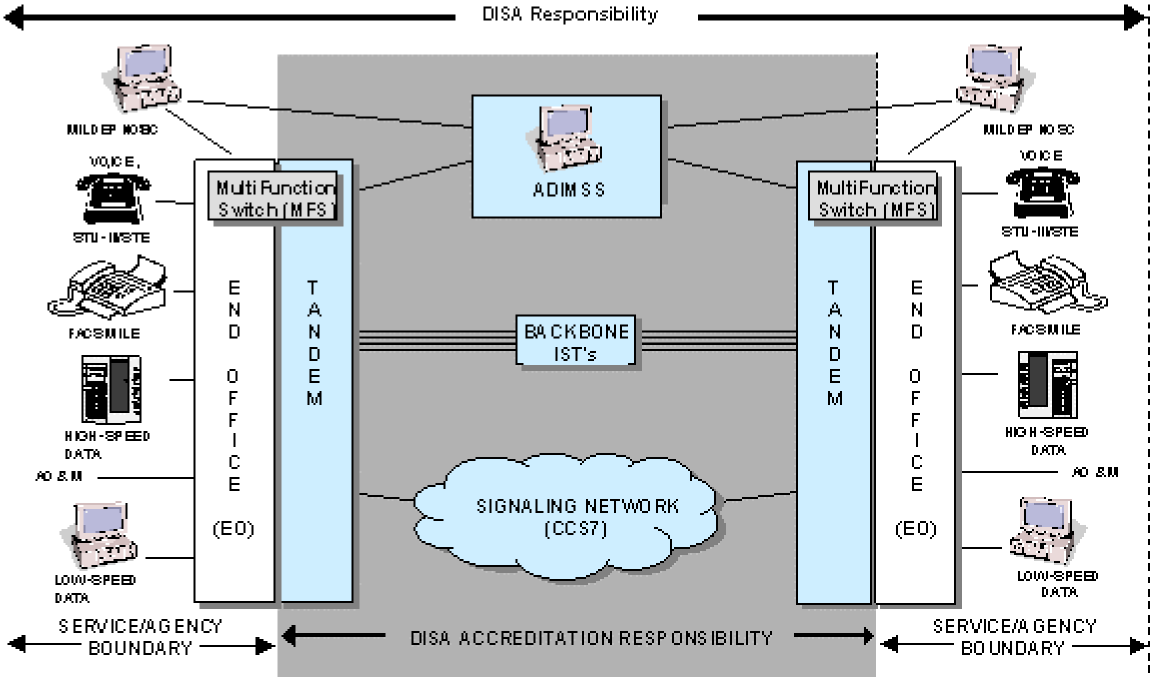


Figure 2. DOD Component and DISA Responsibility

Additionally, *Figure 2* shows the certification and accreditation boundaries between the DSN Backbone and the base level end user systems. Each section requires its own certification and accreditation.

The subsequent sections of this document will describe the various sub-systems that make up the DSN and present sub-system specific requirements as necessary.

The following diagram, *Figure 3*, provides an overview of the DSN components and vulnerable access points within the network.

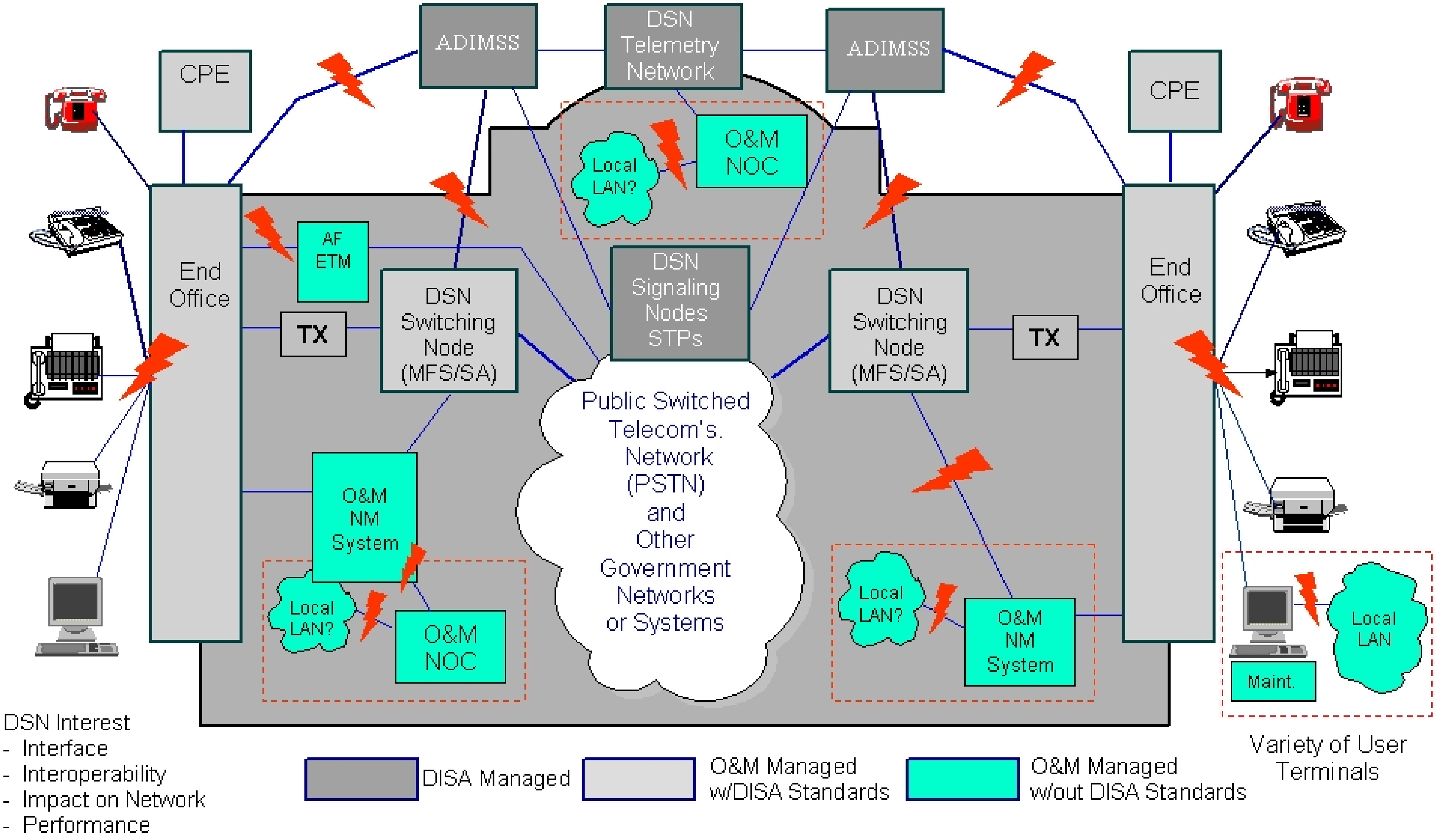


Figure 3. Overview of the DSN Components and Vulnerability Points

This page is intentionally left blank.

2.2 DSN Backbone Devices And Sub-Systems

In this section we will describe the various backbone components and sub-systems.
For the purposes of this document, the DSN is comprised of the following sub-systems or networks:

- Node switches
- Signaling network
- Network management
- Transmission/transport
- Timing and synchronization

2.2.1 Node Switches

A Node or Tandem Switch (TS) is a “backbone” device and is the component in the DSN that originates, switches, and terminates circuits (trunks) in the DSN. A tandem switch in the DSN provides inter-connectivity to other nodes and connects to multiple end office (EO) switches, provides access to a variety of transmission media, routes calls to other nodal switches, and provides network features, such as Multilevel Precedence and Preemption (MLPP). Nodal switches are supervised by and interconnected to the DSN Administration and Network Management subsystem.

The two types of nodal switches in the DSN are as follows:

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

2.2.2 Signaling Network

Inter-switch signaling in the DSN is a mix of in-band and out-of-band systems. In-band signaling is an older technology and normally found with channelized T-1 trunks (channel associated signaling – CAS). Common Channel Signaling (CCS7) is the DSN out-of-band signaling system and provides call set up, routing, call tear down, and control information between switches. It provides the capability necessary to meet the DSN requirements for circuit-switched call control and signaling network management. It consists of the following ANSI communications protocols:

- Message Transfer Part (MTP)
- Signaling Connection Control Part (SCCP)
- ISDN User Part (ISUP)
- Transaction Capability Application Part (TCAP)
- Monitoring and Measurements
- Operation and Maintenance Application Part (OMAP)

Timing and synchronization are also key to the well being of any synchronous network. Timing and synchronization are required to ensure that all devices within a network operate in coordination. This is particularly important as the network migrates toward CCS7, Advanced Intelligent Network (AIN) features, and ISDN offerings. Various clock sources are available, including internal clocks within switches. Switches can operate in a master-slave relationship, with a switch deriving its timing from another switch. The preferred approach is to utilize a common timing source, as described in section 2.2.5.

2.2.3 Network Management

Telecommunications Network Management (NM or TNM) includes Operations, Administration, Management, and Provisioning (OAM&P) functions. The DISA OAM&P and NM support system for the DSN is the Advanced DSN Integrated Management Support System (ADIMSS). This system along with similar systems owned and operated by DoD Components and Commercial Service Providers monitors the health of the DSN and manages its assets. See section 2.7 for further details.

2.2.4 Transmission and Transport

This subsystem consists of all communications media and is designed to achieve the highest reliability and can include media from dedicated wire line circuits to satellite and high-frequency radio communication. This subsystem represents transmission assets that provide DSN switching and signaling access lines and inter-switch trunk (IST) elements. The transmission and transport subsystem may be provided by various Government-owned or leased facilities, and may include several transmission media operating in either analog or digital mode.

2.2.5 Timing and Synchronization

The timing and synchronization subsystem represents the clocking element required to integrate digital switching systems directly interconnected by digital transmission facilities into the DSN. Synchronization refers to an arrangement for operating digital switching systems at a common (or synchronized) clock rate. Improperly synchronized clock rates cause portions of the bit streams being transmitted to be lost. The timing and synchronization subsystem for the DSN uses a Stratum 1 frequency reference derived from a station clock synchronized either to the Global Positioning System (GPS) or other highly accurate source such as a cesium beam atomic clock. DSN timing and synchronization is disseminated hierarchically throughout the network as EO switches and digital PBXs receive their timing reference from DSN SA or MFS switches.

2.3 DSN Topology

The following generic diagram (*Figure4*) depicts the switching components of the DSN from a very high level.

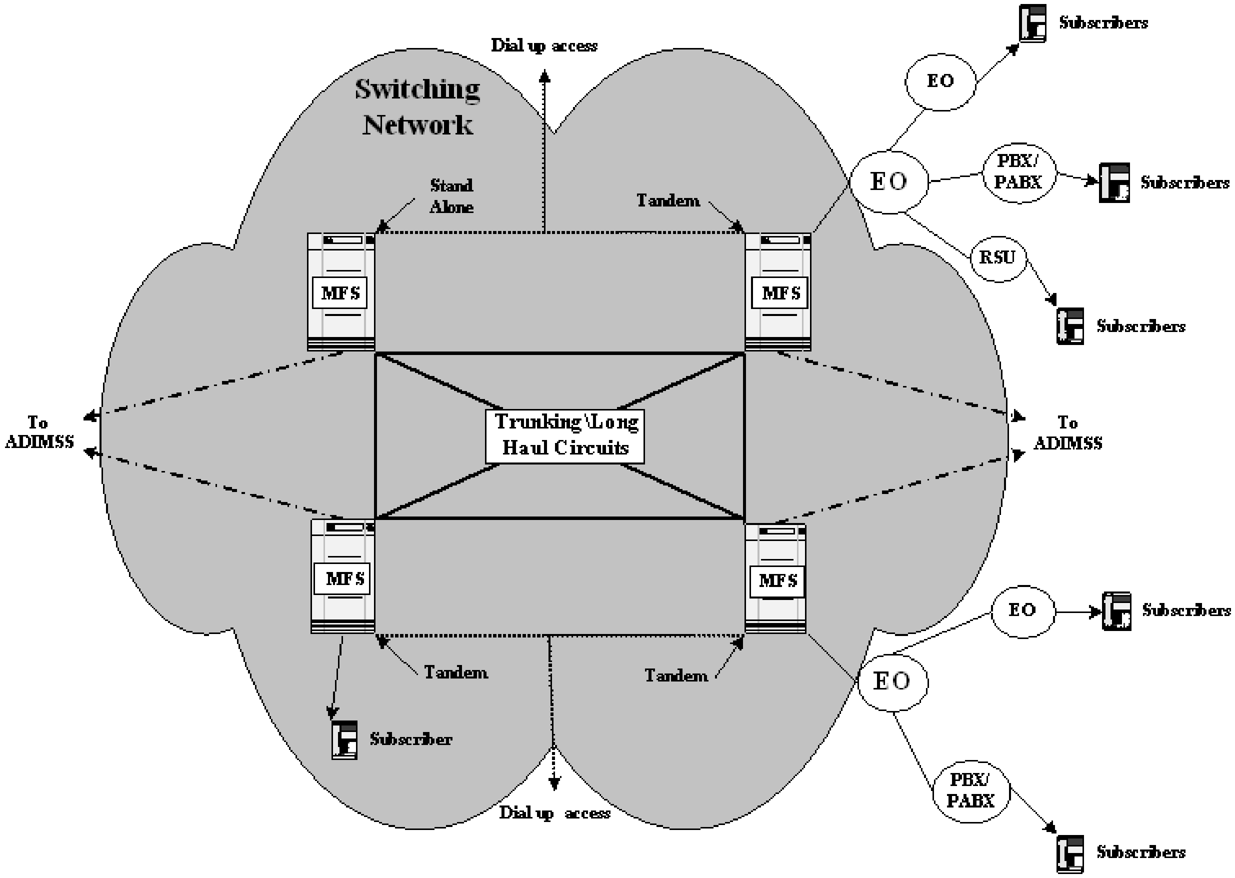


Figure 4. DSN Topology and Switching Components

2.4 DSN Switching System Descriptions

This STIG is applicable to all DSN switch types and installations. The following descriptions are listed to provide some basic understanding of their purpose. Additional information and definitions can be found in *CJCSI 6215.01B and the DOD Generic Switching Center Requirements (GSCR) document*.

The DSN Switch types are:

- Stand Alone Switch (SA)
- Multifunction Switch (MFS)
- End Office (EO)
- Small End Office (SMEO)
- Private Branch Exchange (PBX)

2.4.1 DSN Backbone Switches

Two backbone switch types provide the switching subsystems for the DSN backbone as follows:

- Stand Alone Switch (SA). The SA switch functions in the DSN as a Tandem Switch (TS). A TS is a switch that only provides trunking access and network routing between nodes and does not typically provide service directly to end-users. DSN SA switches provide services to the user through subtending EO switches and provide long-distance services via interconnections with MFSs and other SA switches.
- Multifunction Switch (MFS). This switch incorporates the combined functions of a Tandem switch with an EO. Therefore this term describes the switch in terms of its capability. A MFS switch provides both trunking and subscriber services. An MFS can connect to multiple end office (EO) switches, and directly supports users/subscribers through its EO element. It provides access to a variety of transmission media, routes calls to other nodal switches, and provides network features, such as Multilevel Precedence and Preemption (MLPP). There is no physical or electrical division between the tandem and end office switch functions. Functional differentiation is accomplished through software tables.

2.4.1.1 DSN Backbone Switch Vendor Models

Backbone switches deployed in the field vary from theater to theater and vary within theater with respect to vendor types and models. Though the following list is not to be considered all-inclusive some of the more predominant vendor switch types found within the DSN are listed below:

- Nortel DMS-100/200, Meridian SL-100 (MSL-100)
- Siemens KN-S 4100 / Italtel BX5000
- Siemens EWSD systems
- Lucent 5ESS

2.4.2 Base, Post, Camp, or Station Functional Switch Types

The following are functional definitions of switches residing on bases, posts, camps, or stations:

- End Office (EO). EO switches are integral to the DSN and serve as the primary switching facilities for installations' long-distance switched services by interconnecting with DSN nodal switches. EO switches provide switched call connections and all DSN service features to the end users, including MLPP. The EO will provide long-distance services by interconnections with SA switches and/or MFSs. An EO does not serve as a tandem in the DSN but may connect to other EOs where direct traffic volume requires. This is accomplished via community of interest trunks or as part of a metropolitan calling area (MAN) configuration. EOs support users and provide connections to the DSN for Private Branch Exchanges (PBXs) and Remote Switch Units (RSUs).
- Small End Office (SMEO). The SMEO provides for 1,000 terminations or less, performs the functions of a military dial central office, and functions as a terminating office in the DSN. The SMEO will use access lines to interface with EOs and MFSs. It will not provide Precedence Access Threshold (PAT) capability. SMEO access line groups are class-marked for various combinations of maximum precedence levels and calling area. SMEO switching systems will be equipped to route outgoing calls to SMEO access line groups class-marked to permit call precedence and calling area capability. This configuration will permit C2 users to be terminated on the SMEO switch.
- Private Branch Exchange (PBX). The PBX is a local secondary voice-switching facility on the users' installations. They derive their DSN service through the local DSN EOs or SMEOs; and they are considered customer premise equipment (CPE). PBXs primarily function as concentrators for local base or facility services distribution. There are two types:
    1. PBX Type 1 (PBX1). A PBX1 has MLPP capabilities. Based on mission requirements, this switch may serve those non-C2 users defined as DoD users having a military mission that might receive C2 calls for orders or direction at precedence levels above ROUTINE, even though they do not have a C2 mission for issuing guidance or orders.
    2. PBX Type 2 (PBX2). A PBX2 has no MLPP capabilities. This switch can only serve DoD, non-DoD, non-governmental, and foreign government users having no missions or communications requirement to ever originate or receive C2 communications under existing military scenarios. These users are provided access to the DSN for the economic or policy benefits of the DoD, when it is not in conflict with local Public Telephone and Telegraph (PTT) ordinances. During a crisis or contingency, they may be denied access to the DSN.

- Remote Switching Unit (RSU). The RSU is a remote subset of a larger switch (typically an End Office). The RSU derives much of its software functionality from its “mother” switch, and provides a less expensive alternative to a small EO or PBX with DSN functionality. RSUs are categorized by function, either as an EO or PBX. If an RSU is employed as a “functional” EO switch (i.e., provides full command and control capabilities with MLPP, and serves as the primary DSN switch for that location), then that RSU is considered a DSN EO switch. However, if an RSU cannot satisfy the MLPP requirement or serves as a secondary switch behind the base EO, it is considered a PBX switch.

2.5 Common Channel Signaling (CCS)

As noted earlier, DSN uses a combination of in-band and out-of-band signaling, depending on various factors (including cost and available technology). Channel Associated Signaling (CAS) is an older signaling system and is less efficient, in terms of bandwidth utilization, than Common Channel Signaling (CCS). CCS is a network architecture, which uses the Signaling System 7 (SS7) protocol for the exchange of information between telecommunications nodes and networks on an out-of-band basis. It is optimized for message-oriented signaling using dedicated point-to-point circuits that interconnect signaling systems. SS7 is the protocol used in the CCS network for the DSN.

2.5.1 Signaling System 7 (SS7)

SS7 is a highly reliable, fault-tolerant telecommunications network protocol that links telephone nodes and networks, allowing them to share signaling and control information. The SS7 protocol suite transfers information over dedicated data links that use packet switching techniques.

SS7 provides the data communications link between central office and telephone company databases, allowing faster call setup. SS7 can also relay messages from one central office to the next. This allows two central office systems to call up features within each switch without setting up a voice circuit between the switches.

The SS7 Network consists of three types of signaling nodes that complete the common channel signaling throughout the network. They are as follows:

- Signal Service Point (SSP). The SSP is the node switch. An SSP originates, switches, and terminates calls. This node is commonly seen in the field as a Nortel DMS-100/SL-100, Lucent 5ESS, and the Siemens EWSD.
- Switching Transfer Point (STP). The STP serves as the router within the SS7 network. Basically, no signaling messages originate from the STP; its function is to route all signaling from one SSP to another. The main function of an STP is to provide call setup and teardown. Please note that the STP performs many other functions as well. Within the DSN, this node is commonly a Nortel or Tekelec product.

- Signal Control Point (SCP). The SCP serves as a database for the STP to access when the routing information is not common. Calls such as 1-800, 888, 900, etc., are sent to the STP for routing information from the SSP. The STP takes this call and queries the SCP for proper routing information.

To better understand the SS7 network, following is a sample call transaction.

- If a caller served by SSP A places a call to another party that is served by SSP B, the following gives a basic flow of messages between the STP and the two SSPs involved.
- Caller A picks up receiver. The SSP that serves this caller sends dial tone to the caller indicating that it is ready to place a call.
- The caller dials a number that is not served by his SSP. The SSP recognizes this and sends a message to the STP that it is connected to, relaying the calling party's termination number and a trunk that can be used between the two SSPs to place the call.
- The STP takes this information and finds the SSP that serves the number that the calling party is trying to reach. The STP sends a message to the SSP that serves the called party and asks whether or not the call can be placed.
- If the call can be placed (the line is available), the SSP sends a message back to the STP telling it that the called party is available and that the call is being placed on the trunk that the originating SSP selected.
- The call is placed and the STP is notified that a call is active between the two parties. When the call is terminated (by either party), similar messaging is sent between the two SSPs via the STP to "tear down" the call, releasing resources for another call.

This is a very high level explanation of how a typical call is managed by the SS7 network.

***NOTE*:** No IST facilities are used between the two SSPs until there is confirmation that the call will be successful. *Figure 5* is a graphic depiction of this process.

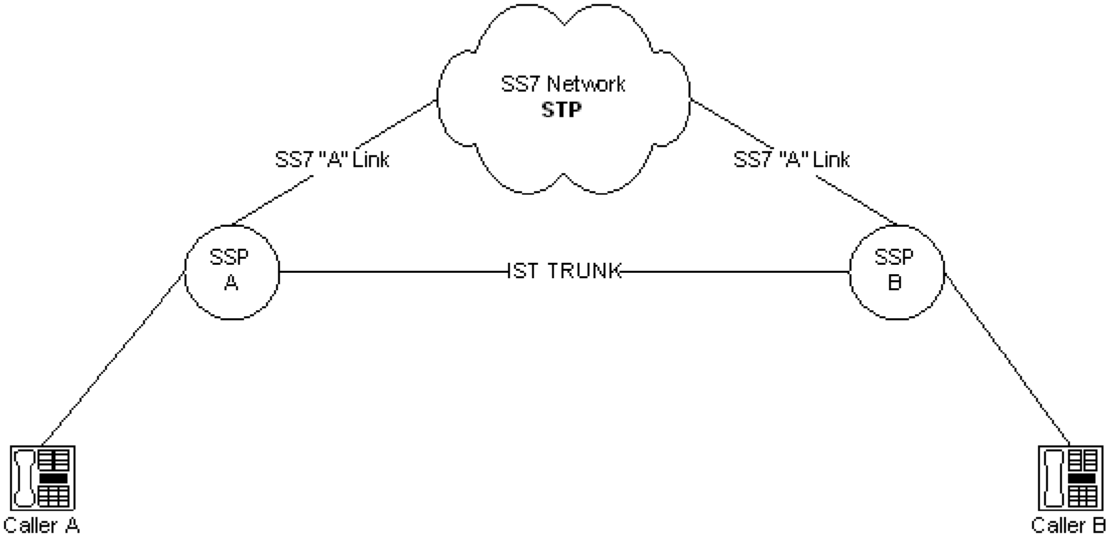


Figure 5. SS7 Call Transaction

Dedicated point-to-point circuits provide the physical connections or links between two adjacent signaling points in a SS7 network. These links are designated based on their purpose with the network.

For example:

- A Links; Access Links-Used to connect a SSP or SCP to a STP. These links are almost always deployed in pairs, one to each of the mated STPs that serve the SSP/SCP.
- B Links; Bridge Links-Used to connect two mated pairs of STPs. These links may be referred to as B/D links as well.
- C Links; Cross Links-Used to connect two mated STPs.
- D Links; Diagonal Links-Used to connect two mated pairs of STPs; these links may be referred to as B/D Links as well.
- E Links; Extended Links-Used to connect a SSP to a STP that is not its local STP. This is performed to add increased reliability.
- F Links; Fully Associated Links-Used to connect two SSPs that have a large volume of traffic.

Figure 6 below shows a typical SS7 network showing all of these links except the F Link.

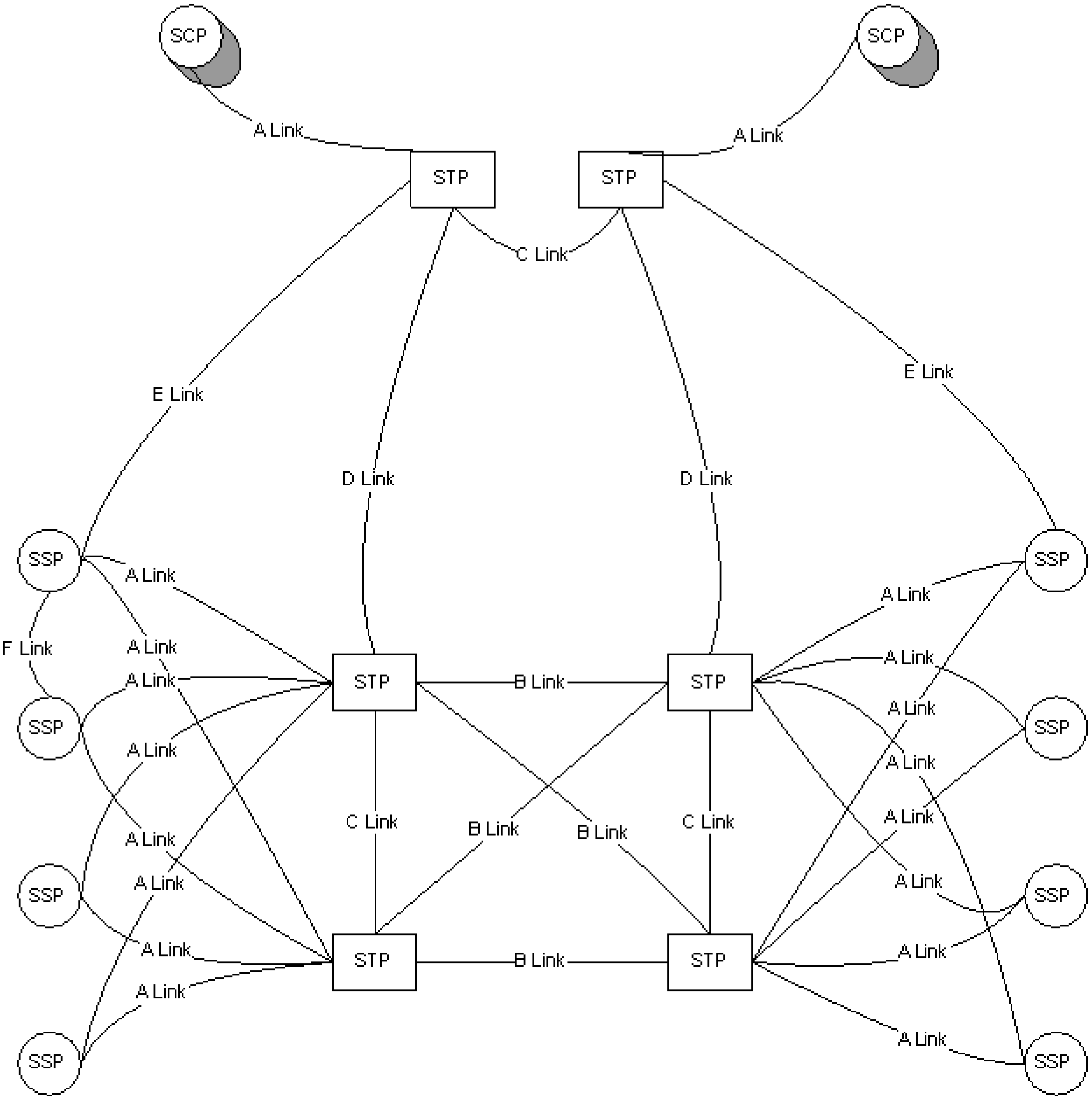


Figure 6. A Typical SS7 Network

This page is intentionally left blank.

2.6 Transmission and Transport

The transport and transport sub-system of the DSN system is responsible for delivery of voice and data circuits from one switch node to a distant switch node. The DSN uses copper, fiber optics, and radio/satellite as mediums between switch nodes. Part of the transport system is leased from commercial providers and part is maintained by DISA through the DISN.

2.7 Advanced DSN Integrated Management Support System (ADIMSS)

As noted earlier, The OAM&P and NM system used by DISA is the Advanced Defense Switched Network Integrated Management Support System (ADIMSS). It resides in the DISA OCONUS RNOSCs in Europe, the Pacific, and the CENTCOM AOR (both in the DISA RNOSC in Bahrain and the DISA facility at MacDill AFB, FL). In its simplest form, the ADIMSS is a network management system that includes the ADIMSS server in the RNOSC, the telemetry network (mainly routers and DISN circuits) that connect the ADIMSS to the DSN switches it monitors, and, in some cases, a Front End Processor (FEP) at the switch location to protect against switch engineering/billing data loss.

2.7.1 ADIMSS Mission

The primary mission of the ADIMSS is:

- Support near real-time operational management, direction, monitoring of DSN nodal switches
- Support provisioning of end-to-end service that is transparent to the customer
- Maintain the prescribed availability, security, and quality of service to DSN customers in Europe, the Pacific, and Southwest Asia
- Collect traffic and billing data from the global DSN

2.7.2 ADIMSS Description

The ADIMSS is comprised of three major subsystems. The ADIMSS Network Element (NE) Telemetry System, ADIMSS Core System, and the ADIMSS WAN. These provide a full suite of the five Telecommunication Management Network (TMN) functional areas in a client-server environment:

- Accounting management
- Configuration management
- Fault management
- Performance management
- Security management

The ADIMSS is a modular system that uses the following:

- Client-server architecture
- Servers and workstations connected by a dedicated Ethernet LAN using transmission control protocol (TCP/IP)
- Sun Solaris (UNIX) environment

- Relational database management system (Oracle)
- Artificial intelligence and a rule-based expert system (Gensym G2)
- Modular flexible software (COTS, GOTS, and custom)
- C, C++ languages
- Simple network management protocol (SNMP)

ADIMSS software consists of Commercial-Off-The-Shelf (COTS) packages in conjunction with customized integration software, and GOTS products to provide comprehensive network management functionality. The current COTS software includes the following:

- GENSYM G2 — System analysis and display of real-time data.
- ORACLE — Storage of performance and fault data. Historic data review.
- HPOV — LAN monitoring. ADIMSS software process monitoring.
- Netscape — Voice network management control feature.
- G2 Telewindows — Graphical Network Diagrams with colored status icons.
- Motif Windows — Display of real-time data.
- XV — Display of GIF, MPEG, and JIF-type graphics files.

2.7.3 Network Management; DOD Components and Contracted Service

The Operations, Administration, Management, and Provisioning (OAM&P) and Network Management (NM) of the DSN is a joint responsibility between DISA and the DoD Components that own the switches.

The term NM refers to the real-time status monitoring of numerous telephone switches from a centralized location (e.g. DISA RNOSC). NM is viewed as a separate function from the base-level function of switches OAM&P, although some of the NM and OAM&P functions overlap. NM is primarily concerned with real time switch status based on alarm and performance metrics and non-real time network level performance assessments and cost recovery (billing). OAM&P covers such functions as: telephone assignments (moves/adds/changes), cable records, directory services, local switch billing, and switch inventory. Another term used by the DSN for OAM&P is Administration, Operations, and Management (AO&M). The provisioning function is implied.

The NM function requires the monitoring of multiple switches from a central location (e.g. a DISA RNOSC) while the OAM&P function can be performed either from a centralized facility overseeing multiple switches or at an individual switch location.

Depending on the geographical location, the OAM&P / NM responsibilities within the DSN are as follows:

Geographical Location	AO&M Responsibility	NM Responsibility
OCONUS	Service/Agency	DISA
CONUS	Service/Agency (all switches except the Stand Alone (SA) Tandem switches)	DISA (Through a Leased Services Contract with MCI)
	DISA (the 12 SA Tandem Switches through a Leased Services Contract with MCI)	
HAWAII (HITS)	DISA (the 11 MFSs and EOs covered under the HITS Leased Services Contract with AT&T)	DISA (Through Leased Services Contract with AT&T)
	Service/Agency (All switches not specifically covered under the HITS contract)	

Both DISA and the DoD Components use various software application products to fulfill their OAM&P and NM roles. In addition, the operational environments in which these software applications reside differ from theater to theater and service/agency to service/agency.

The remainder of this section provides an overview of these configurations/arrangements.

2.7.4 ADIMSS Topology

The following diagram (*Figure 7*) depicts the ADIMSS enclave, enclave elements, and connectivity. This diagram reflects typical ADIMSS switch access.

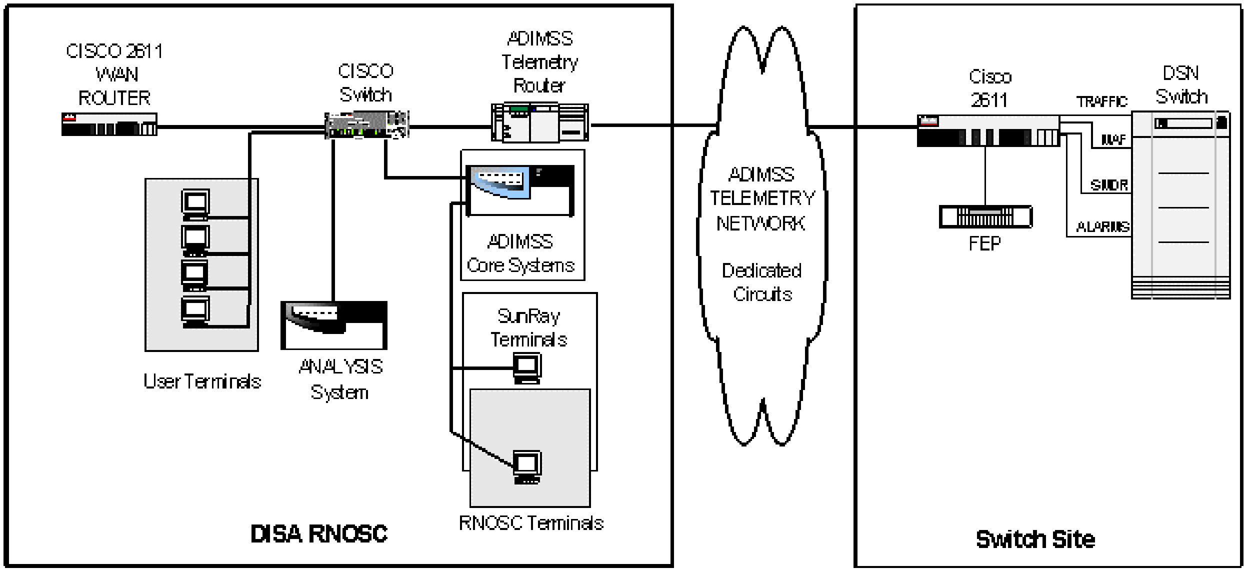


Figure 7. Typical ADIMSS Switch Access

As of the writing of this document, the ADIMSS network is migrating to a closed and dedicated network supporting the DSN. This target architecture will enhance ADIMSS security by incorporating a private non-routable addressing scheme across dedicated point-to-point circuit connections between ADIMSS sites. It will also allow for only one external connection to the NIPRNet located at Chantilly, VA.

2.7.5 OAM&P / NM - OCONUS DSN

DISA OCONUS (Europe, Pacific, and Southwest Asia), theater RNOSCs perform the NM function. The OAM&P function is performed by the services/agencies using both centralized facilities that cover numerous switches and "on-site" switch level OAM&P.

The OCONUS DSN security boundaries are shown Figure 8.

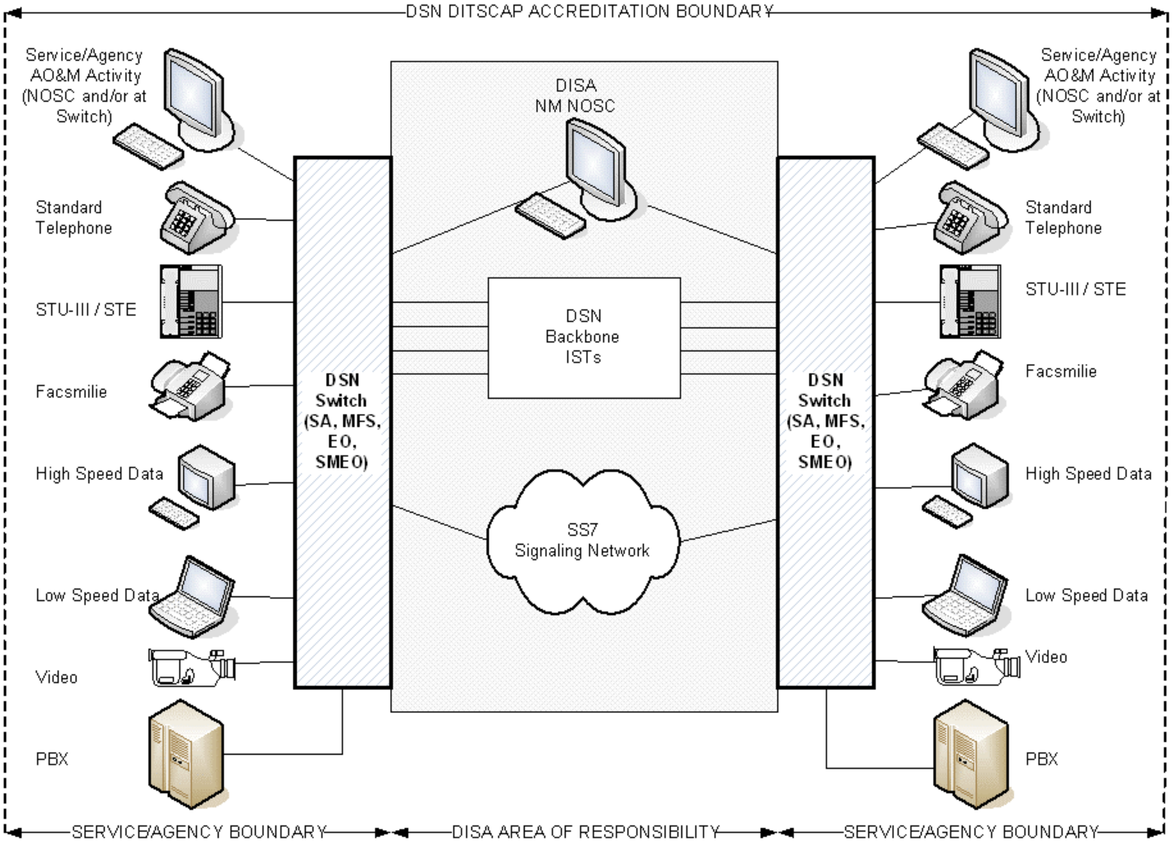


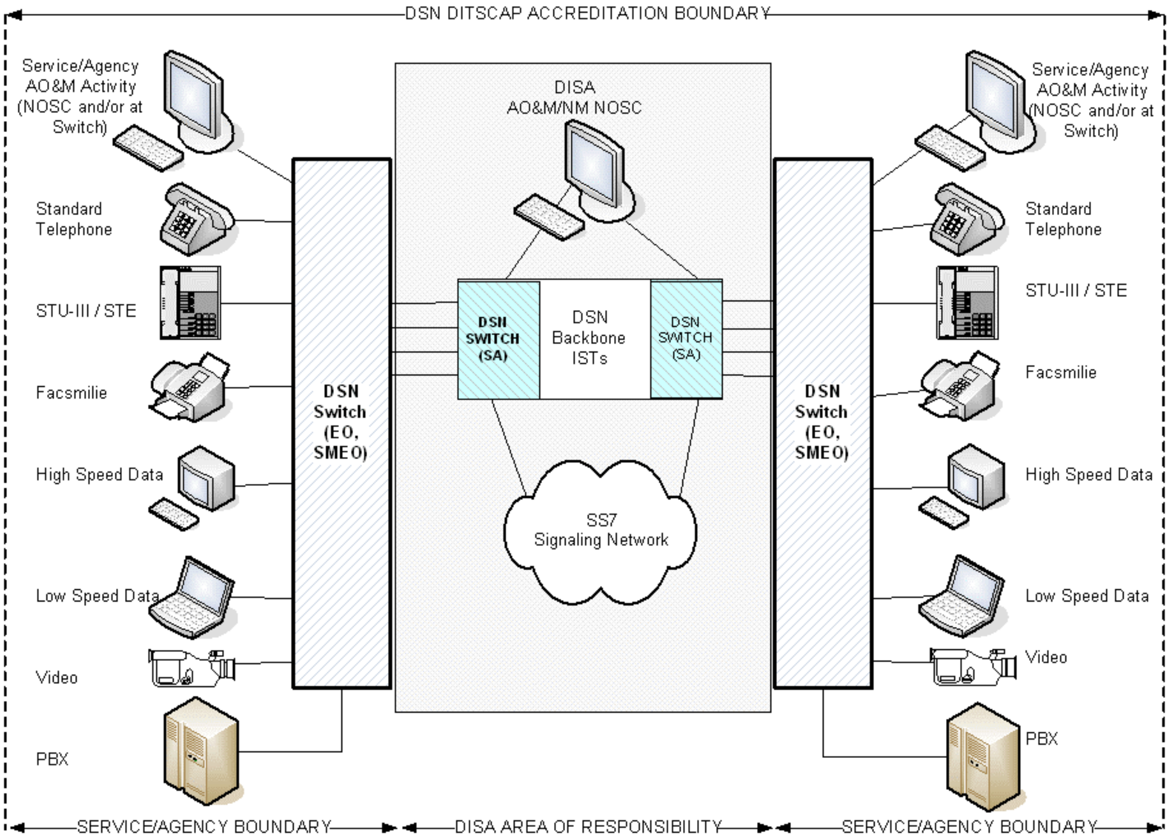
Figure 8. OCONUS DSN DITSCAP Responsibilities

2.7.6 OAM&P / NM - CONUS DSN

In the CONUS, DISA performs the OAM&P / NM function for the 12 backbone tandem switches through its service provider MCI. MCI has a network operations center (NOC) at Rockville, MD. All other CONUS switches have the OAM&P function performed by the respective services/agencies. They perform the OAM&P function using both centralized facilities that cover numerous switches and "on-site" switch level OAM&P.

The ADIMSS is not used in the CONUS.

The CONUS DSN is configured as shown Figure 9



NOTE: DISA AO&M/NM NOSC is Operated by MCI Under a Leased Services Contract

Figure 9. CONUS DSN DITSCAP Responsibilities

2.7.7 OAM&P / NM Hawaii DSN (HITS)

AT&T under the DISA administered Hawaii Information Transfer System (HITS) contract operates the backbone/tandem portion of the DSN network in Hawaii. Under this arrangement, the HITS contractor performs both the OAM&P and NM functions for the major switches on the island of Oahu. They perform these functions from a centralized facility that has access to all the switches under its control.

The ADIMSS at DISA-PAC does monitor the same major switching systems that are monitored by AT&T under HITS.

There are, however, other DoD telephone switches on Oahu. These switches fall under the OAM&P responsibility of the owning service/agency.

The DSN/HITS is configured as shown Figure 10

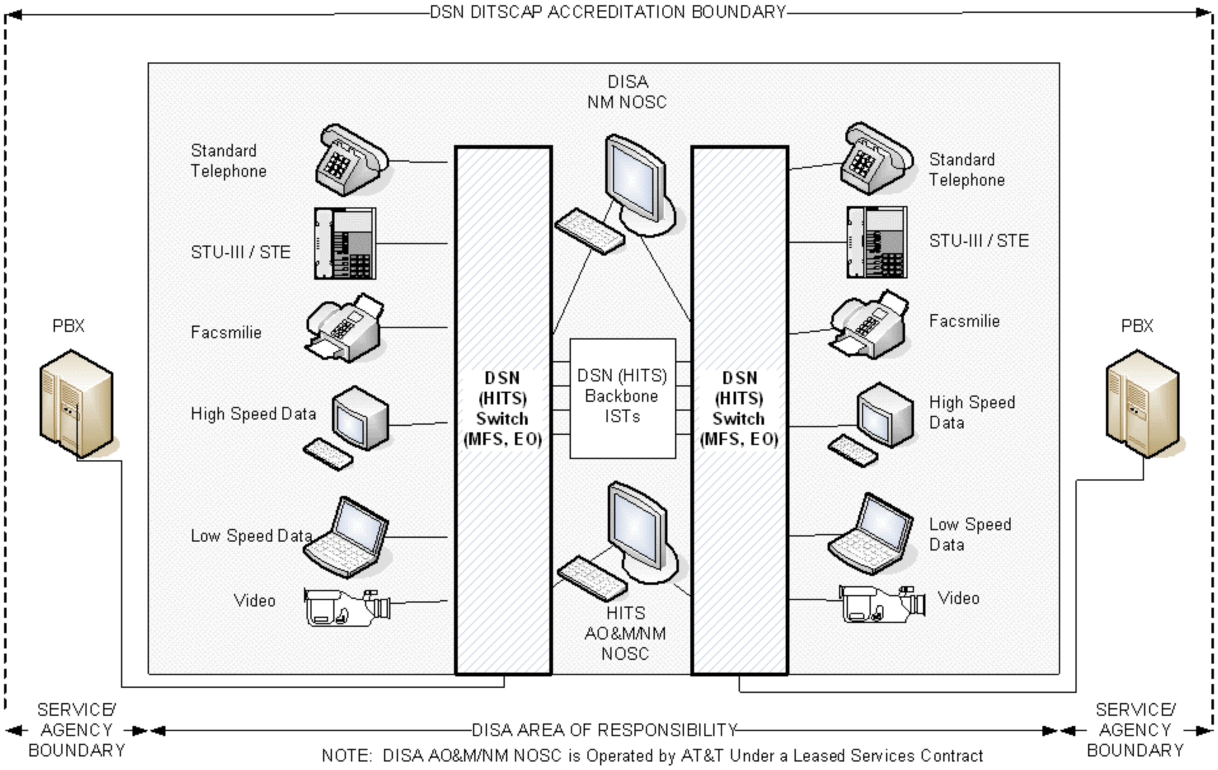


Figure 10. Hawaii DSN DITSCAP Responsibilities

This page is intentionally left blank.

3. DSN AND DOD TELECOMMUNICATIONS SECURITY CONCERNS AND REQUIREMENTS

For the purpose of this document, a “DSN Site” or “Site” refers to any Base, Camp, Post, Station, or facility, government or otherwise, that supports DoD telecommunications and/or receives DSN service or contains systems connected to the DSN. This refers to all connected systems whether for the purpose of receiving DSN service or for performing any other function supporting the DSN and/or DoD telecommunications. This includes any site owned, operated, or managed by any DoD component, government agency, or commercial establishment.

3.1 Administrative and General Requirements

This section presents the common administrative and general security requirements necessary to secure the DSN and/or DoD telecommunications as a whole.

3.1.1 Information Assurance Officer

All DSN sites (to include contracted sites) will have a DSN Information Assurance Officer (IAO) designated to oversee the security of the systems within the site(s). This individual should be knowledgeable of the security features available in the site’s switching and management systems and how these features are employed. In general this individual will be responsible for establishing, implementing, monitoring, and controlling the site’s telephone system security program. This security program will ensure the evaluation of all components of the sites telephone system (i.e., switch room, telephone system, peripheral systems, and auxiliary devices such as processors, modems, fax machines, printers, administration terminals, etc.) for security risks in order to minimize any vulnerability. Additionally the security program will minimize any vulnerability caused by unauthorized access to it components. The designated DSN IAO may also have responsibility for other systems at the site and/or may have responsibility over multiple remote sites that are part of the systems under his/her control.

- *(DSN01.01: CAT III) The IAO will ensure self-inspections of the telephone components, are conducted and documented for security risks at least semi annually.*

- *(DSN01.02: CAT III) The IAO will ensure the site’s telephone switch is frequently monitored for changing calling patterns and system uses for possible security concerns.*

- *(DSN01.03: CAT II) The IAO will ensure internal and external administrator/maintenance personnel have appropriate but limited access to the facilities, functions, commands, and calling privileges in accordance with their role as required when performing their job.*

- *(DSN16.01: CAT II) The DSN Program Management Office (PMO) or local site command/management, as appropriate, will document and ensure an IAO is designated to oversee the IA posture and security of each switch, site, system, and facility. The IAO will have the proper training and clearance level as directed by DODI 8500.2 E3.4.8. The DSN PMO should maintain documentation regarding IAO assignments for all sites and/or systems in the inventory. The DSN IAO may have responsibility for systems other than DSN systems and may be responsible for remote sites attached to his/her main site or system.*

3.1.2 Information Assurance Vulnerability Management (IAVM) Program

The DoD Joint Staff has mandated that all IAVMs are received and acted on by all Combatant Commands, Services and Agencies (CC/S/As) within the DoD. The IAVM process provides notification of vulnerability alerts and requires that each organization take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site, http://www.cert.mil.

- *(DSN02.03: CAT II) The IAO will ensure all IAVM notices are responded to within the time period specified within the notice.*

- *(DSN02.04: CAT II) The IAO will ensure all IAVM notices relating to the installation of security or other patches for general-purpose operating systems and software on devices other than workstations is vetted through the system vendor and approved by the local DAA before installation.*

3.1.3 Vulnerability Management Systems

The DoD Joint Staff and DoDD 8500.2 have mandated that all CC/S/As will implement a comprehensive vulnerability management process/system that provides for the systematic identification and mitigation of software and hardware vulnerabilities. Such systems, to be effective, must identify all assets (software and hardware) and their responsible individuals or SAs.

The DISA Vulnerability Management System (VMS) has been developed as a DISA tool to notify commands, agencies, and organizations of new and potential security vulnerabilities. The VMS meets the DoD mandate to ensure Information Assurance Vulnerability Alert (IAVA) notifications are received and acted on by all SAs. It provides a mechanism to ensure that new vulnerabilities are corrected within the specified period by tracking the site implementation status of all IAVM alerts, bulletins, and technical advisories. The VMS can provide Security Readiness Review (SRR) teams with a list of system specific vulnerabilities and IAVM notices as well as the applicable fixes and patches required for specific registered systems. The appropriate STIGs include detailed information on all IAVM notices issued that apply to the associated technology. Where applicable, these IAVM notices are referenced or included in summary format in the document. Use of the DISA VMS is mandated within DISA for DISA owned and operated assets. The DISA VMS is also available for use throughout DoD by the other CC/S/As.

The DISA VMS is specifically mandated for all Service-owned Multifunction and Tandem switches (MFS and TS) that support the DSN backbone network. Each MFS or TS site will ensure all SAs and DSN components; to include the ADIMSS information systems and STPs are registered with the DISA VMS. The DISA VMS is also specifically mandated for all EOs, SMEOs, PBX1s, PBX2s and RSUs or their OAM&P systems and any other auxiliary system that are owned and operated by DISA.

All other DSN connected systems that are owned, operated, and maintained by DoD components (CC/S/As other than DISA) such as EOs, SMEOs, PBX1s, PBX2s and RSUs or their OAM&P systems and any other auxiliary system are NOT required to be registered with the DISA VMS. However, it is required that such systems are registered and IAVAs tracked with a similar asset and vulnerability management system.

Users who require access to VMS should contact the DISA Operational Support Team in Oklahoma City at DSN 339-5600 (Option 5), Commercial: 405-739-5600 (Option 5) or 1-800-490-1643; EMAIL address: disa-emost@okc.disa.mil. Once access is obtained, there is a VMS CBT available in the help section under “Training”.

- *(DSN02.01: CAT III) The IAO will ensure all DSN critical assets are registered with the VMS as follows:*

    - *All backbone switches and components (TSs, STPs, MFSs)*
    - *All other switches (EOs, SMEOs, PBX1s, PBX2s and RSUs) owned by DISA*
    - *All components of the ADIMSS*
    - *All components of auxiliary/adjunct or peripheral systems owned by DISA*
    - *All TSs or MFSs owned and operated by DOD components that are part of the DSN backbone*

  Exception: This requirement is not applicable to EOs, SMEOs, PBX1s, PBX2s and RSUs or their OAM&P and auxiliary/adjunct or peripheral systems owned, operated, and maintained by DOD components other than DISA. See DSN02.04 below.

- *(DSN02.02: CAT III) The IAO will ensure all Switch and System Administrators (SAs) responsible for VMS registered DSN critical assets will also be registered with the VMS. This includes non DISA personnel responsible for TSs or MFSs owned and operated by DOD components*
  Exception: This does not apply to SAs that are ONLY responsible for systems owned, operated, and maintained by DOD components other than DISA.

- *(DSN02.05: CAT III) The IAO will ensure all systems including switches, OAM&P systems, auxiliary/adjunct, and peripheral systems connected to the DSN along with their SAs are registered and tracked with an asset and vulnerability management system similar to VMS.*

3.1.4 Compliance With Other STIGs

Telecommunications system developers and vendors, in order to minimize "time to market" and system cost, as well as to add flexibility, are employing equipment and software that are general-purpose or multi-purpose in nature. Software applications are then developed that run on this foundation to provide the specific and unique functions that make up the vendor's product. Commonly used hardware "servers" and their associated Operating Systems (OSs), as well as general-purpose web server and database programs add all of their well-known vulnerabilities to the product in which they are used. Additionally telecommunications switches or systems are being connected to data networks for OAM&P purposes or for auxiliary/adjunct functions like Computer Telephony Interface (CTI) systems, Automatic Call Directors (ACD), automated directories, or emergency services. Some utilize data networking and protocols to fulfill some of or all of their telecommunications functions. In the case of VoIP systems, the data network is an integral part of the telecommunications system. Systems utilizing data networks inherit all of the data network vulnerabilities. All of these inherited vulnerabilities must be mitigated and the system secured.

DISA develops STIGs that cover most general-purpose or multi-purpose OSs, applications and networks. The STIGS may provide configuration guidelines for specific popular systems or software packages, however the guidance provided is generally applicable to all systems or software in the related category.

The following is a partial list of the available STIGs and technology categories:

- Telecommunications; Defense Switched Network (DSN) & VoIP
- Enclave & Network Infrastructure (IP centric)
- Network Operations Center (NOC) and Network Management (future)
- Enterprise Systems Management (ESM)
- Secure Remote Computing (Remote network access for travelers and teleworkers)
- Operating Systems (OS)
  - Windows NT, 2000, XP, 2003 Server, Unix (also Linux)
- Applications
  - "Large" Applications (server or mainframe based)
  - Desktop Applications (specifically Microsoft Office and Browsers)
  - Database (specifically MS SQL and Oracle)(soon to include DB2)
  - Web Server (specifically MS IIS, Netscape, and Apache and other web technology)
- Domain Name Services (DNS)
- Wireless Networks

Compliance with all applicable STIGs is mandatory for all DoD Information Systems (ISs). All sites and/or systems providing DSN OAM&P and/or NM services as well as sites and/or systems providing auxiliary/adjunct services/functions will be subject to the requirements of all applicable STIGs and Checklists.

- *(DSN03.01: CAT III) The IAO will ensure all systems connected to DOD telecommunications systems that use technologies covered by a DISA/DOD STIG, is secured in compliance with the applicable STIG(s)*

As stated earlier, the DSN infrastructure is a mix of government owned and leased switches, transmission facilities, and peripheral systems. Even though the use of government controlled and owned assets is preferred, the DSN does incorporate commercial leased telecommunications services where cost-effective or when mission-essential requirements dictate. These commercial systems and services are also subject to the requirements in this and all other applicable STIGs. This requirement should be made part of the procurement process and contracts along with a means of enforcement.

- *(DSN03.02: CAT III) The DSN PMO and/or site command/management will ensure "compliance with all applicable STIGs" requirements and validation measures are added to specifications and contracts for commercially leased or procured telecommunications services or systems.*

- *(DSN03.03: CAT IV) The IAO will ensure commercially contracted (leased or procured) systems and services supporting the DSN comply with all applicable STIGs in accordance with contract requirements.*

3.1.5 System Procurement and DSN Connection Approval

DoD Instruction 8100.3 which governs DoD telecommunications and the Defense Switched Network (DSN), requires that "Telecommunications switches (and associated software releases) leased, procured (whether systems or services), or operated by the 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 Defense Information System Network (DISN) Designated Approval Authorities (DAAs)." DAA certification is obtained through the DISN Security Accreditation Working Group (DSAWG). DoDI 8100.3 also requires that the DoD use (or connect to the DSN) only devices that appear on the DSN Approved Products List (APL). Both IA and Interoperability certification requirements must be met for inclusion on the DSN APL.

The DSN PMO as represented by the Voice Connection Approval Office (VCAO) coordinates the certification of systems and new software releases for them as required for placement on the DSN APL. Additionally, they approve temporary and final connection of installed systems to the DSN. The DSN VCAO can be contacted at NS534-WEB@disa.mil. Product certification information and the VCAO application can be accessed at http://www.disa.mil/gs/dsn/jic/index.html.

The DSN APL is maintained by JITC and can be accessed at http://jitc.fhu.disa.mil/tssi/apl.html.

- *(DSN03.04: CAT II) The IAO will ensure all installed systems and associated software releases for which he/she is responsible appear on the DSN APL in accordance with DODI 8100.3 requirements. This applies to previously installed, new, and upgraded systems.*

NOTE: This finding can be reduced to a CAT IV if the system is in process of being certified for placement on the APL.

- *(DSN03.05: CAT III) The IAO will ensure products or software releases are installed and maintained in accordance with all applicable STIGs AND the installation restrictions and vulnerability mitigations presented in the Security Assessment Report and Certifying Authority's (CA's) Recommendation Memo to the DSAWG.*

- *(DSN03.06: CAT IV) The IAO will ensure systems are implemented using the configuration that was approved and for the approved purpose. Alternate configurations and purposes must be resubmitted for certification.*

- *(DSN03.07: CAT IV) The DSN PMO, DOD Component command, site command/management, or the IAO will ensure products being considered for procurement, installation, connection, or upgrade to the DSN are certified and appear on the DSN APL, OR are in the process of being certified, OR will sponsor the product for certification.*

3.1.6 DSN APL Relationship to DITSCAP

DoDI 5200.40 mandates the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) for all DoD Information Systems. There has been confusion in the DSN and vendor community regarding the use of or applicability of the DSN APL testing for the DITSCAP process. The following should eliminate any confusion.

The process of interoperability and IA testing at JITC is for the purpose of placing a product or system on the DSN Approved Products List (APL) in accordance with DoDI 8100.3. This allows DoD components to purchase or upgrade a listed product or software release. This also allows DoD components to continue operating systems that were in use prior to the signing and implementation of the 8100.3.

Placement on the DSN APL is a statement that:

- The product possesses certain Military Unique Features (MUFs) and will interoperate with other DoD systems in accordance with the General Switching Center Requirements (GSCR),

AND

- The product is CAPABLE of being configured in a secure manner that presents minimal acceptable risk as accepted by the DISN Security Accreditation Working Group (DSAWG), which represents the DISN DAAs.

The DITSCAP process is a site-by-site VALIDATION that the installed system(s) is (are) configured in accordance with all DoD guidance. The DITSCAP process is intended to validate and accredit the security posture of the INSTALLED system. Each installed instance of a given system must be separately accredited this way. This accreditation requires that a Site Security Authorization Agreement (SSAA) be written that states the configuration of the system and all security measures that will be applied to the site and system to mitigate all threats and vulnerabilities. The SSAA should reference the fact that the system is on the DSN APL.

Test results from the DSN APL process CANNOT be used for the DITSCAP process since there are two different Targets of Evaluation (TOE). That is the system installed at JITC for certification testing and the system installed at the user's site. Therefore, there WILL be duplication or overlapping of testing efforts.

The bottom line is that:

- The DSN APL listing says that a product **CAN** meet DoD security requirements.
- The DITSCAP process documents and validates that an installation **DOES** meet DoD security requirements.

- *(DSN03.08: CAT III) The DSN PMO, DOD Component command, site command/management and/or the IAO will ensure the DOD telecommunications system is certified and accredited per the DITSCAP either separately or as part of a larger site accreditation. The system must either have its own SSAA or be included in a larger site SSAA.*

3.1.6.1 Site Security Baseline

As part of site accreditation and to ensure security of the telephone system, a security baseline must initially be established. As part of this baseline an administrator must know the security features or services available in the system, how they are employed, and who is to receive those services. The following provides some basic protection elements the IAO should consider in developing standard operating procedures (SOP) to be used in securing telephone systems:

- *(DSN04.06: CAT III) The IAO will establish a standard operating procedure (SOP) or other form of record that will accomplish the following:*

  - *Identify and document all users, administrators, maintainers, managers, and their associated training requirements.*
  - *Identify and document all telephone system assets.*
  - *Identify and document all telephone services required.*
  - *Identify and document all telephone services that are not to be allowed.*
  - *Identify and document all telephone system threats.*
  - *Identify and document all audit items as required by this document.*

3.1.7 Security Documentation

The IAO will ensure that the following documents and any other appropriate documentation is available to users, administrators, maintenance personnel, and managers associated with the DSN. Additionally, a security awareness program will require key individuals involved in the administration, maintenance, and management of DSN assets to review these documents and remain abreast of their content and requirements.

- *(DSN12.01: CAT III) The site IAO will maintain an up-to-date library to include, at a minimum:*

    - *CJCSI 6215.01B, 23SEP01, Policy For Department Of Defense Voice Networks*
    - *CJCSM 6510.01, 15 MAR02, Defense In Depth Information Assurance and Computer Network Defense*
    - *DODI 8100.3, 16 JAN 03, Department of Defense DOD Voice Networks*
    - *DODD 8500.1, 24OCT02, Information Assurance*
    - *DODI 8500.2, 6FEB03, Information Assurance Implementation*
    - *DSN STIG*
    - *Other STIGs applicable to equipment or systems that are the responsibility of the IAO*
    - *A copy of the Security Assessment Report and Certifying Authority's Recommendation Memo to the DSAWG for each DSN APL certified system or product installed at the site that are the responsibility of the IAO*
    - *The SSAA for the site(s)and system(s) for which the IAO is responsible.*

3.1.8 Physical Security

The obvious sensitivity of the switch and its peripheral systems and devices as a critical component of the global DSN mandates that physical access to it and any associated device which may offer some privileged level of access by personnel, be managed and limited to essential and authorized personnel. Controlled access can significantly decrease the possibilities for sabotage of hardware or software.

The DSN switches, peripheral systems, and OAM&P / NM systems will be located in controlled access areas. DoDD 5200.8, Security of DoD Installations and Resources, 25 April 1991, assigns responsibilities and prescribes minimum standards for the physical security of the DoD fixed station communications facilities. Defense Information System Network Long Haul Block Security Policy, May 1999, provides information and guidance for implementing physical security measures. Anti-tamper devices should be considered to further limit or dissuade unauthorized access.

- *(DSN14.01: CAT II) The IAO will ensure DSN switches, peripheral, and OAM&P systems are installed in a controlled space with personnel and visitor access controls applied.*

If a switch has been unattended, authorized personnel entering the facility must inspect it in enough depth to reasonably ensure that no forced entry has occurred. If evidence of unauthorized entry exists, the observer will notify the appropriate security officer and make every effort to verify the continued integrity of the switch or system. Hardware, communications connectivity (i.e., cabling and circuit cross-connect points), software, and switch tables should be addressed in this verification. Similar actions will be taken if the unauthorized entry is identified as a result of local or remote alarms activated by the entry. In preparation for this kind of event the security officer will ensure procedures are documented to aid in the recovery of possible compromise.

- *(DSN14.02: CAT II) The IAO will ensure compromise recovery procedures are documented that will accomplish the following:*

    - *Verify the integrity of the hardware, software, and communication lines configuration.*
    - *Verify the integrity of the switch tables (database).*
    - *Perform an audit trail analysis and evaluation.*
    - *Enforce the change of all passwords for accessing the A/NM domain.*
    - *Report to the Theater and other concerned authorities the detection of possible unauthorized physical intrusion.*

3.1.9 Personnel Security

A personnel security program combined with other protective measures make up a security plan to keep DSN assets safe from intrusion or other types of disruptions. The DSN Security Guide describes the personnel security requirements for various types of individuals. Minimum requirements follow:

- *(DSN16.02: CAT II) The IAO will ensure personnel are familiar with the security practices outlined by applicable documents found in the site's library and have received the appropriate security training.*

- *(DSN16.03: CAT II) The IAO will ensure a DSN Personnel Security Certification letter is signed and on file for each person involved in DSN OAM&P / NM duties.*

- *(DSN16.04: CAT II) The IAO will ensure all System Administrators are appropriately cleared.*

3.1.9.1 Foreign National Personnel

In some cases Foreign National or Local National personnel may require access to DSN OAM&P / NM functions and switches in order to achieve operational objectives or for installation purposes. This access, however, must be controlled and held to a minimum. If Foreign National access is required, it is to be provided under the following conditions.

- *(DSN06.01: CAT II) The IAO will ensure all temporary Foreign/Local National personnel given access to DSN switches and subsystems for the purpose of installation and maintenance, is controlled and provided direct supervision and oversight (e.g. escort) by a knowledgeable and appropriately cleared U.S. citizen.*

- *(DSN06.02: CAT II) The IAO and IAM will ensure all Foreign/Local National personnel hired by a base/post/camp/station for the purpose of operating or performing OAM&P / NM functions on DSN switches and subsystems shall be vetted through the normal process for providing SA clearance as dictated by the local Status of Forces Agreement (SOFA).*

- *(DSN06.03: CAT II) The IAO and IAM will ensure all Foreign/Local National personnel hired by a base/post/camp/station for the purpose of operating or performing OAM&P / NM functions on DSN switches and subsystems shall be granted duties and system access in accordance with DODI 8500.2 E3.4.8.*

3.1.10 Configuration Management

Configuration management is detailed in DISAC 310-70-85, DSN Network Configuration Management Plan and DCAC 370-175-13, DSN System Interface Criteria. The goal of this section is to ensure that the site is aware that a process is in place, which if followed, mitigates the risk of implementing problem software or hardware.

In summary, the configuration management plan will ensure the following is in place:

- *(DSN17.01: CAT II) The IAO will ensure site staff will verify and record the identity of individuals installing or modifying a device or software.*

- *(DSN17.02: CAT II) The IAO will ensure systems will be backed up on a weekly basis to the local system and a copy will be stored on a removable storage device, off site, by the Switch Administrator.*

- *(DSN17.03: CAT II) The IAO will ensure site staff will ensure back-up media is available and up-to-date prior to software modification that could cause a significant disruption to service if the new software is corrupted.*

Additional requirements:

- *(DSN17.04: CAT II) The IAO will ensure the latest software loads and patches are applied to all systems to take advantage of security enhancements.*

- *(DSN17.05: CAT II) The IAO will ensure maintenance and security patches that are applied to a system are approved by the local DAA before installation.*

- *(DSN17.06: CAT II) The IAO will ensure major software version upgrades have been tested, certified, and placed on the DSN APL before installation.*

Also see IAVM compliance and DSN APL requirements above.

3.1.11 Emergency Services

Users have become dependent upon the availability of emergency life safety services by dialing an emergency access number such as 911or 112 as in Europe. For this reason the equipment that handles emergency life safety services must be clearly marked to avoid accidental disruption of service by maintenance personnel.

- *(DSN08.01: CAT IV) The IAO will ensure all equipment that provides emergency life safety services such as 911 services are clearly identified.*

Additionally, as a result of the attacks on 11 September 2001, public law mandates additional life safety measures and systems be implemented.

- *(DSN08.02: CAT IV) The IAO should ensure a system is installed to provide emergency announcements and messages in accordance with public law in response to 11 September 2001 and/or local building codes.*

3.1.12 Speakerphones and Instruments In Classified Work Areas

All telephone instruments present a potential risk to the security of areas where classified conversations are conducted. This is due to the ability of some phones to pick up room audio and transmitting it or sending it down the wire even when the phone is on hook. This ability is usually caused by poor design or malfunction in the hook switch circuitry. Additionally speakerphones in such areas may be activated by accident or surreptitiously. These vulnerabilities can affect the security or confidentiality of any conversation at any classification level. Of particular concern are those areas or rooms used for classified meetings, conversations, or work.

The following controls are required to mitigate this risk:

- *(DSN08.03: CAT II) The IAO will ensure a policy is in place and enforced regarding the use of telephone instruments connected to unclassified telecommunications systems located in areas or rooms where classified meetings, conversations, or work normally occur.*

- *(DSN08: CAT II) In the event that a telephone instrument connected to an unclassified telecommunications system are placed within a Sensitive Compartmented Information Facility (SCIF), the IAO will ensure the instrument is configured such that the instrument provides on-hook audio protection and that speakerphone audio pickup feature (microphone) is disabled or is nonexistent. (RE: Director of Central Intelligence Directive (DCID) 6/9 Annex G, Paragraphs 2.2.1, 2.2.1.1, 2.2.1.6, and Telecommunications Security Group (TSG) Standard 2)*

Additionally, VoIP systems in which the central call manager controls the telephone instrument, there is the potential of hijacking control of the instrument from somewhere else on the network. This potential vulnerability means that audio pickup might be activated clandestinely without the knowledge of the people near it. This vulnerability and other similar ones will be addressed in the VoIP STIG.

3.2 System Specific Technical Security Requirements

This section will discuss security requirements applicable to specific portions of the DoD telecommunications systems.

3.2.1 Switch Security Concerns

The DSN employs Stored Program Control switching systems. Switching system security procedures must be implemented that will prevent unauthorized access to the switch's stored program control database entries. Unauthorized changes to the switch database entries (or call processing/translation tables) can result in denial of service, misrouted calls, and unauthorized subscriber calling capabilities.

The switch database tables are accessed via the switch Man-Machine Interface (MMI). Switch access though the MMI, in turn can be accomplished in several ways within the DSN. They are:

- A direct physical connection to a switch by a Switch Database Administrator's workstation usually located within the switch room. This is via either a serial connection or a network connection that is isolated from the Base/Post/Camp/Station (BPCS) LAN or Base Area Network (BAN). Typically local switch OAM&P personnel use this type of access. Access to this point is therefore not possible from a telephone subscriber or a user of the BAN.
- Remotely from a centralized OAM&P / NM switch operations support center. This access is via a closed, dedicated telemetry network between switches and the OAM&P / NM support centers such as in the ADIMSS. Access to this point is also not possible from a telephone subscriber or a user of the BAN.
- Remotely via dial-up modem connection. This type of access is usually used by remote OAM&P / NM support centers for small remote switches. Emergency Technical Assistance Centers also use this method as needed on an emergency basis. Access to this point is possible from any telephone subscriber if the dial-up number is known and the modem is connected.

For the purpose of this document, a user is defined as a telephone system administrator, switch technician or one who has the ability to access, modify, add, or delete switch data or functions. User access may be accomplished by direct connection of an administration or maintenance console or via a remote or dial-up port as previously described. One of the greatest security concerns as related to a telephone switch is user remote access capability to the switch administrative/maintenance port. It is imperative that this connection be strictly controlled.

As we proceed through the following sections of this STIG, we will develop the technical requirements for securing telecom switch and associated systems.

3.2.1.1 Switch Security Capabilities

In order for the requirements of this STIG to be met, a number of specific security software packages may need to be loaded on each switch. However, in most cases these packages will be part of the software load at the time of purchase and no additional steps will need to be taken. It is, however, the responsibility of the IAO to ensure that all necessary software is installed and up-to-date as dictated by the PMO in coordination with the DSN APL certifications.

- *(DSN05.02: CAT II) The IAO will ensure all applicable security feature packages have been installed on the system to enable the required security features.*

3.2.1.2 PBXs & Attendant Console

PBXs are used to extend the services of an EO switch at a BCPS. All PBXs will be subject to the general requirements in this STIG to the extent that they are technically able to do so.

Vulnerabilities exist in some systems whereby if the attendant console connects to the PBX via the same ports as the telephone instruments e.g. the console or an instrument will function on any port. This situation should be avoided if at all possible. If the attendant console connects to the PBX in the same manner as the telephone instruments, the attendant console line should be configured to only connect to the attendant console instrument. Additionally system ports not designated for the attendant console instrument should be restricted from accepting the attendant console.

- *(DSN04.05: CAT III) The IAO will ensure attendant console ports will not be available to unauthorized users by not allowing any instrument other than the attendant console to connect to the attendant console port. Additionally the attendant console shall not be able to connect to a regular instrument port.*

3.2.1.3 Remote Switching Units (RSUs)

Remote Switching Units (RSUs), and other components not specifically mentioned in this document used to extend the capabilities of the DSN, will be subject to the requirements of this document.

3.2.1.4 Direct Inward System Access and Voice Mail Services

Direct inward system access is a feature provided by a telephone system that enables an authorized outside caller to dial directly into the telephone system and access the systems features and facilities.

This feature can be offered to subscribers providing remote DSN access to common services such as voice mail, to retrieve base or station recordings, or to make local and long distance calls over the DSN. This feature can be restricted by class of service or controlled by a special authorization code, or Personal Identification Number (PIN) if the service is provided to a specific subscriber. One of the most common causes for direct inward system access and voice mail abuse is unchanged default PINs, or the changing of PINs to an easily guessed combination (i.e., last four digits of phone number, last name of user, etc.). Measures should be in place to ensure users are observing suggested PIN/password assigning practices, and ensure users are aware of the threats associated with poor PIN/password practices. If not properly controlled, these features can render any switch vulnerable to toll call or voice mail abuse by unauthorized subscribers.

If direct inward system access or voice Mail services are offered to the subscriber community, the IAO will establish policy and the appropriate SA will enforce the following requirements:

- *(DSN07.01: CAT III) The IAO will ensure either class of service, special authorization code or PIN controls access to Voice Mail services.*

- *(DSN07.02: CAT III) The IAO will ensure if Voice Mail services are controlled by special authorization code, this code will be controlled and changed semi-annually.*

- *(DSN07.03: CAT III) The IAO will ensure if Voice Mail services are controlled by a PIN assigned to an individual or special subscriber, this PIN will be controlled like a password to include the mandatory changing of default PINs, the changing of initially assigned PINs, and PIN deactivation when no longer required.*

- *(DSN07.04: CAT III) The IAO will ensure all Voice Mail special authorization codes or individually assigned PINs are changed immediately if it is determined that they are compromised.*

3.2.2 OAM&P / NM and ADIMSS System Security Concerns

All sites and/or systems providing DSN OAM&P and/or NM services will have security reviews conducted using other applicable STIGs and Checklists (e.g., Enclave, NOC, Network, UNIX, Microsoft Windows, Web Server, Database, Application, ESM, and Desktop Application STIGs).

All network management platforms for the DSN must adhere to all applicable STIGs.

For security responsibility and accreditation purposes, the boundary between the DSN switch and the ADIMSS system is the switch Input/Output (I/O) port the ADIMSS uses. All internal switch or OAM&P / NM network security requirements fall under the responsibility of the switch OAM&P / NM activity.

Each system or network performing the OAM&P / NM function that is interconnected or connected to a DSN switch is considered an enclave. If the OAM&P / NM functions are performed from a centralized/remote location, then the telemetry system and remote network and equipment used to establish the necessary connection to the switch will be considered a part of the enclave. Such networks or systems must have the appropriate enclave boundary protections in place in accordance with the Enclave STIGs. Centralized OAM&P / NM systems such as the ADIMSS are subject to the NOC and ESM STIGs.

As part of a DSN security review, the following individual and technology-specific reviews will be accomplished as related to the particular OAM&P / NM system or Network Operations Center (NOC or RNOSC) site being reviewed:

- Operating system (i.e., UNIX / Microsoft Windows) security reviews will be conducted on site Front End Processors (FEPs), and Network Management Systems (NMSs) including servers and management workstations. If all NMS components cannot be reviewed, an acceptable sampling will be completed.
- Database security reviews will be conducted on systems supporting the ADIMSS database.
- A Network, Enclave, and NOC Security review will be conducted on the site’s ADIMSS network segment, which encompasses the dedicated Tier 1 router and firewall.
- An Application security review will be conducted on the ADIMSS application itself.

See “Compliance With Other STIGs” above for a further discussion of this topic and the PDIs.

Additional requirement guides to be used for OAM&P / NM system accreditation and DSN APL certification are as follows:

- Telcordia GR-815-CORE (Generic Requirements for Network Element/Network System (NE/NS) Security (Issue 2, March 2002)
- Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane (T1M1.5/2003-007R5 May 24, 2003)

3.2.3 SS7 Security Concerns and Requirements

Security concerns for the SS7 network fall into two major categories; STP database protection and signaling link protection. Database tables control STPs. Unauthorized access and modification of these tables must be protected. As discussed earlier in this document, the SS7 network is essential to the operation of the DSN. For this reason, there are some specific requirements regarding the SS7 links and the power supplied to this equipment.

The following discussion and requirements are in accordance with telecommunications industry "best practices" and standards. A-links that connect an SSP to the STPs should be clearly identified throughout the switching facility and network. A-Links should take diverse (separate) routes from termination point to termination point. The termination blocks of the A links should be clearly identified at the main distribution frame (MDF). In addition, power cabling of the SS7 equipment needs to be routed diversely and terminate in separate Power Distribution Frames (PDF). All power cabling should be clearly marked near the termination of the cabling and near the fuse assignments. These precautions will enhance system reliability and limit possible service degradations to the SS7 network by making service personnel aware of their location and to ensure that the switching facility is not isolated from the DSN network.

Additionally, DSN Switches will not be directly connected to Commercial STPs. SS7 signaling to commercial switches must be via the DSN STPs, which will contain Gateway Screening and Security software to prevent intrusion and provide a sanitized SS7 Network. (CONUS DSN Switches are exempt from this requirement pending transition from the current MCI backbone to a DoD owned and operated backbone.)

All security requirements contained in of this document apply to the SS7 network components in addition to the following:

- *(DSN09.01: CAT IV) The IAO will ensure all SS7 Links are clearly identified and redundant links are diversely routed from termination point to termination point.*

- *(DSN09.02: CAT IV) The IAO will ensure the SS7 termination blocks are clearly identified at the MDF.*

- *(DSN09.03: CAT IV) The IAO will ensure the power cabling serving SS7 equipment is diversely routed to separate and redundant PDFs.*

- *(DSN09.04: CAT IV) The IAO will ensure the power cabling serving SS7 equipment is clearly identified at both the termination point and at the fusing position.*

Examining traffic patterns and statistics can reveal compromising information. Such information may include call source, destination, duration, frequency, and precedence level. The DSN common channel signaling links contain this type of information and must be protected.

- *(DSN09.05: CAT IV) The IAO will ensure all SS7 links leaving a base/post/camp/station are encrypted.*

3.2.4 Transmission & Transport Security Concerns and Requirements

The Transport system of the DSN also needs to be considered in accessing the security vulnerabilities of the DSN and DoD telecommunications systems. The transport system is responsible for delivery of voice and data circuits from one switch node to a distant switch node. The DSN uses copper, fiber optics, and radio/satellite as mediums between switch nodes. Part of the transport system is leased from commercial providers and part is maintained by DISA through the DISN. Measures that must be in place to secure the Transport system are as follows:

- *(DSN11.01: CAT II) The IAO will ensure all circuits leaving the B/C/P/S are bulk encrypted.*

- *(DSN11.02: CAT II) The IAO or other responsible party will ensure the physical access to commercial Add/Drop Multiplexers (ADMs) is limited.*

Since part of the transport system is not directly controlled by DISA, but leased from commercial companies, a limited amount of control is available to ensure non-authorized users do not gain access to this equipment. Systems that are controlled by DISA will conform to the requirements of this STIG and be subject to the SRR process. In addition, contractors providing commercial transmission/transport services and support to the DSN under DISA contract are also required to comply with the requirements contained in this STIG.

3.3 Common Technical Security Requirements

This section discusses technical security measures common to all switches, peripheral systems, and devices in the DSN and DoD telecommunications systems. These requirements pertain primarily to the OAM&P / NM access and functions of these systems.

3.3.1 Authentication, Authorization, and Accountability (AAA)

The DSN is an unclassified system that does not require mandatory access controls for its general use. However, it does require access controls to ensure that unauthorized personnel are not allowed access to a switch's peripheral systems or OAM&P / NM functions or systems. Access controls also ensure that trusted and skilled personnel access only domains or sub-domains that correspond to their areas of expertise.

AAA intelligently controls access to resources, enforces policy, and audits user actions. The concepts of AAA provide the necessary access controls required of all DoD ISs. We will discuss these concepts and their requirements below.

3.3.1.1 Authentication: User Accounts and Passwords

Authentication is the process of identifying a user and granting access to a resource. Capabilities vary from system to system and device to device. Authentication typically requires a valid user name and a valid password before access is granted.

The term "remote authentication" refers to a system or device that communicates with a remote authentication server to validate the user's account information before granting access. The remote server can also control user rights. Systems such as RADIUS and TACACS+ provide this functionality for network devices. Systems such as domain controllers provide this functionality for network management stations.

The term "strong two-factor authentication" refers to the use of two forms of identification. This is usually "something you know" and "something you have". A username and password is not considered two-factor authentication. It is actually the "something you know". This could also be a security code. The "something you have" is a typically physical token. An example of this is a bankcard and PIN. Additionally there are tokens available such as RSA Security's SecurID that provide a "one time password" or code.

Remote authentication and strong two-factor authentication should be implemented for all systems that support it. Intermediary devices may be implemented for devices that do not support it.

- *(DSN13.16: CAT II) The IAO will ensure remote authentication is used to control to access all management system workstations and administrative / management ports on any device or system.*

NOTE: This finding can be reduced to a CAT IV where access to the noncompliant device (except management stations) is directly controlled by a device that is compliant such as an access router.

- *(DSN13.017: CAT II) The IAO will ensure strong two-factor authentication is required to access all management system workstations and administrative / management ports on any device or system.*

NOTE: This finding can be reduced to a CAT IV where access to the noncompliant device (except management stations) is directly controlled by a device that is compliant such as an access router.

As a minimum, user account management along with strong usernames and passwords must be implemented and enforced. The following minimum requirements apply:

- *(DSN13.05: CAT I) The IAO will ensure a valid username and a valid password are required to access all management system workstations and administrative / management ports on any device or system.*

NOTE: This finding can be reduced to a CAT II where access to the noncompliant device (except management stations) is directly controlled by a device that is compliant such as an access router.

- *(DSN13.01: CAT II) The IAO will ensure user passwords are assigned with the requirement for the user to change their password at first logon.*

- *(DSN13.02: CAT I) The IAO will ensure all system default passwords and user names are changed prior to connection to the DSN.*

- *(DSN13.03: CAT II) The IAO will ensure shared user accounts will not be used.*

NOTE 1: Use of shared user accounts is operationally essential and the device in question does not support multiple accounts

NOTE 2: In the following cases, findings can be reduced to CAT III:

- Should the use of shared user accounts be operationally essential then the local DAA must document approval.
- The IAO will document the requirement and authorized users.
- The policy for mitigation of the vulnerability is devised and followed.
- Efforts should be made to replace or upgrade any substandard devices to meet requirements.

NOTE 3: This is not a finding if a device that is compliant directly controls access to the noncompliant device. This could be a device such as an access router.

- *(DSN13.12: CAT II) The IAO will ensure switches capable of randomly generating unique passwords will use this capability as a first choice for password generation.*

- *(DSN13.06: CAT III) The IAO will ensure passwords are required and contain at a minimum, a case sensitive, eight-character mix of upper-case letters, lower-case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!).*

- *(DSN13.07: CAT II) The IAO will ensure all user passwords are changed at intervals of 90 days or less.*

- *(DSN13.08: CAT II) The IAO will ensure NO user passwords will be changed at an interval of less than 24 hours without IAO intervention.*

- *(DSN13.09: CAT III) The IAO will ensure user passwords are not reused within eight of the previous passwords used.*

- *(DSN13.04: CAT III) The IAO will ensure user accounts are disabled after 30 days of inactivity.*

- *(DSN13.13: CAT II) The IAO will ensure users will be prompted by the system three times to change their passwords before or after the password has reached the maximum password lifetime. If the user fails to change their password, their account will be disabled.*

- *(DSN13.10: CAT I) The IAO will ensure no user (to include Administrator) is permitted to retrieve the password of any user in clear text.*

- *(DSN13.11: CAT I) The IAO will ensure users' passwords are not displayed in the clear when logging into the system.*

With some switching systems (i.e., Nortel) it is necessary to temporarily take the switch out of service to recover the ADMIN password. Therefore, it is good security practice to record and secure the passwords of high-level users.

- *(DSN13.14: CAT II) The IAO will record the passwords of high-level users (ADMIN) used on DSN components and store them in a secure and controlled manner.*

Additionally, some devices have embedded logon IDs and passwords that are restored upon rebooting. These IDs and passwords can be used to restore a system following a system crash. This feature is a significant vulnerability that presents a significant opportunity to an adversary. If applicable:

- *(DSN13.15: CAT II) The IAO will ensure tests are performed for crash-restart vulnerabilities and develop procedures to eliminate vulnerabilities found (i.e., ensure ENHANCED_PASSWORD_CONTROL is active to prevent system logons after restart on Nortel switches).*

3.3.1.2 Authorization: Discretionary Access Control (DAC)

Discretionary Access Control (DAC) provides authorization control. DAC is a role-based feature that grants a user specific permissions to perform various functions when accessing an IS. Such permissions are established in accordance with the job functions and responsibilities of the individual. Permissions are established by the responsible security officer (i.e. the IAO), and stored in the system memory or its configuration files. The security officer also establishes the relationship in the system between authorized command class(es) or groups. The security officer generates a personal ID and a temporary password, and provides this information to the individual.

Many network and telecommunications devices are developed with various levels of authorization or access. This feature supports DAC requirements. The methods to access resources may vary depending on hardware and software products.

DAC is to be used for all OAM&P / NM access to all switches, peripheral systems, and other devices to the extent capable within the system or device. Auxiliary devices such as access routers may provide DAC functionality for less capable devices.

- *(DSN06.03: CAT II) The IAO will ensure all systems and devices employ a role-based Discretionary Access Control system used to control access to OAM&P / NM systems, the devices they manage, and their command classes for administrative and maintenance users commensurate with their assigned responsibilities.*

NOTE: This finding can be closed if a specific device does not support DAC but another device or system provides the DAC function. This situation must be documented and accepted by the local DAA. Additionally, this finding can be closed if the device appears on the DSN APL and is installed in accordance with its certification requirements.

- *(DSN06.04: CAT IV) The IAO will ensure user access is restricted based on duty hours, where technically feasible.*

Input screening in telecommunications switches is the feature that permits an authorized individual to use one or more command classes. This feature supports DAC requirements and is used for both local administration and ADIMSS access to the switches.

Most switches utilize user password protection to access the operation and configuration of the switch. Most switch designs utilize levels of privileged access, each using password submission and validation at each level, to allow access to that particular function. The lowest privilege level would allow user access to perform various routine maintenance tasks or entry of subscriber data. A second level would give access to perform highly important routines, configuration changes, and change capability of first and second level passwords. Changing a second level password often requires a distinct identification or special password.

Discretionary access control for system administration and maintenance access to the switch or peripheral system commands must be restricted based on the required functions or role of the user where technically feasible.

Input command screening can be implemented in switches to further control user access and privileges. To do this, individual commands available in the switch are first assigned a specific command class. Each Administrative/Maintenance user is then assigned a primary function that is associated with a collection of input commands that the system accepts from that specific user.

- *(DSN06.02: CAT III) The IAO will document all system administrative and maintenance user accounts.*

- *(DSN06.02: CAT III) The IAO will ensure devices that are capable of command screening or command classes are configured to use this feature in conjunction with DAC.*

Assigning valid commands to a specific terminal and assigning a User ID to be associated with that terminal can also achieve command screening. This feature restricts the usage of commands based on terminal identity instead of User ID.

Remote access to the switch can also be controlled to a degree, within the switch itself. When remote access to the switch is accomplished via a modem connection, dial back and dial back suppression will be enabled. See the section below for additional requirements regarding modem access.

3.3.1.3 Accountability: Auditing and History

Auditing events occurring to or within a system component or device is critical to maintaining accountability, tracking security and configuration related changes, and providing the manager vital information to reconstruct what may have occurred prior to a system crash or any other situation. This information may allow the manager to restore a system to its correct configuration and also determine the cause of the problem. The term "history file" may or may not relate to security. Most systems such as telecommunications switches record every transaction performed by the switch. History files may or may not contain auditable security events. A determination must be made for each device regarding the location of the security audits.

- *(DSN15.01: CAT II) The IAO will ensure auditing records are placed in an unalterable audit or history file that is available only to those individuals authorized to analyze switch access and configuration activity.*

- *(DSN15.02: CAT II) The IAO will ensure the auditing process records the identity of each person and terminal device having access to switch software or databases.*

- *(DSN15.03: CAT II) The IAO will ensure the auditing process records the time of the access.*

- *(DSN15.04: CAT II) The IAO will ensure the auditing process records commands, actions, and activities executed during each session that might change, bypass, or negate safeguards built into the software.*

- *(DSN15.05: CAT II) The IAO will ensure the auditing process records security relevant actions (e.g., the changing of security levels or categories of information).*

- *(DSN15.06: CAT II) The IAO will ensure audit records (files) are stored on-line for 90 days and off-line for an additional 12 months.*

- *(DSN15.07: CAT II) The IAO will ensure audit records are reviewed weekly.*

3.3.2 Data Network Connectivity

Modern telecommunications systems utilize data networking technology and data networks to enhance the flexibility, features, and management capabilities of the telecommunications switch. In the case of VoIP, the data network is the telecommunications distribution system. Additional requirements for VoIP networks and systems are contained in the VoIP STIG. Other systems utilizing data networks are OAM&P and Computer Telephony Interface (CTI) systems. Examples of CTI systems are as follows:

- Emergency 911 systems and their associated mapping systems
- Computerized operators stations, local or remote
- Call Center systems
- Automatic Call Director (ACD) systems
- Automated Directory systems
- Automated Voice Response systems

As discussed earlier, these systems are required to be compliant with all applicable DoD STIGs including the Enclave and Network Infrastructure STIGs. These systems are an integral part of the telecommunications infrastructure and need special consideration to maintain the security posture of the DoD telecommunications systems. Additional considerations and requirements for OAM&P and CTI networks that are not covered in other STIGs are as follows:

- *(DSN04.03: CAT II) The IAO will ensure OAM&P / NM and CTI system workstations are not used for other day-to-day functions (i.e., e-mail, web browsing, etc).*

- *(DSN04.04: CAT II) The IAO will ensure switch/device administration terminals are connected directly to the administration port of the switch/device or are connected via an out-of-band network used only for administration support.*

- *(DSN04.07: CAT I) The IAO will ensure out-of-band OAM&P / NM and CTI networks are dedicated to the system that they serve in accordance with their separate DSN APL certifications. CTI networks may be combined taking into consideration the vulnerabilities of each system and with documented local DAA approval.*

- *(DSN04.08: CAT I) The IAO will ensure OAM&P / NM and CTI networks are not connected to the local general use (base) LAN.*

NOTE: This is not a finding if there is a DAA approved and documented requirement where the connection is controlled through a dedicated firewall or router ACL that only allows restricted access from specific devices or management stations.

- *(DSN04.09: CAT I) The IAO will ensure OAM&P / NM and CTI networks are not connected to the local general use (base) WAN.*

NOTE: This is not a finding if there is a DAA approved and documented requirement where the connection is controlled through a dedicated firewall that only allows restricted access from specific devices or management stations.

- *(DSN04.10: CAT II) The IAO will ensure OAM&P / NM and CTI networks comply with the Enclave and Network Infrastructure STIGs.*

3.3.3 Remote and Local System Management Access

Systems management can be performed via a number of connection means as discussed earlier. The ports through which system management is performed go by various names. Some of these are MMI port, craft port, console port, and maintenance port. For the purpose of this document we will refer to these as the management port. The types of connections are as follows:

- Local direct serial console connection to a console or craft port using a dumb terminal or personal computer running terminal emulation software such as Hyperlink. This implies that the management station is located within the reach of a RS232 serial cable. According to the standard, this is 50 feet but can be longer.
- Remote serial console connection to a console or craft port using a modem pair remotely connected to dumb terminal or personal computer running terminal emulation software.
- Network connectivity via an Ethernet port or serial network adaptor. This implies a “remote” form of connectivity to one or many management workstations that could be located in the same room, next room, or anywhere else the network might reach.

3.3.3.1 General Requirements

The following general requirements apply to management connectivity as noted in the requirement.

- *(DSN18.07: CAT I) The IAO will ensure identification and authentication is required for every session requested in accordance with password policy.*

- *(DSN18.10: CAT IV) The IAO will ensure remote access ports require two-factor authentication. This is defined as requiring something along the lines of a token in addition to a User ID and password combination.*

- *(DSN18.09: CAT IV) The IAO will ensure a FIPS 140-2 compliant encryption mechanism is used to provide security of all data streams between the management port of the DSN component and a remote management station whether connected via a modem or network.*

- *(DSN18.12: CAT II) The IAO will ensure a timeout feature, set to 15 minutes, is used to disconnect idle connections.*

- *(DSN18.13: CAT II) The IAO will ensure management ports that receive three consecutive failed logon attempts will be unavailable for at least 60 seconds.*

3.3.3.2 Serial Console Ports and Modem Access

In many cases, device management relies on out-of-band dial-up modem connections for the remote management of switching and signaling components. Modems can provide an unchecked gateway to sensitive workings of a network. They provide an access window to systems to anyone who can dial a telephone number. In addition, if an unauthorized person has physical access to a site's modems, its configuration settings can be changed to affect the security of a system. In essence, if a modem is connected to the system, worldwide connectivity is implied. It is recommended that all modems be connected to approved lines using the switched voice network or approved leased lines maintained under Government contract. Limit or configure modem phone line connections to their purpose (out/in) as dictated by mission requirements. It is recommended that modems used to provide MMI to switching and signaling systems conform to the following:

- *(DSN18.01: CAT II) The IAO will ensure all modems are physically protected to prevent unauthorized device changes.*

- *(DSN18.02: CAT II) The IAO will maintain a listing of all modems by model number, serial number, associated phone number, and location.*

- *(DSN18.03: CAT II) The IAO will ensure only authorized modems are installed that appear on the DSN APL.*

- *(DSN18.04: CAT II) The IAO will ensure all modem phone lines are restricted and configured to their mission required purpose (inward dial only or outward dial only).*

- *(DSN18.05: CAT II) The IAO will ensure all modem phone lines are restricted to single-line operation without any special features such as the call forwarding capability.*

- *(DSN18.06: CAT IV) The IAO will ensure Automatic Number Identification (ANI) is enabled on modem lines to record access to remote access ports if this function is available. The IAO, or authorized security personnel, will maintain and review ANI logs. These records should be kept for the previous twelve months.*

- *(DSN18.08: CAT III) The IAO will ensure modem access to remote management ports incorporates the "callback" feature where technically feasible.*

- *(DSN18.11: CAT II) The IAO will ensure the control of serial management ports by deactivating or physically disconnecting access devices (i.e. modems or terminals) that are not in use.*

- *(DSN18.14: CAT I) The IAO will ensure serial management ports immediately drop any connection that is interrupted for any reason. Reasons include modem power failure, link disconnection, loss of carrier, time-out, etc.*

3.3.3.3 Management Port Connectivity Via A Network

Network connectivity greatly increases the number of avenues through which a device can be accessed and thereby increases its vulnerability. OAM&P / NM should not occur over the same network as the bearer or production traffic. Separate networks such as this are called “out-of-band” management networks. These networks are configured as an enclave unto itself. Any connectivity to base LANs or WANs must be controlled as stated earlier.

- *(DSN18.15: CAT II) The IAO will ensure out-of-band management networks comply with the Enclave and Network Infrastructure STIGs.*

- *(DSN18.16: CAT I) The IAO will ensure network connected switch and device management ports are connected to a network dedicated to management of the device only and/or that of other associated devices, i.e. an out-of-band management network.*

- *(DSN18.17: CAT I) The IAO will ensure network connected management ports drop a connection or session that is interrupted for any reason within 15 seconds.*

- *(DSN04.02: CAT II) The IAO will ensure routers that provide remote connectivity to out-of-band management networks located at switch sites provide IP and packet level filtering/protection.*

3.3.4 Security Logon Banner

The purpose of the security logon banner is two-fold. First, it warns unauthorized users that unless they are authorized they should not proceed. It is like an electronic “No Trespassing” sign that allows prosecution of those who do trespass. Secondly, it warns both authorized and unauthorized users that they are subject to monitoring to detect unauthorized use. This provides the informed consent that again allows prosecution of those who abuse the system.

The security logon banner will appear on or prior to the initial log-on page of the telephone system or associated component regardless of access methodology (e.g., network, website, remote access, dial-in, etc.). If technically feasible, the banner should be read and acknowledged via a keystroke or button click prior to granting access to the log on screen. Since this method is not auditable prior to login, it is additionally recommended that the banner be displayed again after login so that the acknowledgement can be audited.

The Joint Staff manual for Defense In Depth: Information Assurance (IA) and Computer Network Defense (CND), CJCSM 6510.01 provides details on the “log-on notice and consent banner” requirement and an example. While this example can be considered an officially approved banner, a banner can be any size. The banner must, however, inform the person logging in of certain legal points as noted in the requirement below.

- *(DSN19.01: CAT II) The IAO will ensure all telecommunications devices and auxiliary systems display a DOD approved "log-on notice and consent banner" prior to granting access regardless of access methodology (e.g., network, website, remote access, dial-in, etc.).*

- *The banner must inform the user of the following points:*

  - *The system is a DOD system.*
  - *The system is subject to monitoring.*
  - *Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.*
  - *Use of the system constitutes consent to monitoring.*
  - *This system is for authorized US government use only.*

NOTE: If the system is incapable of displaying the approved banner due to its size, a smaller banner may be used.

Below are some examples of banners that can be used. Previously approved versions are acceptable but should be updated when possible.

This is the example security logon banner taken from the CJCSM 6510.01 I This should be considered the DoD approved banner.
It contains 1180 characters with spaces.

> THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED US GOVERNMENT USE. DoD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DoD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM, MAY BE MONITORED.

> USE OF THIS DoD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

The following is an example of small size banner that should meet the minimum requirement:
It contains 246 characters with spaces.

> USE OF THIS DOD COMPUTER SYSTEM CONSTITUTES YOUR CONSENT TO MONITORING FOR COMPUTER SECURITY. THIS COMPUTER SYSTEM IS TO BE USED FOR OFFICIAL U.S. GOVERNMENT BUSINESS ONLY. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

This is a possible minimal banner using the points and verbiage from the CJCSM 6510.01.
It contains 420 characters with spaces.

> THIS IS A DOD SYSTEM AND IS SUBJECT TO MONITORING. MONITORING IS AUTHORIZED IN ACCORDANCE WITH APPLICABLE LAWS AND REGULATIONS AND CONDUCTED FOR PURPOSES OF SYSTEMS MANAGEMENT AND PROTECTION, PROTECTION AGAINST IMPROPER OR UNAUTHORIZED USE OR ACCESS, AND VERIFICATION OF APPLICABLE SECURITY FEATURES OR PROCEDURES. USE OF THE SYSTEM CONSTITUTES CONSENT TO MONITORING. THIS SYSTEM IS FOR AUTHORIZED US GOVERNMENT USE ONLY.

It is also suggested that this statement be added.
It adds 95 characters with spaces for a total of 515 characters.

> UNAUTHORIZED USE MAY SUBJECT YOU TO ADMINISTRATIVE ACTION OR CRIMINAL PROSECUTION AND PENALTIES.

This page is intentionally left blank.

4. VOICE OVER INTERNET PROTOCOL (VOIP)

VoIP and IP Telephony is an emerging technology that is a critical component of network centric warfare. VoIP is associated with potential command center desktop convergence, mobility enhancements, infrastructure reduction, multi-media collaboration, and cost avoidance. Implementing VoIP is a critical step toward DoD's ability to effectively provide all DoD communications traffic (data, voice, video, etc.) on an IP network that is central to effective network centric warfare.

Both data network and circuit switch telephony vendors are investing in VoIP and are aggressively marketing their approaches. In some cases, DoD Components and Agencies have instituted VoIP pilots, trials and implementations that provide DSN phone numbers and dial tone for access to origination and reception of DSN services. Currently, VoIP is being employed without C2 capability at the campus level network edge of DSN, NIPRNet and SIPRNet. It is also being employed in the backbones of SIPRNet and NIPRNet without C2 features.

CJCSI 6215.01B Enclosure A paragraph 10, defines network security requirements for the DSN. While denial-of-service attacks on the circuit-switched DSN are quite rare, denial-of-service attacks on the DoD’s data infrastructure occur frequently. This denial-of-service can include: intrusion, spoofing, snooping, or virus attacks such as the Melissa virus. While these attacks have no effect on today’s circuit-switched voice community, they virtually shut down some data networks while other data networks are impacted by the congestion generated by these viruses. During these periods, VoIP customers would lose their data and voice capabilities all together. This could have tragic consequences in a military environment.

Security in a VoIP environment differs from security in a closed, circuit-switched network. Most of the security concerns in the circuit-switched network are focused on the central telephone switch. In a VoIP environment, service is no longer based on a central telephone switch with dedicated physical loops to each instrument, but provided by functional elements distributed throughout the customer service area. Each of these distributed elements, which include terminals (IP phones), gateways, gatekeepers, and call control agents, present an opportunity for security to be compromised. Also, the switching fabric that used to reside inside the PBX cabinet is now distributed and available for malicious attack and eavesdropping. In short, the breaking out of the functional elements of a contained and proprietary switching system into distributed pieces of equipment operating with open protocols complicates the issues involved in making IP telephony secure.

Security issues can be approached from two perspectives: signal ports and operations ports. Signal ports are those involved with call setup and teardown and the transport of bearer traffic. Operations ports are those involved in administration of the distributed architecture, e.g. Command Line Interface (CLI) on routers, gatekeepers, and gateways. Operations ports are network management ports. As VoIP further develops and standardizes, additional specific security measures will be required and will be outlined in future releases of the VoIP STIG.

There are ongoing testing efforts to certify the interoperability and security of VoIP technology. Any VoIP network element connected to any DSN switch poses a potential security risk to the entire network and should not be connected until interoperability certified by the DISA Joint Interoperability Test Command (JITC) and security certified for connection through the DISN Security Accreditation Working Group (DSAWG).

- *(DSN10.02: CAT II) Voice Over IP systems and networks will comply with the DSN, VoIP, and all other applicable STIGs as well as other applicable DOD Component guides.*

5. SWITCH MULTIPLEX UNIT (SMU)

The Defense Information Systems Agency (DISA) uses the SMU as an integral part of the Standardized Tactical Entry Point (STEP) program. The STEP program concept will improve the military departments and Special Operations access capability to strategic DISN networks such as the DSN and Defense RED Switch Network (DRSN) for voice; the Unclassified-but-sensitive Internet Protocol Router Network (NIPRNet); the Secret Internet Protocol Router Network (SIPRNet); and the Joint Worldwide Intelligence Communications System (JWICS) for data and special user video; and Video Teleconferencing (VTC) for common user video.

The Switch Multiplex Unit (SMU) is a tactical circuit switch. There is a SMU located at 15 operational STEP sites and it is used to provide tactical-to-strategic voice service to deployed elements. The SMU provides gateway access for deployed tactical units to the DSN. In this capacity the SMU is considered as an extension or tandem switch in the DSN.

The system design and architecture of the SMU provides for no security configuration capability (i.e., user account, password, privileged user, or auditing capability). Trunk and subscriber provisioning is accomplished via an administrator's terminal, which is a dumb terminal, connected to the system via serial connection. From this terminal, at power up, the user has direct access to provisioning features of the system. Therefore, security protection to the SMU is provided through the physical security of the unit.

- *(DSN20.01: CAT I) The IAO at the SMU site will ensure the SMU has adequate physical security protection.*

In addition to the administrator terminal connection, a secondary connection is also provided for the ADIMSS network. This connection is used for remote access to the system to collect call processing and billing information. This connection is also a serial connection to the SMU from an ADIMSS server physically located on site. This ADIMSS server is in turn connected to the ADIMSS network via an Ethernet connection. This server should be dedicated to the ADIMSS and SMU and not connected to any other network.

- *(DSN20.02: CAT II) The IAO at the SMU site will ensure the SMU ADIMSS connection is dedicated to the ADIMSS network.*

- *(DSN20.03: CAT II) The IAO at the SMU site will ensure the ADIMSS server connected to the SMU is dedicated to ADIMSS functions.*

- *(DSN20.04: CAT II) The IAO at the SMU site will ensure the SMU management port or management workstations stations are not connected to any network other than one dedicated to management of the SMU.*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense (DoD) Directive 8500.1, 24 October 2002.

Department of Defense Instruction (DODI) 8100.3, 16 JAN 03.

Department of Defense Instruction 8500.2, 6 February 2003.

Department of Defense CSC-STD-002-85, "DoD Password Management Guideline," 12 April 1985.

Department of Defense Instruction 5200.40, "DoD Information Technology Security and Accreditation Process (DITSCAP)," 30 December 1997.

Department of Defense 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 31 July 2000.

Department of Defense Voice Network Generic Switching Center Requirements (GSCR) Document, 8 September 2003

CJCSM 6510.10, Defense-In-Depth: Information Assurance (IA) and Computer Network Defense (CND), 15 March 2002.

CJCSI 6215.01b, Policy for Department of Defense Voice Networks, 23 September 2001.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," July 1996.

Defense Information Systems Agency (DISA) Computing Services Security Handbook, Version 3, 1 December 2000.

DISA Network Infrastructure Security Technical Implementation Guide.
Addendum to the NSA Guide to Securing Microsoft Windows NT Networks and NSA Guides to Securing Windows 2000, Version 4, Release 1, dated 26 February 2004.

DISA UNIX Security Technical Implementation Guide.

DISA Enclave Security Technical Implementation Guide.

DISA Web Server Security Technical Implementation Guide, Version 4, Release 1, dated 29 August 2003.

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," 9 June 1993.

Army Regulation (AR) 380-19, “Information Systems Security,” 27 February 1998.

Air Force Instruction 33-111, “Telephone Systems Management,” 1 June 2001.

Secretary of the Navy Instruction (SECNAVINST) 5239.3, “Department of the Navy Automated Information Systems (AIS) Security Program,” 14 July 1995.

Navy Staff Office Publication (NAVSO Pub) 5239-15, “Controlled Access Protection Guidebook,” August 1992.

Public Law 100-235, 100th Congress, An Act cited as the “Computer Security Act of 1987,” 8 January 1988.

Memorandum for Secretaries of Military Departments, et al, “Web Site Administration,” 7 December 1998.

Generic Requirements for Network Element/Network System (NE/NS) Security, Issue 2, Telcordia Technologies, March 2002

General Information Sites

http://www.disa.mil	Defense Information Systems Agency (DISA) Web Page
http://www.cert.mil	Department of Defense Computer Emergency Response Team (CERT)
http://www.specbench.org	The Standard Performance Evaluation Corporation
http://www.ciac.org/ciac	The U.S. Department of Energy's Computer Incident Advisory Capability
http://nsi.org	National Security Institute's Security Resource Net Home Page
http://csrc.nist.gov	National Institute of Standards and Technology's Computer Security Resource Clearinghouse
http://www.icsa.net	ICSA.NET Internet Security
http://www.redbooks.ibm.com	“How to” books, written by very experienced IBM professionals from all over the world

APPENDIX B. ACRONYMS

AAA	Authentication, Authorization, and Accountability
ACD	Automatic Call Director
ADIMSS	Advanced Defense Switched Network Integrated Management Support System
ADM	Add-Drop Multiplexer
A/NM	Administration and Network Management
AIN	Advanced Intelligent Network
AIS	Automated Information Systems
ANI	Automatic Number Identification
AO&M/NM	Administration, Operation and Management/Network Management
APL	Approved Products List
ATM	Asynchronous Transmission Mode
BAN	Base Area Network
BPCS	Base/Post/Camp/Station
C2	Command and Control
CA	Certification Authority
CAT	Category
C&A	Certification and Accreditation
CAN	Campus Area Network
CCB	Configuration Control Board
CCS	Common Channel Signaling
CCS7	Common Channel Signaling System No. 7
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CLI	Command Line Interface
CM	Configuration Management
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental/Contiguous United States
COS	Class of Service
COTS	Commercial-Off-The-Shelf
CPE	Customer Premise Equipment
CTI	Computer Telephony Interface
CTIM	Computer Telephone Integration Manager
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DC	Domain Component
DECC	Defense Enterprise Computing Center
DIAM	Defense Intelligence Agency Manual
DISA	Defense Information Systems Agency
DoS	Denial of Service
DISAC	DISA Circular
DISAI	DISA Instruction

DISN	Defense Information Systems Network
DISN-C	DISN CONUS
DISN-E	DISN EUR
DISN-P	DISN PAC
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMS	Defense Messaging System
DNS	Domain Name System
DoD	Department of Defense
DoDD	Department of Defense Directive
DRSN	Defense Red Switched Network
DSA	Dial Service Assistant
DSAWG	DISN Security Accreditation Working Group
DSN	Defense Switched Network
DTSW	Defense Telecommunications System Washington
EAL	Evaluation Assurance Level
ECP	Engineering Change Proposal
EMP	Electromagnetic Pulse
EMS	Element Management System
EN	End Office Node
EO	End Office
EOS	End Office Switch
ES	End System
ESP	Essential Service Protection
EUR	Europe
ESM	Enterprise System Management
FEP	Front End Processor
FIPS	Federal Information Processing Standard
FM	Fault Management
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FSO	Field Security Operations
FY	Fiscal Year
FTS	Federal Telecommunications System
GETS	Government Emergency Telecommunications System
GOSC	Global Operations and Security Center
GOTS	Government-Off-The-Shelf
GPS	Global Positioning System
GSCR	General Switching Center Requirements
GUI	Graphical User Interface
HID	Host Intrusion Detection
HITS	Hawaii Information Transfer System
HTTP	Hyper Text Transfer Protocol

I/O	Input / Output
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAW	In Accordance With
IAVA	Information Assurance Vulnerability Announcement
IETF	Internet Engineering Task Force
IAVM	Information Assurance Vulnerability Management
I&A	Identification and Authentication
ID	Identification
IDNX	Integrated Digital Network Exchange
INFOSEC	Information Systems Security
IP	Internet Protocol
IPSEC	IP Security
IS	
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part (SS7 protocol)
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
IT	Information Technology
ITU	International Telecommunications Union
JITC	Joint Interoperability Test Command
JWICS	Joint Worldwide Intelligence Communications System
KBPS	Kilobits Per Second
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mission Assurance Category
MAC	Media Access Control
MAN	Metropolitan Area Network
MBPS	Megabit Per Second
MCU	Multipoint Control Units
MFS	Multifunction Switch
MG	Media Gateway
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MILDEP	Military Department
MLPP	Multi-Level Precedence and Preemption
MMI	Man Machine Interface
MS	Microsoft
MTP	Message Transfer Part (SS7 protocol)
MUX	Multiplexer

MUF	Military Unique Feature(s)
NAT	Network Address Translation
NCS	National Communications System
NIPRNet	Non-Classified (But Sensitive) Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NM	Network Management
NMC	Network Management Center
NMS	Network Management System
NNM	Network Node Manager
NOC	Network Operations Center
NSA	National Security Agency
NSO	Network Security Officer
NTISSP	National Telecommunications and Information Systems Security Policy
NOC	Network Operations Center
NTP	Network Time Protocol
O&M	Operations and Maintenance
OAM&P	Operations, Administration, Maintenance, and Provisioning
OCONUS	Outside CONUS
OMAP	Operation and Maintenance Application Part (SS7 protocol)
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
OS	Operating System
OMAP	Operation and Maintenance Application Part (SS7 protocol)
PAC	Pacific
PACOM	Pacific Command
PAT	Precedence Access Threshold
PABX	Private Automated Branch Exchange (old term)
PBX	Private Branch Exchange
PBX1	Private Branch Exchange Type 1 (basic, no MLPP MUF)
PBX2	Private Branch Exchange Type 2 (MLPP capable)
PC	Personal Computer
PCM	Pulse Code Modulation
PDI	Potential Discrepancy Item
PIN	Personal Identification Number
PM	Project or Program Manager
PMO	Program Management Office
PRI	Primary Rate Interface
PSN	Packet Switched Node
PSTN	Public Switched Telephone Network
PTT	Push-To-Talk
QBE	Query by Example

QoS	Quality of Service
RAS	Remote Access Service
RFC	Request For Comment
RNOSC	Regional Network Operations and Security Center
RSU	Remote Switching Unit
SA	System Administrator
SAS	Stand Alone Switch
SCCP	Signaling Connection Control Part (SS7 protocol)
SCCS	Source Code Control System
SCP	Signal Control Point (CCS7 device)
SDID	Short Description Identifier
SG	Signaling Gateway
SIPRNet	Secure Internet Protocol Router Network
SIP	Session Initiation Protocol
SM	Security Manager
SNMP	Simple Network Management Protocol
SMEO	SMall End Office
SMB	Server Message Block
SMU	Switch Multiplex Unit
SOP	Standard Operating Procedure
SQL	Structured Query Language
SRR	Security Readiness Review
SRRDB	Security Readiness Review Database
SSAA	System Security Authorization Agreement
SS7	Signaling System 7 (protocol suit)
SSL	Secure Socket Layer
SSM	Single System Manager
SSP	Signal Service Point (CCS7 device)
STE	Secure Terminal Equipment
ST&E	Security Test and Evaluation
STEP	Standardized Tactical Entry Point
STIG	Security Technical Implementation Guide
STP	Signaling Transfer Point (CCS7 device)
SWA	South West Asia
T&S	Timing and Synchronization
TAPI	Telephony Application Programming Interface
TAFIM	Technical Architecture Framework for Information Management
TCAP	Transaction Capability Application Part (SS7 protocol)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
TNM	Telecommunications Network Management

TOE	Target of Evaluation
TS	Tandem Switch
TSSO	Telephone Systems Security Officer
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UNIX	Name of an Operating System
URL	Uniform Resource Locator
UPS	Uninterruptible Power Source
VCAO	Voice Connection Approval Office
VCTS	Vulnerability Compliance Tracking System
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconferencing
VMS	Vulnerability Management System
WAN	Wide Area Network
WLAN	Wireless Local Area Network