



Defense Information Systems Agency

A Combat Support Agency

INFRASTRUCTURE EXECUTIVE (IE) DIRECTORATE

TELECOMMUNICATIONS SERVICE LEVEL AGREEMENT (SLA)

Version 4.1
December 09, 2016

UNCLASSIFIED

DISN Program Management Office
P.O. Box 549
Ft. Meade, MD 20755-0549

This page intentionally left blank.

Signature Page for Key Official

Approved by:

SHOWERS.JESSIE
.L.JR.1119211235

Digitally signed by
SHOWERS.JESSIE.L.JR.1119211235
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=DISA,
cn=SHOWERS.JESSIE.L.JR.1119211235
Date: 2016.12.14 14:06:01 -05'00'

Mr. Jessie L. Showers, JR., SES
Infrastructure Executive, Infrastructure Directorate (IE)
Operations Center (OPC)
Defense Information Systems Agency (DISA)

Date

This page intentionally left blank.

Document History

Document Revision

This document has been revised and approved by the following parties.

Name	Organization	Title	Role
IE6 SLA Team	IE	IE6 SLA Team	Creators
Kenneth Garofalo	IE6	Division Chief	Approver
Susan Simon	IE	Acting Technical Director for Infrastructure Directorate	Approver
Charles Osborn	IE	Civilian Deputy Director for Infrastructure Directorate	Approver
Jessie Showers, JR	IE, SES	Senior Executive Services (SES)	Approver

Document Location

This document has been stored in the following location(s).

Location	
Document Library	http://www.disa.mil/network-services

Revision History

Version Number	Date	Summary of Changes	Org
1.0	December 30, 2010	Prepared for Signature	NS7
1.1	December 30, 2010	Initial Release	NS7
2.0	November 30, 2012	Second release includes additions of SME-PED, Private IP Service, and additional technologies for Dedicated service in the Transport Portfolio section and revised management thresholds as provided by internal mission partners. Conducted annual review of all sections by internal mission partners.	NS7
2.1	January 13, 2014	Incorporated NS input from AIM	NSP4
3.0	March 12, 2014	Third release includes additions of VPN Services, Satellite Communications Services Portfolio, and revised management thresholds as provided by internal mission partners. Conducted annual review of all sections by internal mission partners.	NSP4
4.0	July 19, 2016	Forth release includes the addition of twelve services as defined with in sections 8.8 through 8.16. In addition, Wireless Services Portfolio and Secure Mobile Environment - Portable Electronic	IE6

Version Number	Date	Summary of Changes	Org
		Device (SME-PED) have been removed. Conducted annual review of all sections by internal mission partners.	
4.1	December 09, 2016	Removed DISA Enterprise Voice and Video Services. Incorporated minor document formatting and administrative updates.	IE

Document Origination

This document has been originated by the following parties.

Name	Organization	Title	Role
SLM Team	NSP4	Telecommunications SME	Creator
Martha Buck	NSP4	Division Chief	Approver
Paul Filios	NS	Acting Vice Director for Network Services	Approver
Cindy Moran	NS	Director of Network Services	Approver
Jessie Showers, JR	IE	Senior Executive Services (SES)	Approver

Table of Contents

1. Introduction.....	11
2. Purpose.....	11
3. Scope.....	11
4. Applicability	11
5. Authority.....	11
6. Reference	12
7. Effective Date	12
8. Service Descriptions.....	12
8.1 Network Service Restoral	12
8.2 Transport Services Portfolio	12
8.2.1 <i>Dedicated</i>	13
8.3 Data Services Portfolio	16
8.3.1 <i>Sensitive but Unclassified (SBU) IP Data</i>	16
8.3.2 <i>Secret IP Data</i>	16
8.3.3 <i>Virtual Private Network (VPN) Services</i>	16
8.3.4 <i>Multilevel Secure Voice</i>	18
8.4 Messaging Services Portfolio	19
8.4.1 <i>Organizational Messaging Service</i>	19
8.5 Satellite Communications Services Portfolio	20
8.5.1 <i>MILSATCOM and COMSATCOM</i>	20
8.5.2 <i>SATCOM Gateway</i>	21
8.5.3 <i>Control Portfolio</i>	21
8.5.4 <i>Enhanced Mobile Satellite Services (EMSS)</i>	21
8.6 Combined Enterprise Regional Information Exchange System (CENTRIXS) Environment.....	22
8.7 Combined Federated Battle Laboratory Network (CFBLNet)	23
8.8 Common Mission Network Transport (CMNT).....	24
8.9 Pegasus.....	24
8.10 Unclassified Information Sharing Services/All Partners Access Network (UISS/APAN)	24
8.11 Domain Name Service (DNS)	25
8.12 DoD Enterprise Classified Travel Kit (DECTK).....	26
8.13 Internet Access Point (IAP)	26
8.14 NIPR Federated Gateway (NFG).....	27
8.15 Secure Voice Gateway (SVG)	27
8.16 Unified Video Dissemination System (UVDS)	27
8.17 Senior National Leadership Communications	28
9. Service Support Information	29



10. Service Performance Reporting..... 29
 Glossary 30
Appendix A Acronym List..... 31

Tables

Table 1: Network Service Restoral Time..... 12

Table 2: DATMS-Switch Availability 13

Table 3: DATMS-Trunk Availability 13

Table 4: Low Speed TDM - Switch Availability 14

Table 5: Low Speed TDM - Trunk Availability 14

Table 6: Low Speed TDM - Network Availability 14

Table 7: OTS - Switch Availability..... 14

Table 8: OTS - Trunk Availability 15

Table 9: ODXC - Switch Availability..... 15

Table 10: ODXC - Trunk Availability 15

Table 11: MSPP - Switch Availability..... 15

Table 12: MSPP - Trunk Availability 16

Table 13: SBU IP Data/Secret IP Data - Switch Availability..... 17

Table 14: SBU IP Data/Secret IP Data - Trunk Availability 17

Table 15: SBU IP Data/Secret IP Data - Network Availability 17

Table 16: SBU IP Data/Secret IP Data - Access Circuit Availability..... 17

Table 17: SBU IP Data/Secret IP Data Latency/Packet Loss - Intra-Theater 18

Table 18: SBU IP Data/Secret IP Data Latency/Packet Loss - Inter-Theater 18

Table 19: Multilevel Secure Voice - Switch Availability 19

Table 20: Multilevel Secure Voice - Trunk Availability..... 19

Table 21: Multilevel Secure Voice - Network Availability..... 19

Table 22: Organizational Messaging Service - ECGS Availability 20

Table 23: Organizational Messaging Service - AMHS Availability 20

Table 24: MILSATCOM & COMSATCOM Availability 21

Table 25: SATCOM Gateway Availability..... 21

Table 26: Control Portfolio Availability 21

Table 27: EMSS - Availability 22

Table 28: EMSS – MOC Call Success Rate Availability..... 22

Table 29: Combined Enterprise Regional Information Exchange System (CENTRIXS) ... 23

Table 30: Combined Federated Battle Laboratory Network (CFBLNet) 23

Table 31: Common Mission Network Transport (CMNT) 24

Table 32: Pegasus..... 24

Table 33: (UISS/APAN)..... 25

Table 34: Domain Name System (DNS) 25

Table 35: DoD Enterprise Classified Travel Kit (DECTK) 26

Table 36: Internet Access Point (IAP) 26

Table 37: NIPR Federated Gateway (NFG) 27

Table 38: Secure Voice Gateway (SVG) 27

Table 39: Unified Video Dissemination System (UVDS)..... 28

Table 40: Senior National Leadership Communications 29



This page intentionally left blank.

1. Introduction

The Defense Information Systems Network (DISN) is the Department of Defense's (DoD's) worldwide, interoperable, secure and highly available enterprise network infrastructure used to provide converged, net-centric, Internet Protocol (IP)-based voice, video, and/or data services through a combination of DoD and commercial terrestrial, wireless, and satellite communications capabilities, providing end-to-end (E2E) information transfer and management in support of military operations and national security. To ensure specific and measurable service, performance targets are documented for DISN telecommunications services. The Joint Requirements Oversight Council Memorandum (JROCM) 095-09 GIG 2.0 Initial Capabilities Document (ICD) provides threshold and objective measures for a globally interconnected, interoperable, secured system of systems. The Defense Information Systems Agency (DISA) Infrastructure Executive Directorate (IE) has established this Service Level Agreement (SLA) as a means of defining the funded performance thresholds for the services delivered to DISA mission partners. Operational performance of the services defined in the SLA will be monitored, measured, and reported against the commitments defined in this agreement.

2. Purpose

The purpose of this Telecommunications SLA is to define the services and their respective service performance objectives supported by Network Services. The service performance objectives are represented as Management Thresholds (MTs) and reflect the numerical baselines against which operational performance will be measured and reported.

3. Scope

The scope of services covered under the terms of this SLA includes the Transport Network, Unified Capabilities (voice, video, messaging, wireless, and mobile), IP data, and Satellite Communications. Service thresholds will be modified as a result of a change to validated requirements.

4. Applicability

This SLA is directly applicable to equipment, software, and facilities within the DISA Telecommunication Services.

5. Authority

This SLA is published in accordance with the authority contained in Department of Defense (DoD) Directive 5105.19, Defense Information Systems Agency (DISA), 25 July 2006 and

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 621 1.02D, DISN Responsibilities, 24 January 2012.

6. Reference

- (a) DISA Circular 310-130-2, 1 October 2012
- (b) DoD Directive 5105.19, Defense Information Systems Agency (DISA), 25 July 2006
- (c) The Defense Information Systems Network (DISN) Technical Evolution Plan (DTEP), 19 April 2016
- (d) DODI 8100.04, DoD Unified Capabilities (UC), 9 December 2010
- (e) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D, DISN Responsibilities, 24 January 2012
- (f) Initial Capabilities Document (ICD) for Joint Information Environment (JIE) , 17 July 2014
- (g) Global Information Grid (GIG) 2.0 ICD, JROCM 095-09, 29 May 2009
- (h) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6250.01E, Satellite Communications, 14 Mar 2013

7. Effective Date

This document is effective upon signature. Revision and review will be conducted as required, or at a minimum annually, to maintain its completeness and accuracy of the service information contained herein.

8. Service Descriptions

This section describes the telecommunication services and technologies covered under this commitment along with the associated management thresholds.

8.1 Network Service Restoral

In accordance with the GIG Service Management - Operations (GSM-0) contract, Acceptable Levels of Performance (ALPs), the average restoral time for all network service follows:

Commitment	MT	Metric
All Network Service	<= 15 hours	Average Restoral Time

Table 1: Network Service Restoral Time

8.2 Transport Services Portfolio

The Transport Services portfolio provides point-to-point services at various transmission rates. The Transport Services portfolio covered under this SLA consists of the dedicated service.

8.2.1 Dedicated

Dedicated service is a private-line-transport service that provides point-to-point connectivity to mission partner locations. Dedicated service relies on many different technologies such as DISN Asynchronous Transfer Mode (ATM) Service (DATMS), Low Speed Time Division Multiplexing (LSTDM), Optical Transport System (OTS), Optical Digital Cross Connect (ODXC), and Multi-Service Provisioning Platform (MSPP) technology.

8.2.1.1 DISN Asynchronous Transfer Mode (ATM) Service (DATMS)

The DISN ATM technology is a private-line-transport service that provides cell-based, point-to-point and point-to-multipoint connectivity to DISA mission partners. The technology offers ATM permanent virtual circuit and ATM permanent virtual path services, but it does not support mission partner-initiated ATM Switched Virtual Circuits.

The following tables show the management thresholds and metrics for DATMS technology.

DISN Asynchronous Transfer Mode Service

Commitment	Management Threshold	Metric
DISA CONUS	99.5	% Availability
DISA PACIFIC	99.5	% Availability
DISA EUROPE	99.5	% Availability
DISA CENTRAL	99.5	% Availability

Table 2: DATMS-Switch Availability

Commitment	Management Threshold	Metric
DISA CONUS	98.5	% Availability
DISA PACIFIC	98.5	% Availability
DISA EUROPE	98.5	% Availability
DISA CENTRAL	98.5*	% Availability

Table 3: DATMS-Trunk Availability

8.2.1.2 DISN Low Speed Time Division Multiplexing (LSTDM) Technology

The DISN LSTDM transport technology also known as PROMINA, offers end-to-end dedicated, fixed bandwidth, point-to-point services, and point-to-multipoint services.

The following tables show the management thresholds and metrics for LSTDM technology.

Low Speed Time Division Multiplexing

Commitment	Management Threshold	Metric
DISA CONUS	99.5	% Availability
DISA PACIFIC	99.5	% Availability
DISA EUROPE	99.5	% Availability
DISA CENTRAL	99.5	% Availability

Table 4: Low Speed TDM - Switch Availability

Commitment	Management Threshold	Metric
DISA CONUS	98.5	% Availability
DISA PACIFIC	98.5	% Availability
DISA EUROPE	98.5	% Availability
DISA CENTRAL	98.5*	% Availability

Table 5: Low Speed TDM - Trunk Availability

Commitment	Management Threshold	Metric
DISA CONUS	98.5	% Availability
DISA PACIFIC	98.5	% Availability
DISA EUROPE	98.5	% Availability
DISA CENTRAL	98.5*	% Availability

Table 6: Low Speed TDM - Network Availability

* The trunk and network availability actual performance may be lower in this Area of Responsibility (AOR), based on the commercial capabilities.

8.2.1.3 Optical Transport System (OTS) Technology

The OTS technology is a system that provides connectivity between DISN locations. This service is not available to DISA's external mission partners.

The following tables show the management thresholds and metrics for OTS technology.

Optical Transport System

Commitment	Management Threshold	Metric
DISA CONUS	99.9	% Availability
DISA EUROPE	99.9	% Availability

Table 7: OTS - Switch Availability

Commitment	Management Threshold	Metric
DISA CONUS	99.5	% Availability

DISA EUROPE	99.5	% Availability
-------------	------	----------------

Table 8: OTS - Trunk Availability

8.2.1.4 Optical Digital Cross Connect (ODXC) Technology

The ODXC transport technology offers end-to-end dedicated fixed bandwidth, and point-to-point services.

The following tables show the management thresholds and metrics for ODXC technology.

Optical Digital Cross Connect

Commitment	Management Threshold	Metric
DISA CONUS	99.9	% Availability
DISA PACIFIC	99.9	% Availability
DISA EUROPE	99.9	% Availability
DISA CENTRAL	99.9	% Availability

Table 9: ODXC - Switch Availability

Commitment	Management Threshold	Metric
DISA CONUS	99.5	% Availability
DISA PACIFIC	99.5	% Availability
DISA EUROPE	99.5	% Availability
DISA CENTRAL	99.5*	% Availability

Table 10: ODXC - Trunk Availability

* The trunk and network availability actual performance may be lower in this Area of Responsibility (AOR), based on the commercial capabilities.

8.2.1.5 Multi-Service Provisioning Platform (MSPP) Technology

The MSPP technology offers end-to-end dedicated fixed bandwidth, and point-to-point services. The following tables show the management thresholds and metrics for MSPP technology.

Multi-Service Provisioning Platform (MSPP)

Commitment	Management Threshold	Metric
DISA CONUS	99.9	% Availability
DISA PACIFIC	99.9	% Availability
DISA EUROPE	99.9	% Availability

Table 11: MSPP - Switch Availability

Commitment	Management Threshold	Metric
DISA CONUS	99.5	% Availability
DISA PACIFIC	99.5	% Availability
DISA EUROPE	99.5	% Availability

Table 12: MSPP - Trunk Availability

8.3 Data Services Portfolio

The Data Services portfolio provides best effort Internet Protocol (IP)-based services across the DoD enterprise based on the classification level of the information accessible. The Data Services portfolio covered under this SLA consists of three services: Sensitive but Unclassified (SBU) IP Data (formerly known as NIPRNet), Secret IP Data (formerly known as SIPRNet), and Private IP Service.

8.3.1 Sensitive but Unclassified (SBU) IP Data

SBU IP Data provides point-to-point connectivity to DISA mission partners. This unclassified IP data service for internet connectivity and information transfer supports DoD applications such as e-mail, web services, and file transfer. The SBU IP Data service also provides DoD customers with centralized and protected access to the public internet.

8.3.2 Secret IP Data

The Secret IP Data service provides point-to-point connectivity to DISA mission partners. It also provides IP-based secret information transfer across DoD for official DoD business applications such as e-mail, web services, and file transfer. The Secret IP Data service gateway function provides DoD customers with centralized and protected connectivity to federal, Intelligence Community (IC), and allied information at the secret level.

The Secret IP Data service includes IP-based secret information exchange within DoD (DoD intranet) and centralized, gateway external network information exchange (extranet). The intranet function provides access to a joint, shared DoD environment at the secret classification level for the exchange of information among DoD components.

8.3.3 Virtual Private Network (VPN) Services

The DISN Virtual Private Network (VPN) services providing data privacy to DISA mission partners across the SBU IP Data network (formerly known as NIPRNet). As data services, VPN services falls within DISN Infrastructure Services (DISN-IS) formerly known as the DISN Subscription Service (DSS) structure.

Operational VPN services include the following:

- Private IP Service

- Private Local Area Network (LAN) Service
- Label Transport Service
- Medical Community of Interest (MEDCOI)
- Common Mission Network Transport (CMNT)
- DISN Test and Evaluation (DISN T&E) Service

The following tables show the management thresholds and metrics for SBU IP Data and Secret IP Data. As noted above, VPN services rides across the SBU IP Data network; therefore, the management thresholds and metrics for VPN services are identical to SBU IP Data.

Sensitive but Unclassified IP Data/Secret IP Data

Commitment	Management Threshold	Metric
DISA CONUS	99.9	% Availability
DISA PACIFIC	99.9	% Availability
DISA EUROPE	99.9	% Availability
DISA CENTRAL	99.9	% Availability

Table 13: SBU IP Data/Secret IP Data - Switch Availability

Commitment	Management Threshold	Metric
DISA CONUS	99.5	% Availability
DISA PACIFIC	99.5	% Availability
DISA EUROPE	99.5	% Availability
DISA CENTRAL	99.5*	% Availability

Table 14: SBU IP Data/Secret IP Data - Trunk Availability

Commitment	Management Threshold	Metric
DISA CONUS	99.5	% Availability
DISA PACIFIC	99.5	% Availability
DISA EUROPE	99.5	% Availability
DISA CENTRAL	99.5*	% Availability

Table 15: SBU IP Data/Secret IP Data - Network Availability

Commitment	Management Threshold	Metric
DISA CONUS	98.5	% Availability
DISA PACIFIC	98.5	% Availability
DISA EUROPE	98.5	% Availability
DISA CENTRAL	98.5	% Availability

Table 16: SBU IP Data/Secret IP Data - Access Circuit Availability

Commitment	Latency MT (ms)	Packet Loss MT
Intra-CONUS	<100*	<.5%
Intra-EUROPE	<100	<.5%
Intra-PACIFIC (Oahu, HI-Western Pacific)	<150*	<.5%
Intra-CENTRAL	<100	<.5%

Table 17: SBU IP Data/Secret IP Data Latency/Packet Loss - Intra-Theater

* Due to the commercial architecture and Alaska communications connectivity, Alaska is part of CONUS in this SLA. Singapore is excluded in Intra and Inter measurements in the Pacific AOR.

Commitment	Latency MT (ms)	Packet Loss MT
CONUS-EUROPE	<130	<.5%
CONUS-PACIFIC (Oahu, HI-Western Pacific)	<130	<.5%
CONUS-CENTRAL	<350	<.5%

Table 18: SBU IP Data/Secret IP Data Latency/Packet Loss - Inter-Theater

** Due to the commercial architecture and Alaska communications connectivity, Alaska is part of CONUS in this SLA. Singapore is excluded in Intra and Inter measurements in the Pacific AOR.

8.3.4 Multilevel Secure Voice

The Multilevel Secure Voice service provides DoD with high-quality secure voice telephone and conferencing services for end-to-end use by DoD authorized users. Provision of this service is in accordance with national security directives in support of Command and Control (C2) and crisis management mission functions.

The Multilevel Secure Voice service includes a range of assured services to C2 users and their missions in an environment of a robust and feature-rich set of capabilities. This service is provided at major C2 facilities (e.g., the National Military Command Center (NMCC) and Combatant Command (COCOM) headquarters) interconnected through a cryptographically secured network. The service is the core of a DoD Global Secure Voice System (GSVS) during peacetime, crisis and time of conventional war by hosting national level conferencing and connectivity requirements and providing interoperability with both DoD tactical and strategic communities.

The following tables show the management thresholds and metrics for Multilevel Secure Voice.

Multi-level Secure Voice

Commitment	Management Threshold	Metric
DISA CONUS	99.5	% Availability
DISA PACIFIC	99.5	% Availability
DISA EUROPE	99.5	% Availability
DISA CENTRAL	99.5	% Availability

Table 19: Multilevel Secure Voice - Switch Availability

Commitment	Management Threshold	Metric
DISA CONUS	98.5	% Availability
DISA PACIFIC	98.5	% Availability
DISA EUROPE	98.5	% Availability
DISA CENTRAL	98.5*	% Availability

Table 20: Multilevel Secure Voice - Trunk Availability

Commitment	Management Threshold	Metric
DISA CONUS	98.5	% Availability
DISA PACIFIC	98.5	% Availability
DISA EUROPE	98.5	% Availability
DISA CENTRAL	98.5*	% Availability

Table 21: Multilevel Secure Voice - Network Availability

* The trunk and network availability actual performance may be lower in this Area of Responsibility (AOR), based on the commercial capabilities.

8.4 Messaging Services Portfolio

The Messaging Services portfolio provides organizational and assured messaging services to users including military services, DoD agencies, Combatant Commanders (COCOMs), non-DoD US government activities and the Intelligence Community (IC). The Messaging Services portfolio covered under this SLA consists of the Organizational Messaging service [formerly known as Defense Message System (DMS)].

8.4.1 Organizational Messaging Service

The Organizational Messaging service provides a range of assured services to the customer community that includes the military services, DoD agencies, COCOMs, non-DoD US government activities and the IC. These services include the ability to exchange official

information between military organizations and to support interoperability with allied nations, non-DoD activities and the IC operating in both the strategic/fixed-base and the tactical/deployed Enhanced Communication Gateway System (ECGS), General Service (GENSER), and Automated Message Handling System (AMHS) environments.

The following tables show the management thresholds and metrics for Organizational Messaging Service.

Organizational Messaging Service

Commitment	Management Threshold	Metric
NGC-D GENSER ECGS	98.7	% Availability
NGC-D DSSCS ECGS	98.7	% Availability
NGC-P GENSER ECGS	98.7	% Availability
NGC-D NIPR MINI-ECGS	98.7	% Availability
NGC-D SIPR MINI-ECGS	98.7	% Availability

Table 22: Organizational Messaging Service - ECGS Availability

Commitment	Management Threshold	Metric
NGC-P OMS NIPR AMHS	98.7	% Availability
NGC-P OMS SIPR AMHS	98.7	% Availability
NGC-P OMS TS/C AMHS	98.7	% Availability
NGC-D OMS NIPR AMHS	98.7	% Availability
NGC-D OMS SIPR AMHS	98.7	% Availability

Table 23: Organizational Messaging Service - AMHS Availability

8.5 Satellite Communications Services Portfolio

The Satellite Communications (SATCOM) Services portfolio is a critical portion of the DISN and provides reliable, secure, high-quality transport for voice, video and data services over Military and Commercial SATCOM (MILSATCOM and COMSATCOM). The SATCOM Services portfolio covered under this SLA consists of four services: MILSATCOM and COMSATCOM, Gateway, Control and EMSS.

8.5.1 MILSATCOM and COMSATCOM

MILSATCOM and COMSATCOM provide users with a wide range of military (SHF, EHF and UHF) and commercially available frequency bands to support mission requirements. All metrics within the SATCOM enclave cannot be retrieved without assistance from the DISA IE2 government leads.

The following tables show the management thresholds and metrics for SATCOM.

MILSATCOM & COMSATCOM

Commitment	Management Threshold	Metric
MILSATCOM & COMSATCOM	99.8	% Availability

Table 24: MILSATCOM & COMSATCOM Availability

8.5.2 SATCOM Gateway

The Gateway provides voice, video, data, Airborne-Intelligence, Surveillance and Reconnaissance (A-ISR) dissemination and transport of user networks for Command and Control (C2) and non-C2 customers with the capability to communicate directly using point-to-point or point-to-multipoint networks. It supports both strategic and tactical user requirements, and can readily insert additional equipment and services capabilities to provide a rapid and flexible response to emerging requirements.

The following tables show the management thresholds and metrics for SATCOM Gateways.

SATCOM Gateway

Commitment	Management Threshold	Metric
SATCOM Gateway	98.0	% Availability

Table 25: SATCOM Gateway Availability

8.5.3 Control Portfolio

The Control portfolio supports overall SATCOM as well as gateway and other equipment and software used within the SATCOM enclave. The control systems ensure SATCOM is deliberately managed and accurate status is uplinked to a central management suite for distribution to Stakeholders.

The following tables show the management thresholds and metrics for Control platforms.

Control Portfolio

Commitment	Management Threshold	Metric
Control Systems	98.0	% Availability

Table 26: Control Portfolio Availability

8.5.4 Enhanced Mobile Satellite Services (EMSS)

EMSS provides deployed warfighters and partnering agencies with global communications through security and user prioritization enhancements to commercial Mobile Satellite Services (MSS). EMSS includes global handheld voice, data, paging and sim-less Short Burst Data (SBD) communications.

EMSS is a capability provided by DoD that features global data transfer and securable voice communications. The service allows real-time access to other EMSS users, the SBU Voice and commercial US and international telephone networks through the Iridium satellite network. The EMSS handsets (satellite phones) enable the warfighter to communicate with the SBU Voice, Public Switched Telephone Network (PSTN), and SBU IP Data services by leveraging the EMSS gateway that interfaces with those services.

EMSS also offers the Distributed Tactical Communications System (DTCS), which is a secure tactical handheld satellite radio that provides on-the-move, over-the-horizon, beyond line-of-sight, voice, position location information and narrow band data communications to disadvantaged users in austere environments.

The following tables show the management thresholds and metrics for EMSS.

Enhanced Mobile Satellite Services

Commitment	Management Threshold	Metric
Constellation	95.0	% Availability
Gateway	98.5	% Availability
Terrestrial Connectivity	98.5	% Availability
JHITS I DSN (EMSS DISN Services)	98.5	% Availability
Data (EMSS DISN Services)	98.5	% Availability

Table 27: EMSS - Availability

Commitment	Management Threshold	Metric
MOC Call Success Rate	96.0	% Availability

Table 28: EMSS – MOC Call Success Rate Availability

8.6 Combined Enterprise Regional Information Exchange System (CENTRIXS) Environment

Combined Enterprise Regional Information Exchange System (CENTRIXS) environment is designed to be a global, interoperable, interconnected, and easy-to-use system to share and exchange intelligence and operations information through reliable communications connectivity, data manipulation, and automated processes. The CENTRIXS environment is a combination of network and applications services. All US CCMDs, national agencies, and foreign partner nations on individual CENTRIXS networks communicate with each other in a seamless manner. Most application services are provided by mainstream commercial-off-the-shelf (COTS) products; a few government-off-the-shelf (GOTS) solutions (e.g., guards, ISR capabilities) are used. CENTRIXS uses existing communications infrastructures such as the Secret Internet

Protocol Network (SIPRNet) and the Common Mission Network Transport (CMNT) whenever possible. The system employs National Security Agency (NSA)-approved encryption to establish an encrypted channel to users at command headquarters, theater/regional sites and forward points of presence servicing tactical sites. The next employment of CENTRIXS, version 2.0, will be Virtual Data Centers (VDC). The VDC solution provides consolidated end user multi-national collaboration services based on mission requirements while maintaining security boundaries as outlined by DoD and NSA security guidelines. VDC nodes are presented in a single virtualized platform containing connectivity and management of COI services while providing logical separation of networks by using hardened software applications to create non-crossable security boundaries. Hosted services include directory services, email, chat, VoIP, VTC, and data collaboration from within the COI environment while using secure connections to facilitate use of external services such as log aggregation, COP, and FMV.

Combined Enterprise Regional Information Exchange System (CENTRIXS)

Commitment	Management Threshold	Metric
DECC Hosting Nodes Available	98.5	% Availability
Transport Availability	99.5	% Availability
Critical Failover Services	98.5	% Availability
Tier III Node Availability	98.5	% Availability
DECC Hosting Nodes Available	98.5	% Availability

Table 29: Combined Enterprise Regional Information Exchange System (CENTRIXS)

8.7 Combined Federated Battle Laboratory Network (CFBLNet)

Combined Federated Battle Laboratory Network (CFBLNet) evaluates shortfalls in Multinational Information Sharing capabilities by providing continuously available network infrastructure to test technologies with mission partners and ease transition into an operational coalition network environment.

Combined Federated Battle Laboratory Network (CFBLNet)

Commitment	Management Threshold	Metric
Lab Nodes Availability	98.5	% Availability
Transport Availability	99.5	% Availability
Critical Failover Services	98.5	% Availability

Table 30: Combined Federated Battle Laboratory Network (CFBLNet)

8.8 Common Mission Network Transport (CMNT)

Common Mission Network Transport (CMNT) provides an enterprise common transport for information sharing among US and Multinational Information Sharing (MNIS) Communities of interest (COIs) by separating coalition network requirements (e.g. CENTRIXS) from the SIPRNet through the use of Multiprotocol Label Switching (MPLS) Layer 3 VPN service. CMNT facilitates a convergence of networks (e.g. CENTRIXS, BICES, BILATS, APIINetc) and increases operational effectiveness of the US Joint Forces and their mission partners. CMNT provides a capability to allow for the optimization of the maritime environment.

Common Mission Network Transport (CMNT)

Commitment	Management Threshold	Metric
DECC Host Services Available	98.5	% Availability
Transport Availability	99.5	% Availability
Critical Failover Services	98.5	% Availability

Table 31: Common Mission Network Transport (CMNT)

8.9 Pegasus

Pegasus is a Combined Communication Electronic Board (CCED) initiative that delivers significantly improved information sharing and dissemination of classified information between among the Five-Eyes (AUS/CAN/NZL/UK/USA) nations from national classified and Command and Control (C2) systems. Information sharing is based on National-to-National secret network connectivity (e.g., US SIPRNet, AUS Defence Secret Network (DSN), CAN Consolidated Secret Network Infrastructure (CSNI), UK Defence Information Infrastructure (DII) and NZL Secure Wide Area Network (SWAN). Under the Pegasus construct, each nation provides a gateway for proxying services to protect its national infrastructure and information.

Pegasus

Commitment	Management Threshold	Metric
DECC Host Services Available	98.5	% Availability
Transport Availability	99.5	% Availability
Tier III Node Availability	98.5	% Availability

Table 32: Pegasus

8.10 Unclassified Information Sharing Services/All Partners Access Network (UISS/APAN)

(UISS/APAN) provides the single enterprise solution for sharing non-classified information with non-traditional partners for Humanitarian Assistance and Disaster Recovery mission. UISS/APAN is an unclassified environment, non-dot-mil, providing structured (e.g. file sharing, calendaring) and unstructured (e.g. wiki, blogs, chat, and forums) collaboration capability for the purposes of Unclassified Information Sharing (UIS) with multinational partners, non-

governmental organizations, and among various United States Federal and State agencies. This environment is a DISA shared service hosted in DECC-Montgomery on its own internet connection completely disconnected from the DOD Information Network.

(UISS/APAN)

Commitment	Management Threshold	Metric
DECC Host Services Available	98.5	% Availability
Critical Failover Services	98.5	% Availability

Table 33: (UISS/APAN)

8.11 Domain Name Service (DNS)

The Domain Name System (DNS) service transLates queries for domain names into IP addresses for the purpose of locating computer services and devices worldwide. The Root represents the first order of the DNS hierarchy and is used by not only DoD, but all other global users of the public Internet. The G-Root, managed by IE72, is one of thirteen global Internet Root DNS servers in the world today. The G-Root is an unclassified network service but is not a direct DoD asset. The G-Root resolved over 770 billion DNS queries in 2015.

IE72 also maintains the master DNS Registry for the Unclassified (.mil) and Classified (.smil/.sgov) domains. The master DNS zone files point to other name servers for sub-domains in the ".mil" and ".smil/.sgov" domains. The DNS implementation for the .mil domain cooperatively interoperates with the DNS for the rest of the Internet. The Classified domains operate only within the closed SIPRNet environment. The performance, integrity, and reliability of DNS are mission-critical to the overall integrity of the DoDIN, and to the networks, systems, services, and applications that it supports. DNS Server environments are distributed through several diverse sites in order to provide reliable forward and reverse lookup service for the Unclassified and Classified domains.

Domain Name System (DNS)

Commitment	Management Threshold	Metric
DNS Service Availability	99.975	% Availability
DNS Server Capacity (Mem, CPU, Network)	<85	% Availability
DNS Query Average Response Time (ms)	<500ms	Time

Table 34: Domain Name System (DNS)

8.12 DoD Enterprise Classified Travel Kit (DECTK)

A gateway that provides portable, classified voice and data reach-back capabilities through any internet connection, anywhere in the world, by enabling a Virtual Private Network (VPN) connection to the Secret Internet Protocol Router Network (SIPRNet).

DoD Enterprise Classified Travel Kit (DECTK)

Commitment	Management Threshold	Metric
Is VISP Packet loss meeting requirements	<.5%	% dropped packets
Is VISP Latency meeting requirements	<200ms	Time
Is VISP Jitter meeting requirements	0-10ms	Time

Table 35: DoD Enterprise Classified Travel Kit (DECTK)

8.13 Internet Access Point (IAP)

The DODIN Internet Access Point (IAP) platform enables secure flow of traffic between the DoD NIPRNet and the Internet. The IAP router is physically connected to the Internet Service Provider (ISP) through triple 10G Ethernet connections that are co-located to Unclassified Provider Edge (U-PE) and DISN Joint IA (DJI) routers. The DJI router connects all of the Defensive Cyber Operations capabilities, which contains various router/firewalls that implements ports/protocol filters on ingress/egress traffic.

Internet Access Point (IAP)

Commitment	Management Threshold	Metric
Are IAP services meeting the Availability requirements established in the Service Level Agreement (SLA)?	99.5	% Availability
Are IAP services within Latency SLA Perspectives?	100ms	*Latency
Are IAP services affected by packet loss?	<1%	.5% dropped packets

Table 36: Internet Access Point (IAP)

- Measures are for within CONUS transactions only. Overseas will vary depending on location, up to 350ms.

8.14 NIPR Federated Gateway (NFG)

The NIPR Federated Gateway (NFG) provides a NIPRNet Demilitarized Zone (DMZ) as an enterprise gateway for non-DoD Federal Agencies to connect to Mission Partners. The establishment of the NFG satisfies the requirement for maintaining a line of defense for NIPRNet applications, users, and devices. The NFG inspects and protects all traffic originating from non-DoD federal partners and agencies whose physical and logical circuits terminate at the NFG external router (NFE).

NIPR Federated Gateway (NFG)

Commitment	Management Threshold	Metric
Are NFG services meeting the Availability requirements established in the Service Level Agreement (SLA)?	99.5	% Availability
Are NFG services within Latency SLA Perspectives?	100ms	Latency
Are NFG services affected by packet loss?	<1%	% dropped packets

Table 37: NIPR Federated Gateway (NFG)

8.15 Secure Voice Gateway (SVG)

A gateway utilizing Secure Communications Interoperability Protocol (SCIP) between secure IP Networks (e.g., SIPR/JWICS) and non-secure IP or TDM networks (e.g., NIPR/Internet or PSTN/DSN). The gateway provides a secure voice capability, eliminating the need for separate SCIP devices on every desk in the secure network. This gateway is in initial fielding and does not have final performance standards.

Secure Voice Gateway (SVG)

Commitment	Management Threshold	Metric
Is SVG gateway availability meeting requirements	99.6	% Availability
Is SVG call success rate (commercial) meeting requirements	90	% Availability

Table 38: Secure Voice Gateway (SVG)

8.16 Unified Video Dissemination System (UVDS)

The UVDS provides an enterprise-wide global distribution of Airborne-Intelligence, Surveillance and Reconnaissance data and information to our Intelligence Communities, Combatant Commanders, Services and Agencies. The Full motion Video Products are stored for a finite

period, and also high definition streaming video is available of target execution. The UVDS portals (two in CONUS, one in Europe being installed and activated by end of FY16 and one SWA in planning for FY17) provide an intermediate point for future dissemination to authorized users. The V3 Capability is also tied into the DoD mobility Classified Component for support to hand held devices.

Unified Video Dissemination System (UVDS)

Commitment	Management Threshold	Metric
UVDS Application Availability	99.6	% Availability

Table 39: Unified Video Dissemination System (UVDS)

8.17 Senior National Leadership Communications

Provide program management, technical solutions, and coordination assistance; establish and maintain direct and secure voice, data, and video communication links between to the President, Vice President, Secretary of Defense (SecDef), Joint Chiefs of Staff (JCS), combatant commanders (CCDRs), and other DoD components and its allies and other foreign nation counterparts. Provide the necessary secure communications to prevent the outbreak of nuclear war, resolve misunderstanding and regional security issues, support the elimination or reduction of weapons of mass destruction, support the war on international terrorism, support humanitarian and life-saving efforts.

Senior National Leadership Communications

Commitment	Management Threshold	Metric
HoS Circuit availability of 99.9% to support mission.	99.9	% Availability
DTL Circuit availability of 99.9% to support mission.	99.9	% Availability
FAL Circuit availability of 99.9% to support mission.	99.9	% Availability
DCL Circuit availability of 99.9% to support mission.	99.9	% Availability
NRRC Circuit availability of 99.9% to support mission.	99.9	% Availability
DHS Circuit availability of 99.9% to support mission.	99.9	% Availability
CJCS Circuit availability of 99.9% to support mission.	99.9	% Availability
COCOMs Circuit availability of 99.9% to support mission.	99.9	% Availability
SEWS Circuit availability of 99.9% to support mission.	99.9	% Availability

Table 40: Senior National Leadership Communications

9. Service Support Information

The DISN Customer Contact Center (DCCC) serves as the customer point of contact for telecommunication services.

Contact Information:

DSN: 1-844-DISA-HLP (347-2457), Option 2

SBU IP Data e-mail: disa.scott.global.mbx.dccc@mail.mil

Secret IP Data e-mail: disa.scott.global.mbx.dccc@mail.smil.mil

10. Service Performance Reporting

Service Level Agreement Monitoring (SLAM) reports will be generated on a monthly basis to provide service performance information.

Please note that CAC card authentication is required for viewing SLAM reports via the link below:

[IE SLAM Report Repository](#)

Glossary

Term	Definition
Availability	Availability indicates the percentage of time that a system or group of systems within a unit are operationally capable of performing an assigned mission and can be expressed as $100 \times \frac{(\text{Total time} - \text{Outage time})}{\text{Total time}}$ where Outage time is the period of time the system is unavailable for use by customers.
Call Blocking	Expresses the number of blocked calls by the number of attempted calls and is measured as the probability of a call not being completed (i.e., Grade of Service).
Grade of Service	Expresses the call blocking ratio on routine calls based on call volume. The number is based on calls blocked out of 100.
Latency	Round Trip Time (RTT) transmission times between two points in the network and is based on the routed performance of the network.
Management Threshold	Management thresholds are numerical baselines against which operational performance is measured to highlight where management action is required.
Packet Loss Non-Delivery Notification Ratios	The number of dropped packets between two points in the network and is based on the routed performance of the network. Expresses the percentage of non-delivery messages to the total messages sent.
Packet Loss Threshold	The minimum acceptable value considered achievable within the available cost, schedule, and technology at low-to-moderate risk. The number of dropped packets between two points in the network and is based on the routed performance of the network.
Threshold	The minimum acceptable value considered achievable within the available cost, schedule, and technology at low-to-moderate risk.

Appendix A Acronym List

Acronym	Term
AOR	Area of Responsibility
ATM	Asynchronous Transfer Mode
C2	Command and Control
CENTCOM	Central Command
COCOM	Combatant Command
CONUS	Continental United States
DCCC	DISN Customer Contact Center
DATMS	DISN ATM Service
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD DMS	Department of Defense Defense Message System
DRSN DoD	Defense Red Switch Network Department of Defense
DSN DRSN	Defense Switched Network Defense Red Switch Network
DSSDSN	DISN Subscription Service Defense Switched Network
DTCS DSS	Distributed Tactical Communications System DISN Subscription Service
DVSDTCS	DISN Video Services Distributed Tactical Communications System
DVS-GDVS	DYS –Global DISN Video Services
E2EDVS-G	End-to-End DYS-Global
EMSS E2E	Enhanced Mobile Satellite Services End-to-End
GoS EMSS	Grade of Service Enhanced Mobile Satellite Services
GSVS GoS	Global Secure Voice System Grade of Service
HIGSVS	Hawaii Global Secure Voice System
ICHI	Intelligence Community Hawaii

Acronym	Term
IPIC	Internet Protocol Intelligence Community
JHITSIP	Joint Hawaii Information Transfer System Internet Protocol
LSTDM JHITS	Low Speed Time Division Multiplexing Joint Hawaii Information Transfer System
MCEP LSTDM	Multi-Carrier Entry PointLow Speed Time Division Multiplexing
MLPPMFIMCEP	Multiple Level Precedence and Preemption Multi-Function Interpreter Multi-Carrier Entry Point
MOC MLPP MFI	Mobile Originated Calls Multiple Level Precedence and Preemption Multi-Function Interpreter
MPLS MOC MLPP	Multi-Protocol Labeled Switching Mobile Originated Calls Multiple Level Precedence and Preemption
MSPPMPLSMOC	Multi-Service Provisioning Platform Multi-Protocol Labeled Switching Mobile Originated Calls
MSS MSPP MPLS	Mobile Satellite Services Multi-Service Provisioning Platform Multi-Protocol Labeled Switching
MT MSS MSPP	Management Threshold Mobile Satellite Services Multi-Service Provisioning Platform
NDNMTMSS	Non-Delivery Notification Management Threshold Mobile Satellite Services
NIPRNet NDNMT	Unclassified but Sensitive Internet Protocol Router Network Non-Delivery Notification Management Threshold
NMCC NIPRNet NDN	National Military Command Center Unclassified but Sensitive Internet Protocol Router NetworkNon-Delivery Notification
NSNMCC NIPRNet	Network ServicesNational Military Command Center Unclassified but Sensitive Internet Protocol Router Network
ODXCNS NMCC	Optical Digital Cross Connect Network Services National Military Command Center
OTS ODXCNS	Optical Transport System Optical Digital Cross Connect Network Services
PSTN OTS ODXC	Public Switched Telephone Network Optical Transport System Optical Digital Cross Connect
RTTTPS TNOTS	Round Trip Time Public Switched Telephone NetworkOptical Transport System
SBDRTT PSTN	Short Burst Data Round Trip Time Public Switched Telephone Network
SBU SBDRTT	Sensitive but Unclassified Short Burst Data Round Trip Time
SIPR SBU SBD	Secret Internet Protocol Router Sensitive but UnclassifiedShort Burst Data
SIPRNet SIPRSBU	Secret Internet Protocol Router NetworkSecret Internet Protocol Router Sensitive but Unclassified
SLA SIPRNet SIPR	Service Level AgreementSecret Internet Protocol Router Network Secret Internet Protocol Router
SME-PED SLA SIPRNet	Secure Mobile Environment - Portable Electronic Device Service Level Agreement Secret Internet Protocol Router Network

Acronym	Term
TDMSME-PEDSLA	Time Division Multiplexing Secure Mobile Environment - Portable Electronic Device Service Level Agreement
U-ARTDMSME-PED	Unclassified-Aggregation Router Time Division Multiplexing Secure Mobile Environment - Portable Electronic Device
U-PEU-ARTDM	Unclassified-Provider Edge Unclassified-Aggregation Router Time Division Multiplexing
VoSIPU-PEU-AR	Voice over Secure Internet Protocol Unclassified-Provider Edge Unclassified-Aggregation Router
VPNVoSIPU-PE	Virtual Private Network Voice over Secure Internet Protocol Unclassified-Provider Edge
VTC VPN VoSIP	Video Conferencing Virtual Private Network Voice over Secure Internet Protocol
VTF VTC VPN	Video Conferencing Facility Video Conferencing Virtual Private Network
VTF VTC	Video Conferencing Facility Video Conferencing
VTF	Video Conferencing Facility



Defense Information Systems Agency
P.O. Box 549
Ft. Meade, MD 20755-0549
www.disa.mil