NETWORK SERVICES DIRECTORATE (NS)
ENTERPRISE CONNECTION DIVISION (NSC)

CONNECTION PROCESS GUIDE

VERSION 4.1
SEPTEMBER 2012

Defense Information Systems Agency
Enterprise Connection Division (NSC)
Post Office Box 549
Fort Meade, Maryland 20755-0549
www.disa.mil/connect

EXECUTIVE SUMMARY

This Connection Process Guide (CPG) implements the requirement in Department of Defense Directive (DoDD) 8500.01E *Information Assurance (IA),* 24 October 2002 (ref c), DoD Instruction (DoDI) 8500.02 *Information Assurance (IA) Implementation,* 6 February 2003 (ref f), and CJCSI 6211.02D *Defense Information System Network (DISN): Responsibilities*, *24 January 2012* (ref a), that Director, Defense Information Systems Agency (DISA), establish, manage, maintain, and promulgate a partner connection process guide describing steps that must be followed to request and implement a DISN connection. The goal of the CPG is to describe a transparent, user-friendly, and agile process that will help the warfighter and mission partners, as defined in directive DoDD 8000.01, *Management of the Department of Defense Information Enterprise*, 10 February 2009 (ref m), get connected quickly, and in a manner that does not bring an unacceptable level of risk to the DISN at large.
This release of the CPG:

- Updates and cancels the previous DISN Connection Process Guide, June 2012.
- Outlines the step-by-step process that all DoD and non-DoD mission partners, which includes non-DoD federal agencies, state and local government activities, contractors, foreign entities, etc., must follow. While the connection process can be complex, close adherence to the procedures described in this guide will ensure the most expeditious and secure completion of required tasks.
- Adds or revises several specific areas to include:
  - Improving clarity of the non-DoD connection request letter to Office of the Assistant Secretary of Defense for DoD Chief Information Officer (ASD/ DCIO)
  - Specifics on the network/topology diagram requirements for package submission

This guide is approved for public release and is available on the Internet from the DISA website at http://www.disa.mil/connect.

Please send your CPG version 4.1 improvement comments directly to DISA Ft. Meade NS Mailbox Unclassified Connection Approval disa.meade.ns.mbx.unclassified-connection-approval@mail.mil or DISA Ft. Meade NS Mailbox Classified Connection Approval disa.meade.ns.mbx.classified-connection-approval@mail.mil as applicable.

The instructions in this guide are effective immediately.

SIGNATURE PAGE FOR KEY OFFICIALS

Approved by:

10 September 2012

Teri C. Netter
Chief, Enterprise Connection Division

Date

REVISION HISTORY

This document will be reviewed and updated as needed (minimum semiannually). Critical and Substantive changes will be reflected in the revision history table. History will be populated starting with the Version 3.0 release.

Version	Date	Comments
3.0	May 2010	Baseline document released based on stakeholder input and extensive reformatting.
3.1	April 2011	Administrative changes to incorporate current policy and correct errors.
3.2	May 2011	Updated telephone numbers due to DISA BRAC relocation to Ft. Meade, MD.
4.0	June 2012	Major document layout changes. Document divided into Partner Type/Connection Type sections for ease of use. Several process updates. Email adress updates due to Defense Enterprise Email (DEE) migration. Private IP (Layer 2/3 VPN) registration in SNAP was added. Included several Frequently Asked Questions (FAQs) into appendices.
4.1	September 2012	Incorporated DSAWG clarifications in several areas. Includes updated Cross Domain Solutions (CDS) process flow chart. Updated email addresses due to Enterprise email changes.

This page intentionally left blank.

TABLE OF CONTENTS

SIGNATURE PAGE FOR KEY OFFICIALS ..... **iii**

REVISION HISTORY ..... **iv**

SECTION 1 INTRODUCTION **1-1**

1.1 Purpose **1-1**
1.2 Applicability **1-2**

SECTION 2 DISN CONNECTION PROCESS OVERVIEW **2-1**

2.1 Key Connection Process Areas and Terms **2-1**
2.1.1 DISN Technical Fundamentals 2-1
2.1.2 DISN Partners 2-2
2.1.3 DISN Networks/Services and Connections 2-2
2.1.4 Request Fulfillment 2-2
2.1.5 DISN Network/Service Specific Requirements 2-3
2.1.6 Certification and Accreditation (C&A) 2-3
2.1.7 Connection Approval Office (CAO) 2-3
2.1.8 Connection Approval Process (CAP) Package 2-4
2.1.9 Risk Assessment 2-4
2.1.10 Connection Decision 2-4
2.2 Determine Partner Connection Profile **2-4**
2.3 Determine Appropriate DISN Service or Process Appendix **2-5**

SECTION 3 DOD NEW CONNECTION PROCESS **3-1**

3.1 Identify the Type of DISN Network/Service Required **3-2**
3.2 Mission Partner Initiates DISA Direct Order Entry (DDOE) Process **3-2**
3.3 Mission Partner Initiates the Certification and Accreditation Process **3-2**
3.4 Mission Partner Registers the Connection Information **3-3**
3.5 Connection Approval Package Submission **3-3**
3.5.1 SNAP Registration and Submittal Process for Unclassified Packages 3-4
3.5.2 SGS Registration and Submittal Process for Classified Packages 3-4
3.5.3 CAP Package Contact Information 3-5
3.6 CAP Package Review and the Authorization to Connect Decision **3-5**
3.7 Notification of Connection Approval or Denial **3-6**
3.7.1 Connection Approval 3-6
3.7.2 Denial of Approval to Connect 3-6

SECTION 4 DOD REACCREDITATION PROCESS **4-1**

4.1 Reaccreditation Connection Evaluation **4-2**
4.2 Mission Partner Initiates the C&A Reaccreditation Process **4-3**
4.3 Mission Partner Updates the Connection Information **4-3**
4.4 Connection Approval Package Submission **4-3**
4.4.1 SNAP Registration Submittal Process for Unclassified Packages 4-4
4.4.2 SGS Registration and Submittal Process for Classified Packages 4-4
4.4.3 CAP Package Contact Information 4-4
4.5 CAP Package Review and the Authorization to Connect Decision **4-5**
4.6 Notification of Connection Approval or Denial **4-6**
4.6.1 Connection Approval 4-6
4.6.2 Denial of Approval to Connect 4-6

SECTION 5 NON-DOD NEW CONNECTION PROCESS **5-1**

5.1 Identify the Type of DISN Network/Service Required **5-2**
5.2 Complete and Submit Non-DoD Connection Request Letter **5-3**

5.3 Service Manager Review **5-3**
5.3.1 Concurs with Solution 5-3
5.3.2 Non-Concurs with Solution 5-4
5.4 CC/S/A/ Review **5-4**
5.4.1 CC/S/A Validated Request 5-4
5.4.2 CC/S/A Rejected Request 5-4
5.5 DOD CIO Review **5-4**
5.5.1 Approved Request 5-4
5.5.2 Denied Request 5-4
5.6 Partner/Sponsor Initiates DISA Direct Order Entry (DDOE) Process **5-4**
5.7 Partner/Sponsor Initiates the Certification and Accreditation Process **5-4**
5.8 Mission Partner/Sponsor Registers the Connection Information **5-5**
5.9 Partner/Sponsor Connection Approval Package Submission **5-5**
5.9.1 SNAP Registration Submittal Process for Unclassified Packages 5-7
5.9.2 SGS Registration and Submittal Process for Classified Packages 5-7
5.9.3 CAP Package Contact Information 5-8
5.10 CAP Package Review and the Authorization to Connect Decision **5-8**
5.11 Notification of Connection Approval or Denial **5-9**
5.11.1 Connection Approval 5-9
5.11.2 Denial of Approval to Connect 5-9

SECTION 6 NON-DOD REACCREDITATION PROCESS **6-1**

6.1 Reaccreditation Connection Evaluation **6-2**
6.2 Partner/Sponsor Initiates the C&A Reaccreditation Process **6-3**
6.3 Partner/Sponsor Updates the Connection Information **6-4**
6.4 Connection Approval Package Submission **6-4**
6.4.1 SNAP Registration Submittal Process for Unclassified Packages 6-5
6.4.2 SGS Registration and Submittal Process for Classified Packages 6-5
6.4.3 CAP Package Contact Information 6-5
6.5 CAP Package Review and the Authorization to Connect Decision **6-6**
6.6 Notification of Connection Approval or Denial **6-7**
6.6.1 Connection Approval 6-7
6.6.2 Denial of Approval to Connect 6-7

APPENDIX A NON-DOD DISN CONNECTION VALIDATION TEMPLATE **A-1**

A.1 Sample of an IT Topology Diagram **A-3**

APPENDIX B NON-DOD DISN CONNECTION REVALIDATION TEMPLATE **B-1**

APPENDIX C DEFENSE RED SWITCH NETWORK (DRSN) – CLASSIFIED **C-1**

C.1 DRSN Connection Process **C-1**
C.2 Process Deviations and/or Additional Requirements **C-1**
C.3 DRSN Connection Process Checklist **C-2**
C.4 Points of Contact **C-2**
C.5 Additional Policy and Guidance Documents **C-2**

APPENDIX D DEFENSE SWITCH NETWORK (DSN)/UNIFIED CAPABILITIES (UC) PRODUCTS – UNCLASSIFIED **D-1**

D.1 DSN Connection Process **D-1**
D.2 Process Deviations and/or Additional Requirements **D-1**
D.3 DSN Connection Process Checklist **D-4**
D.4 Points of Contact **D-5**
D.5 Additional Policy and Guidance Documents **D-5**
D.6 Topology Diagram Requirements **D-6**
D.7 SNAP DSN switch registration and DIACAP submittal process: **D-7**
D.8 Sample Topology Diagrams (with and without VOIP) **D-8**

D.9 Example Installation Configurations D-9

APPENDIX E DISN TEST AND EVALUATION (T&E) NETWORK (DTEN) VPN REGISTRATION E-1

E.1 DTEN VPN Service Description E-1
E.2 DTEN Connection Process E-1
E.3 DTEN COI Registration and Documentation E-1
E.4 Points of Contact E-2
E.5 DTEN VPN Registration and PTC Process Diagram E-3

APPENDIX F DISN VIDEO SERVICES (DVS) – CLASSIFIED AND UNCLASSIFIED F-1

F.1 DVS Connection Process F-1
F.2 Process Deviations and/or Additional Requirements F-1
F.3 DVS Connection Process Checklist F-2
F.4 Points of Contact F-5
F.5 Additional Policy and Guidance Documents F-6
F.6 Topology Diagram Requirements F-6

APPENDIX G NIPRNET – UNCLASSIFIED G-1

G.1 NIPRNet Connection Process G-1
G.2 Process Deviations and/or Additional Requirements G-1
G.3 NIPRNet Connection Process Checklist G-1
G.4 Points of Contact G-2
G.5 Topology Diagram Requirements G-5

APPENDIX H OSD GIG WAIVER PROCESS - UNCLASSIFIED H-1

H.1 Baseline Commercial ISP/Network Connection Approval Criteria H-1
H.2 Types of Waivers Required for Alternate Connections H-1
H.3 Process Deviations and/or Additional Requirements H-3
H.4 Waivers Process Flow H-5
H.5 Waiver Renewals H-6
H.6 Points of Contact H-7
H.7 Additional Policy and Guidance Documents H-7
H.8 FAQs H-8

APPENDIX I REMOTE COMPLIANCE MONITORING I-1

I.1 Vulnerability Scanning I-1
I.2 Scan Types I-1
I.3 Frequently Asked Questions (FAQs) I-2
I.4 IATT Process Checklist I-3

APPENDIX J SIPRNET – CLASSIFIED J-1

J.1 SIPRNet Connection Process Checklist J-1
J.2 Process Deviations and/or Additional Requirements J-2
J.3 IATT Process Checklist J-2
J.4 Points of Contact J-3
J.5 Additional Policy and Guidance Documents J-3
J.6 Sample SIPRNET Topology J-3

APPENDIX K CDS – CLASSIFIED AND UNCLASSIFIED K-1

K.1 Mandatory CDS Requirements for Connection to the SIPRNet K-1
K.2 CDS Authorization Process: Standard Point-to-Point Solution K-1
K.3 CDS Authorization Process: Cross Domain Enterprise Services K-7
K.4 Frequently Asked Questions K-11
K.5 Points of Contact K-13
K.6 Additional Policy and Guidance Documents K-13

APPENDIX L SME-PED – CLASSIFIED AND UNCLASSIFIED L-1

L.1 SME-PED Description L-1
L.2 SME-PED Connection Process L-1
L.3 Points of Contact L-1
L.4 Additional Policy and Guidance Documents L-2

APPENDIX M PRIVATE IP REGISTRATION IN SNAP M-1

M.1 Private IP Service – Unclassified – Description M-1
M.2 Complete the VPN registration in SNAP M-1
M.3 Documentation Requirements M-1

APPENDIX N DISA SERVICE MANAGER POINT OF CONTACT LIST N-1

APPENDIX O REFERENCES O-1

APPENDIX P ACRONYMS P-1

APPENDIX Q GLOSSARY Q-1

LIST OF FIGURES AND TABLES

Figure 1 Enterprise Connection Process Elements 2-1
Figure 2 DoD New Connection Process Flow 3-1
Figure 3 DoD Reaccreditation Process Flow 4-1
Figure 4 Non-DoD New Connection Process Flow 5-1
Figure 5 NoN-DOD Reaccreditation Process Flow 6-1
Figure 6 Sample DSN Topology with and without VOIP D-8
Figure 7 Example Installation Configurations D-9
Figure 8 DTEN VPN Registration and PTC Process E-3
Figure 9 DVS-G Registration Process F-2
Figure 10 DVS Secure Configuration -Example 1 ..... F-8
Figure 11 DVS Secure Configuration -Example 2 ..... F-8
Figure 12 DVS Secure Configuration -Example 3 ..... F-9
Figure 13 DVS Secure Configuration -Example 4 ..... F-9
Figure 14 DVS Secure Configuration -Example 5 ..... F-10
Figure 15 NIPR/SIPR Topology Sample G-6
Figure 16 ISP Waivers Process Flow H-6
Figure 17 NIPRNET/SIPRNET Topology Sample J-5
Figure 18 CDS Connection Process K-2

Table 1 DISN Networks/Services and Supported Classification 1-2
Table 2 DISN Global Support Center Contact Information 3-2
Table 3 Connection Approval Office Contact Information 3-5
Table 4 DISN DGSC Contact Information 5-2
Table 5 DISN Service Names 5-3
Table 6 DRSN Connection Process Checklist C-2
Table 7 DSN Connection Process Checklist D-4
Table 8 DTEN PTC Documentation - SGS Series E-2
Table 9 DVS Checklist F-3
Table 10 NIPRNet Connection Process Checklist G-2
Table 11 SIPRNet Connection Process Checklist J-2
Table 12 IATT Process Checklist J-3

This page intentionally left blank.

SECTION 1
INTRODUCTION

1.1 Purpose

The security of cyberspace is a Presidential national security priority, all DoD components must work together to provide the vital security elements to DoD's portion of cyberspace – the Defense Information Enterprise, which includes the DISN. Fundamentally, cyberspace is made possible by the millions of connections that make up the fabric of this truly global infrastructure. Stated simply, our combined connection approval actions significantly influence the security of the Defense Information Enterprise as a part of cyberspace. Together we must take this responsibility seriously and perform the necessary due diligence to ensure all the appropriate policies, procedures, and guidelines are followed. In short, there is a reason behind DoD's IA strategy, architecture, governance, and policies, such that every time the warfighter presses the "push to talk" button or the "Enter" key, they are ultimately connected clearly, reliably, and securely to the sovereign power of the United States.

Deriving authority from DoDD 8500.01 *Information Assurance (IA),* 24 October 2002 (ref c), DoDI 8500.02 *Information Assurance (IA) Implementation,* 6 February 2003 (ref f), CJCSI 6211.02D Defense Information System Network (DISN): Responsibilities, 24 January 2012 (ref a), and DoDI 8100.04 - DoD Unified Capabilities (UC). (ref n)

This guide is a living document that continues to evolve as connection processes for new and existing networks/services are refined and as additional networks/services become available. While this version of the CPG is limited to the DISN as detailed below, future versions of the CPG will expand to cover DoD's ever-evolving capabilities such as Unified Capabilities (UC), layer 3 VPNs, and cloud computing.

Use and consult the CPG often to assist you through the connection process. However, before employing this guide, always check for the current version on our website at: http://www.disa.mil/connect.

DISN networks/services and controlled processes addressed in this guide are included in

Current Name	Previous Name
Transport Services	
Dedicated	N/A
Data Services	
Non-Classified IP Data	NIPRNet
Secret IP Data	SIPRNet
TS/SCI IP Data	Joint Worldwide Intelligence Communications System (JWICS)
Secret Test and Evaluation (T&E) IP Data	DISN LES
Private IP Service	N/A
Voice Services	
CUI Voice	Voice over IP (VoIP) and/or DSN

Current Name	Previous Name
Voice over Secure IP (VoSIP)	
TS/SCI Voice	JWICS Voice
Multilevel Secure Voice	DRSN
DISA Enterprise Classified Voice and Video over IP (CVVoIP)	N/A
Video Services	
Dial-up, Internet Protocol (IP) and Dedicated Video Teleconferencing	DISN Video Services – Global (DVS-G)
TS/SCI Videoconferencing	JWICS Videoconferencing
Messaging Services	
Organizational Messaging Service	DMS
Wireless Services	
Enhanced Mobile Satellite Services (EMSS)	N/A
Secure Mobile Environment Portable Electronic Device (SME-PED)	N/A
Satellite Services	
International Maritime Satellite (INMARSAT)	N/A
Commercial Satellite Service (CSS)	N/A

Table 1.

Current Name	Previous Name
Transport Services	
Dedicated	N/A
Data Services	
Non-Classified IP Data	NIPRNet
Secret IP Data	SIPRNet
TS/SCI IP Data	Joint Worldwide Intelligence Communications System (JWICS)
Secret Test and Evaluation (T&E) IP Data	DISN LES
Private IP Service	N/A
Voice Services	
CUI Voice	Voice over IP (VoIP) and/or DSN
Voice over Secure IP (VoSIP)	
TS/SCI Voice	JWICS Voice
Multilevel Secure Voice	DRSN
DISA Enterprise Classified Voice and Video over IP (CVVoIP)	N/A
Video Services	
Dial-up, Internet Protocol (IP) and Dedicated Video Teleconferencing	DISN Video Services – Global (DVS-G)

Current Name	Previous Name
TS/SCI Videoconferencing	JWICS Videoconferencing
Messaging Services	
Organizational Messaging Service	DMS
Wireless Services	
Enhanced Mobile Satellite Services (EMSS)	N/A
Secure Mobile Environment Portable Electronic Device (SME-PED)	N/A
Satellite Services	
International Maritime Satellite (INMARSAT)	N/A
Commercial Satellite Service (CSS)	N/A

Table 1 DISN Networks/Services and Supported Classification

1.2 Applicability

This guide applies to all DoD and non-DoD information systems (ISs) seeking to connect to the DISN. For definitions and descriptions of a DoD IS and a non-DoD entity, refer to DoDD 8500.01E *Information Assurance (IA)*, 24 October 2002 (certified current as of 23 April 2007) (ref c), and CJCSI 6211.02D Defense Information System Network (DISN):Responsibilities, 24 January 2012 (ref a), respectively.

SECTION 2
DISN CONNECTION PROCESS OVERVIEW

The CPG is a step-by-step guide to the detailed procedures that all DoD and non-DoD mission partners must follow to obtain and retain connections to the DISN. The guide consolidates the connection processes for all networks and services into one document, helps partners understand connection requirements and timelines, and provides contacts for assistance throughout the process. The Enterprise Connection Division is not the process owner for the entire "connection process." The CPG points partners to appropriate information services, websites, or offices wherever possible to help guide partners through the entire process.

This section presents a high-level overview of the DISN connection process, focusing on the key areas that the partner must thoroughly understand and properly execute to obtain and retain a connection to the network/service appropriate for their mission. The figure below provides a graphical depiction of the overall process.

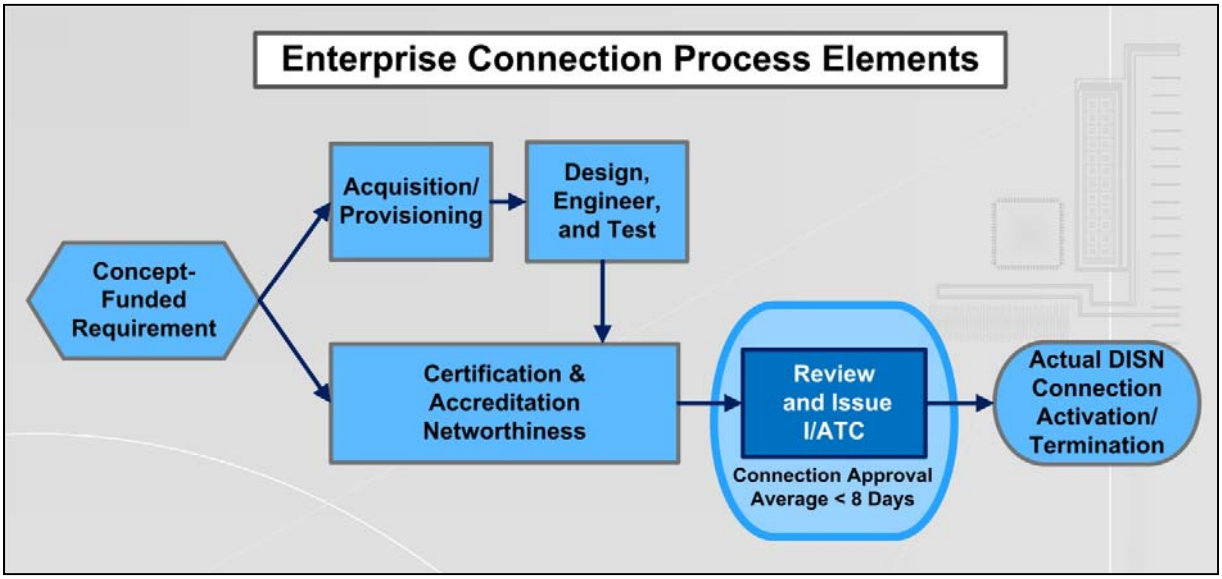


Figure 1 Enterprise Connection Process Elements

This very simplified conceptual view of the request fulfillment process shows major elements of the end-to-end process. This diagram is by no means all-inclusive, nor does it attempt to represent the request fulfillment process for all connections in DoD. The request fulfillment process does not end with the actual connection because the C&A cycle repeats until the IS is physically disconnected and discontinued via the request fulfillment process.

2.1 Key Connection Process Areas and Terms

2.1.1 DISN Technical Fundamentals

The DISN has the following generalized components:

- Long-haul transport (Wide Area Network (WAN))
- Components to manage/operate the long-haul transport

- Services that are enabled on the long-haul transport (Network-Enabled Services)
- Enclaves that derive access to the network-enabled services by connecting Local Area Networks (LANs) to the WAN to gain access to WAN services; enclaves may include voice, video, email, Web access, and other services in the local environment; enterprise-level services, such as Cross Domain Enterprise Services, Defense Enterprise Computing Centers (DECC), Network Operations Centers (NOC), Teleport, etc.

2.1.2 DISN Partners

There are two types of partners that connect to the DISN to utilize its networks/services: DoD and non-DoD. DoD partners are DoD Combatant Commands, Military Services and Organizations, and Agencies (DoD CC/S/A/), collectively referred to as "DoD Components." Per Reference (ref a) in the REFERENCES Appendix, non-DoD mission partners and defense contractors include all organizations and entities that are not components of the DoD. This includes: contractors and federally funded research and development centers; other U.S. government federal departments and agencies; state, local, and tribal governments; foreign government organizations/entities (e.g., allies or coalition partners); non-government organizations; commercial companies and industry; academia (e.g., universities, colleges, or research and development centers); etc. Non-DoD mission partners must have a validated requirement approved by a sponsoring CC/S/A or field activity headquarters and approval from the DOD CIO/DoD Chief Information Officer (CIO)). In addition, all DISN partners must have a Computer Network Defense Service Provider (CNDSP) for their Information System.

2.1.3 DISN Networks/Services and Connections

The DISN offers classified and unclassified voice, video, and data services to its partners. A detailed description of each of the services via DISA Direct is available at the following website: https://www.disadirect.disa.mil/products/asp/welcome.asp.

2.1.4 Request Fulfillment

Partners requiring a new connection to the DISN and its services must use the DISA Direct Order Entry (DDOE) request fulfillment process to initiate the provisioning requirement and circuit activation (go to https://www.disadirect.disa.mil/products/asp/welcome.asp for further information and guidance). The Telecommunications Service Request (TSR) and Telecommunication Service Order (TSO) processes involve the ordering, engineering, acquisition, and installation of the circuit and equipment necessary to connect to the DISN. Request fulfillment may only be initiated by a DoD entity. A DoD CC/S/A entity may sponsor a non-DoD mission partner, but the DoD sponsor remains responsible for all request fulfillment actions to include but not limited to completing and/or assisting the non-DoD mission partner with Certification and Accreditation (C&A) requirements. See sponsor memo at http://www.disa.mil/Services/Network-Services/DISN-Connection-Process/~/media/Files/DISA/Services/DISN-Connect/Policy/Memo_Summary_of_DoD_Sponsor_Responsibilities.pdf

2.1.5 DISN Network/Service Specific Requirements

While all DISN networks/services follow similar connection process steps, there may be network/service-specific requirements for requesting and obtaining a connection, e.g., registering the connection request in an IS/database dedicated to that network/service and/or ensuring components are listed on the DoD Approved Products List (APL) prior to purchase or lease, as designated in each network/service-specific appendix. The common connection process steps are presented in sections 3-6, while any unique network/service-specific requirements are provided in the appendices.

2.1.6 Certification and Accreditation (C&A)

All ISs, including network enclaves connecting to the DISN, require certification and accreditation in accordance with an appropriate and acceptable process. For new and additional connections, the IS C&A process should be initiated parallel to or soon after beginning the request fulfillment process. For reaccreditations, the partner should initiate IS reaccreditation actions with sufficient time prior to expiration of the current accreditation and connection approval to prevent a potential circuit disconnect recommendation. Expiration notices are sent to the POC's for the subject IS every 30 days starting 90 days prior to the expiration.

DoD CC/S/As and field activities must execute the DoD Information Assurance Certification and Accreditation Process (DIACAP). For non-DoD mission partners and defense contractors, the appropriate C&A process (i.e., DIACAP, NISPOM, NIST, DCID, etc.) depends on the type of non-DoD mission partners and defense contractor and the network/service to be accessed. At the completion of the C&A process, the Designated Accrediting Authority (DAA), Chief Information Officer (CIO), or Authorizing Official issues an accreditation decision in the form of an Authorization to Operate (ATO), Interim ATO (IATO), or Interim Authorization to Test (IATT). This artifact (for DIACAP actions it's the signed Scorecard) is required in the Connection Approval Process (CAP) package before an Approval to Connect (ATC) or Interim ATC (IATC) can be issued by the DISN Connection Approval Office (CAO).

2.1.7 Connection Approval Office (CAO)

The Enterprise Connection Division's Information Assurance (IA) Branch includes two functional areas: Connection Approval and Cross Domain Solutions (CDS). The CAO is responsible for processing GIG waivers, performing SIPRNet enclave scans and reviewing and approving all routine DISN connection requests, which are primarily addressed in this CPG. The CAO also receives some other types of connection requests that are not routine; they involve a higher level of risk to the DISN than the CAO is authorized to accept. The CDS team reviews Cross Domain requests and analyzes the threat posed to the GIG, assigns a Grid Connectivity Threat rating, and prepares cross domain tickets to be presented to the CDTAB (Cross Domain Technical Advisory Board). Those requests (e.g., CDS) are reviewed/approved by the Defense IA/Security Accreditation Working Group (DSAWG), and in cases of even higher risk, by the DISN/GIG Flag Panel.

2.1.8 Connection Approval Process (CAP) Package

Connection requests are sent to the CAO in the form of a CAP package. These packages provide the CAO the information necessary to make the connection approval decision. The baseline requirements for what must be included in the CAP package depend on whether the partner is DoD or non-DoD and whether the connection is new or due for reaccreditation. There may also be additional requirements, depending on the specific DISN network/service the partner needs to access. The baseline requirements are provided in sections 3-6 of this guide. Any additional network/service-specific requirements are provided in the appendix that corresponds to that specific network/service.

2.1.9 Risk Assessment

As an integral part of the connection approval process, the CAO conducts an initial assessment of the risk that a new or reaccreditation connection presents to the DISN. Risk assessments are based on the level of partner compliance with governance, DISA/FSO Security Technical Information Guides (STIGs) and on-site and remote compliance monitoring and vulnerability assessment scans, DSAWG/Flag Panel decisions, etc.

When non-compliance issues are identified and confirmed, the CAO works with the partner and others to validate and correct the weaknesses that generated the risk. Weaknesses can include, among other elements, incomplete and/or incorrect information submitted as part of the CAP package documentation and artifacts.

2.1.10 Connection Decision

After the CAP package is reviewed and the risk assessment conducted, the CAO makes a connection decision and notifies the partner. Partners approved for connection to the DISN are granted either an ATC or an IATC, which is normally assigned an expiration date to coincide with the Authorization Termination Date (ATD) of the partner IS ATO or IATO. In the event of a high risk assessment for a new connection, the CAO works with the partner to address the issue until the risk can be downgraded or mitigated, allowing the issuance of an ATC or IATC.

2.2 Determine Partner Connection Profile

The process for network/service request fulfillment and approval of a connection to the DISN or service varies depending on: 1) whether the partner is a DoD CC/S/A or a non-DoD mission partner; 2) whether the request is for a new connection or a reaccreditation; and 3) what network/service is being accessed. When requesting network/service request fulfillment and approval of a connection to the DISN or service, the process varies depending on partner type and partner requirements. The CPG is broken up into four process sections based on partner type and connection type. Each section describes the connection process requirements and steps that are common to all networks/services specific to the Partner Connection profile. The four process sections are:

- **DoD**

  DOD NEW CONNECTION PROCESS
  DoD REACCREDITATION PROCESS

- **Non-DoD Mission Partner or Defense Contractor**
  NON-DoD NEW CONNECTION PROCESS
  NON-DoD REACCREDITATION PROCESS

Regardless of whether or not the partner is DoD or non-DoD, to initiate the connection process, the partner must first determine if this is a requirement for a new connection or a re-accreditation.

2.3 Determine Appropriate DISN Service or Process Appendix

After you have reviewed the process for your Partner connection profile, proceed to the appropriate appendices that identify the specific DISN Service connection for additional requirements and guidance. The appendices also include waiver processes, exception processes, templates, points of contact tables, references, and acronym lists.

SECTION 3

DOD NEW CONNECTION PROCESS

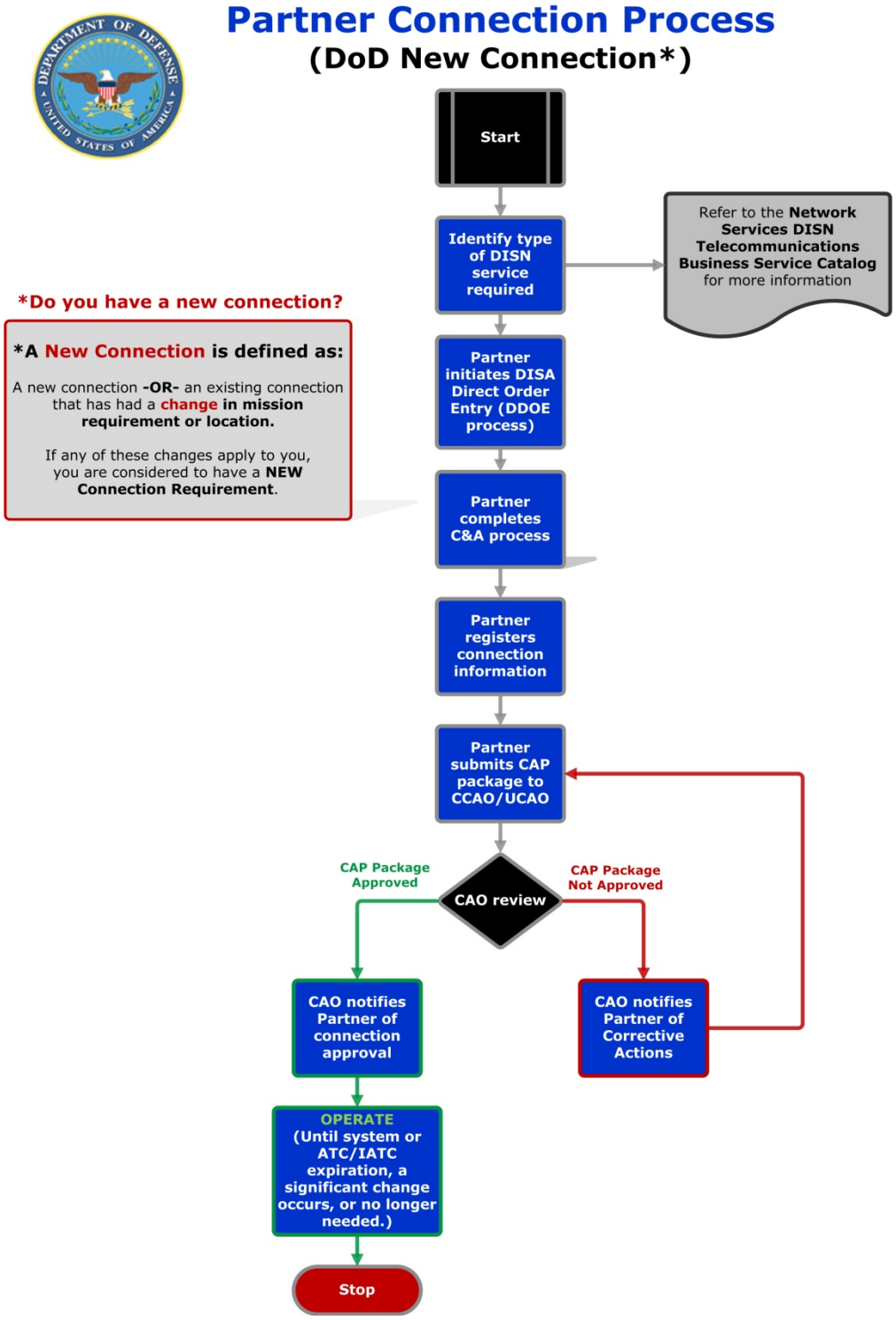


Figure 2 DoD New Connection Process Flow

3.1 Identify the Type of DISN Network/Service Required

Once the partner determines that this is a new connection requirement, the next step is to identify the DISN network/service that is required. This involves matching partner needs to the most appropriate DISN network/service. All partners desiring connections to the DISN must first confirm with the applicable Service Manager (SM) that the desired network/service is appropriate for the mission.

Partners who are not sure which network/service best meets their needs should review the description of DISN voice, video, and data services available at https://www.disadirect.disa.mil/products/asp/welcome.asp and/or contact the DISN Global Support Center (DGSC). The DGSC will facilitate contact with the appropriate DISN SM.

DISN Global Support Center (DGSC)	
Unclassified email	DGSC@csd.disa.mil
Classified email	DGSC@cols.csd.disa.smil.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

Table 2 DISN Global Support Center Contact Information

Partners who know which DISN service they require will find POCs for each of the DISN networks/services in this guide's individual appendices.

3.2 Mission Partner Initiates DISA Direct Order Entry (DDOE) Process

Identify your appropriate network/service through the DISN Telecommunications Business Services guide on the DDOE website:
https://www.disadirect.disa.mil/products/asp/welcome.asp.

After the appropriate network/service is identified and applicable approvals are received, the partner initiates a request for service fulfillment through the DDOE process on the DISA direct website listed above. This is the ordering tool for DISN Telecommunications Business Services guide.

3.3 Mission Partner Initiates the Certification and Accreditation Process

In parallel, or shortly after initiating the request for service through DDOE, the partner should begin the C&A process for the IS/enclave for which a connection to the DISN is required.

DoD partners are required to use the DIACAP and to submit (at a minimum) a complete and accurate DIACAP Executive Package, which includes the following documents/artifacts.

- System Identification Profile (SIP)
- DIACAP Scorecard
- IT Security Plan of Action and Milestones (POA&M), if required
- Detailed Topology Diagram (not a DIACAP artifact, however it is required for Connection Approval)

(For instructions on how to complete these requirements, see (ref g)/DIACAP and the DIACAP Knowledge Service at https://diacap.iaportal.navy.mil/login.htm.)

3.4 Mission Partner Registers the Connection Information

Partners are required to register the connection information (new or legacy) within applicable systems/databases.

Once the DDOE process has been completed with the receipt of a Command Communications Service Designator (CCSD), partners are required to register their IS information (IP address ranges, hosts, POCs, etc.) in the appropriate databases based on classification of the connection:

- Network Information Center (www.nic.mil) for all unclassified connections
- SNAP (https://snap.dod.mil) for:
  - Voice, video, data circuit registrations and connections to unclassified networks/services
  - OSD GIG Waivers for Internet Service Provider registrations (Appendix H)

or

- SIPRNet Support Center (www.ssc.smil.mil) for all classified connections
- GIAP/SGS (https://giap.disa.smil.mil) for:
  - Voice, video, and data circuit registrations and connections to classified networks/services

and

- Ports, Protocols, and Services Management (PPSM) (https://pnp.cert.smil.mil) on SIPRNet for all networks/systems ports, protocols, and services for all IP solutions or applications, including Voice over Internet Protocol (VoIP), Voice over Secure Internet Protocol (VoSIP)), and Classified Video Voice over IP (CVVoIP).

DoD policy requires that partners register their IS information in the DoD Information Technology Portfolio Repository (DITPR) at https://ditpr.dod.mil.
An enclave/network may also be registered in the SIPRNet IT Registry, by first requesting an account to the application at https://arm.osd.smil.mil.
Once you have an account, the link to the SIPR IT Registry is: http://osdext.osd.smil.mil/sites/dodcio/itregistry/default.aspx.

CC/S/A may have internal databases that need to be updated with connection information. Check with your CC/S/A for additional requirements.

3.5 Connection Approval Package Submission

The Mission Partner connection requests are submitted to the CAO in the form of a CAP package. This package provides the CAO the information necessary to make a connection approval decision. CAP packages should be submitted at least 30 days prior to the desired connection date for new connections.

Tactical exercise/mission CAP packages must be submitted a minimum of eight (8) days prior to the start of the exercise/mission. Tactical mission/exercise requests should include the mission number found on the Gateway Access Authorization (GAA) subject line or the timeframe of the exercise. The GAA message must be released by the appropriate Contingency and Exercise office (CONEX) prior to an IATC/ATC letter being issued by the CAO. Tactical exercise/mission CAP packages do not submit a complete DIACAP package. However, they must include at a minimum, an ATO/IATO letter, GAA, SCQ (SIPR only), and topology.

Connection Package document requirements are listed in the applicable appendix at the end of this document.

3.5.1 SNAP Registration and Submittal Process for Unclassified Packages

CAP packages for unclassified connections will be uploaded by the partner in the SNAP registration database.

- Create SNAP profile: https://snap.dod.mil/gcap/request-account.cfm
- Upload completed DD Form 2875 (SAAR). The 2875 can be downloaded from the SNAP website.
- Complete section 13 "Justification for Access" by specifying the SNAP module and user role for your CC/S/A.
- Complete your profile data, asterisked items are required fields.
- Submit the account for approval

Once the account is approved, proceed with the creation/registration of the unclassified connection to include the submittal/upload of the DIACAP executive package artifacts once your local DIACAP C&A is completed:

- Logon to SNAP NIPR: https://snap.dod.mil/gcap/home.cfm
- Hover the mouse over "NIPR" and select "New Registration"
- Complete all sections (0-4 and 6, Section 5 is for CAO use only.) and required fields identified by an asterisks.
- Upload Attachments for your DIACAP executive package artifacts in Sections 7.1 through 7.6 as applicable. Please note: Only Sections 7.1 through 7.5 require the upload of attachments.
- Once all sections are completed, with the exception of Section 5, a submit button at the bottom of the screen will be available in order to submit the entire registration.

NOTE: For 24/7 SNAP assistance; contact the DISN Global Support Center – (800) 554-3476

3.5.2 SGS Registration and Submittal Process for Classified Packages

Partners should request read-only access to SGS to have access to their circuits. To request access, a DD 2875 to include all CCDSs they are responsible for, should be sent to the Connection Approval Office. The appropriate email addresses are listed in the contact information table below.

CAP packages are normally submitted as Unclassified/For Official Use Only (FOUO). However, it is recommended that the network topology diagram be provided over SIPRNet. The

partner/sponsor must determine, based on DoD component and local guidance, if any part of the CAP package contents must be labeled and handled as classified documents.

NOTE: Incomplete packages will not be accepted, and will be returned for rework.

3.5.3 CAP Package Contact Information

The CAP package submission email addresses, phone numbers, and mailing addresses are**:**

Connection Approval Office (CAO)	
Connection Approval Office for Unclassified Connections (UCAO)	disa.meade.ns.mbx.unclassified-connection-approval@mail.mil ucao@disa.smil.mil
Connection Approval Office for Classified Connections (CCAO)	disa.meade.ns.mbx.classified-connection-approval@mail.mil ccao@disa.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901
Address	Defense Information Systems Agency ATTN: NSC1 PO Box 549 Fort Meade, MD20755-0549

Table 3 Connection Approval Office Contact Information

3.6 CAP Package Review and the Authorization to Connect Decision

Upon receipt of the CAP package, the CAO reviews the contents for completeness. In the event an incomplete package is received by the CAO, the package will be rejected and no CAO tracking number assigned. The partner will receive notification of a rejected package to include what documentation is missing from the package. Typically, when all the connection approval requirements are met an ATC or IATC will be issued within eight (8) business days.

As an integral part of the process, the CAO assesses the level of risk the partner's IS or network enclave poses to the specific DISN network/service and to the GIG community at large. The identification of IA vulnerabilities or other non-compliance issues and the responsiveness of the affected enclave in implementing appropriate remediation or mitigation measures against validated vulnerabilities will have a direct impact on the risk assessment, and subsequently on the connection approval decision.

The following are some of the indicators that would contribute to the assessment of an elevated risk:

- Missing, incomplete, or inaccurate CAP package input (because unknowns lead to a lower level of confidence in the IA status of the partner IS/enclave).
- Unsatisfactory results during remote compliance monitoring/vulnerability assessment where policy compliance is reviewed.

If the risk is "low" or "medium," the CAO will issue an ATC or IATC. A "medium" risk assessment will cause the CAO to more closely monitor the IA status of the IS/enclave during the connection life cycle. "Low" risk assessments will not affect a new connection request.

An ATC/IATC will normally authorize the partner to connect to the DISN network/service defined in the connection approval, up to the accreditation decision ATD. The results of the risk assessment may warrant the issuance of a connection approval decision with a validity period shorter than that of the accreditation decision ATD. In such cases, the CAO will provide justification to the DAA for the shorter validity period.

If the CAO assesses a "high" risk, it will provide the DAA the justification for the assessment and inform the DAA that current guidance (i.e., policy, DSAWG decision, STIGs, etc.) from DISN/GIG DAAs precludes the issuance of an ATC without additional review of the IS/enclave IA status by the community accreditation bodies.

3.7 Notification of Connection Approval or Denial

Once the CAO makes a connection decision, the partner is notified.

3.7.1 Connection Approval

If the connection request is approved, the partner is issued an ATC or IATC. The validity period is specified in the ATC/IATC letter. After the connection is approved, the partner must work with DISN Implementation to complete the installation of the circuit. The connection approval is valid until the expiration date. The DAA must notify the CAO of significant changes, such as architecture changes requiring re-accreditation, movement of the IS enclave to a new location, changes in risk posture, etc., that may cause a modification in the IA status of the system/enclave or if the connection is no longer needed.

3.7.2 Denial of Approval to Connect

If the connection request is rejected, the CAO will provide the partner a list of corrective actions required before the connection can be approved. The process will restart at Section 3.5.

SECTION 4

DOD REACCREDITATION PROCESS

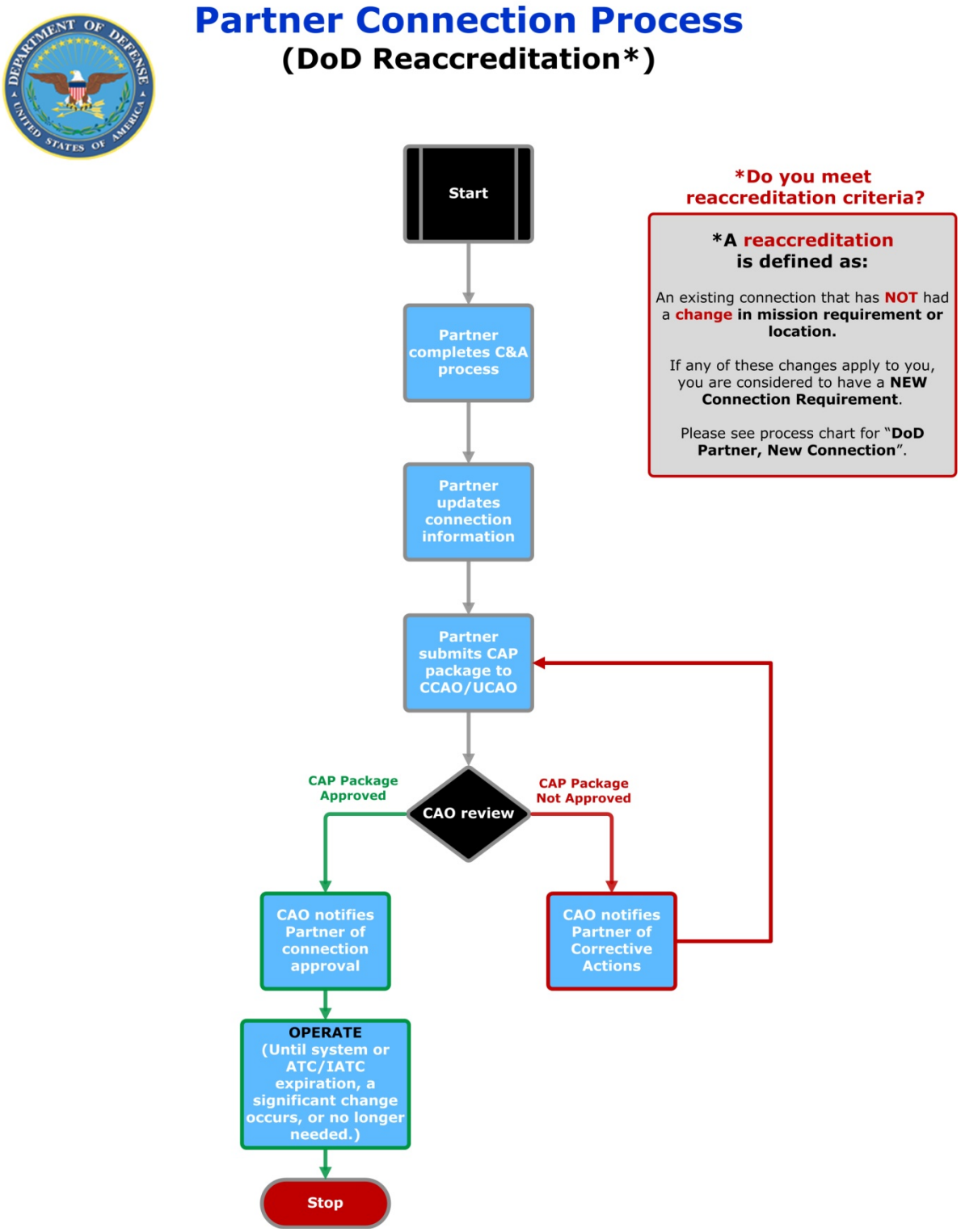


Figure 3 DoD Reaccreditation Process Flow

4.1 Reaccreditation Connection Evaluation

If an accreditation decision is approaching its Authorization Termination Date (ATD), the DAA must reinitiate the C&A process and issue a new accreditation decision. Ideally, the new ATO/IATO will be issued and an updated CAP package forwarded to the CAO a minimum of 30-days prior to the expiration of the current ATC/IATC.

The expiration date of an ATC/IATC is usually the same as (and will never go beyond) the ATD expiration date of the associated scorecard. In some instances, the results of the CAO or DSAWG risk assessment may warrant the issuance of an ATC/IATC with an accreditation period shorter than that of the associated scorecard. An expired ATC/IATC will prompt a review by USCYBERCOM, and may possibly result in an order to disconnect the IS/enclave from the DISN network/service.

The DAA could decide that planned changes to an IS/enclave are significant enough to warrant reinitiating the full C&A process, with subsequent issuance of a new accreditation decision inside the normal 3-year ATO (or 180-day IATO) cycle. If no physical reconfiguration of the DISN circuit is needed to effect the planned changes, such modifications to an IS/enclave (even if significant enough to warrant a new accreditation decision) do not need to be coordinated with the corresponding DISN Service Manager (SM). However, the planned events may have a significant impact on the IA security posture of the IS/enclave, and consequently on the risk the IS/enclave poses to the DISN community at large. Pre-coordination with the CAO is necessary to ensure the updated topologies, accreditation, and risk decision artifacts are updated and available for the connection approval decision.

Examples of high-impact events:

- Deployment of a cross domain solution (CDS)
- Deployment of a UC product enhancing the capability of the enclave (i.e., Soft Switch VoIP, VoSIP, CVVoIP,), even if the application is already accredited by the IS/enclave DAA
- Rehoming of an accredited enclave to a new DEMARC; such as moving to a new facility where a new CCSD(s) is issued by DITCO.

NOTE: The deployment to a DoD mission partner enclave of an AIS accredited by the DISA DAA for DISN/GIG Enterprise deployment generally does not trigger a requirement for pre-coordination with the CAO prior to deployment.

The following medium-impact events do not need to be pre-coordinated with the CAO prior to deployment/implementation. However, these events must be identified to the CAO no later than deployment/implementation by providing an updated network topology diagram, SIP, and SCQ as applicable.

Examples of medium-impact events:

- Deployment of new VoIP phones requiring a new VLAN segment within the enclave

- Deployment of new VTC products (on DoD UC APL)
- Changes in the IP address range assigned to the IS/enclave
- DISA transport re-homing actions that change entry points and DISN, not the partner's reaccreditation enclave where the enclave remains at the same facility.
- Upgrade of bandwidth service

4.2 Mission Partner Initiates the C&A Reaccreditation Process

DoD partners are required to use the DIACAP and to submit (at a minimum) a complete and accurate DIACAP Executive Package, which includes the following documents/artifacts.

- System Identification Profile (SIP)
- DIACAP Scorecard
- IT Security Plan of Action and Milestones (POA&M), if required
- Detailed Topology Diagram (not a DIACAP artifact, however it is required for Connection Approval)

(For instructions on how to complete these requirements, see DIACAP and the DIACAP Knowledge Service at https://diacap.iaportal.navy.mil/login.htm.)

At the completion of the C&A process, the DAA makes a reaccreditation decision. An ATO decision has a maximum validity period of 3 years, while the IATO has a maximum validity period of 180 days. In accordance with the DIACAP, consecutive IATOs shall not exceed 360 consecutive days (unless approved in writing by the DoD component CIO).

4.3 Mission Partner Updates the Connection Information

DoD mission partners are required to update the system of record registration for their Information System using the following processes.

- The NIPRNet SNAP NIPR module to update their registrations and submit their updated DIACAP executive package artifacts for unclassified connections to the DISN.
- The NIPRNet SNAP DSN module to update their registrations and submit their updated DIACAP executive package artifacts for their voice switch connections.
- The NIPRNet SNAP Waiver module to update their registrations and submit their updated briefing for ISP GIG Waiver.
- DoD mission partners will email their updated DIACAP executive package artifacts for their classified connection to the DISN.

4.4 Connection Approval Package Submission

The Mission Partner reaccreditation requests are submitted to the CAO in the form of a CAP package. This package provides the CAO the information necessary to make a connection approval decision. CAP packages should be submitted at least 30 days prior to the existing ATC or IATC date to ensure service continuity.

CAP Package document requirements are listed in the applicable appendix at the end of this document.

4.4.1 SNAP Registration Submittal Process for Unclassified Packages

CAP packages for unclassified connections will be uploaded by the partner in the SNAP registration database.

- Create SNAP profile: https://snap.dod.mil/gcap/request-account.cfm
- Upload completed DD Form 2875 (SAAR). The 2875 can be downloaded from the SNAP website.
- Complete section 13 "Justification for Access" by specifying the SNAP module and user role for your CC/SA.
- Complete your profile data, asterisked items are required fields.
- Submit the account for approval.

Once the account is approved, proceed with the creation/registration of the unclassified connection to include the submittal/upload of the DIACAP executive package artifacts once your local DIACAP C&A is completed:

- Logon to SNAP NIPR: https://snap.dod.mil/gcap/home.cfm
- Hover the mouse over "NIPR" and select "New Registration"
- Complete all sections (0-4 and 6, Section 5 is for CAO use only.) and required fields identified by an asterisks.
- Upload Attachments for your DIACAP executive package artifacts in Sections 7.1 through 7.6 as applicable. Please note: Only Sections 7.1 through 7.5 require the upload of attachments.
- Once all sections are completed, with the exception of Section 5, a submit button at the bottom of the screen will be available in order to submit the entire registration.

NOTE: For 24/7 SNAP assistance; contact the DISN Global Support Center – (800) 554-3476

4.4.2 SGS Registration and Submittal Process for Classified Packages

Partners should request read-only access to SGS to have access to their circuits. To request access, a DD 2875 to include all CCDSs they are responsible for should be sent to the Connection Approval Office. The appropriate email addresses are listed in the contact information table below.

CAP packages are normally submitted as Unclassified/For Official Use Only (FOUO). However, it is recommended that the network topology diagram be provided over SIPRNet. The partner/sponsor must determine, based on DoD component and local guidance, if any part of the CAP package contents must be labeled and handled as classified documents.

NOTE: Incomplete packages will not be accepted, and will be returned for rework.

4.4.3 CAP Package Contact Information

The CAP package submission email addresses, phone numbers, and mailing addresses are**:**

Connection Approval Office (CAO)	
Connection Approval Office for Unclassified Connections (UCAO)	disa.meade.ns.mbx.unclassified-connection-approval@mail.mil ucao@disa.smil.mil
Connection Approval Office for Classified Connections (CCAO)	disa.meade.ns.mbx.classified-connection-approval@mail.mil ccao@disa.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901
Address	Defense Information Systems Agency ATTN: NSC1 PO Box 549 Fort Meade, MD20755-0549

4.5 CAP Package Review and the Authorization to Connect Decision

Upon receipt of the CAP package, the CAO reviews the contents for completeness. In the event an incomplete package is received by the CAO, the package will be rejected and no CAO tracking number assigned. The partner will receive notification of a rejected package to include what documentation is missing from the package. Typically, when all the connection approval requirements are met an ATC or IATC will be issued within eight (8) business days.

As an integral part of the process, the CAO assesses the level of risk the partner's IS or network enclave poses to the specific DISN network/service and to the GIG community at large. The identification of IA vulnerabilities or other non-compliance issues and the responsiveness of the affected enclave in implementing appropriate remediation or mitigation measures against validated vulnerabilities will have a direct impact on the risk assessment, and subsequently on the connection approval decision.

The following are some of the indicators that would contribute to the assessment of an elevated risk:

- Missing, incomplete, or inaccurate CAP package input (because unknowns lead to a lower level of confidence in the IA status of the partner IS/enclave).
- Unsatisfactory results during remote compliance monitoring/vulnerability assessment where policy compliance is reviewed.

If the risk is "low" or "medium," the CAO will issue an ATC or IATC. A "medium" risk assessment will cause the CAO to monitor more closely the IA status of the IS/enclave during the connection life cycle. "Low" risk assessments will not affect a new connection request.

An ATC/IATC will normally authorize the partner to remain connected to the DISN network/service defined in the connection approval, up to the accreditation decision ATD. The results of the risk assessment may warrant the issuance of a connection approval decision with a validity period shorter than that of the accreditation decision ATD. In such cases, the CAO will provide justification to the DAA for the shorter validity period.

If the CAO assesses a "high" risk, it will provide the DAA the justification for the assessment and inform the DAA that current guidance (i.e., policy, DSAWG decision, STIGs, etc.) from DISN/GIG DAAs precludes the issuance of an ATC without additional review of the IS/enclave IA status by the community accreditation bodies.

4.6 Notification of Connection Approval or Denial

Once the CAO makes a connection decision, the partner is notified.

4.6.1 Connection Approval

If the reaccreditation request is approved, the partner is issued an ATC or IATC. The connection approval validity period is specified in the ATC/IATC letter. The DAA must notify the CAO of significant changes, such as architecture changes requiring re-accreditation, movement of the IS enclave to a new location, changes in risk posture, etc., that may cause a modification in the IA status of the system/enclave or if the connection is no longer needed.

4.6.2 Denial of Approval to Connect

If the reaccreditation request is denied, the CAO will provide the partner a list of corrective actions required before the connection can be approved.

SECTION 5

NON-DOD NEW CONNECTION PROCESS

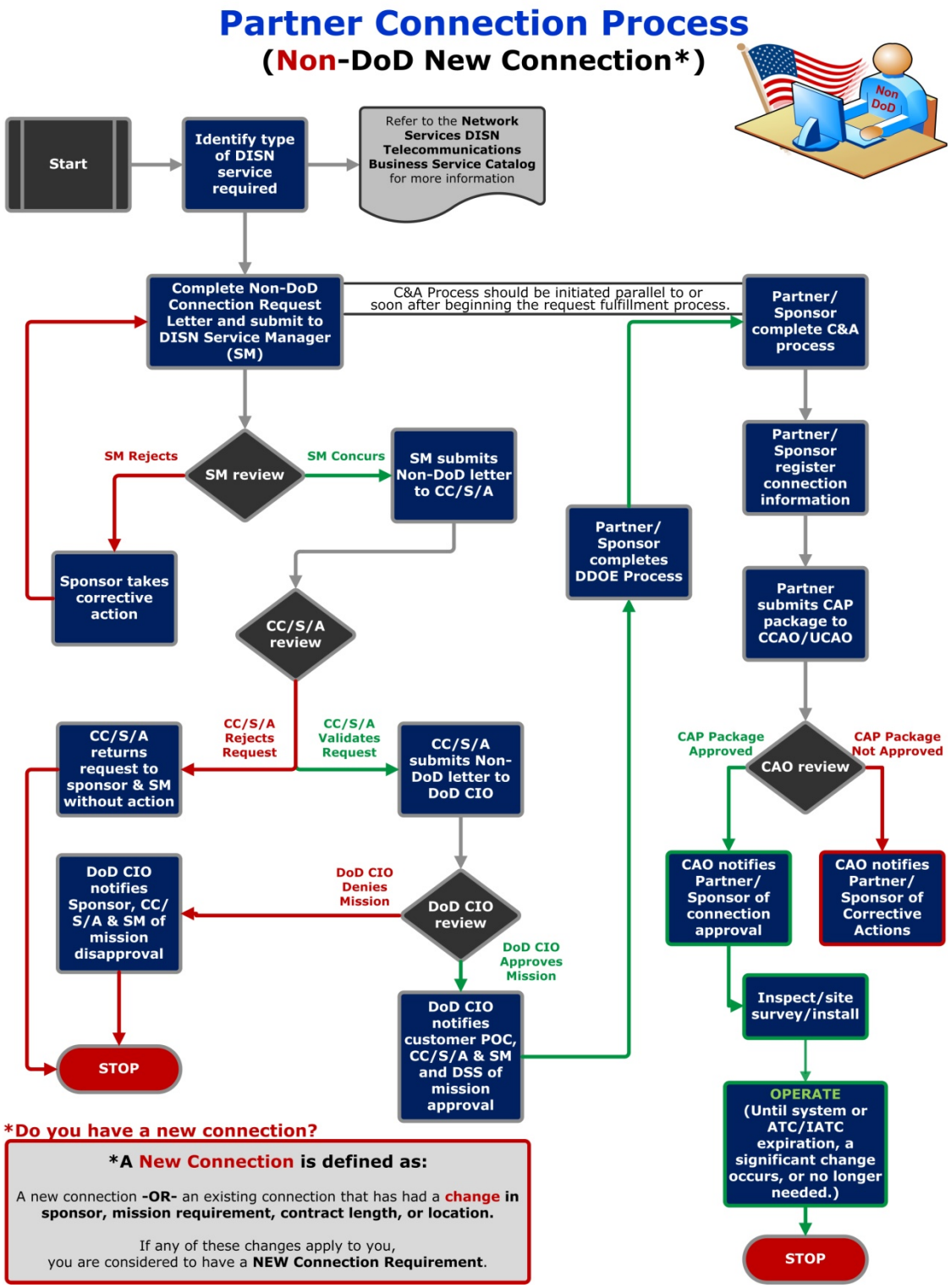


Figure 4 Non-DoD New Connection Process Flow

All Non-DoD connections require a Contract/MOA/MOU and DoD Sponsor to validate DoD mission need for partner access to the DISN. DoD Sponsors must understand and agree to their responsibilities as stated in the DoD CIO Sponsor Memorandum –*Responsibilities of DoD Components Sponsoring Mission Partner Connections to DISN-Provided Transport Infrastructure,* 11 January 2012 (ref q).

Contracts, MOA/MOU's and sponsor letters artifacts are required as part of the DISN connection approval process and are uploaded into either SNAP or SGS as applicable (outlined in 5.9.1 and 5.9.2).

NOTE: For those connections in the process of moving behind the FED/REL DMZ (Federal/Releaseable Demilitarzed Zone) that do not yet have signed and executed MOA/MOU's, the connection approval office will allow the connection based on sponsor coordination with the DoD CIO's office approval.

5.1 Identify the Type of DISN Network/Service Required

Once the partner/sponsor determines that this is a new connection requirement, the next step is to identify the DISN network/service that is required. This involves matching partner needs to the most appropriate DISN network/service. All partners desiring connections to the DISN must first confirm with the applicable SM that the desired network/service is appropriate for the mission.
Partners who are not sure which network/service best meets their needs should review the description of DISN voice, video, and data services available at https://www.disadirect.disa.mil/products/asp/welcome.asp and/or contact the DISN Global Support Center (DGSC). The DGSC will facilitate contact with the appropriate DISN SM.

DISN Global Support Center (DGSC)	
Unclassified email	DGSC@csd.disa.mil
Classified email	DGSC@cols.csd.disa.smil.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

Table 4 DISN DGSC Contact Information

Partners who know which DISN service they require will find POCs for each of the DISN networks/services in this guide's individual appendices.

Current Name	Previous Name
Transport Services	
Dedicated	N/A
Data Services	
Non-Classified IP Data	NIPRNet
Secret IP Data	SIPRNet
TS/SCI IP Data	Joint Worldwide Intelligence Communications System (JWICS)
Secret Test and Evaluation (T&E) IP	DISN LES

Current Name	Previous Name
Data	
Private IP Service	N/A
Voice Services	
CUI Voice	Voice over IP (VoIP) and/or DSN
Voice over Secure IP (VoSIP)	
TS/SCI Voice	JWICS Voice
Multilevel Secure Voice	DRSN
DISA Enterprise Classified Voice and Video over IP (CVVoIP)	N/A
Video Services	
Dial-up, Internet Protocol (IP) and Dedicated Video Teleconferencing	DISN Video Services – Global (DVS-G)
TS/SCI Videoconferencing	JWICS Videoconferencing
Messaging Services	
Organizational Messaging Service	DMS
Wireless Services	
Enhanced Mobile Satellite Services (EMSS)	N/A
Secure Mobile Environment Portable Electronic Device (SME-PED)	N/A
Satellite Services	
International Maritime Satellite (INMARSAT)	N/A
Commercial Satellite Service (CSS)	N/A

Table 5 DISN Service Names

5.2 Complete and Submit Non-DoD Connection Request Letter

The sponsor may download the Non-DoD Connection Validation Letter from the DISA Connection Library at www.disa.mil/connect/library. An example is located in Appendix A. The sponsor sends the completed letter, with an attached conceptual network topology diagram, to the appropriate SM. The purpose of the conceptual network topology diagram is to provide the SM enough information to determine if their network/service is appropriate for the partner's mission. A detailed topology diagram is required in the CAP package.

5.3 Service Manager Review

The DISN SM reviews the Non-DoD Connection Validation Letter and network topology to determine whether the proposed DISN solution is appropriate.

5.3.1 Concurs with Solution

If the SM concurs with the request, the SM will sign the letter as validator and return it to the validating CC/S/A.

5.3.2 Non-Concurs with Solution

If the SM non-concurs with the proposed solution, the request will be returned to the sponsor with comment, or routed to another SM (after notifying the sponsor) if a different network/service solution is more appropriate for the mission.

5.4 CC/S/A/ Review

The CC/S/A will review the sponsor's request letter and either validate or reject the request.

5.4.1 CC/S/A Validated Request

If the CC/S/A/ validates the request, the representative will sign the letter and submit it to the GIG Waivers/Connection Approvals office in the DOD CIO, Governance Directorate for DISN access approval (with a copy to the sponsor).

5.4.2 CC/S/A Rejected Request

If the CC/S/A POC rejects the request, it will be returned to the sponsor without action (with a copy to the appropriate SM) and the connection request process ends at this point.

5.5 DOD CIO Review

GIG Waivers/Connection Approvals office in the DOD CIO, Governance Directorate will evaluate the connection request and either approve or deny access to the DISN in support of the sponsor's mission.

5.5.1 Approved Request

If DOD CIO approves the request to access the DISN, the representative will sign and forward the request letter to the DoD sponsor (with a copy to the CC/S/A POC, DSS and DISN SM).

5.5.2 Denied Request

If DoD CIO does not approve the request, the representative will return the request letter to the DoD sponsor without action (with a copy to the CC/S/A POC and DISN SM), and the connection, as proposed, will not be allowed.

5.6 Partner/Sponsor Initiates DISA Direct Order Entry (DDOE) Process

After the appropriate network/service has been identified and applicable approvals received, the partner/sponsor initiates a request for service fulfillment through the DDOE process. This is the ordering tool for DISN telecommunications services. The DDOE website is: https://www.disadirect.disa.mil/products/asp/welcome.asp.
In the event the service request qualifies as an Emergency or Essential National Security/Emergency Preparedness (NS/EP) telecommunications service, there is an expedited process available, both for service fulfillment and for connection approval.

5.7 Partner/Sponsor Initiates the Certification and Accreditation Process

In parallel, or shortly after initiating the request for service through DDOE, the partner/sponsor should begin the C&A process for the IS/enclave for which a connection to the DISN is required.

Non-DoD partner connections to the DISN require the completion of an approved C&A process (e.g ICD 503, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, 28 February 2006, DIACAP, or other equivalent C&A process).

5.8 Mission Partner/Sponsor Registers the Connection Information

Mission partner sponsors are required to register the connection information (new or legacy) within the following applicable systems/databases (see appendix of desired network/service for details.)

Once the DDOE process has been completed with the receipt of a Command Communications Service Designator (CCSD), the Sponsor is required to register the IS information (IP address ranges, hosts, POCs, etc.) in the appropriate databases based on classification of the connection:

- Network Information Center (www.nic.mil) for all unclassified connections
- SNAP (https://snap.dod.mil) for:
  - Voice, video, data circuit registrations and connections to unclassified networks/services
  - OSD GIG Waivers for Internet Service Provider registrations (Appendix H)

or

- SIPRNet Support Center (www.ssc.smil.mil) for all classified connections
- GIAP/SGS (https://giap.disa.smil.mil) for:
  - Voice, video, and data circuit registrations and connections to classified networks/services

and

- Ports, Protocols, and Services Management (PPSM) (https://pnp.cert.smil.mil) on SIPRNet for all networks/systems ports, protocols, and services for all IP solutions or applications, including Voice over Internet Protocol (VoIP), Voice over Secure Internet Protocol (VoSIP)), and Classified Video Voice over IP (CVVoIP).

DoD policy requires that sponsors register the IS information in the DoD Information Technology Portfolio Repository (DITPR) at https://ditpr.dod.mil.
An enclave/network may also be registered in the SIPRNet IT Registry, by first requesting an account to the application at https://arm.osd.smil.mil.
Once you have an account, the link to the SIPR IT Registry is: http://osdext.osd.smil.mil/sites/dodcio/itregistry/default.aspx.

CC/S/A may have internal databases that need to be updated with connection information. Check with your CC/S/A for additional requirements.

5.9 Partner/Sponsor Connection Approval Package Submission

The Mission Partner connection requests are submitted to the CAO in the form of a CAP package. This package provides the CAO the information necessary to make a connection approval decision. CAP packages should be submitted at least 30 days prior to the desired connection date for new connections.

The following documents are minimum requirements for the CAO to analyze a CAP package (see the appropriate network/service appendix for additional requirements):

- Non-DoD Partner connections to the DISN require the completion of a C&A process. In all cases, C&A document and artifact submissions must provide IA status information equivalent to the DIACAP Executive Package.
  - DIACAP Executive Package (DIACAP Scorecard) or equivalent
  - System Identification Profile (SIP)
  - IT Security POA&M, if required
  - Detailed Topology Diagram (not a DIACAP artifact, however it is required for Connection Approval)

- DoD contractor connection to DISN:
  - For Unclassified connections, use DIACAP (the sponsoring DoD component has responsibility for all DAA actions)
  - For Classified connections, use DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 28 February 2006 (ref p) ; the Defense Security Service (DSS) has responsibility for all DAA actions; see the DSS-DISA MOA for further specifics regarding non-DoD classified connections.

- For non-DoD and non-IC federal departments and agencies:
  - For an IS not categorized as a National Security System (NSS), use National Institute of Standards and Technology (NIST) SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010 (ref r)
  - For an IS categorized as an NSS, and IAW CNSS Instruction No. 1253 Security Categorization and Control Selection for National Security Systems, October 2009 (ref o), refer to CNSSI 4009 National Information Assurance Glossary, June 2006, for the definition of an NSS.

NOTE: For other non-DoD entities, the C&A process requirements and inputs will be reviewed on a case-by-case basis. Coalition and allied mission partners will follow their established national C&A process.

- DAA Appointment Letter – must be included if there is a new DAA or if the information is not already on file in the CAO. The letter must appoint an official specifically by name, not the office to which the managerial official is assigned. If the DAA has delegated signature authority to an authorized official, written evidence of a delegation action must be provided to the CAO prior to the acceptance of any CAP package documentation.
- Consent-to-Monitor (CTM) – this is the agreement signed by the DAA granting DISA permission to monitor the connection and assess the level of compliance with IA policy and guidelines. CTM supports electronic monitoring for communications management and network security, which includes site visits, compliance inspections, and remote vulnerability assessments to check system compliance with configuration standards. It is recommended that DAAs provide blanket CTM for the type IS's (e.g., SIPRNet

CCSDs, NIPRNet CCSDs, and/or DSN voice switches) under their authority to be kept on file in the CAO.

- SIPRNet Connection Question (SCQ). The SCQ is a DISA required document that must be completed in its entirety by contractor. The SCQ requires DAA signature. DAA Signature will be obtained at the time of accreditation decision/SSP approval.
- Residual Risk memorandum template. This document must be completed and signed by the contractor.
- DoD CIO approval letter.

5.9.1 SNAP Registration Submittal Process for Unclassified Packages

CAP packages for unclassified connections will be uploaded in the SNAP registration database.

- Create SNAP profile: https://snap.dod.mil/gcap/request-account.cfm
- Upload of your completed DD Form 2875 (SAAR). The 2875 can be downloaded from the SNAP website.
- Complete section 13 "Justification for Access" by specifying the SNAP module and user role for your CC/SA.
- Complete your profile data, asterisked items are required fields
- Submit the account for approval.

Once the account is approved, proceed with the creation/registration of the unclassified connection to include the submittal/upload of the DIACAP executive package artifacts once your local DIACAP C&A is completed:

- Logon to SNAP NIPR: https://snap.dod.mil/gcap/home.cfm
- Hover the mouse over "NIPR" and select "New Registration"
- Complete all sections (0-4 and 6, Section 5 is for CAO use only.) and required fields identified by an asterisks.
- Upload Attachments for your DIACAP executive package artifacts in Sections 7.1 through 7.6 as applicable. Please note: Only Sections 7.1 through 7.5 require the upload of attachments.
- Once all sections are completed, with the exception of Section 5, a submit button at the bottom of the screen will be available in order to submit the entire registration.

NOTE: For 24/7 SNAP assistance; contact the DISN Global Support Center – (800) 554-3476

5.9.2 SGS Registration and Submittal Process for Classified Packages

Partners should request read-only access to SGS to have access to their circuits. To request access, a DD 2875 to include all CCDSs they are responsible for should be sent to the Connection Approval Office. The appropriate email addresses are listed in the contact information table below.

CAP packages are normally submitted as Unclassified/For Official Use Only (FOUO). However, it is recommended that the network topology diagram be provided over SIPRNet. The partner/sponsor must determine, based on DoD component and local guidance, if any part of the CAP package contents must be labeled and handled as classified documents.

NOTE: Incomplete packages will not be accepted, and be returned for rework.

5.9.3 CAP Package Contact Information

The CAP package submission email addresses, phone numbers, and mailing addresses are**:**

Connection Approval Office (CAO)	
Connection Approval Office for Unclassified Connections (UCAO)	disa.meade.ns.mbx.unclassified-connection-approval@mail.mil ucao@disa.smil.mil
Connection Approval Office for Classified Connections (CCAO	disa.meade.ns.mbx.classified-connection-approval@mail.mil ccao@disa.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901
Address	Defense Information Systems Agency ATTN: NSC1 PO Box 549 Fort Meade, MD20755-0549

5.10 CAP Package Review and the Authorization to Connect Decision

Upon receipt of the CAP package, the CAO reviews the contents for completeness. In the event an incomplete package is received by the CAO, the package will be rejected and no CAO tracking number assigned. The partner will receive notification of a rejected package to include what documentation is missing from the package. Typically, when all the connection approval requirements are met an ATC or IATC will be issued within eight (8) business days.

As an integral part of the process, the CAO assesses the level of risk the partner's IS or network enclave poses to the specific DISN network/service and to the GIG community at large. The identification of IA vulnerabilities or other non-compliance issues and the responsiveness of the affected enclave in implementing appropriate remediation or mitigation measures against validated vulnerabilities will have a direct impact on the risk assessment, and subsequently on the connection approval decision.

The following are some of the indicators that would contribute to the assessment of an elevated risk:

- Missing, incomplete, or inaccurate CAP package input (because unknowns lead to a lower level of confidence in the IA status of the partner IS/enclave).
- Unsatisfactory results during remote compliance monitoring/vulnerability assessment where policy compliance is reviewed.

If the risk is "low" or "medium," the CAO will issue an ATC or IATC. A "medium" risk assessment will cause the CAO to monitor more closely the IA status of the IS/enclave during the connection life cycle. "Low" risk assessments will not affect a new connection request.

An ATC/IATC will normally authorize the partner to remain connected to the DISN network/service defined in the connection approval, up to the accreditation decision ATD. The results of the risk assessment may warrant the issuance of a connection approval decision with a validity period shorter than that of the accreditation decision ATD. In such cases, the CAO will provide justification to the DAA for the shorter validity period.

If the CAO assesses a "high" risk, it will provide the DAA the justification for the assessment and inform the DAA that current guidance (i.e., policy, DSAWG decision, STIGs, etc.) from DISN/GIG DAAs precludes the issuance of an ATC without additional review of the IS/enclave IA status by the community accreditation bodies.

5.11 Notification of Connection Approval or Denial

Once the CAO makes a connection decision, the partner is notified.

5.11.1 Connection Approval

If the connection request is approved, the partner is issued an ATC or IATC. The validity period is specified in the ATC/IATC letter. After the connection is approved, the partner must work with DISN Implementation to complete the installation of the circuit. The connection approval is valid until the expiration date. The DAA must notify the CAO of significant changes, such as architecture changes requiring re-accreditation, movement of the IS enclave to a new location, changes in risk posture, etc., that may cause a modification in the IA status of the system/enclave or if the connection is no longer needed.

5.11.2 Denial of Approval to Connect

If the connection request is rejected, the CAO will provide the partner a list of corrective actions required before the connection can be approved. The process will restart at Section 5.9.

This page intentionally left blank.

SECTION 6

NON-DOD REACCREDITATION PROCESS

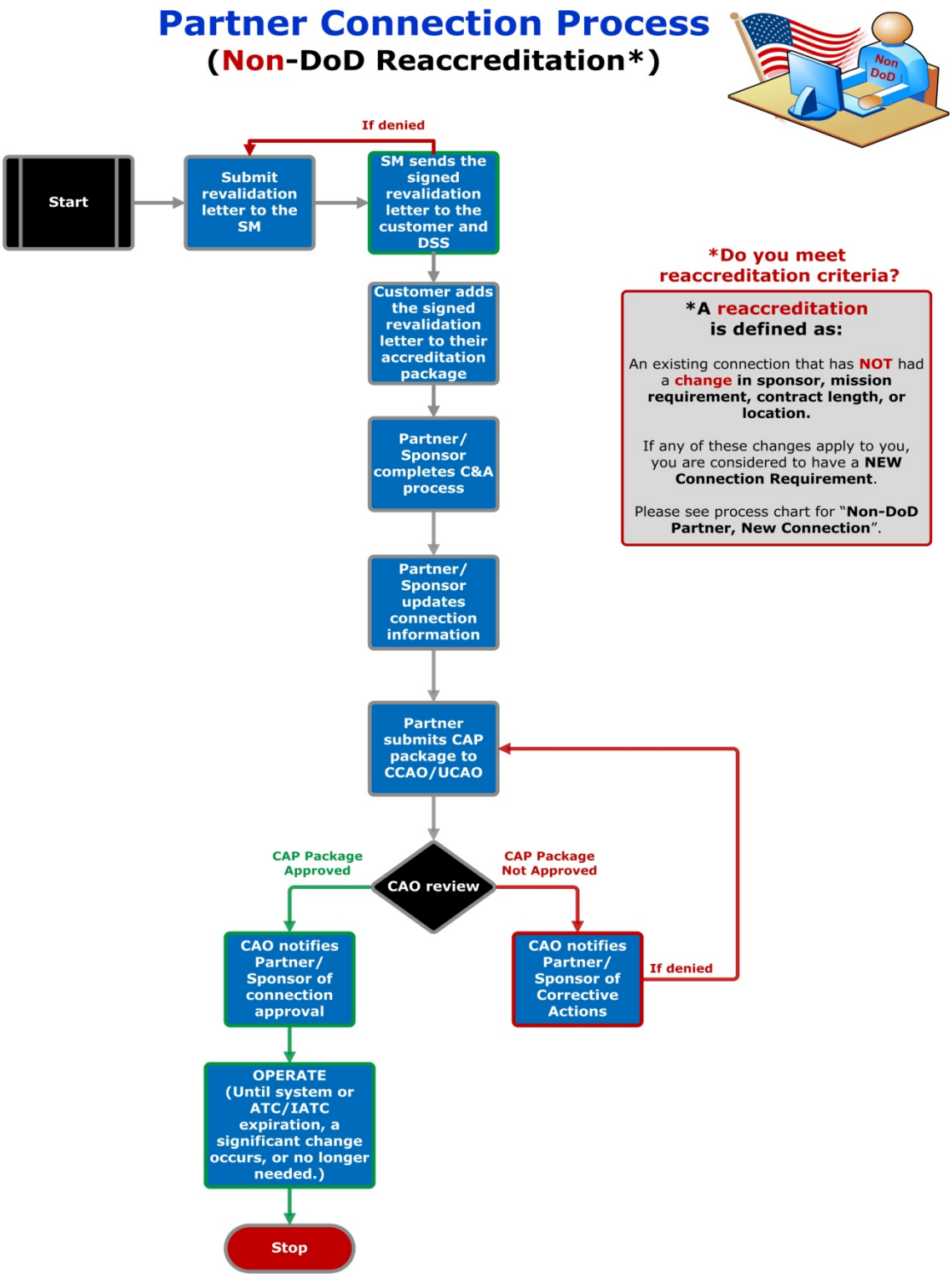


Figure 5 NoN-DOD Reaccreditation Process Flow

All Non-DoD reaccreditations require a Contract/MOA/MOU and DoD Sponsor to revalidate DoD mission need for partner access to the DISN. DoD Sponsors must understand and agree to their responsibilities as stated in the DoD CIO Sponsor Memorandum –*Responsibilities of DoD Components Sponsoring Mission Partner Connections to DISN-Provided Transport Infrastructure,* 11 January 2012 (ref q).

Contracts, MOA/MOU's and sponsor letters artifacts are required as part of the DISN connection approval process and uploaded into either SNAP or SGS as applicable (outlined in 6.4.1 and 6.4.2).

NOTE: For those connections in the process of moving behind the FED/REL DMZ (Federal/Releaseable Demilitarzed Zone) that do not yet have signed and executed MOA/MOU's, the connection approval office will allow the connection based on sponsor coordination with the DoD CIO's office approval.

6.1 Reaccreditation Connection Evaluation

If an accreditation decision is approaching its Authorization Termination Date (ATD), the DAA must reinitiate the C&A process and issue a new accreditation decision. Ideally, the new ATO/IATO will be issued and an updated CAP package forwarded to the CAO a minimum of 30-days prior to the expiration of the current ATC/IATC.

The expiration date of an ATC/IATC is usually the same as (and will never go beyond) the expiration date of the associated ATO/IATO. In some instances, the results of the CAO or DSAWG risk assessment may warrant the issuance of an ATC/IATC with a validity period shorter than that of the associated ATO/IATO. An expired ATC/IATC will prompt a review by USCYBERCOM, and may possibly result in an order to disconnect the IS/enclave from the DISN network/service.

The DAA could decide that planned changes to an IS/enclave are significant enough to warrant reinitiating the full C&A process, with subsequent issuance of a new accreditation decision inside the normal 3-year ATO (or 180-day IATO) cycle. If no physical reconfiguration of the DISN circuit is needed to effect the planned changes, such modifications to an IS/enclave (even if significant enough to warrant a new accreditation decision) do not need to be coordinated with the corresponding DISN Service Manager (SM). However, the planned events may have a significant impact on the IA status of the IS/enclave, and consequently on the risk the IS/enclave poses to the DISN community at large. Such cases prompt a requirement for the partner/sponsor to coordinate with the CAO prior to partner implementation of the change.

There may be occasions when a component may experience high impact events and pre-coordination with the CAO would be useful to expedite partner reaccreditation:

Examples of high-impact event:

- Deployment of a cross domain solution (CDS)
- Deployment of a major Automated Information System (AIS) application, even if the application is already accredited by the IS/enclave DAA

- Deployment of a UC product enhancing the capability of the enclave (i.e., Soft Switch VoIP, VoSIP, CVVoIP,), even if the application is already accredited by the IS/enclave DAA
- Rehoming of a reaccreditated enclave to a new DEMARC; such as moving to a new facility where a new CCSD(s) is issued by DITCO.

NOTE: The deployment to a partner enclave of an AIS accredited by the DISA DAA for DISN/GIG Enterprise deployment generally does not trigger a requirement for pre-coordination with the CAO prior to deployment.

Examples of medium-impact events that pose a lesser risk to the DISN are:

- Deployment of additional workstations with new hardware and new approved/accredited software
- Deployment of new VoIP phones requiring a new VLAN segment within the enclave
- Deployment of new VTC (UC APLITS approved) products
- Changes in the IP address range assigned to the IS/enclave
- DISA transport re-homing actions that change entry points and DISN, not the partner's reaccreditation enclave where the enclave remains at the same facility.
- Upgrade of bandwidth service

6.2 Partner/Sponsor Initiates the C&A Reaccreditation Process

The Mission Partner reaccreditation requests are submitted to the CAO in the form of a CAP package. This package provides the CAO the information necessary to make a connection approval decision. CAP packages should be submitted at least 30 days prior to the existing ATC/IATC expiration date.

The following documents are minimum requirements for the CAO to analyze a CAP package (see the appropriate network/service appendix for additional requirements):

- Non-DoD Partner reaccreditation to the DISN requires the completion of a C&A process. In all cases, C&A document and artifact submissions must provide IA status information equivalent to the DIACAP Executive Package.
  - DIACAP Executive Package (DIACAP Scorecard) or equivalent
  - System Identification Profile (SIP)
  - IT Security POA&M, if required
  - Detailed Topology Diagram (not a DIACAP artifact, however it is required for Connection Approval)

- DoD contractor connection to DISN:
  - For Unclassified connections, use DIACAP (the sponsoring DoD component has responsibility for all DAA actions)
  - For Classified connections, use DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 28 February 2006 (ref p) ; the Defense Security Service (DSS) has responsibility for all DAA actions; see

the DSS-DISA MOA for further specifics regarding non-DoD classified connections.

- For non-DoD and non-IC federal departments and agencies:
  - For an IS not categorized as a National Security System (NSS), use National Institute of Standards and Technology (NIST) SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010 (ref r)
  - For an IS categorized as an NSS, and IAW CNSS Instruction No. 1253 Security Categorization and Control Selection for National Security Systems, October 2009 (ref o), refer to CNSSI 4009 National Information Assurance Glossary, June 2006, for the definition of an NSS.

NOTE: For other non-DoD entities, the C&A process requirements and inputs will be reviewed on a case-by-case basis. Coalition and allied mission partners will follow an established national C&A process.
(For instructions on how to complete these requirements, see DIACAP and the DIACAP Knowledge Service at https://diacap.iaportal.navy.mil/login.htm.)

At the completion of the C&A process, the DAA makes a reaccreditation decision. An ATO decision has a maximum validity period of 3 years, while the IATO has a maximum validity period of 180 days. In accordance with the DIACAP, consecutive IATOs shall not exceed 360 consecutive days (unless approved in writing by the DoD component CIO).

6.3 Partner/Sponsor Updates the Connection Information

Non-DoD mission sponsors are required to update the system of record registration for the Information System using one of the following processes.

- The NIPRNet SNAP NIPR module to update their registrations and submit their updated DIACAP executive package artifacts for unclassified connections to the DISN.
- The NIPRNet SNAP DSN module to update their registrations and submit their updated DIACAP executive package artifacts for their voice switch connections.
- The NIPRNet SNAP Waiver module to update their registrations and submit their updated briefing for ISP GIG Waiver.
- DoD mission partner sponsors will email their updated DIACAP executive package artifacts for their classified connection to the DISN.

6.4 Connection Approval Package Submission

The Mission Partner reaccreditation requests are submitted to the CAO in the form of a CAP package. This package provides the CAO the information necessary to make a connection approval decision. CAP packages should be submitted at least 30 days prior to the existing ATC or IATC date to ensure service continuity.
CAP Package document requirements are listed in the applicable appendix at the end of this document.

6.4.1 SNAP Registration Submittal Process for Unclassified Packages

CAP packages for unclassified connections will be uploaded by the partner in the SNAP registration.

- Create SNAP profile: https://snap.dod.mil/gcap/request-account.cfm .
- Upload of your completed DD Form 2875 (SAAR). The 2875 can be downloaded from the SNAP website.
- Complete section 13 "Justification for Access" by specifying the SNAP module and user role for your CC/SA.
- Complete your profile data, asterisked items are required fields
- Submit the account for approval.

Once the account is approved, proceed with the creation/registration of the unclassified connection to include the submittal/upload of the DIACAP executive package artifacts once your local DIACAP C&A is completed:

- Logon to SNAP NIPR: https://snap.dod.mil/gcap/home.cfm
- Hover the mouse over "NIPR" and select "New Registration"
- Complete all sections (0-4 and 6, Section 5 is for CAO use only.) and required fields identified by an asterisks.
- Upload Attachments for your DIACAP executive package artifacts in Sections 7.1 through 7.6 as applicable. Please note: Only Sections 7.1 through 7.5 require the upload of attachments.
- Once all sections are completed, with the exception of Section 5, a submit button at the bottom of the screen will be available in order to submit the entire registration.

NOTE: For 24/7 SNAP assistance; contact the DISN Global Support Center – (800) 554-3476

6.4.2 SGS Registration and Submittal Process for Classified Packages

Partners should request read-only access to SGS to have access to their circuits. To request access, a DD 2875 to include all CCDSs they are responsible for should be sent to the Connection Approval Office. The appropriate email addresses are listed in the contact information table below.
CAP packages are normally submitted as Unclassified/For Official Use Only (FOUO). However, it is recommended that the network topology diagram be provided over SIPRNet. The partner/sponsor must determine, based on DoD component and local guidance, if any part of the CAP package contents must be labeled and handled as classified documents.

NOTE: Incomplete packages will not be accepted, and be returned for rework.

6.4.3 CAP Package Contact Information

The CAP package submission email addresses, phone numbers, and mailing addresses are:

Connection Approval Office (CAO)	
Connection Approval Office for Unclassified Connections (UCAO)	disa.meade.ns.mbx.unclassified-connection-approval@mail.mil ucao@disa.smil.mil
Connection Approval Office for Classified Connections (CCAO)	disa.meade.ns.mbx.classified-connection-approval@mail.mil ccao@disa.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901
Address	Defense Information Systems Agency ATTN: NSC1 PO Box 549 Fort Meade, MD20755-0549

6.5 CAP Package Review and the Authorization to Connect Decision

Upon receipt of the CAP package, the CAO reviews the contents for completeness. In the event an incomplete package is received by the CAO, the package will be rejected and no CAO tracking number assigned. The partner will receive notification of a rejected package to include what documentation is missing from the package. Typically, when all the connection approval requirements are met an ATC or IATC will be issued within eight (8) business days.

As an integral part of the process, the CAO assesses the level of risk the partner's IS or network enclave poses to the specific DISN network/service and to the GIG community at large. The identification of IA vulnerabilities or other non-compliance issues and the responsiveness of the affected enclave in implementing appropriate remediation or mitigation measures against validated vulnerabilities will have a direct impact on the risk assessment, and subsequently on the connection approval decision.

The following are some of the indicators that would contribute to the assessment of an elevated risk:

- Missing, incomplete, or inaccurate CAP package input (because unknowns lead to a lower level of confidence in the IA status of the partner IS/enclave).
- Unsatisfactory results during remote compliance monitoring/vulnerability assessment where policy compliance is reviewed.

If the risk is "low" or "medium," the CAO will issue an ATC or IATC. A "medium" risk assessment will cause the CAO to monitor more closely the IA status of the IS/enclave during the connection life cycle. "Low" risk assessments will not affect a new connection request.

An ATC/IATC will normally authorize the partner to connect to the DISN network/service defined in the connection approval, up to the accreditation decision ATD. The results of the risk assessment may warrant the issuance of a connection approval decision with a validity period shorter than that of the accreditation decision ATD. In such cases, the CAO will provide justification to the DAA for the shorter validity period.

If the CAO assesses a "high" risk, it will provide the DAA the justification for the assessment and inform the DAA that current guidance (i.e., policy, DSAWG decision, STIGs, etc.) from DISN/GIG DAAs precludes the issuance of an ATC without additional review of the IS/enclave IA status by the community accreditation bodies.

6.6 Notification of Connection Approval or Denial

Once the CAO makes a connection decision, the partner is notified.

6.6.1 Connection Approval

If the reaccreditation request is approved, the partner is issued an ATC or IATC. The connection approval validity period is specified in the ATC/IATC letter. The DAA must notify the CAO of significant changes, such as architecture changes requiring re-accreditation, movement of the IS enclave to a new location, changes in risk posture, etc., that may cause a modification in the IA status of the system/enclave or if the connection is no longer needed.

6.6.2 Denial of Approval to Connect

If the reaccreditation request is denied, the CAO will provide the partner a list of corrective actions required before the connection can be approved.

APPENDIX A

NON-DOD DISN CONNECTION VALIDATION TEMPLATE

This appendix provides the template for the Non-DoD DISN Connection Validation Letter. This is the only acceptable template for this letter. Once completed, submit the letter according to the instructions identified in Sections 3-6.

NOTE: Validation letters must be revalidated a minimum of every three years. Validation letters do not extend past the ATO date. A full validation review is required on a connection when any of the following changes/conditions occurs:

- New Sponsor
- New Contract
- Change of Location
- Change of Mission

Revalidation is initiated through the SM's office (see Appendix B).

NOTE: This is the only acceptable template for this letter.

COCOM/Service/Agency/Field Activity Letterhead

From: DoD organization sponsor Date: DoD Sponsor Letter signed

Memorandum For: DISA/NS
Appointed Validation Official (2nd Ind)
DoD CIO

SUBJECT: Non-DoD DISN Connection (Validation) for [Name of Non-DoD Entity or Contractor] located at [City, State]

1. OPERATIONAL REQUIREMENT: (Must answer all sections/questionnaires)
    a. Operational need for connection:
        1. State the DoD mission, program, or project to be supported by this connection
        2. Describe the operational relationship between the DoD sponsor and the contractor or other non-DoD entity as it pertains to the mission, program or project
        3. Describe how the contractor or other non-DoD entity tasks are performed without the connection
        4. Describe specifically how the connection will support the DoD sponsor organization and contractor or other non-DoD entity mission tasks
        5. Indicate any DoD benefit(s) derived by implementing the request as stated (include any mission-criticality and/or time-sensitivity issues)

b. Classification/Type of work to be conducted by the contractor or other non-DoD entity:
   1. Specify Classified or Unclassified and/or level, e.g. (Unclassified//for official use only (U//FOUO) – Secret and Top Secret.
   2. Specify type whether command and control, research and development, modeling and simulation, etc. (Specific to Statement of Work (SOW)/Contract)

c. Frequency of use: Describe how frequently the contractor or other non-DoD entity will be required to use this connection in support of your DoD mission, program or project.

2. MISSION PARTNERS/INFORMATION:

a. DoD Sponsor Unit:

b. DoD Sponsor: *(name/title/unclass email/classified email/phone #)*

c. DoD Security Individual: *(name/title/unclass email/classified email/phone # from the sponsoring organization that will be assuming responsibility for this circuit)*

d. Computer Network Defense Service Provider (CNDSP):

e. DoD Sponsor IA Representative for Combatant Command/Service/Agency/Field Activity (CC/S/A):

f. Non-DoD Entity/Contractor/Corporate (*no acronyms*) including the complete connection location address (*street, city, state*):

g. Cage Code (if revalidating an existing connection, include the CCSD #):

h. Funding Source: Responsible funding Source (may or may not be a DoD Sponsor):

i. If Contractor Info: Contract Number, expiration date, contracting officer name, and phone number

j. Non-DoD Security FSO:

3. CONNECTION DETAILS:

a. Connection location address (Point of Presence):

b. Applications/Databases (What application and Database Connection is required):

c. What Protocols are being utilized: (if applicable)

d. Specific IP/URL destination addresses: (if applicable)

e. Final Topology diagram and revalidation of connection/enclave:
   The topology should annotate all devices and connections in the enclave to include:
   1. Routers
   2. IA equipment (firewalls/IDS/etc.,)
   3. Servers/data storage devices/workstations/etc
   4. All connections, to include enclave entry and exit connections
   5. Security classification of environment

4. As the DoD Sponsor, I must ensure connectivity requirements are properly coordinated, periodic inspections are conducted, and adequate controls are in place in accordance with:

a. DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) dated 28 Nov 07

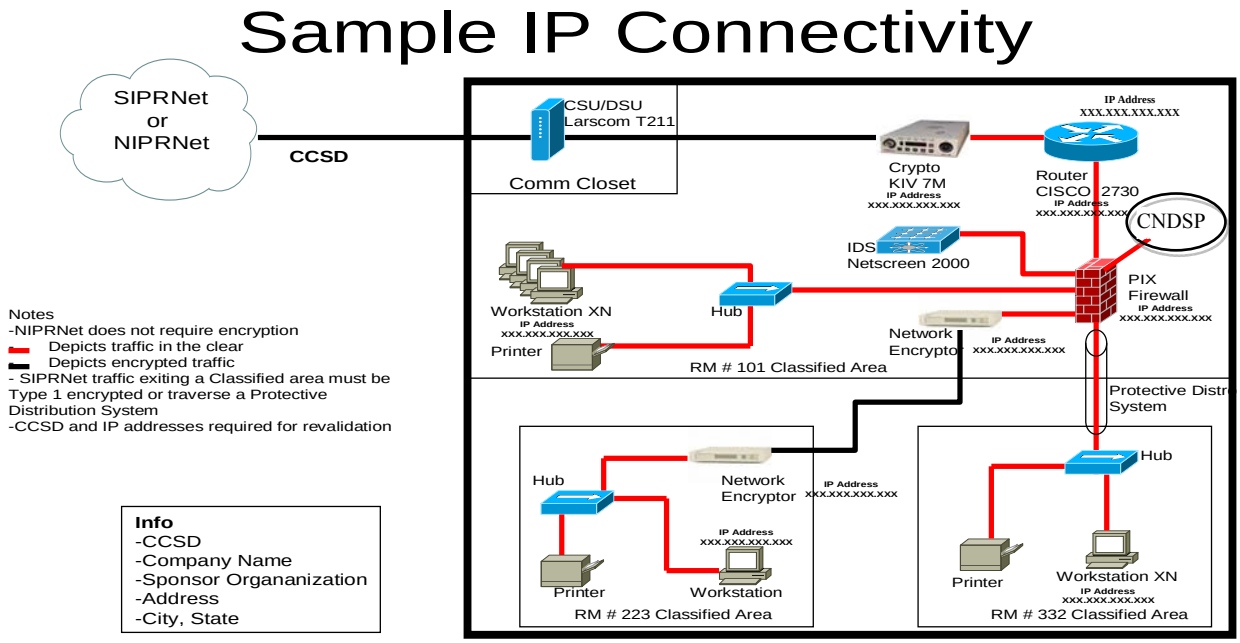
b. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DoD and contractor information systems dated 28 Feb 06

c. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 13 Aug 04
d. DoDI O-8530.2, Support to Computer Network Defense (CND)dated 9 Mar 01
e. CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities dated 24 Jan 12
f. DISN Connection Process Guide (CPG) dated September 2012
g. DoD CIO Office Sponsor Memorandum dated January 2012

Signature _____
Print Name _____
Agency _____
Title/Rank _____
(Signed by an O-6 or equivalent)

A.1 Sample of an IT Topology Diagram

ILAP Domain Configuration @ ABCDEF Systems



Identify equipment ,(e.g., LARSCOM Access T-1 XXX DSU/CSU,; CISCO WC-1DSU-T1-V2-RF; Cisco 3600 Router; Cisco IDS 4210 Sensor,Cisco 4900 Catalyst Switch) and include all IP addresses, etc.
The letter must include signature pages below. All sections in red must be filled out by the Sponsor. Signatures will be obtained within the respective offices.

1st Ind Date

We have reviewed/discussed this connection request with the partner/sponsor. Concur or non-concur.

Mark A. Williams
DISN Classified IP Lead
DISA NS111

2nd Ind (Appointed Validation Official) Date

We have reviewed the DoD Sponsor's request for [Non-DoD Entity/Contractor] to have a DISN connection. Recommend DoD CIO approve this connection.

SIGNATURE
Appointed Validation Official

APPENDIX B

NON-DOD DISN CONNECTION REVALIDATION TEMPLATE

This appendix provides the template for the Non-DoD DISN Connection Revalidation Letter. This is the only acceptable template for this letter. Once completed, submit the letter according to the instructions identified in Sections 3-6.

A revalidation review is required on a reaccreditation connection when OSD approval has expired and one of the listed changes/conditions below occurs:

- New Sponsor
- New Contract
- Change of Location
- Change of Mission

NOTE: *This is the only acceptable template for this letter

Package #_____
[provided by DISA]

COCOMs/Services/Agency's Letterhead

From: DoD organization sponsor Date: DoD Sponsor Letter sign

Memorandum For DISA/NS

SUBJECT: Non-DoD DISN Connection Revalidation for [Name of Non-DoD Agency or Contractor] located at [City, State]

1. OPERATIONAL REQUIREMENT (Must answer all sections/questionnaires):
   a. Operational need for connection:
      1. State the DoD mission, program, or project to be supported by this connection
      2. Describe the operational relationship between the DoD sponsor and the contractor or agency as it pertains to the mission, program or project
      3. Describe how the contractor or agency tasks are performed without the connection
      4. Describe specifically how the connection will support the DoD sponsor organization and contractor or agency mission tasks
      5. Indicate any DoD benefit(s) derived by implementing the request as stated (include any mission-critical and/or time-sensitivity issues

6. State whether there has been any change to the mission, contract, location, or sponsor. Any one single change will require a full evaluation through DISA to the CC/S/A CIO to DoD CIO.

[If revalidating an existing connection, do not short change this section. It must be completed in full detail]

b. Classification/Type of work to be conducted by the contractor or agency:
   1. Specify Classified or Unclassified
   2. Specify whether operations, sustainment, command and control, research and development, modeling and simulation, etc. (Specific to Statement of Work (SOW)/Contract)

c. Frequency of use: Describe how frequently the contractor or agency will be required to use this connection in support of your DoD mission, program or project.

2. MISSION PARTNERS/INFORMATION:
   a. DoD Sponsor Unit:
   b. DoD Sponsor: *(name/unclas email/classified email/phone #)*
   c. DoD Security Individual: *(name/unclas email/classified email/phone # from the sponsoring organization that will be assuming responsibility for this circuit)*
   d. Computer Network Defense Service Provider (CNDSP):
   e. Non-DoD Agency/Contractor/Corporate (*no acronyms*) including the complete connection location address (*street, city, state*):
   f. DoD Contract Name/Number/Expiration Date:
   g. Cage Code:
   h. CCSD #:

3. CONNECTION DETAILS:
   a. Complete Connection location address (Point of Presence):
   b. Applications/Databases (What application and Database Connection is required):
   c. What Protocols are being utilized (if applicable):
   d. Specific IP/URL destination addresses (if applicable):
   e. Final Topology diagram and revalidation of connection/enclave:

The topology should annotate all devices and connections in the enclave to include:
   1. Routers
   2. IA equipment (firewalls/IDS/etc.,)
   3. Servers/data storage devices/workstations/etc
   4. All connections, to include enclave entry and exit connections
   5. Security classification of environment

4. As the DoD Sponsor, I must ensure connectivity requirements are properly coordinated, periodic inspections are conducted and adequate controls are in place IAW:

   a. DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) dated 28 Nov 07

b. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DoD and contractor information systems dated 28 Feb 06
c. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 13 Aug 04
d. DoDI O-8530.2, Support to Computer Network Defense (CND)dated 9 Mar 01
e. CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities dated 24 Jan 12
f. DISN Connection Process Guide (CPG) dated September 2012
g. DoD CIO Office Sponsor Memorandum dated January 2012

Signature _____
Print Name _____
Agency _____
Title/Rank _____
(Signed by an O-6 or equivalent)

NOTE: (Page break to remain between Endorsement template below.)

Endorsement:

1. The DISA NS1 Division has reviewed the supporting documentation for this request and acknowledges SIPRNet is still the appropriate DISN solution for CCSD XXX in support of Non-DoD agency located at *City, State* to the classified DOD enclave SIPRNet through the end of the contract or end of the ATO, whichever comes first.

2. The previous DoD CIO approval will remain in effect unless one of the four following changes occurs:
   a. Sponsor
   b. Mission
   c. Location
   d. Contract

   In the event any one item changes, a full DoD CIO revalidation will be required.

3. As the DoD sponsor, I must also ensure connectivity requirements are properly coordinated, periodic inspections are conducted and adequate controls are in place IAW:

   a. DoDI 8510.01, DoD Information Certification and Accreditation Process (DIACAP) dated 28 Nov 07
   b. DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) for connections between DoD and contractor information systems dated 28 Feb 06
   c. DoDI 8551.1, Ports, Protocols, and Services Management (PPSM) dated 13 Aug 04
   d. DoDI O-8530.2, Support to Computer Network Defense (CND) dated 9 Mar 01
   e. CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities dated 24 Jan 12
   f. DISN Connection Process Guide (CPG) dated Sep 12

4. DoD policy requires that partners register their IS information in the DoD Information Technology Portfolio Repository (DITPR) at https://ditpr.dod.mil. An enclave/network may also be registered in the SIPRNet IT Registry, by first requesting an account to the application at https://arm.osd.smil.mil.

NOTE: Once you have an account, the link to the SIPR IT Registry is: http://osdext.osd.smil.mil/sites/dodcio/itregistry/default.aspx .

5. Failure to comply with the conditions of this endorsement could result in a recommendation for immediate termination of the connection.

6. For additional information contact the SIPRNet Management Office or DGSC at 1-800-554-3476.

Mark A. Williams
DISN Classified IP Lead
DISA NS111

APPENDIX C

DEFENSE RED SWITCH NETWORK (DRSN) – CLASSIFIED

This appendix provides the necessary steps and information for a Defense Red Switched Network (DRSN) connection. It is intended to supplement the detailed information provided in Section 3-6 of this guide with DRSN-specific information. Any deviations from those steps or additional requirements are identified in this appendix.

C.1 DRSN Connection Process

Defense Red Switched Network service requests must be defined, validated, coordinated, and approved through DISA SSM. Requests should be validated by the appropriate CC/S/A. These actions should be approved prior to forwarding to DISA for coordination and implementation.

Per DoDI 8100.4, connection to the DRSN requires purchase of voice equipment that is identified on the UC Approved Products List (APL). All items on the APL are required to be certified and accredited for interoperability and information assurance.
Instructions for requests for an interim certificate to operate (ICTO) can be found in the Unified Capabilities User Guide located at: https://aplits.disa.mil/ .

For information on APL approved products and the APL process for getting equipment added to that list, refer to the link: http://jitc.fhu.disa.mil/apl/drsn.html.

Follow steps in the appropriate Partner Profile Section (3-6) of this guide.

C.2 Process Deviations and/or Additional Requirements

These procedures apply to the Joint Staff, Combatant Commands (COCOMs), Services, and Defense agencies. All DRSN switch connection requests must be forwarded through the requestor's chain of command to the appropriate approval authority. Mission Partner and Defense contractor requests must be sponsored by a DoD partner and forwarded through the Joint Staff to the DOD CIO for final approval.

C.3 DRSN Connection Process Checklist

The checklist below provides the key activities that are performed by assigned organizations during the DRSN connection approval process.

Item	Connection Process	Action
1	User prepares DRSN service request IAW CJCSI 6211.02D. and submits to JS/J6	Authorized User
2	JS/J6 receives user CJCSI 6211.02D. . DRSN request	JS/J6
3	JS/J6 reviews and validates user's request	JS/J6
4	JS/J6 sends user's request to DISA/NS41 for Technical/Engineering service installation	DISA/NS41
5	DISA/NS41 conducts Technical/Engineering review at the user's sites	DISA/NS41
6	DISA/NS41 enters request into the CJCSI 6211.02D. . database record log	DISA/NS41
7	DISA/NS41 submits Technical/Engineering review results to JS/J6C	DISA/NS41
8	JS/J6 approval process occurs	JS/J6
9	DISA/NS41 updates CJCSI 6211.02D. database with results and posts to the DRSN DKO-S website	DISA/NS41
10	To obtain the DKO-S link to view request status, contact Secure Voice Services at the e-mail or phone numbers listed below. General information can be viewed on the DKO link below: https://www.us.army.mil/suite/page/547539	Authorized User

Table 6 DRSN Connection Process Checklist

C.4 Points of Contact

Secure Voice Services	
Unclassified e-mail	hostmaster@nic.mil
Phone (Commercial)	800-554-3476
Phone (DSN)	312-850-4790

C.5 Additional Policy and Guidance Documents

DoDI 4630.8	*Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004
CJCSI 6212.01E	*Interoperability and Supportability of Information Technology and National Security Systems*, 15 December 2008
CJCSI 6211.02D.	*Defense Information Systems Network (DISN): Responsibilities*, 24 January 2012
DoDI 8510.01	*DoD Information Assurance Certification and Accreditation Process*, 28 November 2007
ICD 503	*Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation*, 15 September 2008

APPENDIX D

DEFENSE SWITCH NETWORK (DSN)/UNIFIED CAPABILITIES (UC) PRODUCTS – UNCLASSIFIED

This appendix provides the necessary steps and information to process a Defense Switched Network (DSN) telecommunication switch and UC product connection to the DISN provided transport (including data, voice and video). It is intended to supplement the detailed information provided in Section 3-6 of this guide with DSN unclassified voice switch specific information. Any deviations from those steps or additional requirements are identified in this appendix.

D.1 DSN Connection Process

Follow steps in the appropriate Partner Profile Section (3-6) of this guide.

D.2 Process Deviations and/or Additional Requirements

All DSN telecommunication switches and UC Products that connect to the DISN provided transport, to include data, voice and video, must be registered in SNAP to include the upload of the DIACAP executive package artifacts in order to obtain connection approval. (Ref CJCSI 6211.02D).

Connection of a DSN telecommunication switch or UC product to the DISN requires procurement of interfacing hardware and/or software components that are identified on the DoD UC Approved Products List (APL). All items on the APL are required to be certified and accredited for interoperability and information assurance. If the intended product is not on the APL, it will either need to be JITC IO and IA tested and certified and placed on the APL, or authorized for purchase via DoD Chief Information Officer (ASD DCIO) policy waiver before the product can be purchased and connected to the DISN Ref. DoDI 8100.4.

For information on APL products and the APL process for getting equipment added to that list, refer to the links below:

- DSN/DoD UC APL pages: https://aplits.disa.mil/processAPList.do
- UC Testing and Certification: http://www.disa.mil/ucco/index.html
- DSN Services and Capabilities: http://www.disa.mil/dsn/index.html

Criteria for determining connection approval requirement of an UC APL approved DSN telecommunication switch and/or UC product connected to the DISN:

- Voice soft switches connected to the DISN shall be registered in SNAP DSN and obtain connection approval. (i.e., LSC, MFSS, WANSS)

NOTE: IAW Department of Defense (DoD) Unified Capabilities Master Plan (UC MP); Section 5.d.(1)(h) and (i); Pg. 28,29NOTE: IAW Department of Defense (DoD) Unified Capabilities Master Plan (UC MP); Section 5.d.(1)(h) and (i); Pg. 28,29

(h) Circuit switched based services shall begin migrating to IP-based non-assured/assured services over DoD Component ASLANs/Intranets and UC transport using products from the DoD UC APL (except DRSN, which is discussed in paragraph 5.f). During this implementation timeframe, both converged and non-converged UC shall be provided by TDM/IP hybrid technologies. The VoSIP, DVS, STEP/Teleport, and deployable programs shall upgrade respective infrastructures using products from the DoD UC APL. The phase out of circuit switched technologies shall be based on the following individual conditions:

1. New Circuit Switched Products. New circuit switched products shall no longer be tested and certified for placement on the UC APL as of January 2011.

2. Existing UC APL Circuit Switched Products. Existing circuit switched products on the UC APL may be purchased until certification expires and removed from the APL.

3. Installed UC Circuit Switched Products. Existing circuit switched products already installed, UC APL products procured before the UC APL expiration date, or on the Retired UC APL List may remain until business case or mission need dictates replacement, or vendor is no longer willing to support. Continued testing and certification for software patches is allowed for these components while in use, however this testing and certification shall not result in renewed UC APL status.

(i) During this period, DISA shall deploy MFSSs and WAN SSs, allowing DoD Components to implement UC employing IP while maintaining backward interoperability with the remaining circuit-switch/TDM technologies. DISA's enterprise voice and video services, with collaboration capabilities (IM, presence, and chat), shall be evaluated during UC Pilot Spiral 2 and shall begin operations in select geographic regions during this timeframe.

- VoIP capable soft switches that are configured to function as a PBX1 and connected behind the local user's installation DSN EO/SMEO do not require a SNAP registration or connection approval; unless, directed as a MAJCOM, COCOM or Theater Command requirement. The PBX1 voice switch shall be identified on the partner's host installation enclave topology for the associated DSN EO/SMEO voice switch DIACAP.
- All TDM/DSN voice switches connected to the DSN as a servicing voice switch (Ref 6211.02D) will be registered in SNAP DSN and obtain connection approval
- ALL b/p/c/s TDM/DSN voice switches connected behind the local user's installation DSN EO/SMEO do not require a SNAP registration or connection approval; unless; directed as a MAJCOM, COCOM or Theater Command requirement (e.g., PBX1, PBX2, NE(SHOUTS), RSU). These type of switches will be identified and depict the interconnection to the host installation DSN EO/SMEO in the enclave topology diagram.
- ALL b/p/c/s TDM/DSN voice switches that connect via a TANDEM/NODAL connection to the MFS will be registered in SNAP and obtain a waiver to policy or have a completed Tailored ISP for connection approval (e.g., PBX1, NE-SHOUTS, SMU, IMUX).

- New/additional TDM trunk connections to a operational legacy DSN switch for growth requirements will be allowed, but the legacy switch must be registered in SNAP and obtain connection approval, if they have not previously obtained formal connection approval.
- Partner's requesting connection approval for a legacy switch that has fallen off the UC End of Sale list are required to register the voice switch in SNAP DSN and obtain a waiver to policy.
- Partner's that procure a leagacy voice switch that is on the UC APL End of Sale list are required to register the voice switch in SNAP DSN and obtain a waiver to policy.
- PBX2 switches can only be procured or implemented after being granted a waiver for MUF requirements by the Joint Staff.

D.3 DSN Connection Process Checklist

This checklist provides the key activities that must be performed by the Partner/sponsor during the DSN connection approval process.

Item	DoD Partner		Non-DoD Partner	
	New	Existing	New	Existing
Obtain OSD approval for Non-DoD connection			√	√[1]
Obtain APL approval for voice equipment not currently on the APL list	√		√	
Provision the connection	√		√	√[1]
Perform the C&A process	√	√	√	√
Obtain an accreditation decision (ATO/IATO)	√	√	√	√
Register the connection	√	√[2]	√	√[1]
Register in the SNAP database	√	√[2]	√	√[1]
Register in the PPSM database	√	√[2]	√	√[1]
Register in the DITPR database	√	√[2]	√	√[1]
Complete the CAP Package	√	√	√	√
DIACAP Executive Package (or equivalent)	√	√	√	√
DIACAP Scorecard	√	√	√	√
System Identification Profile (include switching equipment—i.e., vendor model and software)	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√
DAA Appointment current in database	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
Proof of Contract			√	√
ASK DCIO Approval Letter			√	√
Complete ATC Submittal form (see 1.4)	√	√	√	√
Submit the CAP Package to the CAO	√	√	√	√
Receive DSN ATC/IATC	√	√	√	√

Table 7 DSN Connection Process Checklist

[1] This step is not required for existing Non-DoD Partner connections unless there has been a change in Sponsor, mission requirement, contract, or location, or the connection has not been registered.
[2] This step is not required for existing connections that are already registered and where all information is current.

D.4 Points of Contact

Unified Capabilities Certification Office (UCCO)	
Unclassified e-mail	disa.meade.ns.list.unified-capabilities-certification-office@mail.mil

Connection Approval Office (CAO)	
Connection Approval Office for Unclassified Connections (UCAO)	disa.meade.ns.mbx.unclassified-connection-approval@mail.mil ucao@disa.smil.mil
Connection Approval Office for Classified Connections (CCAO)	disa.meade.ns.mbx.classified-connection-approval@mail.mil ccao@disa.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901
Address	Defense Information Systems Agency ATTN: NSC1 PO Box 549 Fort Meade, MD20755-0549

DISN Global Support Center (DGSC)	
Unclassified email	DGSC@csd.disa.mil
Classified email	DGSC@cols.csd.disa.smil.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

D.5 Additional Policy and Guidance Documents

Policy	Name
DoDI 8100.4	*Department of Defense Instruction (DoDI) DoD Unified Capabilities (UC)*, 9 December 2010

D.6 Topology Diagram Requirements

Network Topology Diagram – this diagram depicts the network topology and security posture of the partner IS or network enclave that will be connecting to the DISN. The Network Topology Diagram should:

- Be dated
- Clearly delineate accreditation boundaries
- Identify the CCSDs of all connections to the DISN
- Identify equipment inventory (to include the most recent configuration including any enclave boundary firewalls, Intrusion Detection Systems (IDS), premise router, routers, switches, backside connections, Internet Protocol (IP) addresses, encryption devices, Cross Domain Solutions (CDS).
- Other SIPRNet connections (access points) must be shown; the flow of information to, from, and through all connections, host IP addresses, and CCSD number, if known must be shown.
- Identify any other IA or IA-enabled products deployed in the enclave
- Identify any connections to other systems/networks
- Identification of other connected IS/enclaves must include:
  - The name of the organization that owns the IS/enclave
  - The connection type (e.g., wireless, dedicated point-to-point, etc.)
  - IP addresses for all devices within the enclave
  - The organization type (e.g., DoD, federal agency, contractor, etc.)
- Identify Internetworking Operating System (IOS) version
- Include the model number(s) and IP's of the devices on the diagram; diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections)

NOTE: It is important to note that in accordance with DoD and DISA guidance, firewalls, IDSs and Wireless-IDSs (where applicable) are required on all partner enclaves. Private IP addresses (non-routable) are not permitted on SIPRNet enclaves. Indicate and label all of the devices, features, or information; minimum diagram size: 8.5" x 11

All TDM/IP DSN topologies must include:

- Topology date
- Function, vendor, model, and software version of the voice switch (preferably near the voice switch)
- All CPE or Terminating type equipment used behind the voice switch (Analog, Digital, VoIP, VTC, etc..)
- The function and location of the DSN source switch providing connection to the DSN backbone (preferably near the DSN cloud)
- Trunk type used for DSN connection (i.e., T1/E1 PRI, T1/E1 CAS, ISDN, etc..)
- VTC and Network Elements (NE) as applicable

Addendum for voice switches connecting to ASLAN or ASVLAN:

- Depict vendor, model and IP address of all Media Gateway (MG) routers used for Ethernet/IP connection
- Depict NIPRnet CCSD(s) providing the Ethernet/IP connection within the enclave (preferably near the ASLAN cloud or CER)

Addendum for voice Soft Switch connections to the DISN:

- Depict the function and location of the source soft switch providing connection to the DISN backbone (preferably near the DISN cloud)
- Depict function, vendor, model, soft ware version and IP address of all Edge Boundary Controllers (EBC)
- Depict NIPRnet CCSD(s) providing the Ethernet/IP connection within the enclave (preferably near the CER)

D.7 SNAP DSN switch registration and DIACAP submittal process:

- Create SNAP DSN profile: https://snap.dod.mil/gcap/request-account.cfm
- Upload of your completed DD Form 2875 (SAAR). The 2875 can be downloaded from the SNAP website.
- Complete your profile data, asterisked items are required fields
- Submit the account for approval

Once the account is approved, proceed with the creation/registration of the voice switch to include the submittal/upload of the DIACAP executive package artifacts once your local DIACAP C&A is completed:

- Logon to SNAP DSN: https://snap.dod.mil/gcap/home.cfm
- Hover the mouse over :Defense Switched Network" and select "New Registration"
- Complete all sections (e.g., Sections 0-10) and required fields identified by an asterisks
- Upload Attachments for your DIACAP executive package artifacts in Section 11.1 through 11.12.

NOTE: Only Sections 11.1 through 11.5 require the upload of the respective attachment; thus, Sections 11.6 through 11.12 do not require attachment upload of document(s) in order to complete the registration.

- Once all sections are completed, with the exception of Section 10 and Section 11.12; A Submit button at the bottom of the screen will be available in order to submit the entire registration for "Validator Approval".

SNAP DSN Validator Role

- The SNAP DSN validator reviews the contents of all submitted connection requests within his or her agency or subagency and either approves or rejects the registration based on conformity, completeness, and correctness.
- If the validator rejects a request, the reason is captured in the comment and the POC's identified in the registration are notified via an automated email. The requestor or one of the POC's in the registration must update and complete the rejected sections and resubmit the registration.

Once all individual applicable sections of the registration are approved, the validator may "Validate Approve" the entire registration for the next step of the approval process, CAO review. The validator may also reject the request even though all sections of the request are approved.

NOTE: For 24/7 SNAP assistance; contact the DISN Global Support Center – (800) 554-3476

D.8 Sample Topology Diagrams (with and without VOIP)

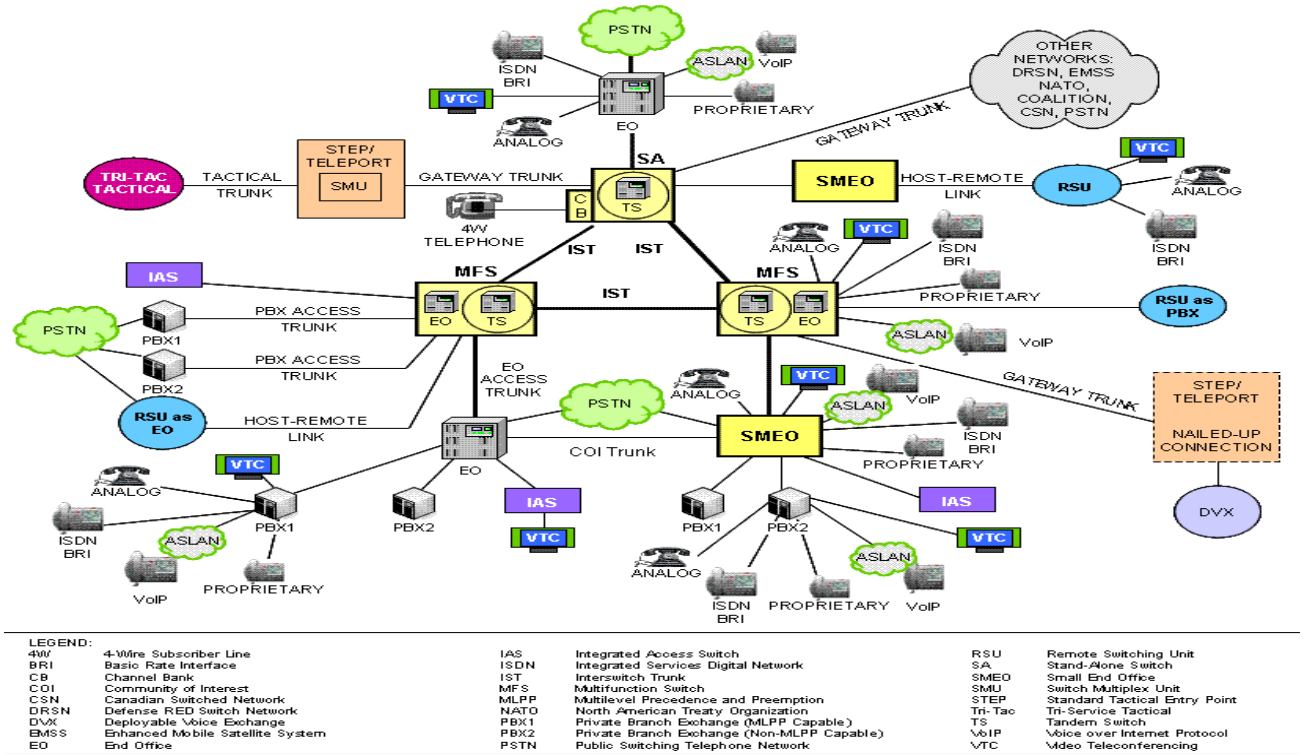


Figure 6 Sample DSN Topology with and without VOIP

D.9 Example Installation Configurations

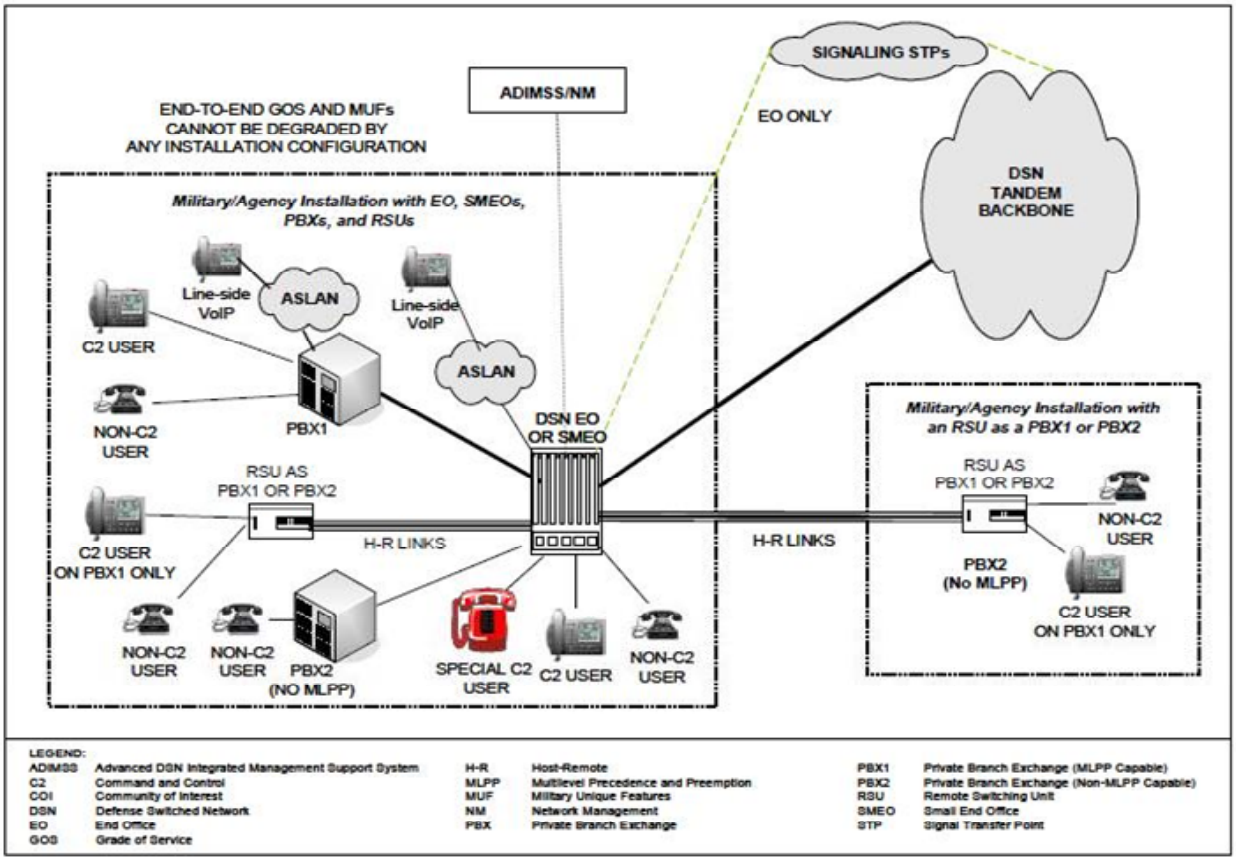


Figure 7 Example Installation Configurations

APPENDIX E

DISN TEST AND EVALUATION (T&E) NETWORK (DTEN) VPN REGISTRATION

E.1 DTEN VPN Service Description

The DTEN is hosted as a Layer 3 VPN (L3VPN) across the DISN Internet Protocol (IP) core, providing IP transport only service for test and evaluation (T&E) and test and development (T&D) Communities of Interest (COIs). VPN solutions isolate COIs as separate enclaves and segregate test traffic from the operational network using Multi Protocol Label Switching (MPLS), VPN tunnels, network encryption, approved Type I encryption devices, and/or other approved solutions as needed. The DTEN is included in the DISN Computer Network Defense Service Provider (CNDSP) environment. For COIs co-located at a DISN Point of Presence (POP), the DISN CNDSP monitoring extends to the DTEN network boundary demarcation but does not extend beyond the COI network interface.

E.2 DTEN Connection Process

DTEN VPN registration is accomplished using SIPRNet GIG Interconnection Approval Process (GIAP) System (SGS) Pilot, URL https://giap.disa.smil.mil/gcap. An account is required, requested by submitting a DoD Form 2875 via the web site. The Community of Interest (COI) Office of Primary Responsibility (OPR) registers the COI and provides updates via the SGS Pilot.

E.3 DTEN COI Registration and Documentation

- COI OPR completes SGS fields as described in Table E-1.
- Entries marked M are mandatory, O are optional.

DTEN PTC Documentation SGS Entries	DISA Enclave Security Technical Implementation Guide (STIG)*			Coalition or Other
Section Questions	Zone A	Zone B	Zone C	VPN
Connection type, Enclave Zone	M	M	M	M
New Connection, Yes or No	M	M	M	M
CC/S/A, Select Agency & Sub-agency	M	M	M	M
Network Internet Protocol (IP) address, enter the encryption device or partner edge router IP address	M	M	M	M
Premise IP Address, enter the DTEN-AR IP address	M	M	M	M
POC for DAA is Kenneth Krause (DTEN-IAM), 618-220-9806, DSN 312-770-9806, email Kenneth.Krause.ctr@disa.mil, SIPRNet Kenneth.Krause.ctr@disa.smil.mil.	M	M	M	M
POC CC/S/A, and Alternates are the COI OPR ISSM, Network POC, NSO, etc	M	M	M	M

General Questions	Zone A	Zone B	Zone C	VPN
Command Communications Service Designator (CCSD)	M	M	M	M
Site Name for the COI interface with the DTEN-AR	M	M	M	M
Accreditation Status of highest enclave	M	M	M	M
Date Accreditation (ATO/IATO/IATT) Granted	O	O	O	O
Date Accreditation (ATO/IATO/IATT) Expires	O	O	O	O

Table 8 DTEN PTC Documentation - SGS Series

* http://iase.disa.mil/stigs/net_perimeter/enclave_dmzs/enclave.html

- COI OPR uploads the documentation described in Table E-2 below

DTEN PTC Documentation	DISA Enclave Security Technical Implementation Guide (STIG)*			Coalition or Other
Required Documentation to be uploaded to SGS	Zone A	Zone B	Zone C	VPN
Network/Enclave Topology Diagram	M	M	M	M
Consent to Monitor	M	M	M	M
ATO, IATO, IATT, or Multinational Security Accreditation Board (MSAB) Certification	M	M	M	M
Security Memorandum, POA&M or similar CJCSI 6510 MOA	M	M	M	M
Permission to Connect (PTC) Will be approved by DISA/NSC after verification by the DTEN Service Managers Office.				

E.4 Points of Contact

DTEN Service Manager, DISA/NS, General, PTC Process	
Debra Jackson	debra.d.jackson.civ@mail.mil
Phone (Commercial)	301-225-2463
Phone (DSN)	312-375-2463

DTEN Service Manager – Technical, Required documents	
Anthony Destefano	anthony.l.destefano.ctr@mail.mil
Phone (Commercial)	301-225-2415
Phone (DSN)	312-375-2415

DISA/NSC , SGS Pilot management, training, and questions	
Unclassified e-mail	disa.meade.ns.mbx.unclassified-connection-approval@mail.mil
Classified e-mail	ccao@disa.smil.mil
Phone (Commercial)	301-225-2522
Phone (DSN)	312-375-2522

E.5 DTEN VPN Registration and PTC Process Diagram

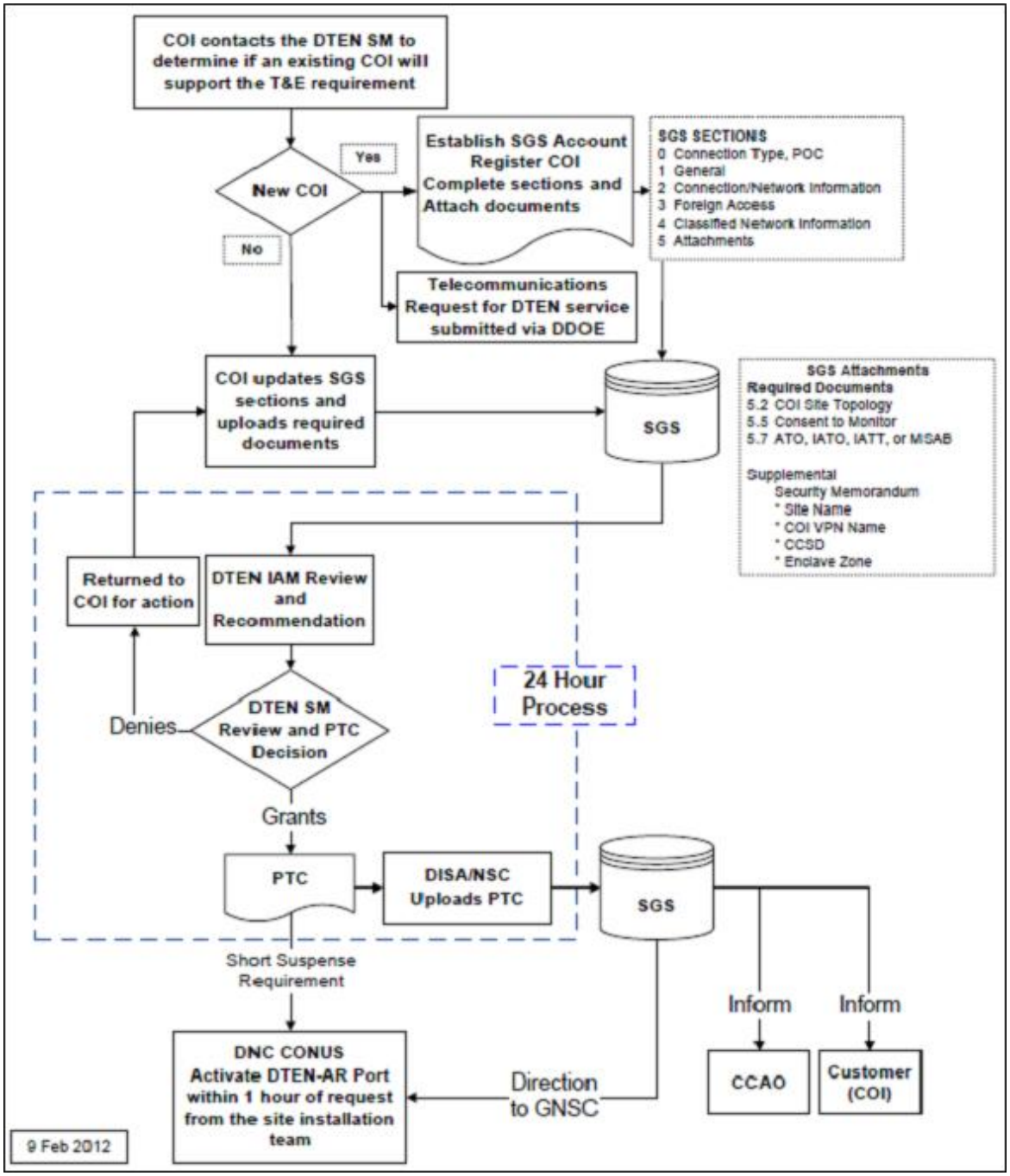


Figure 8 DTEN VPN Registration and PTC Process

APPENDIX F

DISN VIDEO SERVICES (DVS) – CLASSIFIED AND UNCLASSIFIED

This appendix provides the necessary steps and information for a DISN Video Services (DVS) connection.

F.1 DVS Connection Process

To obtain DVS service, the partner/sponsor must have an existing commercial Integrated Services Digital Network (ISDN) service and/or order a DISN transmission path (DSN, Commercial, Federal Telecommunications Service (FTS), or SIPRNET. Information on ordering each of these services is provided in the service's appendix to this guide. Once the transmission path is obtained and corresponding ATC/IATC is granted, the partner/sponsor can then proceed with ordering the DVS service. When the partner adds UC products (for example, VTC Components), the partner is required to follow DoDI 8100.04. Thus, the fielding of the UC product would require a new or updated DAA accreditation decision for the subject enclave.

NOTE: Excerpt from DoDI 8100.04, Enclosure 3, page 17, Section 4(3):
"(3) The UCCO shall place UC products certified for both interoperability and IA on the UC APL. The UC APL is the single authoritative source for certified UC products intended for use on DoD networks. The DoD Components are required to acquire or operate only UC products listed on the UC APL, unless, and until, a waiver is approved. The DoD Components shall issue a new or update an existing accreditation decision when UC products are installed, pursuant to Reference (n). This new or updated accreditation decision may result in an authorization to operate (ATO), interim authorization to operate (IATO), or interim authorization to test (IATT). DISA shall provide connection approval to the DISN (i.e., approval to connect (ATC) or interim approval to connect (IATC)). When installed and connected, UC products shall be operated and maintained pursuant to DISA STIGs and the JITC interoperability certified configuration."

F.2 Process Deviations and/or Additional Requirements

To access the DISN Video Services network bridges you must become a subscriber. Please note, however, that due to the limited number of Integrated Services Digital Network (ISDN) resources currently available to existing DVS-G users, DISA NS24 (the DVS Program Management Office [PMO]) has determined that **new ISDN subscribers will be determined on a strict case-by-case basis** and, in most cases, will only be authorized using a "one-in, one-out" policy whereby the DVS business office will have to identify an existing site to be removed for every new subscriber proposed. For example, a prospective EUCOM site requesting ISDN service might be approved if another EUCOM site is discontinuing its service.

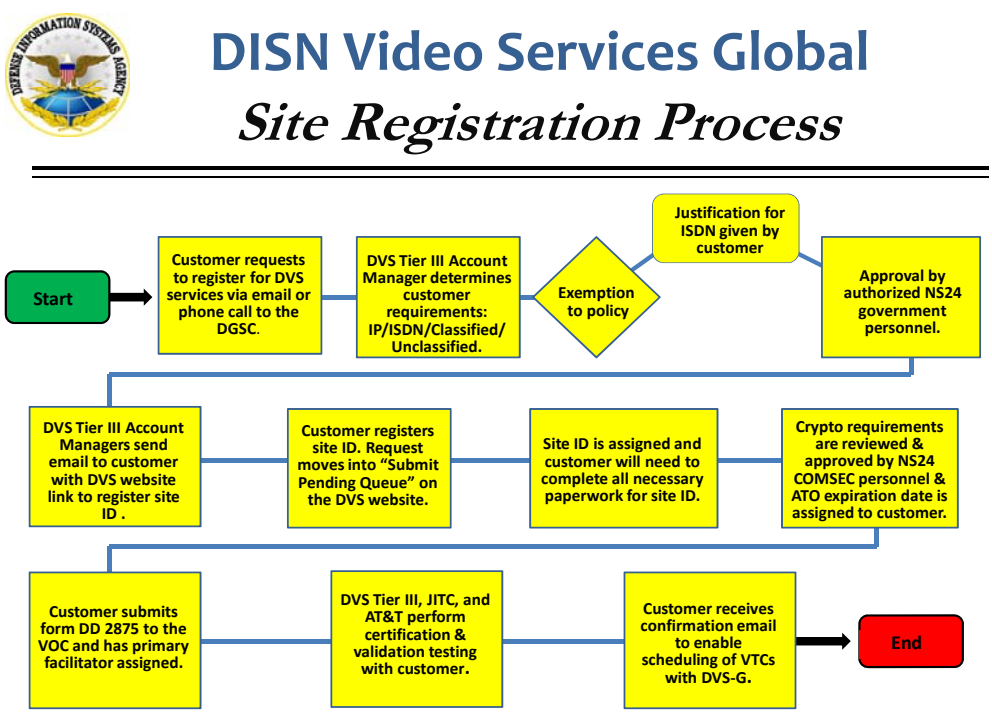


Figure 9 DVS-G Registration Process

F.3 DVS Connection Process Checklist

Item	DoD Partner		Non-DoD Partner	
	New	Existing	New	Existing
Obtain OSD approval for non-DoD connection			√	
Register the connection	√	√	√	√
Register in the DISN Video Services – Web Site (DVS-WS) database http://www.disa.mil/Services/Network-Services/Video/DVS-G/Becoming-a-Customer	√	√	√	√
Complete the CAP package ISDN/SIPR IP (Classified: up to and including SECRET)	√	√	√	√
Authorization to Operate	√	√	√	√
Topology Diagram	√	√	√	√
Copy of Transport (DSN) ATC	√	√	√	√
DAA Appointment Letter (If DAA is not SES or GO)	√	√	√	√
SIPR CCSD & Network topology	√	√	√	√
Complete the CAP package (Unclassified ISDN sites)	√	√	√	√

Item	DoD Partner		Non-DoD Partner	
	New	Existing	New	Existing
Authority To Connect Request	√	√	√	√
Topology diagram	√	√	√	√
Designate primary facilitation	√	√	√	√
Complete DD Form 2875	√	√	√	√
Complete JITC verification	√	√	√	√
Complete AT&T validation	√	√	√	√

Table 9 DVS Checklist

F.3.1 Complete Initial Registration with Business Development

- Requesting an ISDN Site Id will require an exemption to policy statement submitted to DVSTIERIII@disa.mil.
- Business Development (BD) answers all questions, acts as primary POC to the partner through the registration process, and refers them to the DVS-WS website http://www.disa.mil/Services/Network-Services/Video/DVS-G/Becoming-a-Customer to complete all required documents.
- Upon online registration, partner provides required information; BD will assist the partner in completing this process as necessary.
- BD then reviews the completed Site Profile, assigns a Site ID and "Submits pending site" via DVS-WS.
- After the site ID is assigned, BD tracks the process using DVS-WS "New Site Registration Queue".

F.3.2 Submit CAP Documents to (COMSEC) Manager

- Classified ISDN (up to and including SECRET) Sites: The partner completes an ATO with DAA signatures and submits them with a room configuration drawing and a copy of the transport (DSN) ATC to the DVS COMSEC Manager for approval. Classified partners should allow 4-6 weeks to receive the traditional COMSEC Keymat from the National Security Agency (NSA). Electronic Keymat is received via EKMS in 1-2 days. Contact the CAO to register new transports.
- SIPR IP requires sites submit a network configuration drawing with the Site ID and SIPR CCSD. The drawing is received, reviewed and SIPR CCSD is verified in SGS. If the CCSD is valid, then ATO expiration date assigned is based on the ATC expiration date of the SIPR CCSD.
- Unclassified Sites: The partner submits ATC-R request with DAA signature (or the signature of a DAA designee) and submits it with a room configuration drawing to the DVS COMSEC Manager. Contact the CAO to register new transports.

NOTE: The ATC-R request can be located at: http://www.disa.mil/Services/Network-Services/Video/DVS-G. Select "Becoming a Customer"; Go to Step 2: Select/Download the Authority to Connect Reuest (MS Word) form.

- COMSEC Manager reviews/approves all documents.

NOTE: If the connection is Classified, the COMSEC Manager orders the KEYMAT and checks the "Crypto approved" column in DVS-WS Site Registration Queue.

F.3.3 Business Development Site Information Review

- Reviews Site Profile information for any changes made since initial registration
- After the review is completed, BD checks the "BD Approved" column in the DVS-WS New Site Registration Queue.
- If it is a SIPR IP, the site contacts Tier III for IP pre test.

F.3.4 Designate Primary Facilitator with the Video Operations Center (VOC)

- The partner completes and submits a signed System Authorization Access Request (DD Form 2875) to the VOC designating a Primary Facilitator for the site (see POC information in F.4)
- VOC processes DD Form 2875 and checks the "PF Assigned" column in DVS-WS New Site Registration Queue

NOTE: An automated DVS-WS generated email is subsequently sent to the partners advising them to contact JITC to schedule Verification Test.

F.3.5 Complete JITC Site Profile and Equipment/Facility Verification

- JITC verifies the partner's site profile information and tests their equipment capabilities and room functionality. Classified partners must have already received an Over The Air Rekey (OTAR) from the VOC before performing the verification test
- Upon successful completion, JITC checks the "JITC Approved" column in the DVS-WS New Site Registration Queue

NOTE: An automated DVS-WS generated email is subsequently sent to partners advising them to contact AT&T to schedule a Validation Test.

F.3.6 Complete AT&T Validation

- AT&T validates partners can connect to DVS-G as indicated on their site profile
- Upon successful completion, AT&T checks "AT&T Approved" column in the DVS-WS New Site Registration Queue

NOTE: An automated DVS-WS generated email is subsequently sent to partners advising them that the process is completed and that they can now schedule VTCs on DVS-G.

F.4 Points of Contact

DVS Connection Process POCs CONUS (Continental United States), DISA NS24	
Unclassified Email	dgsc@csd.disa.mil
Phone (Commercial)	800-554-DISN (3476)
Phone (DSN)	312-850-4790
Fax (Commercial)	703-681-3826
Fax (DSN)	312-761-3826

DVS Connection Process POCs Europe, DISA EU52	
Unclassified Email	vtcopseur@disa.mil
Phone (Commercial)	011-49-711-68639-5260/5840/5445
Phone (DSN)	314-434-5260/5840/5445
Fax (Commercial)	011-49-711-68639-5312
Fax (DSN)	314-434-5312

DVS Connection Process POCs Pacific, DISA PC54	
Unclassified Email	vtcopspac@disa.mil
Phone (Commercial)	808-472-0223
Phone (DSN)	315-472-0223
Fax (Commercial)	808-656-3838
Fax (DSN)	315-456-3838

DVS Connection Process POCs Southwest Asia (SWA), DISA NS5	
Unclassified Email	DVSTierIII@disa.mil
Phone (Commercial)	800-554-DISN(3476),614-692-479090
Phone (DSN)	312-850-4790
Fax (Commercial)	703-681-3826
Fax (DSN)	312-761-3826

DVS Connection Process POCs DVS COMSEC Manager	
Unclassified Email	DVSTierIII@disa.mil
Phone (Commercial)	800-554-DISN(3476),614-692-4790
Phone (DSN)	312-850-4790
Fax (Commercial)	703-681-3826

FSO POC for Circuit and CNDSP Inquiries	
Contact Name	Robert Mawhinney, Chief CNDSP & Planning Branch
Unclassified Email	robert.j.mawhinney.civ@mail.mil
Phone (Commercial)	717-267-9715
Phone (DSN)	312-570-9715

Designate Primary Facilitator with the VOC	
Unclassified Email	VOC@disa.mil
Phone (Commercial)	618-220- 9921
Phone (DSN)	312-770-9921
Fax (DSN)	312-770-8688
Fax (Commercial)	618-220-8688

AT&T Validation Test	
Phone (Commercial)	800-367-8722
Phone (DSN)	312-533-3000

JITC Certification Test	
Phone (DSN)	312-821-9332/9333
Phone (Commercial)	520-533-9332/9333

DISN Global Support Center (DGSC)	
Unclassified Email	dgsc@csd.disa.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

F.5 Additional Policy and Guidance Documents

DVS website: http://www.disa.mil/Services/Network-Services/Video/DVS-G/Becoming-a-Customer.

F.6 Topology Diagram Requirements

Network Topology Diagram – this diagram depicts the network topology and security posture of the partner IS or network enclave that will be connecting to the DISN. The Network Topology Diagram should:

- Be dated
- Clearly delineate accreditation boundaries

- Identify the CCSDs of all connections to the DISN
- Identify equipment inventory (to include the most recent configuration including any enclave boundary firewalls, Intrusion Detection Systems (IDS), premise router, routers, switches, backside connections, Internet Protocol (IP) addresses, encryption devices, Cross Domain Solutions (CDS).
- Other SIPRNet connections (access points) must be shown; the flow of information to, from, and through all connections, host IP addresses, and CCSD number, if known must be shown
- Identify any other IA or IA-enabled products deployed in the enclave
- Identify any connections to other systems/networks
- Identification of other connected IS/enclaves must include:
  - The name of the organization that owns the IS/enclave
  - The connection type (e.g., wireless, dedicated point-to-point, etc.)
  - IP addresses for all devices within the enclave
  - The organization type (e.g., DoD, federal agency, contractor, etc.)
- Identify Internetworking Operating System (IOS) version
- Include the model number(s) and IP's of the devices on the diagram; diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections)

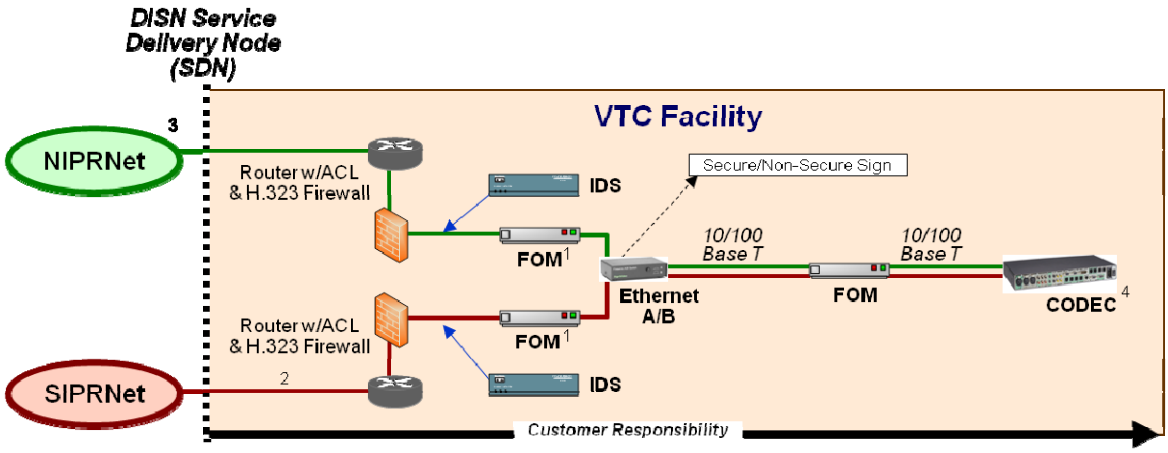
NOTE: It is important to note that in accordance with DoD and DISA guidance, firewalls, IDSs and Wireless-IDSs (where applicable) are required on all partner enclaves. Private IP addresses (non-routable) are not permitted on SIPRNet enclaves. Indicate and label all of the devices, features, or information; minimum diagram size: 8.5" x 11
The IA and IA-enabled products must be in the DoD UC Approved Products List and can be found at the DISA APLITS web page: https://aplits.disa.mil.

All configuration drawings must include the vendor make and model of the Coder-Decoder (CODEC), Inverse Multiplexor (IMUX), Dial Isolator, and all switches. This information is required prior to processing your request for service or renewal of service.
Equipment must be in accordance with the Unified Capabilities Approved Product Listing. https://aplits.disa.mil/processAPList.do

The Video Teleconferencing Facility (VTF) connectivity diagram must include all associated devices including video equipment, Multipoint Control Units (MCUs), line interface units, hubs, IP connections, routers, firewalls, gateways, modems, encryption devices, backup devices, type of transport, bandwidth being utilized, your Site ID, and building/room locations of all equipment. Additionally, depict the function and location of the DSN source switch providing connection to the DSN backbone for the IMUX voice switch.

OPTION 1

CCSD: XXXX



1 Fiber Optic Modem (FOM)/Tranceiver powered-off in the path that is not used

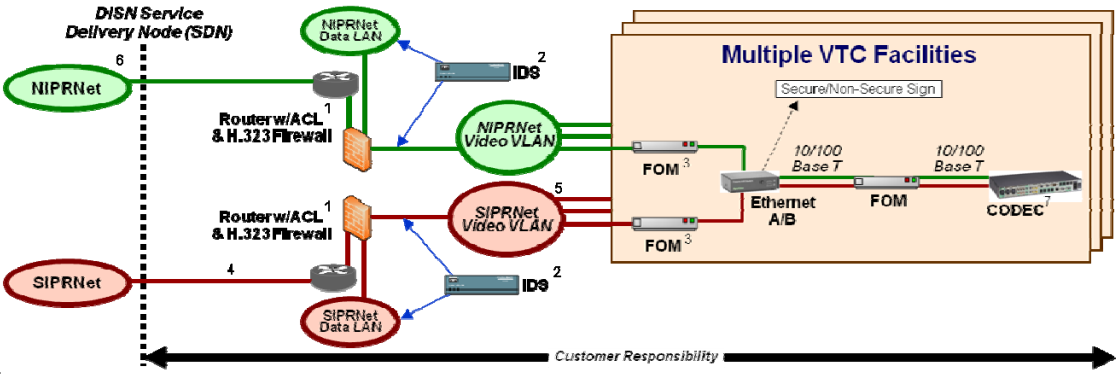
2 A pair of customer crypto or a Protected Distribution System (PDS) is required if the path between the SIPRNet SDN and the customer Premise router traverse an uncontrolled area

3 Unclassified video via NIPRNet is not currently offered as a service by DVS

4 If utilizing two CODECs, please see page 5

Figure 10 DVS Secure Configuration -Example 1

OPTION 2
CCSD: XXXX



1 The same Firewall could be used for both video and data provided it has the required performance and functionality, i.e. H.323 aware

2 IDS to monitor each network segment IAW the Network STIG

3 Fiber Optic Modem (FOM)/Tranceiver powered-off in the path that is not used

4 A pair of customer crypto or a Protected Distribution System (PDS) is required if the path between the SIPRNet SDN and the customer Premise router traverse an uncontrolled area

5 A pair of customer crypto or a Protected Distribution System (PDS) is required if the path between the SIPRNet Video VLAN and the room traverse an uncontrolled area

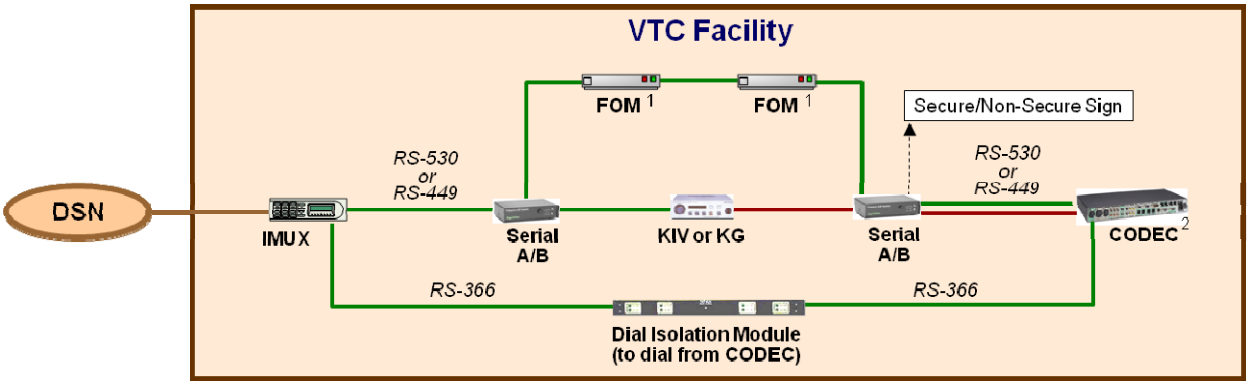
6 Unclassified video via NIPRNet is not currently offered as a service by DVS

7 If utilizing two CODECS, please see page 5

Figure 11 DVS Secure Configuration -Example 2

OPTION 3

CCSD: XXXX

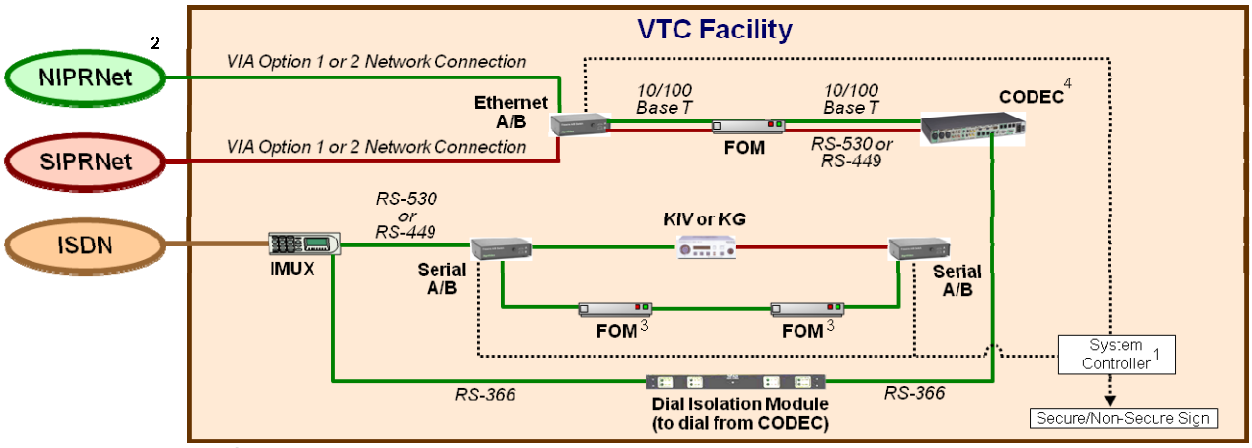


[1] Fiber Optic Modem (FOM)/Transceiver powered off in the path that is not used. FOMs are not required if the Serial A/B switch used is certified for Red/Black isolation as listed on http://disa.dtic.mil/disnvtc/red_black_peripherals.xls - Serial AB Switches

[2] If utilizing two CODECS, please see page 5

Figure 12 DVS Secure Configuration -Example 3

OPTION 4
CCSD: XXXX



[1] A/B Switches centrally controlled to ensure that both IP and Dial-up connections are at the same classification level

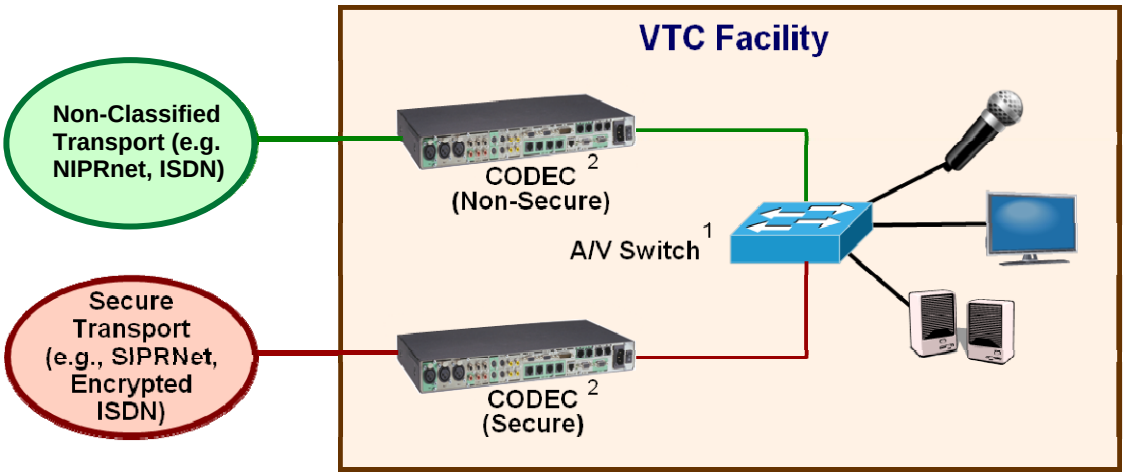
[2] Unclassified video via NIPRNet is not currently offered as a service by DVS

[3] Fiber Optic Modem (FOM)/Transceiver powered off in the path that is not used. FOMs are not required if the Serial A/B switch used is certified for Red/Black isolation as listed on http://disa.dtic.mil/disnvtc/red_black_peripherals.xls - Serial AB Switches

[4] If utilizing two CODECS, please see page 5

Figure 13 DVS Secure Configuration -Example 4

OPTION 5
CCSD: XXXX



[1] Shared peripherals, e.g. speaker, display, microphone, should be connected using an approved peripheral sharing device/switch listed at http://www.niap-ccevs.org/vpl/?tech_name=Peripheral+Switch

[2] CODEC that is not active must be powered off

Figure 14 DVS Secure Configuration -Example 5

APPENDIX G

NIPRNET – UNCLASSIFIED

This appendix provides the necessary steps and information for a Non-classified Internet Protocol Router Network (NIPRNet) connection. It is intended to supplement the detailed information provided in Sections 3-6 of this guide with NIPRNet-specific information. Any deviations or additional requirements are identified in this appendix.

G.1 NIPRNet Connection Process

Follow steps in the appropriate Partner Profile Section (3-6) of this guide.

G.2 Process Deviations and/or Additional Requirements

There are no additional requirements and/or process deviations.

G.3 NIPRNet Connection Process Checklist

This checklist provides the key activities that must be performed by the Partner/sponsor during the NIPRNet connection approval process.

Item	DoD Partner		Non-DoD Partner	
	New	Reaccreditation	New	Reaccreditation
Obtain OSD approval for Non-DoD connection			√	√[3]
Provision the connection	√		√	√[3]
Perform the C&A process	√	√	√	√
Obtain an accreditation decision (ATO/IATO/IATT)	√	√	√	√
Register the connection	√	√[4]	√	√[3]
Register in the SNAP database	√	√[4]	√	√[3]
Register in the PPSM database	√	√[4]	√	√[3]
Register in the DITPR database	√	√[4]	√	√[3]

[3] This step is not required for reaccreditation Non-DoD Partner connections unless there has been a change in Sponsor, mission requirement, contract, or location.
[4] This step is not required for reaccreditation connections that are already registered and all information is current.

Item	DoD Partner		Non-DoD Partner	
	New	Reaccreditation	New	Reaccreditation
Complete the CAP Package	√	√	√	√
DIACAP Executive Package (or equivalent for Non-DoD entities)	√	√	√	√
DIACAP Scorecard	√	√	√	√
System Identification Profile	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√
DAA Appointment Letter	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
Proof of Contract			√	√
DOD CIO Approval Letter			√	√
Submit the CAP Package to the CAO	√	√	√	√
Receive NIPRNet ATC/IATC	√	√	√	√

Table 10 NIPRNet Connection Process Checklist

G.4 Points of Contact

SIPRNet Support Center (SSC)	
Unclassified e-mail	hostmaster@nic.mil
Phone (Commercial)	800-582-2567
Phone (DSN)	312-850-2713
Fax (Commercial)	614-692-3452
Fax (DSN)	312-850-3452
Website	www.ssc.smil.mil

DISN Global Support Center (DGSC)	
Unclassified email	DGSC@csd.disa.mil
Classified email	DGSC@cols.csd.disa.smil.mil
Phone (Commercial)	800-554-DISN (3476), 614-692-4790
Phone (DSN)	312-850-4790

Primary POCs

Connection Approval Office (CAO)	
Connection Approval Office for Unclassified Connections (UCAO)	disa.meade.ns.mbx.unclassified-connection-approval@mail.mil ucao@disa.smil.mil

Connection Approval Office for Classified Connections (CCAO	disa.meade.ns.mbx.classified-connection-approval@mail.mil ccao@disa.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901
Address	Defense Information Systems Agency ATTN: NSC1 PO Box 549 Fort Meade, MD20755-0549

U.S. Army

Army, Army National Guard, and Army Reserve organizations/offices with a requirement for NIPRNet service should contact US ARMY NETCOM, Ft Huachuca, AZ.

NETCOM ESTA, ATD	
Phone (Commercial)	520-538-8029/8036
Phone (DSN)	312-879-8029/8036
Fax (Commercial)	520-538-0766

U.S. Air Force

For information on the AF NIPRNet provisioning process and AF DISN Subscription Service (DSS) locations, please contact:

AFCA DISN Command Lead	
Phone (Commercial)	618-229-6186/5732
Phone (DSN)	312-779-6186/5732

U.S. Navy/U.S. Marine Corps

USN and USMC organizations/offices with a requirement for NIPRNet service should contact:

NCMO Office of Record, Pensacola, FL	
Phone (Commercial)	850-452-7700
Phone (DSN)	312-992-7700

DISA Activities

Other DoD agencies should contact the DISA activity responsible for areas as indicated below:

GIG Areas 1, 2, and inter-GIG:

DISA CONUS Provisioning Center	
Unclassified e-mail	provtms@scott.disa.mil
Address	PO Box 25860 Scott AFB, IL 62225-5860

G.5 Topology Diagram Requirements

Network Topology Diagram – this diagram depicts the network topology and security posture of the partner IS or network enclave that will be connecting to the DISN. The Network Topology Diagram should:

- Be dated
- Clearly delineate accreditation boundaries
- Identify the CCSDs of all connections to the DISN
- Identify equipment inventory (to include the most recent configuration including any enclave boundary firewalls, Intrusion Detection Systems (IDS), premise router, routers, switches, backside connections, Internet Protocol (IP) addresses, encryption devices, Cross Domain Solutions (CDS).
- Other SIPRNet connections (access points) must be shown; the flow of information to, from, and through all connections, host IP addresses, and CCSD number, if known must be shown
- Identify any other IA or IA-enabled products deployed in the enclave
- Identify any connections to other systems/networks
- Identification of other connected IS/enclaves must include:
  - The name of the organization that owns the IS/enclave
  - The connection type (e.g., wireless, dedicated point-to-point, etc.)
  - IP addresses for all devices within the enclave
  - The organization type (e.g., DoD, federal agency, contractor, etc.)
- Identify Internetworking Operating System (IOS) version
- Include the model number(s) and IP's of the devices on the diagram; diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections)

NOTE: It is important to note that in accordance with DoD and DISA guidance, firewalls, IDSs and Wireless-IDSs (where applicable) are required on all partner enclaves. Private IP addresses (non-routable) are not permitted on SIPRNet enclaves. Indicate and label all of the devices, features, or information; minimum diagram size: 8.5" x 11

The IA and IA-enabled products must be in the DoD UC Approved Products List and can be found at the DISA APLITS web page: https://aplits.disa.mil.

NOTE: All Topologies MUST include IP addresses and ranges

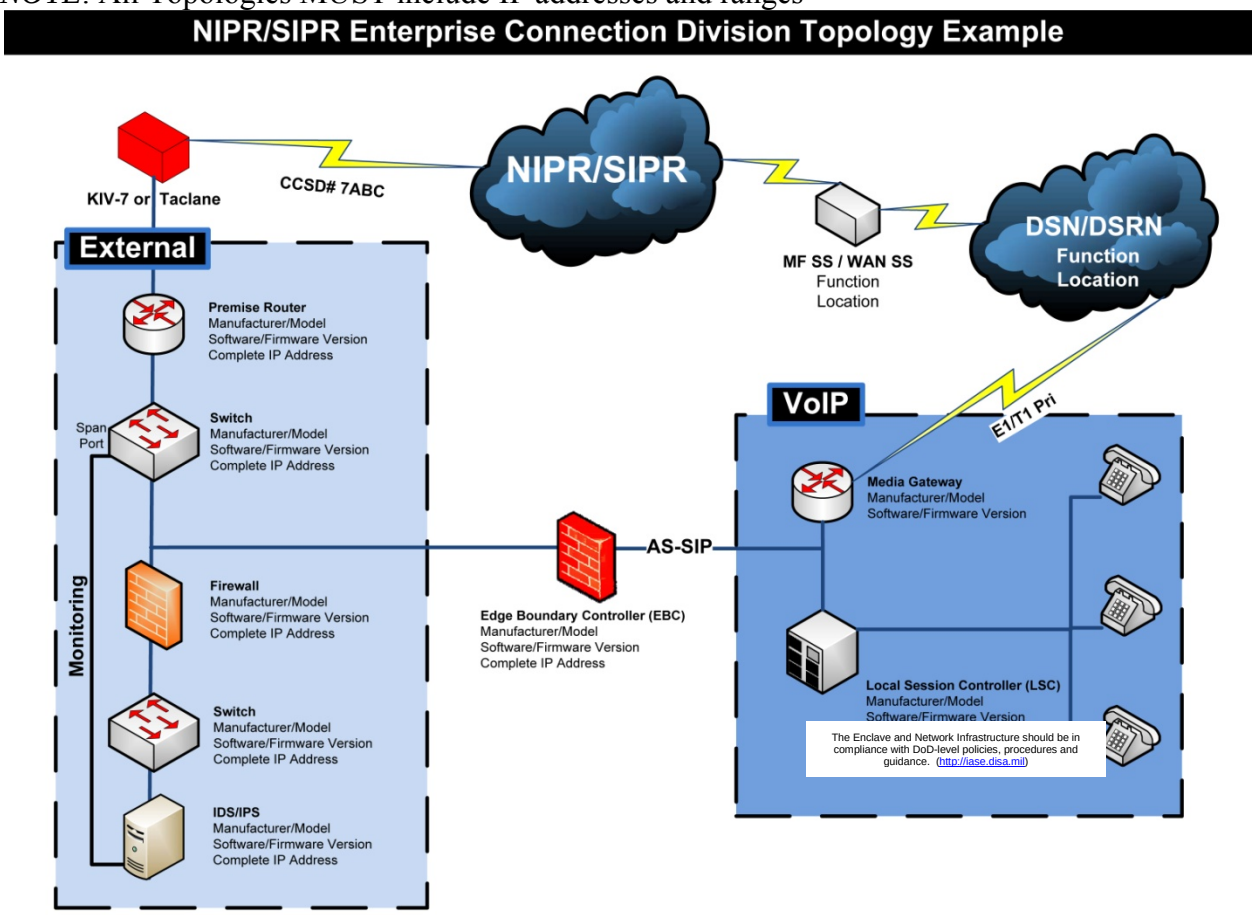


Figure 15 NIPR/SIPR Topology Sample

APPENDIX H

OSD GIG WAIVER PROCESS - UNCLASSIFIED

If an alternative connection path (i.e., commercial Internet Service Provider (ISP)) is required for NIPRNet access (i.e., enclave/standalone), or Network connection, a waiver must be approved by the GIG Waiver Panel and signed by DOD CIO.

H.1 Baseline Commercial ISP/Network Connection Approval Criteria

DoDI 8100.04, December 9, 2010, states the Defense Information System Agency (DISA) is the preferred unified capabilities transport provider for Internet and commercial satellite connections used for voice, video, and/or data services in Department of Defense (DoD) networks. The DoD components shall be permitted to use non-DISA enterprise-level infrastructures only if:

- A compelling business case justification is provided and approved by Assistant Secretary of Defense /DoD Chief Information Officer (DoD CIO); or
- The head of the Office of the Secretary of Defense (OSD) or DoD component, in coordination with the director of DISA, provides a justification to the ASD/DoD CIO that the unique mission requirements cannot be met by DISA.

These types of alternate connections require the OSD Global Information Grid (GIG) Waiver Panel to grant a waiver prior to operation.

If DISA has determined that the CC/S/A requirements cannot be fulfilled by DoD common user-systems, an exemption (i.e., GIG Waiver) may be requested by the CC/S/A. These types of alternate connections require the OSD GIG Waiver Board to grant a waiver prior to operation.

The CC/S/A should contact their Service Representative Officer (SRO) /CIO Office for validation of the mission and requirements prior to beginning the waiver process. If it has been determined by the SRO that a waiver is needed, it is the responsibility of the CC/S/A to register their request in the Systems/Networks Approval Process (SNAP) database. It is the responsibility of the SRO to validate this request in SNAP.

DISA and DSAWG will review all CC/S/A GIG waiver requests and provide a recommendation to the OSD GIG Waiver Panel prior to adjudication of the request. It is the responsibility of the CC/S/A and the partner to present the GIG waiver request to the OSD GIG Waiver Panel. If the GIG waiver request is approved, the CC/S/A shall utilize the appropriate DITCO contracting office to obtain the Internet service from a commercial ISP.

H.2 Types of Waivers Required for Alternate Connections

The following are types of alternate connections that will require the OSD GIG Waiver Panel to a grant a waiver:

- **Stand –Alone:** A connection that is paid for using appropriated funds and/or stores, processes, or transmits DoD information to the Internet using a commercial Internet Service Provider that is not connected to the unclassified Defense Information System Network (DISN).
- **NIPRNet to Internet:** A connection that is paid for using appropriated funds and/or stores, processes, or transmits DoD information connected to the DISN to the Internet using Non-Classified Internet protocol router network (NIPRNet) Internet access point.
- **Network:** Unless explicitly permitted by DoD policy, all telecommunications and IT networks and circuits that extend beyond the confines of the B/P/C/S shall be procured and /or contracted for by the Defense Information System Agency. Existing or planned networks being built, modified, or discovered as operating outside these parameters or those networks that have a Telecommunications Service Order (TSO,) but the CC/S/As needs to operate immediately and requires a waiver to meet urgent or critical operational mission requirements. If an alternative connection path (i.e., commercial Internet Service Provider (ISP) is required for NIPRNet access (i.e., enclave/standalone), or Network connection, a waiver must be approved by the GIG Waiver Panel and signed by DOD CIO.
  - As examples, if an alternative connection path (a path that uses other than DISN transport) is required such as:
    - A Commercial Internet Service Provider (C-ISP) for a stand-alone network
    - A C-ISP used to tunnel a DISN circuit between enclaves, or
    - A C-ISP connection to an enclave connected to the DISN that does not transverse an IAP or any Non-standard connection to a DISN circuit, such as a connection that does not follow all applicable STIGs, then a waiver must be approved by the GIG Waiver Panel and signed by the DoD CIO.

NOTE: Consideration for waiver approval will be based on compliance with DoD IA and CND policies and USSTRATCOM directives.

Requesting mission partner will:

- Acquire CC/S/A or field activity validation and endorsement of the alternate connection.
- Complete the waiver request form for the alternate connection via the SNAP system web-based application. (https://snap.dod.mil/.)
- Provide required connection documentation. (Reference H.3)
- Prepare an explanatory brief IAW OSD GIG Waiver presentation. (Instruction located on the SNAP system website.)
  - The OSD GIG Waiver Board will review assessments from DISA, DSAWG, and other IA technical review activities before making a final approval.

NOTE: If required from DSAWG chair: Prepare a brief IAW the standard brief format contained on the DSAWG website and submit the prepared brief to the DSAWG for waiver approval

review. The DSAWG will perform a technical review of the IA compliance assessment of the waiver and make a recommendation to the required reviewing body.

H.3 Process Deviations and/or Additional Requirements

Documentation Requirements
Develop a PowerPoint briefing based on provided guidance and the waiver criteria. The briefing will cover the points below and be conducted at the Secret level or below. New and renewal waiver briefing templates are located in SNAP at https://snap.dod.mil/gcap/reference-docs.cfm. A Soft copy of the briefing must be uploaded electronically in SNAP for review at least six weeks prior to the OSD GIG Waiver Panel meeting. All CC/S/A partners are required to coordinate the presentation with their SRO.

NOTE: Prior to submission of this brief the SRO's must validate the brief, including the mission in SNAP, and ensure the DAA has provided the applicable IATO/ATO.

- Accreditation - All DoD ISs require certification and accreditation through DIACAP (DoDI 8510.01 (ref g)). Waivers will not be processed further if the accreditation is not current. DAA approved Scorecard with expiration date should assert the DAA's acknowledgement of mission and connection requirements, and acceptance of the risk associated with deviation from standard architecture.

NOTE: The scorecard must be signed and dated by the DAA

- Independent verification (Certification and Accreditation (CA) letter) of physical and logical separation from the DoD network may be required.

- PowerPoint Briefs should include the following slides:

  1. Cover slide
     - Type of Waiver Request, Name of Component/Agency, Waiver Request Identification #, Submission Date, CIO, and POC.
  2. Request Summary Slide
     - Specify what you are requesting and for how long. Also specify if the connection will be procured through DITCO or another DISN service in the future.
  3. Organization and Mission Requirement Slide
     - Mission of component/agency and of the network/computing function/satellite support/ISP.
     - What is it your organization does and how does the requirement support that mission?
     - Does the Organization's Charter or DoD Directive drive a requirement?
  4. Requirements Overview Slide
     - What is the operational requirement?
     - What has DISA provided as a DISN solution and why does it not fulfill your requirement?
     - Data Transfer Movement Policy (what policy is currently in place for the command/headquarters?)

- Data Information (what data and information is crossing the connection. How is traffic being introduced to the DISN?)
  - Other questions the panel/board will consider:
- Is the requirement National Security System (NSS), command and control, mission essential?
- What operational considerations merit deviation from the DoD DISN/GIG architecture?
- Is this a requirement or a solution?
- Is the time requirement valid?

5. Security Evaluation Status Slide
   - Describe the security status of the system and its information assurance components
6. Topology Diagram Slide
   - Provide a communications diagram of current architecture and proposed architectures. At a minimum, the drawing must identify any Intrusion Detection Systems (IDSs), premise router, firewalls, any other security-related systems that are installed, and any connections to other systems/networks. If NIPRNet-to-Internet connection, identify the command communications service designators (CCSDs) of all connections to the DISN. Identifications to other connected systems should include the name of the organization that owns the system/enclave, the connection type (e.g., wireless, dedicated point-to-point), and the organization type (e.g., federal, DoD, contractor, etc.).
7. Waiver Architecture Slide (see topology guidance at the end of this section)
   - Architectural Congruence - Coordination with the DISA NIPRNet Manager is required to ensure DoD Global Information Grid (GIG) architecture compliance.
     - Other questions the panel/board will consider:
   - Is this a defined technical requirement?
   - Is the request duplicative of other reaccreditation service?
   - Does this deviate from DoD architecture and preserve interoperability?
   - Does this deviate from DoD architecture and preserve positive control?
   - Does this deviate from DoD architecture and enable network control?
   - Does this deviate from DoD architecture and enable configuration management?
   - How much time will it take DISA to migrate the network to DISN?
   - Using current offerings, can DISA provide the services requested?
   - Will DISA expand current offerings to include the services requested?
8. Identified Vulnerabilities & Risk Mitigation Slide
   - Identify and describe the vulnerabilities identified in the SSAA during the vulnerability assessment.
   - Identify any associated risk mitigation measures and include risk mitigation processes indentified during the Information Flow discussion.
9. Residual Risk Slide
   - Discuss all of the residual security risks that cannot be mitigated (or will not be mitigated until a future date).
10. Business Case/Best Practices Slide
    - How much will it cost? Include all costs. This must be coordinated with DISA.
      - Questions the panel/board will consider:

  - Is the request funded?
  - Is there a supporting business case?
  - If a service network solution is not possible, what is the business case for transport only solution?
  - Time requirement – Commercial Contract expires/Waiver expires.
  - Monthly Reoccurring or Annual Cost for the ISP connection.
  - What is the total cost to DoD?

11. Alternative Solutions Slide
    - Specify why the CC/S/A cannot use a Defense Information System Network (DISN) solution to perform the requirement being requested.
12. Cost Alternatives Slide
13. Alternative Comparisons Slide
14. Business Plan Alternatives Slide
    - Plan for obtaining the commercial ISP connection through the appropriate DITCO contracting office.
15. Recommendation & Actions Slide
    - Provide recommendation and actions of chosen alternative required to make it happen.

H.4 Waivers Process Flow

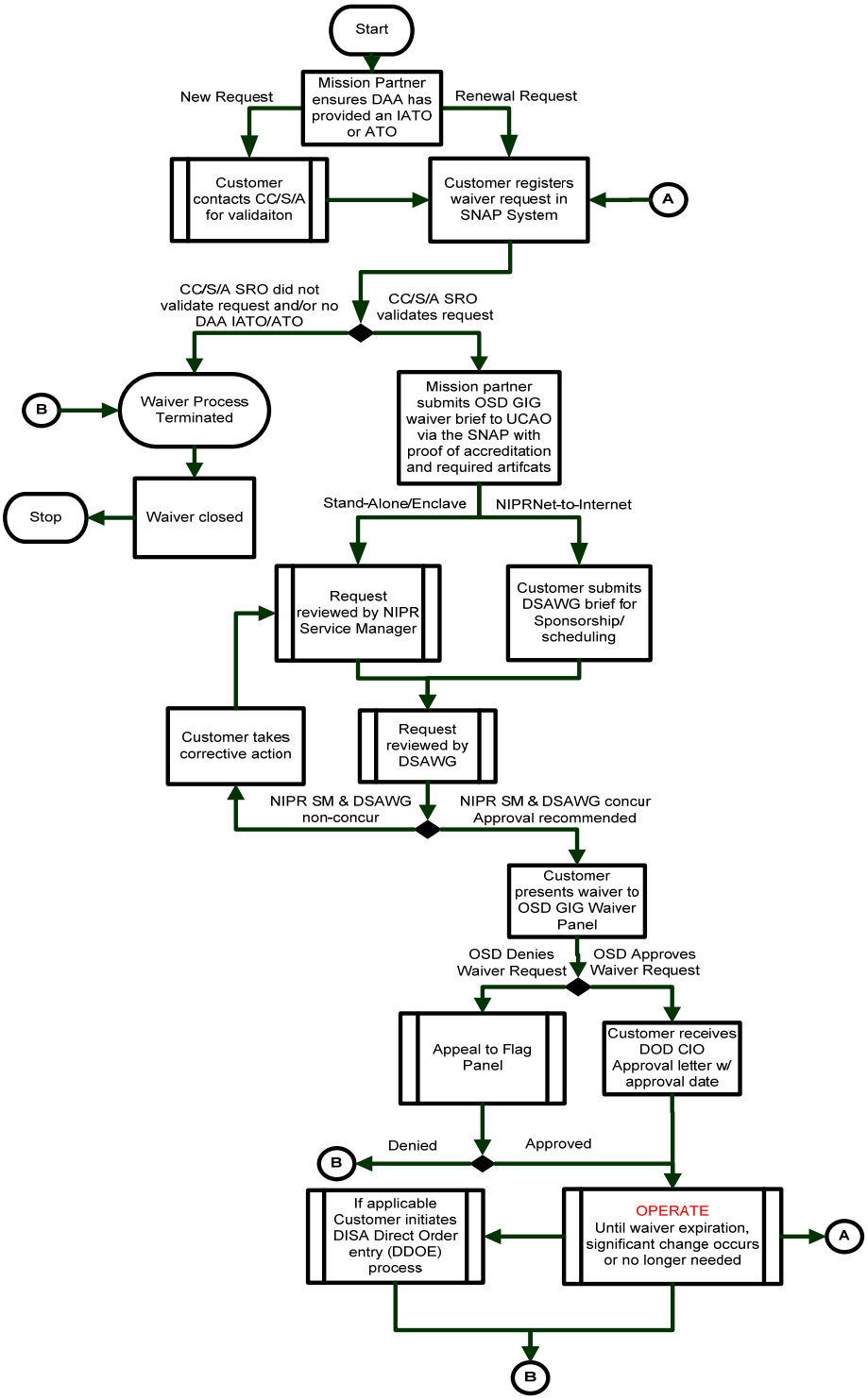


Figure 16 ISP Waivers Process Flow

H.5 Waiver Renewals

Once a waiver has expired, the CC/S/A has the option of renewing. If it has been determined that the waiver needs to be renewed, the CC/S/A must do the following:

- Update the SNAP registration
- Complete and upload the Renewal ISP Waiver Brief Template (located in SNAP).
- Upload the accreditation requirements (if expired)
- Submit the registration

The renewal request will then follow the same process as a new waiver request.

NOTE: For waiver renewals (no changes to topology, IA, etc) that have full Panel consensus, there will not be a brief presented at the GWP, only a note of the vote will be made during the meeting.

H.6 Points of Contact

Connection Approval Office	
Connection Approval Office for Unclassified Connections (UCAO)	disa.meade.ns.mbx.connection-approval-waivers-team@mail.mil ucao@disa.smil.mil
Connection Approval Office for Classified Connections (CCAO)	UCAO-Waivers@disa.smil.mil ccao@disa.smil.mil
Phone (Commercial)	301-225-2900
Phone (DSN)	312-375-2900

H.7 Additional Policy and Guidance Documents

CJCSI 6211.02D	Defense Information System Network (DISN): Policy and Responsibilities, 24 Jan 2012 (ref d)
DoDD 8500.01E	*Information Assurance (IA)*, 24 October 2002 (ref c)
DoDI 8500.2	*Information Assurance (IA) Implementation*, 6 February 2003 (ref f)
DoDI 8100.4	*DoD Unified Capabilities*, 9 December 2010 (ref n)
DoDD 8100.02	*Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2007* (ref v)

*Network Topology Diagram – this diagram depicts the network topology and security posture of the partner IS or network enclave that will be connecting to the DISN. The Network Topology Diagram should:

- Be dated
- Clearly delineate accreditation boundaries

- Identify the CCSDs of all connections to the DISN
- Identify equipment inventory (to include the most recent configuration including any enclave boundary firewalls, Intrusion Detection Systems (IDS), premise router, routers, switches, backside connections, Internet Protocol (IP) addresses, encryption devices, Cross Domain Solutions (CDS).
- Other SIPRNet connections (access points) must be shown; the flow of information to, from, and through all connections, host IP addresses, and CCSD number, if known must be shown
- Identify any other IA or IA-enabled products deployed in the enclave
- Identify any connections to other systems/networks
- Identification of other connected IS/enclaves must include:
  - The name of the organization that owns the IS/enclave
  - The connection type (e.g., wireless, dedicated point-to-point, etc.)
  - IP addresses for all devices within the enclave
  - The organization type (e.g., DoD, federal agency, contractor, etc.)
- Identify Internetworking Operating System (IOS) version
- Include the model number(s) and IP's of the devices on the diagram; diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections)

NOTE: It is important to note that in accordance with DoD and DISA guidance, firewalls, IDSs and Wireless-IDSs (where applicable) are required on all partner enclaves. Private IP addresses (non-routable) are not permitted on SIPRNet enclaves. Indicate and label all of the devices, features, or information; minimum diagram size: 8.5" x 11*.

The IA and IA-enabled products must be in the DoD UC Approved Products List and can be found at the DISA APLITS web page: https://aplits.disa.mil.

H.8 FAQs

Q: When is a GIG Waiver required?
A: A GIG waiver is required if DISA cannot provide the service and when atleast one of the following is true:

- The ISP connection is purchased with Appropriated Funds. Appropriated funds are government funds set aside for a specific use.
- The connection will store, process, or transmit any DoD data.

A GIG Waiver is NOT required if ALL of the following are true:

- The ISP connection is not purchased with appropriated funds.
- The connection will not store, process, or transmit any DoD data.
- The connection is physically and logically separated from the DISN.

Even if a GIG Waiver is not required, the DAA must perform a risk assessment endorsed by the facility or installation on file if the connection is co-located on the same premise as a DoD network.

Q: When does the OSD GIG Waiver Panel meet?
A: The OSD GIG Waiver Panel meets on the third Wednesday of every month. If you are scheduled for the panel and the panel date is rescheduled, the CAO will inform you of the change.

Q: Must I attend in person to present my brief to OSD or can a phone bridge be made available for me?
A: You can attend in person or via phone. The OSD secretariat will establish a phone bridge for the meeting. The CAO will request that you inform them of the names of who will be presenting and a contact number for day of the meeting.

Q: I have an ISP connection co-located on the same premise as a DOD network, however, this connection is not paid for using appropriated funds and the connection is physically and logically separated from the DISN. Furthermore, it does not store, process, or transmit any DoD data. Does this require a waiver?
A: No, this does not require a waiver. However, the DAA must perform and have a risk assessment endorsed by the facility or installation command on file.

Q: What is a complete ISP waiver package?
A: A complete package includes the following:

- Registration in SNAP
- Completed brief
- Waiver validation from the SRO
- Independent verification of physical and logical separation from the DoD network may be required. (Must be singed by the Certifying Authority) – for Stand Alone only.
- Accreditation (ATO\IATO\IATT and Scorecard)

APPENDIX I

REMOTE COMPLIANCE MONITORING

I.1 Vulnerability Scanning

The Defense Information Systems Agency Enterprise Connection Division vulnerability scanning team is assigned the mission per Communications Tasking Order (CTO) 07-09 of assessing every SIPRNet Command Communications Service Designator (CCSD) perimeter defense in depth stance and vulnerabilities semi-annually.

I.2 Scan Types

In accordance with the requirements outlined in CTO 07-09, the vulnerability scanning team conducts two distinct scan actions on a semi-annual basis, unannounced and announced scans.

- For unannounced scans, the CCSD's circuit perimeter is tested with penetration tools in order to assess its ability to deny intrusion from an unknown source.
- An announced scan focuses on the CCSD using a known or "trusted" IP Address, and assesses the current state of machines within the CCSD.

The trusted IP is identified in CTO- 07-09 for reference.

- In addition to these scans, the team also conducts IATT scans for new connection requests, and ad hoc scanning at the request of partner organizations.

NOTE: Partners must review the monthly CTO scan schedule, available on SIPRNet at http://www.disa.smil.mil/connect/schedule and/or https://www.cybercom.smil.mil/j3/pages/IPsonarmappingschedule.aspx.

- All scan results are added to the Global Information Grid (GIG) Interconnection Approval Process (GIAP) database for review and sent to the CCSD point of contacts via email.

I.2.1 Unannounced Scan

- All semiannual scans mandated by CTO 07-09 are first scanned as Unannounced (penetration testing).
- Performed from a server which uses an unknown IP, rather than the IP given in CTO 07-09, in an attempt ascertain the defense in depth stance of the site's enclave/circuit.
- Passing results are attained when none of the devices on the inside of the network can be identified. Should any devices be identifiable within the internal network, it will be considered a failure of the perimeter's defense.
- If the scan is a failure, the results will be uploaded into GIAP and sent to the CCSD POCs for review and mitigation.

I.2.2 Announced Scan

- Any site that passes the Unannounced CTO 07-09 scan is then required to undergo an Announced Scan.

- Performed from a server with the CTO 07-09 IP address.
- Passing results are attained when no Category (CAT) I vulnerabilities are found IAW current STIGs. Should any CAT I vulnerabilities be found, or the announced scan was unable to access the circuit, the result will be a failure. NSC provides letters to mission partners based on POCs listed in SGS on the details of all failed scan results.
- Results will be uploaded into GIAP and sent to the CCSD POCs for review and mitigation.

I.2.3 IATT Scan

- Performed on all new SIPR circuit requests as a requirement for an Authority to Connect/Interim Authority to Connect (ATC/IATC).
- IATT scan uses the same criteria as an announced scan.
- Please reference the IATT Process Checklist below.

I.2.4 AD HOC Scan

- Sites that fail any type of scan may request a rescan be conducted.
- The AD HOC scan will begin with the scan that failed (i.e. a failed Announced Scan would not be subject to an Unannounced scan)
- The requirements for pass/fail remain the same as the original scan.
- An AD HOC Scan typically takes up to 8 business days to complete, but may require more time depending on network size.

I.3 Frequently Asked Questions (FAQs)

Q: I received results from a semiannual scan, but some of the recipients no longer work for/with my site. What do I need to do to get this changed?
A: If the POCs or site information for the CCSD change, a revised SIPRNet Connection Questionnaire (SCQ) should be submitted to the CAO office.

Q: What do I need to do to prepare for the CTO Scans?
A: Review the posted monthly CTO scan schedule, available on SIPRNet at http://www.disa.smil.mil/connect/schedule and/or https://www.cybercom.smil.mil/j3/pages/IPsonarmappingschedule.aspx. If your site is listed for the upcoming month; ensure that the IP address listed in the CTO 07-09 is configured to "allow" in all Access Control Lists (ACLs), Host Based Security System (HBSS) and Intrusion Detection System (IDS).

Q: I received a failure on an Unannounced/Announced scan. What steps do I need to take now?
A: For unannounced scans, review your boundary protection systems to ensure they are locked down as much as possible. For Announced scans, review the CAT I findings and fix/mitigate them. Once these items have been addressed, you should contact the CAO Scan Team to schedule an AD HOC scan.

I.4 IATT Process Checklist

	To be completed PRIOR to an initial scan for ATC/IATC issuance:
1	Equipment installed, configured, and turned on.
2	72 hr. burn-in completed by IT&A.
3	Per CTO 07-09, SIPRNet Connection Approval Office (SCAO) "Announced" IP Address configured in the firewall(s) and router(s) ACL to allow access for inbound and outbound traffic.
4	At least (1) server, workstation, or laptop with at least (1) port, protocol or service enabled. (Please refer to PPSM for allowed ports and protocols – disa.meade.ns.mbx.ppsm@mail.mil)
5	HBSS disabled for initial scan or SCAO's "Announced" IP Address added to the HBSS allowed IP's.
6	Windows firewall disabled for the target system(s) initial scan.

CAO Remote Compliance Monitoring Contact Information	
NIPR Scan Email	disa.meade.ns.mbx.connection-approval-scan-team@mail.mil
SIPR Scan Email	CAOSCANS@DISA.SMIL.MIL
Phone (Commercial)	301-225-2902
Phone (DSN)	312-375-2902

IT&A Contact Information	
Phone (Commercial)	618-220-9041

SIPR NOC Contact Information	
Phone (Commercial)	618-220-9980

This page intentionally left blank.

APPENDIX J

SIPRNET – CLASSIFIED

The following provides the necessary steps and information for a Secret Internet Protocol Router Network (SIPRNet) connection. This is intended to supplement information provided in Sections 3-6. Any deviations from those or additional requirements are identified in this appendix.

J.1 SIPRNet Connection Process Checklist

This checklist provides the key activities that must be performed by the partner/sponsor during the SIPRNet connection approval process.

Item	DoD Partner		Non-DoD Partner	
	New	R	New	Reaccreditation
Obtain OSD approval for non-DoD connection			√	√[5]
Provision the connection	√		√	√
Perform the C&A process	√	√	√	√
Obtain an accreditation decision (ATO/IATO)	√	√	√	√
Register the connection	√	√[6]	√	√**Error! Bookmark not defined.**
Register in the GIAP/SGS database	√	√**Error! Bookmark not defined.**	√	√
Register in the PPSM database	√	√	√	√
Register in the SIPRNet IT Registry database	√	√	√	√
Register with the SIPRNet Support Center (SSC)	√			
Complete the CAP package	√	√	√	√
DIACAP Executive Package (or equivalent for non-DoD entities)	√	√	√	√
DIACAP Scorecard	√	√	√	√
System Identification Profile	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√

[5] This step is not required for reaccreditation non-DoD Partner connections unless there has been a change in sponsor, mission requirement, contract, or location.
[6] This step is not required for reaccreditation connections that are already registered and all information is current.

Item	DoD Partner		Non-DoD Partner	
	New	R	New	Reaccreditation
DAA Appointment Letter	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
SIPRNet Connection Questionnaire (SCQ)	√	√	√	√
Proof of Contract			√	√
DOD CIO Approval Letter			√	√**Error! Bookmark not defined.**
Submit the CAP package to the CAO	√	√	√	√
Receive remote compliance scan	√		√	
Receive SIPRNet ATC/IATC	√	√	√	√

Table 11 SIPRNet Connection Process Checklist

J.2 Process Deviations and/or Additional Requirements

DoD Contractor connections to the SIPRNet must go through DSS for accreditation of their facilities and information systems. For questions regarding DSS accreditation, contact the DSS SIPRNet Program Management Office at occ.cust.serv@dss.mil by phone at 888-282-7682, Option 2.

All DoD and non-DoD partners/sponsors must complete the SIPRNet Connection Questionnaire (SCQ) and submit it with the CAP package. The DAA is responsible for the content of the SCQ but may delegate the signatory responsibility to a lower level. The SCQ is available on the CAO web page at www.disa.mil/connect/library.

- All 'Yes' responses must be explained, with the exception of questions 14, 15, and 16
- All POC information must be completed for the questionnaire to be accepted by the CAO

NOTE: Partners cannot register their information directly into GIAP/SGS. This must be accomplished by submitting a CAP package to include the SIPRNet Connection Questionnaire (SCQ).

The CAO review of the SIPRNet CAP package for new connections includes an on-line remote compliance assessment. This is a vulnerability scan of the IS requesting SIPRNet connection, performed by the CAO, to identify possible vulnerabilities that exist within the IS. The results are used during the connection approval decision-making process.

J.3 IATT Process Checklist

	To be completed PRIOR to an initial scan for ATC/IATC issuance:
1	Equipment installed, configured, and turned on.
2	72 hr. burn-in completed by IT&A.

3	Per CTO 07-09, SIPRNet Connection Approval Office (SCAO) "Announced" IP Address configured in the firewall(s) and router(s) ACL to allow access for inbound and outbound traffic.
4	At least (1) server, workstation, or laptop with at least (1) port, protocol or service enabled. (Please refer to PPSM for allowed ports and protocols – disa.meade.ns.mbx.ppsm@mail.mil)
5	HBSS disabled for initial scan or SCAO's "Announced" IP Address added to the HBSS allowed IP's.
6	Windows firewall disabled for the target system(s) initial scan.

Table 12 IATT Process Checklist

J.4 Points of Contact

SIPRNet Support Center (SSC)	
Unclassified email	hostmaster@nic.mil
Phone (Commercial)	800-582-2567
Phone (DSN)	312-850-2713
Fax (Commercial)	614-692-3452
Fax (DSN)	312-850-3452
Website	www.ssc.smil.mil

SIPRNet Service Manager	
Phone (Commercial)	301-225-2484

CAO Remote Compliance Monitoring Contact Information	
NIPR Scan Email	disa.meade.ns.mbx.connection-approval-scan-team@mail.mil
SIPR Scan Email	CAOSCANS@DISA.SMIL.MIL
Phone (Commercial)	301-225-2902
Phone (DSN)	312-375-2902

IT&A Contact Information	
Phone (Commercial)	618-220-9041

SIPR NOC Contact Information	
Phone (Commercial)	618-220-9980

J.5 Additional Policy and Guidance Documents

Cross Domain Solutions (CDS) are a special case of the SIPRNet connection process. Please refer to the CDS Process (Appendix K) for more information.

J.6 Sample SIPRNET Topology

Network Topology Diagram – this diagram depicts the network topology and security posture of the partner IS or network enclave that will be connecting to the DISN. The Network Topology Diagram should:

- Be dated
- Clearly delineate accreditation boundaries
- Identify the CCSDs of all connections to the DISN
- Identify equipment inventory (to include the most recent configuration including any enclave boundary firewalls, Intrusion Detection Systems (IDS), premise router, routers, switches, backside connections, Internet Protocol (IP) addresses, encryption devices, Cross Domain Solutions (CDS).
- Other SIPRNet connections (access points) must be shown; the flow of information to, from, and through all connections, host IP addresses, and CCSD number, if known must be shown
- Identify any other IA or IA-enabled products deployed in the enclave
- Identify any connections to other systems/networks
- Identification of other connected IS/enclaves must include:
  - The name of the organization that owns the IS/enclave
  - The connection type (e.g., wireless, dedicated point-to-point, etc.)
  - IP addresses for all devices within the enclave
  - The organization type (e.g., DoD, federal agency, contractor, etc.)
- Identify Internetworking Operating System (IOS) version
- Include the model number(s) and IP's of the devices on the diagram; diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections)
  - A representative range of workstations and servers must be identified

NOTE: It is important to note that in accordance with DoD and DISA guidance, firewalls, IDSs and Wireless-IDSs (where applicable) are required on all partner enclaves. Private IP addresses (non-routable) are not permitted on SIPRNet enclaves. Indicate and label all of the devices, features, or information; minimum diagram size: 8.5" x 11

The IA and IA-enabled products must be in the DoD UC Approved Products List and can be found at the DISA APLITS web page: https://aplits.disa.mil.

NOTE: All Topologies MUST include IP addresses and ranges

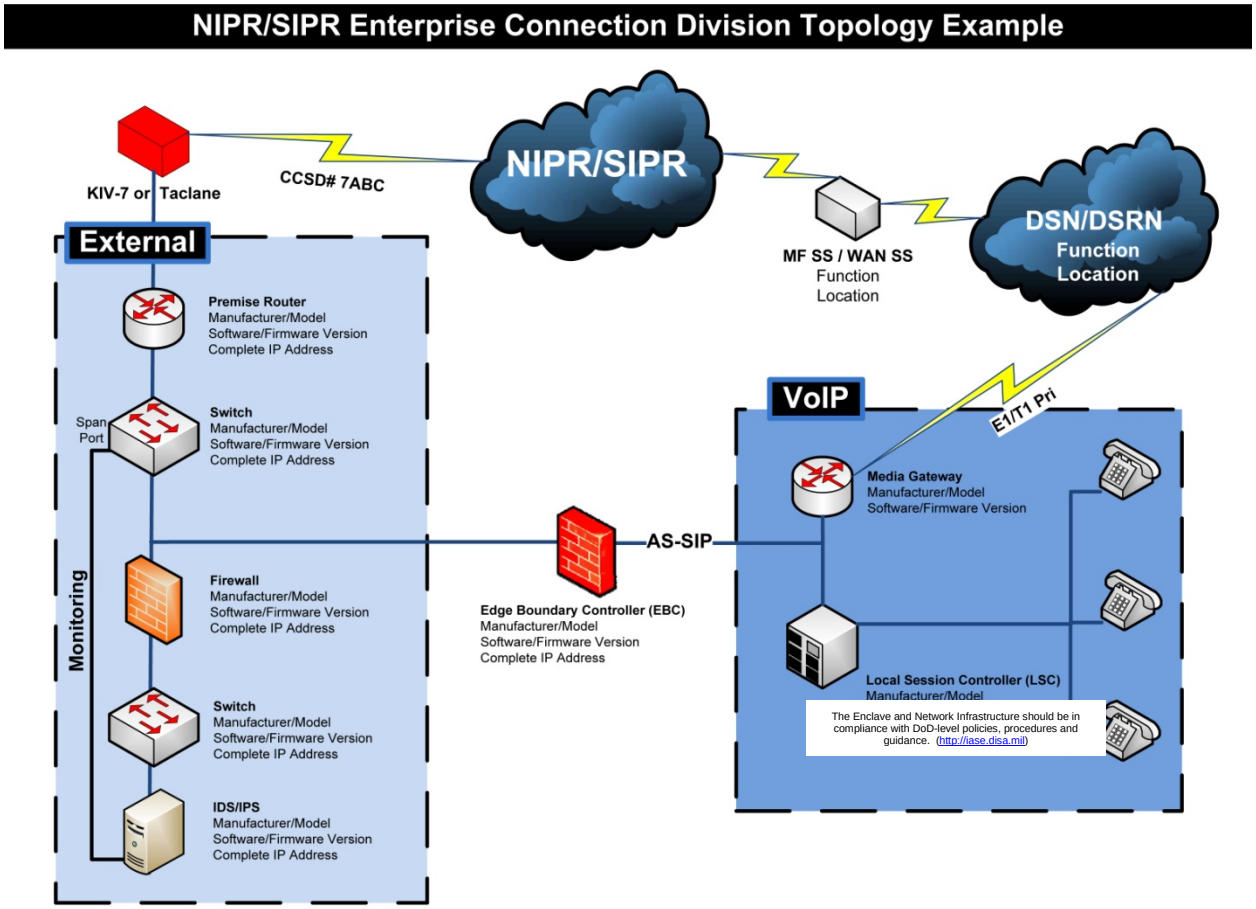


Figure 17 NIPRNET/SIPRNET Topology Sample

APPENDIX K

CDS – CLASSIFIED AND UNCLASSIFIED

Cross Domain Solutions (CDS) require an additional approval process and authorization, separate from the review and approval for the ATC for the CCSD. This appendix provides the steps necessary to obtain a Cross Domain Solution Authorization (CDSA).

NOTE: This process covers CDS devices connecting to networks classified Top Secret and below. CDS devices connecting to networks classified Top Secret – SCI and above follow a different approval process outlined by the Unified Cross Domain Management Office (UCDMO) and DIA.

K.1 Mandatory CDS Requirements for Connection to the SIPRNet

Partners are required to follow the guidelines below to obtain connection approval for their CDS devices. A CDSA will not be granted unless all required documentation and approvals have been completed. There are two main CDS processes, those for Point-to-Point (covered in K.2) and DISA's Cross Domain Enterprise Services (CDES) (covered in K.3).

K.2 CDS Authorization Process: Standard Point-to-Point Solution

The CDS Authorization process for Point-to-Point is comprised of four phases: Phase 1 - Validation, Prioritization, and Requirements Analysis; Phase 2 - Solution Development and Risk Assessment; Phase 3 - Security Engineering and Risk Assessment; and Phase 4 - Annual Risk Review. The following diagram presents a graphical depiction of the CDS process.

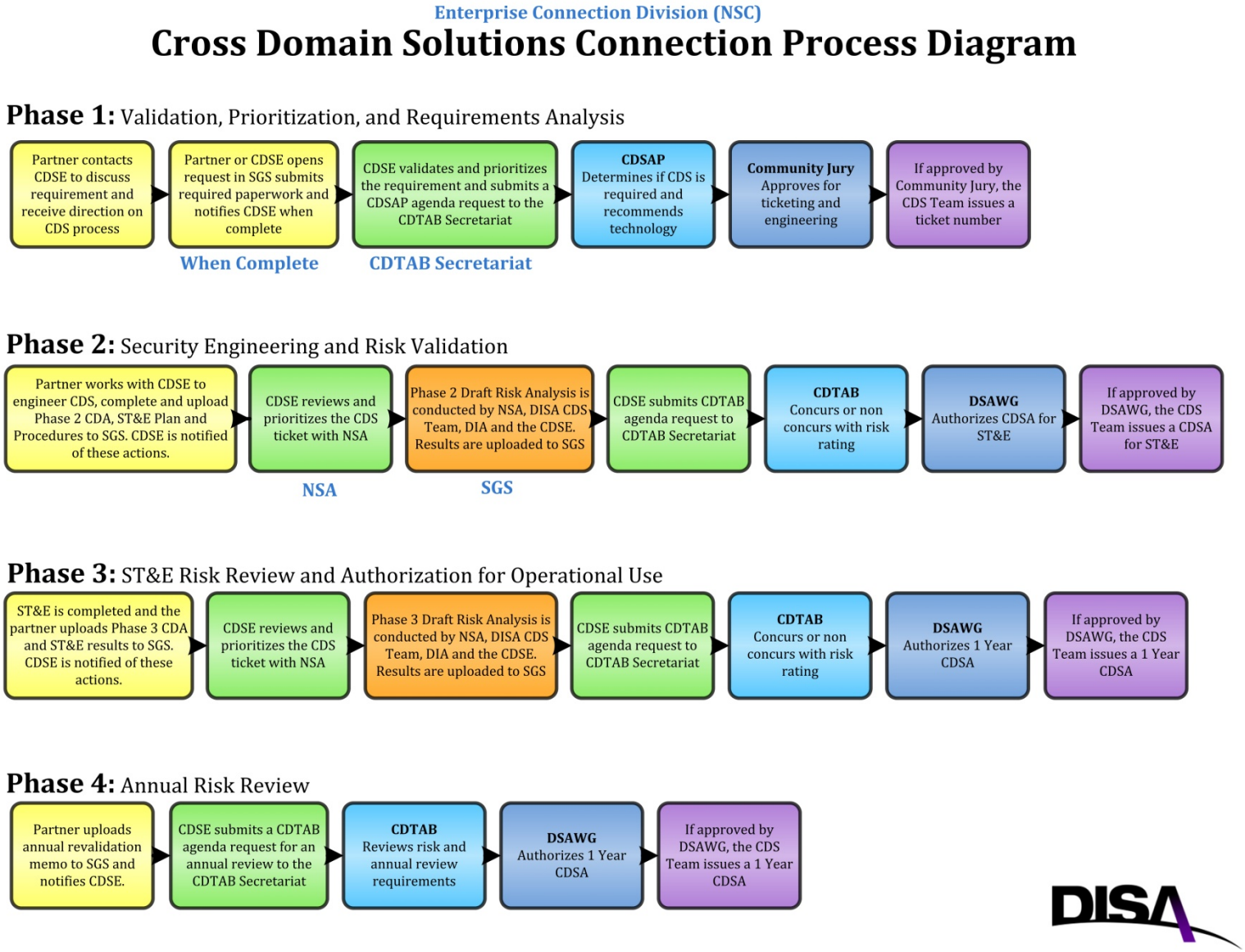


Figure 18 CDS Connection Process

K.2.1 Phase 1 CDS Authorization Process: Point-to-Point Solution

Validation, Prioritization and Requirements Analysis

Phase 1 of the CDS process consists of six specific actions. Any exceptions to the CDS process must be coordinated with your CC/S/A representatives and Cross Domain Technical Advisory Board (CDTAB) chair. The first three actions must be completed in 45 days.

1. The CDS Partner must coordinate with the CC/S/A Cross Domain Solutions Element (CDSE) representatives to determine and document the information transfer and mission requirements. These requirements must be documented in the Cross Domain Appendix (CDA).

NOTE: All COCOMs must utilize the CDSE represented by their supporting agency as referenced in DoDD 5100.3, Support of the Headquarters of Combatant and Subordinate Joint Commands, 9 February 2011.

NOTE: All COCOMs must also work with their CDSE to initiate a review of their mission requirements by DISA (CDES) to determine if DISA CDES can fulfill the technical requirements of their mission. This process must be completed prior to presenting the request to the Community Jury in step 5. If it is found that CDES can fulfill the mission requirements then the Community Jury may direct the COCOM to utilize CDES to perform their mission. In this case the COCOM will move to Phase 2 of the Enterprise Solution Process after ticketing approval of the Community Jury.

2. DoD Partner or CDSE obtains access to the SGS (https://giap.disa.smil.mil) through the CAO, opens a new CDS request filling out all required database fields, uploads a Phase 1 CDA, a validation memo signed by their respective DAA, and notifies their CDSE of completion of these requirements.
3. The DoD Partner's respective CDSE validates and prioritizes the Request and submits a CDSAP agenda request to the CDTAB Secretariat.

NOTE: Agenda requests will not be accepted by the CDTAB Secretariat directly from the Partner. All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Any late submissions will NOT be accepted.

4. The request is brought before the CDSAP to determine if a CDS is required to meet the Partner's requirement and if the proposed solution versus an alternative solution is recommended. This determination is then presented to the Community Jury in Step 5.
5. The CDS Request and CDSAP comments are brought before the Community Jury (a function of the DSAWG) to obtain approval for ticketing and engineering.
6. If approved by the Community Jury and the CDS is going to be implemented as a point-to-point solution, the CDS team will assign a CDS ticket number and the CDS is transitioned into Phase 2. If approved by the Community Jury and DISA CDES is going to meet the requirement, the request number will be closed and the requirement will be met under a CDES ticket number (see K.3).

K.2.2 Phase 2 CDS Authorization Process: Point-to-Point Solution

Security Engineering and Risk Assessment

1. The Partner works with their respective CDSE to engineer the CDS, and to complete and upload the following to the SGS: 1) Phase 2 CDA, 2) a Security, Test, and Evaluation (ST&E) Plan; and 3) ST&E Procedures. The Partner notifies the CDSE when all requirements have been met.

NOTE: The Partner should contact their respective CDSE if they have questions or need assistance with completing the required content in the referenced documents.

2. The respective CDSE reviews and prioritizes the CDS ticket with NSA. The CDS Team will perform a grid connectivity threat (GCT) analysis based on the ticket priority submitted by the CDSE. It is the CDSE's CDTAB Representative's responsibility to complete the Transfer Processing Threat Report and to submit a request for an agenda to be presented to the Cross Domain Solutions Assessment Panel (CDSAP) or CDTAB.

NOTE: Each CDSE must submit all requests for GCT ratings from the CDS Team no later than the first Monday of the month if they intend to bring the ticket before the CDTAB.

3. Draft risk analysis results are completed by NSA, the respective CDSE, the CDS Team, and DIA following the Risk Decision Authority Criteria (RDAC) criteria. These results must be uploaded to SGS.
4. The respective CDSE submits a CDTAB agenda request to the CDTAB Secretariat.

NOTE: Agenda requests will not be accepted by the CDTAB Secretariat directly from the Partner. All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Any late submissions will NOT be accepted.

5. At the CDTAB, the voting members will review the information provided from the Partner's CDA and the compiled risk rating then provide a vote of concur or non-concur with the risk rating.
6. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a CDSA for ST&E.

   If approved and all other enclave documentation has met standard requirements, the CDS team will issue a CDSA for ST&E and the CDS ticket transitions into Phase 3.

NOTE: For a CDSA to be issued, the following items are required:

- Partner's Valid ATC for the enclave where CDS is operating
- DAA Signed CDA referencing CCSD by DAA (Phase 2 – IATC and Phase 3 – ATC) or enclave ATO referencing the CDS
- DAA signed SCQ referencing the CDS tickets
- Topology referencing the specific ticket number of the CDS.

- Signed CDA by DAA (Phase 2 – IATC and Phase 3 – ATC) or ATO signed by DAA. (For Non-DISN Connections)

K.2.3 Phase 3 CDS Authorization Process: Point-to-Point Solution

ST&E Risk Review and Authorization for Operational Use

1. Upon completion of the ST&E the Partner must upload the ST&E results and updated Phase 3 CDA to the SGS. The Partner notifies the CDSE of these actions.
2. The respective CDSE reviews the ST&E results to verify no changes exist between the Draft Risk Analysis and the actual test results. The CDSE must notify the CAO of any changes prior to ticket submission as an agenda request or initiation of a Cross Domain Solution Authorization for operational use.
3. If, prior to Phase 2 approval, the DSAWG also granted approval for operational use, and the CDSE finds the ST&E result concur with the Draft Risk Analysis, the respective CDSE may request a CDSA from the CDS Team as per step 18. Otherwise, the respective CDSE submits a CDTAB agenda request to the CDTAB Secretariat.

NOTE: Agenda requests will not be accepted by the CDTAB Secretariat directly from the Partner. All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Any late submissions will NOT be accepted.

4. At the CDTAB, the voting members will review the information provided from the Partner's CDA and the compiled risk rating and provide a vote of concur or non-concur with the risk rating and comments.
5. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a one-year CDSA.
6. If approved by the DSAWG, and all other enclave documentation has met standard requirements, the CDS Team will issue a one-year CDSA. The CDS ticket transitions into Phase 4.

NOTE: For a CDSA to be issued, the following items are required:

- Partner's Valid ATC for the enclave where CDS is operating
- DAA Signed CDA referencing CCSD by DAA (Phase 2 – IATC and Phase 3 – ATC) or enclave ATO referencing the CDS
- DAA signed SCQ referencing the CDS tickets
- Topology referencing the specific ticket number of the CDS.
- Signed CDA by DAA (Phase 2 – IATC and Phase 3 – ATC) or ATO signed by DAA. (For Non-DISN Connections)

NOTE: The CDS device is marked operational in SGS upon the initial issuance of a CDSA by the CDS Team following a DSAWG approval. It remains operational until the CDTAB Secretariat receives evidence from the DAA through the Partner's respective CDSE that the device is non-operational.

K.2.4 Phase 4 CDS Authorization Process: Point-to-Point Solution

Annual Risk Review

CDS's will receive no more than a 1-year CDSA from the DSAWG. In order to receive approval for following years, the following requirements must be met.

1. Complete a satisfactory scan of the enclave by the CAO (or a POAM if unsatisfactory), submit a revalidation memo from the DAA stating that the CDS is still required and the CDS configuration has not changed, and provide notification to the CDSE of completion of the actions. (see JTF GNO Communications Tasking Order (CTO) 07-09, Support for Remote Vulnerability Assessment and Compliance Monitoring Scans of SIPRNet Enclaves (Revised Guidance), 191640Z Jul 07, Secret https://www.cybercom.smil.mil/J3/orders/CTOs/CTO0709.doc (SIPRNet) and DISN CPG paragraph 1.2. for scan requirements.)

NOTE: The DAA is required to revalidate all CDS devices in enclaves containing CDS devices annually. The DAA revalidates operational and functional requirements, verifies the configuration described in the CDS documentation is correct, ensures and validates annual testing of CDS controls, operational requirements, configuration, and notifies the respective CDSE that this review has been conducted. This notification should be in the form of an annual revalidation letter and should be uploaded to SGS under the respective CDS ticket number.

2. The respective CDSE submits a CDTAB agenda request to the CDTAB Secretariat.

NOTE: Agenda requests will not be accepted by the CDTAB Secretariat directly from the Partner. All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Any late submissions will NOT be accepted.

3. At the CDTAB, the voting members will review the CDS Annual Review requirements, information provided extracted from the Partner's CDA and the previous risk rating, and provide a vote of concur or non-concur with the risk rating and comments.
4. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a 1-year CDSA.
5. If approved by the DSAWG, and all other enclave documentation has met standard requirements, the CDS Team will issue a 1-year CDSA. The CDS Ticket will remain in Phase IV.

NOTE: For a CDSA to be issued, the following items are required:

- Partner's Valid ATC for the enclave where CDS is operating
- DAA Signed CDA referencing CCSD by DAA (Phase 2 – IATC and Phase 3 – ATC) or enclave ATO referencing the CDS
- DAA signed SCQ referencing the CDS tickets
- Topology referencing the specific ticket number of the CDS.
- Signed CDA by DAA (Phase 2 – IATC and Phase 3 – ATC) or ATO signed by DAA. (For Non-DISN Connections)

NOTE: Planned changes to the configuration of the CDS including patches and upgrades must be coordinated with the Partner's respective CDSE and entered into the SGS as Phase I requests. These requests must follow the normal CDS review process and be approved by the DSAWG prior to implementation.

NOTE: If for any reason it becomes necessary to discontinue use of a CDS, the CDSE must submit a closure request memo in order to stop tracking of the CDS ticket in SGS. The CDS analyst who performs the closure will upload the closure request to SGS under the ticket in question, and close the ticket with the comment "Closed per CDSE request".

K.3 CDS Authorization Process: Cross Domain Enterprise Services

The CDS Authorization process for Cross Domain Enterprise Services (CDES) is comprised of four phases:

- Phase 1 - Validation, Prioritization, and Requirements Analysis
- Phase 2 - Solution Development and Risk Assessment
- Phase 3 - Security Engineering and Risk Assessment
- Phase 4 - Annual Risk Review

The process is slightly different for a Partner request being added to a new CDES solution vice an existing CDES solution. If the request is going to be added to an existing CDES solution, they will enter the CDES process at Phase 2. If the request is going to be met by a new CDES solution, they will enter the CDES process at Phase 1 and essentially will be going through Phase 1 twice, since they already went through the same Phase 1 as a point-to-point solution.

K.3.1 Phase 1 CDS Authorization Process: CDES

Validation, Prioritization, and Requirements Analysis

Phase 1 of the CDS process consists of six specific actions. Any exceptions to the CDS process must be coordinated with your CC/S/A representatives and Cross Domain Technical Advisory Board (CDTAB) chair. The first three actions must be completed in 45 days. In order for CDES to go forward with a request to build a new CDES solution, they must come forward with an already approved Partner request that is awaiting implementation in the Enterprise. This is because DSAWG will not approve building a new solution if there is not a Partner requirement for that solution.

1. CDES must coordinate with the DISA Cross Domain Solutions Organization (CDSE) representatives to determine and document the information transfer and mission requirements based on a previously approved Partner request. These requirements must be documented on the Cross Domain Appendix (CDA).
2. CDES opens a new CDS request in the SGS filling out all required database fields, uploads a Phase 1 Cross Domain Appendix (CDA), and notifies their CDSE of completion of these requirements.
3. The Partner's respective CDSE validates and prioritizes the Request and submits a CDSAP agenda request to the CDTAB Secretariat.

NOTE: Agenda requests will not be accepted by the CDTAB Secretariat directly from the Partner. All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Any late submissions will NOT be accepted.

4. The request is brought before the CDSAP to determine if a CDS is required to meet the Partner's requirement and if the proposed solution versus an alternative solution is recommended. This determination is then presented to the Community Jury in Step 5.
5. The CDES Request and CDSAP comments are brought before the Community Jury (a function of the DSAWG) to obtain approval for ticketing and engineering.
6. If approved by the Community Jury the CDS Team will assign a CDS Ticket Number and the CDES Request is transitioned into Phase II.

K.3.2 Phase 2 CDS Authorization Process: CDES

Security Engineering and Risk Assessment

NOTE: If the DoD Partner's request has already been approved by the Community Jury and is going to be added to preexisting CDES solution, the request will enter the CDES process at this phase (see 1.b).

1. New or Existing CDES:
   a. **New CDS:** CDES works with DISA CDSE to engineer the CDS, complete, and upload the following to the SGS:
      - Phase 2 CDA
      - ST&E Plan
      - ST&E Procedures

   NOTE: CDES should contact DISA CDSE if they have questions or need assistance with completing the required content in the referenced documents. CDES notifies the CDSE when all requirements have been met.

   b. **Existing CDS:** The DISA CDSE requests an updated ticket instance from the CDS Team. CDES works with DISA CDSE to engineer the CDS, complete, and upload the following to the SGS:
      - Phase II CDA
      - ST&E Plan
      - ST&E Procedures

NOTE: CDES should contact DISA CDSE if they have questions or need assistance with completing the required content in the referenced documents. CDES notifies the DISA CDSE when all requirements have been met.

2. DISA CDSE reviews and prioritizes the CDS ticket with NSA and the CDS Team who completes the bulk of the draft risk analysis report.

NOTE: Each CDSE must submit all requests for GCT ratings from the CDS Team no later than the first Monday of the month if they intend to bring the ticket before the CDTAB.

3. Draft Risk Analysis results are completed by NSA, the DISA CDSE, the CDS Team, and DIA following the Risk Decision Authority Criteria (RDAC) criteria. These results must be uploaded to SGS.
4. DISA CDSE submits a CDTAB agenda request to the CDTAB Secretariat.

NOTE: Agenda requests will not be accepted by the CDTAB Secretariat directly from the Partner. All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Any late submissions will NOT be accepted.

5. At the CDTAB the voting members will review the information provided from the Partner's CDA and the compiled risk rating and provide a vote of concur or non-concur with the risk rating.
6. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a CDSA for ST&E.
7. If approved and all other enclave documentation has met standard requirements, the CDS Team will issue a CDSA for ST&E and the CDS ticket transitions into Phase III.

K.3.3 Phase 3 CDS Authorization Process: CDES

ST&E Risk Review and Authorization for Operational Use

1. Upon completion of the ST&E CDES must upload the ST&E results and updated Phase III CDA to the SGS. CDES notifies the DISA CDSE of these actions.
2. The respective CDSE reviews the ST&E results to verify no changes exist between the Draft Risk Analysis and the actual test results. The CDSE must notify the CAO of any changes prior to ticket submission as an agenda request or initiation of a Cross Domain Solution Authorization for operational use.
3. If, in concurrence with Phase 2 approval, the DSAWG also granted approval for operational use, and the CDSE finds the ST&E result concur with the Draft Risk Analysis, the respective CDSE may request a CDSA from the CDS Team as per step 7. Otherwise, the respective CDSE submits a CDTAB agenda request to the CDTAB Secretariat.
4. DISA CDSE submits a CDTAB agenda request to the CDTAB Secretariat.

NOTE: All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the Partner.

5. At the CDTAB, the voting members will review the information provided from the CDES CDA and the compiled risk rating and provide a vote of concur or non-concur with the risk rating and comments.
6. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a 1-year CDSA.

7. If approved by the DSAWG, and all other enclave documentation has met standard requirements, the CDS Team will issue a 1-year CDSA. The CDS Ticket transitions into Phase IV.

NOTE: For a CDSA to be issued, the following items are required:

- Partner's Valid ATC for the enclave where CDS is operating
- DAA Signed CDA referencing CCSD by DAA (Phase 2 – IATC and Phase 3 – ATC) or enclave ATO referencing the CDS
- DAA signed SCQ referencing the CDS tickets
- Topology referencing the specific ticket number of the CDS.
- Signed CDA by DAA (Phase 2 – IATC and Phase 3 – ATC) or ATO signed by DAA. (For Non-DISN Connections)

NOTE: The CDS device is marked operational in SGS upon the initial issuance of a CDSA by the CDS Team following a DSAWG approval. It remains operational until the CDTAB Secretariat receives evidence from the DAA through the Partner's respective CDSE that the device is non-operational.

K.3.4 Phase 4 CDS Authorization Process: CDES

Annual Risk Review for CDES Solutions

CDS devices will receive no more than a one-year CDSA from the DSAWG. In order to receive additional operational approval the following requirements must be met:

1. Completion of a satisfactory scan of the enclave by the CAO and all necessary revalidation memorandums (see note below). Once these requirements are completed the mission partner must notify the CDSE that the CDS device is ready for review by CDTAB.

NOTE: All CDS devices require annual mission partner and enterprise DAA revalidation. The DAA owning the enclave where the CDS resides provides a revalidation memorandum stating that the configuration has not been changed since it was last approved and that it has been tested. The DAA of the hosting enclave cannot verify that the requirement still exists since they do not own the mission. Therefore each partner DAA on an enterprise CDS device will need to provide a revalidation memorandum stating they still need the channel/s to meet their mission needs. The mission statement must also be restated in each mission partner revalidation memorandum since some missions differ slightly over time. The responsible enterprise CDS service provider will manage the revalidation process for their respective enterprise guards by coordinating with the hosting enclave DAA and the mission partner DAAs to request the revalidation memorandums. The responsible enterprise CDS service provider will upload all revalidation memorandums in the SGS database under the respective ticket number.

2. DISA CDSE submits a CDTAB agenda request to the CDTAB Secretariat.

NOTE: All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the CDTAB Secretariat directly from the Partner.

3. At the CDTAB, the voting members will review the CDS Annual Review requirements, information provided extracted from the Partner's CDA and the previous risk rating, and provide a vote of concur or non-concur with the risk rating and comments.
4. The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a 1-year CDSA.
5. If approved by the DSAWG, and all other enclave documentation has met standard requirements, the CDS Team will issue a 1-year CDSA. The CDS Ticket will remain in Phase IV.

NOTE: For a CDSA to be issued, the following items are required:

- Partner's Valid ATC for the enclave where CDS is operating
- DAA Signed CDA referencing CCSD by DAA (Phase 2 – IATC and Phase 3 – ATC) or enclave ATO referencing the CDS
- DAA signed SCQ referencing the CDS tickets
- Topology referencing the specific ticket number of the CDS.
- Signed CDA by DAA (Phase 2 – IATC and Phase 3 – ATC) or ATO signed by DAA. (For Non-DISN Connections)

NOTE: Planned changes to the configuration of the CDS including patches and upgrades must be coordinated with the Partner's respective CDSE and entered into the SGS as Phase I requests. These requests must follow the normal CDS review process and be approved by the DSAWG prior to implementation.

NOTE: As the CDES approval process may open multiple Partner requests under one ticket, it is important to remember that each instantiation portion of a CDES ticket number represents an individual Partner Mission. Expiration of an individual instantiation of a CDES ticket should not be interpreted as the expiration of that guard, but instead the expiration of a Partner Mission. CDES should track these instantiations in order to ensure each Partner Mission is revalidated as its yearly approval approaches its expiration.

NOTE: If for any reason it becomes necessary to discontinue use of a CDS or a mission partner is no longer continuing their mission, the DISA CDSE must submit a closure request memo in order to stop tracking of the CDS ticket in SGS. The CDS analyst who performs the closure will upload the closure request to SGS under the ticket in question, and close the ticket with the comment "Closed per CDSE request".

K.4 Frequently Asked Questions

Q. Do I need to create a request for every CDS device/distribution console I intend to meet a specific requirement? What if it is a hot or cold spare or being used for load balancing?
A. A separate request/ticket is required for each CDS device/distribution console if the device is used as a hot spare or load balancing. A separate request is not needed for a cold spare but the cold spare must go through ST&E with the primary and evidence of the ST&E results must be uploaded under the SGS. In the event the cold spare is utilized, the CDSE and CDS Team must be notified and a new request must be opened.

Q. What is the significance of the three partitions of a CDS ticket number?
A. Once a Request (ex: R0001111) is approved at Community Jury, it is assigned a ticket number that is formatted in three partitions (ex: 1234-0001-001). The significance of these partitions is listed below:

a. First partition (*1234*-0001-001): The first partition represents the Partner requirement. If this is a new Partner requirement, the Request will receive a ticket number with a unique first partition; the second and third partitions will be 1.
b. Second partition (1234-*0001*-001): The second partition represents the instantiation of the CDS device. For example, if three CDS devices were needed for load balancing, the ticket numbers would be 1234-0001-001, 1234-0002-001, and 1234-0003-001. The configuration and Partner requirement is the same, but there are three devices meeting this requirement. These devices could be the same configuration at the same location or they could be the same configuration at three different locations.
c. Third partition (1234-0001-*001*): The third partition of the ticket number represents the iteration of the ticket. This number is usually created when a CDS Request is approved to change the configuration or upgrade a previous device. For CDES, this happens often due to the addition of new channels supporting new Partners. For example: If pre-existing ticket 1234-0001-001 were upgrading to the next version of RM, the newly assigned ticket number would be 1234-0001-002.

Q. What is the different between a CDSA and an ATC?

A. Once a DIACAP package is submitted, reviewed and accepted by the CAO an ATC for the CCSD is issued. The ATC contains the statement "This ATC does not authorize any Cross Domain Solutions, a Separate Cross Domain Solution Authorization Letter will be issued authorizing Cross Domains." A CDSA is issued after DSAWG approval of a CDS contingent upon a current ATC for the CCSD and the ATO, SCQ, and Topology properly referencing the CDS ticket number.

NOTE: The CDSA expiration date will not exceed the ATC expiration date if the ATC expires prior to the DSAWG approval expiration. Once a new ATC is issued, another CDSA will be issued for the remainder of the DSAWG approval window.

Q. What is the difference between a point-to-point solution and a DISA Cross Domain Enterprise Solution? Am I required to use Enterprise Services?

A For a point-to-point solution, a Partner has a requirement to pass data across security domains, places a request, and purchases their own Cross Domain device to facilitate the information transfer.

Cross Domain Enterprise Services (CDES) have systems that may be able to facilitate the Partner's information transfer requirement. One CDES CDS device could facilitate the transfer of multiple channels from multiple Partners. Partners are not required, but are strongly encouraged, to utilize DISA's CDES if their requirement can be met by a CDES Solution. To find out if your requirement could be met by DISA CDES, contact the DISA CDSE at cio-cdso2@disa.mil.

K.5 Points of Contact

All e-mail correspondence with the CDTAB Secretariat should to be sent to cdtab@disa.smil.mil.

CAO Cross Domain Solutions	
CDS Process Questions	cdtab@disa.smil.mil
Updated Enclave Paperwork[7]	cdtab@disa.smil.mil
Phone (Commercial)	301-225-2903
Phone (DSN)	312-375-2903
Website	www.disa.mil/connect

K.6 Additional Policy and Guidance Documents

CJCSI 6211.02D	*Defense Information Systems Network (DISN): Policy and Responsibilities*, 24 January 2012
DISA Charter	Cross Domain Technical Advisory Board, 18 April 2010
RDAC 2.3, NSA	Risk Decision Authority Criteria
DISA CPG v4.1	Cross Domain Solutions Appendix, September 2012
DoDD 5100.3	*Support of the Headquarters of Combatant and Subordinate Joint Commands,* 15 November 1999

[7] DIACAP paperwork with an ATO expiration date different from that reviewed upon issuance of your last ATC cannot be submitted to cdtab@disa.smil.mil. Please submit the complete DIACAP package to CCAO@disa.smil.mil.

This page intentionally left blank.

APPENDIX L

SME-PED – CLASSIFIED AND UNCLASSIFIED

L.1 SME-PED Description

The Secure Mobile Environment-Portable Electronic Device (SME-PED) is a DISN offering that provides the DoD with the capability that allows wireless NIPRNet and SIPRNet access, to include e-mail and web browsing, in one device. It also provides the user secure and non-secure voice capabilities. Organizations that implement SME-PED must ensure user procedures are in place for use, protection, and control of SME-PED devices.

Some of the service highlights are as follows:

- Converged secure/voice data product
- Secure and non-secure PDA functionality
- Unclassified and Secret secure data
- "Push E-mail" synchronized with desktop
- Secure and non-secure cellular phone functionality
- Unclassified and "up to" Top Secret secure voice
- Worldwide service capability - GSM/CDMA
- Data at rest - PIN and token

L.2 SME-PED Connection Process

Partners/sponsors that require access to the SME-PED service do not currently follow the connection process identified in this guide. Use of SME-PED is dependent on a SIPRNet connection at the local enclave. Implementation of the SME-PED service requires that a SME-PED server be added to the local SIPRNet enclave. The addition of a server to the local enclave requires an update to the site accreditation package. Once the enclave DAA has approved inclusion of SME-PED into the accreditation boundary, an updated accreditation package should be submitted to the DISA CAO.

L.3 Points of Contact

Connection Approval Office (CAO)	
Connection Approval Office for Unclassified Connections (UCAO)	disa.meade.ns.mbx.unclassified-connection-approval@mail.mil ucao@disa.smil.mil
Connection Approval Office for Classified Connections (CCAO	disa.meade.ns.mbx.classified-connection-approval@mail.mil

	ccao@disa.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901
Address	Defense Information Systems Agency ATTN: NSC1 PO Box 549 Fort Meade, MD20755-0549

SME-PED Program Office	
Phone (Commercial)	410-854-1408/1460/1932

L.4 Additional Policy and Guidance Documents

For more information on the SME-PED program, refer to the following website: http://www.disa.mil/services/smeped.html.

APPENDIX M

PRIVATE IP REGISTRATION IN SNAP

M.1 Private IP Service – Unclassified – Description

The DISN Private IP service provides an enterprise-wide solution to all DISN partners with a need to segregate their IP traffic from the traffic of other partners using multi-protocol Label Switching (MPLS) to create Virtual Private Networks (VPNs). The service is offered as a capability provided on the Non-Sensitive IP Router Network (NIPRNet). This service is an IP transport service only, as such, the connection process differs slightly from that normally required for connection to the Non-Sensitive IP Data Service (NIPRNet). The partner is required to register the VPN, and the connections to it, in the System/Network Approval Process (SNAP) database for tracking. The partner is responsible for ensuring that the appropriate CND capabilities and measures are being performed on the system/network associated with the VPN; based on measures to be provided by the DOD/CIO and/or USCYBERCOM. Private IP Service Connection Process

M.2 Complete the VPN registration in SNAP

- Select NIPR then VPN Registration/Select New or Previously registered
- Complete the mandatory fields within SNAP
- Select Create Registration to finalize the registration

NOTE: For 24/7 SNAP assistance; contact the DISN Global Support Center – (800) 554-3476

M.3 Documentation Requirements

The Partner must be able to upload the current topology diagram into SNAP when requesting the VPN.

- The VPN ID must be annotated on the diagram.
- ATO – Authority To Operate must be signed by the DAA.

APPENDIX N

DISA SERVICE MANAGER POINT OF CONTACT LIST

DISN Service	Information Type	Required Security Level	Connection Purpose (keywords)	Contact Information
Secret IP Data (SIPRNet)	Data	Classified	Operational, C2, Cross Domain Solutions, Narcotics, Anti-drug Network	301-225-4783 DSN (375)
Non-Classified IP Data/Non-Classified IP	Data	Unclassified	Operational, Non-C2	301-225-2083 DSN (761)
Dial-up, Internet Protocol (IP) and Dedicated Video Teleconferenci ng (DISN Video Services [DVS])	Video	Classified/ Unclassified	VTC capability, DVS-G	DISN Global Service Center (DGSC) (800) 554-DISN (3476), option 2 (614) 692-4790 DSN (312) 850-4790 DSN (510) 376-3472 DGSC@csd.disa.mil dvs@disa.smil.mil
Multilevel Secure Voice (Defense RED Switch Network [DRSN])	Voice	Classified	Secure voice, SME-PED, VoSIP, DRSN	DISA MCEP Program Office (301) 225-2718, DSN 375 (301) 225-2720, DSN 375 (301) 225-2696, DSN 375
Non-Classified IP Data/Non-Classified IP (Defense Switched Network [DSN])	Voice	Unclassified	VoIP, Unclassified Voice, DSN	(301) 225-2793, DSN 375-2793

DISN Service	Information Type	Required Security Level	Connection Purpose (keywords)	Contact Information
Secret Test and Evaluation (T&E) IP Data (DISN-Leading Edge Services [DISN-LES])	Data	Classified/ Unclassified	Test and Evaluation; R&D	301-225-2463 DSN (761)
UC (Unified Capabilities) IO and EoIP (Interoperability and Everything over IP)	Data	Classified/ Unclassified	Converged Voice Video, Data over IP	520-538-3234 312-879-3234
EMSS (Enhanced Mobile Satellite Services)	Voice, Data, Paging, Short Burst Data (SBD)	Unclassified, Classified	Operational, C2, Secure Voice	DISA/EMSS/DTCS emssprog@disa.mil (301) 225-2800, DSN: 312-375-2800 EMSS HelpDesk (24 x 7) DSN: (312) 282-1048 Toll Free: 1-877-449-0600 Remote: 4411 (from a working EMSS Handset) customer.service@gdc4s.com

DISN Service	Information Type	Required Security Level	Connection Purpose (keywords)	Contact Information
Organizational Messaging (Defense Message System [DMS])	Data	Unclassified, Classified	Messaging system, Plain Language Messaging, DMS Security Updates, Plain Language Address Distribution System (PLADS), DMS Asset Distribution System (DADS)	(301) 225-2759 DSN (375)

Non-DISN Service	Description	Contact Information
DREN/DREN-S (Defense Research and Eng. Network)	Non-DISN Network; provide contact info	703-812-8205 http://www.hpcmo.hpc.mil/Htdocs/DREN/dren-sa.html
MDA (Missile Defense Agency)	Ask partner if connection requires connection to the DISN: If NO, then provide contact info If YES, then follow guidance above to determine which DISN SM should receive this request	703-882-6944 703-882-6906

DISN Connection Process Guide	Description	Contact Information
CPG	Frequently Asked Questions (FAQ)	www.disa.mil/connect

APPENDIX O

REFERENCES

Reference Number	Title
(a) CJCSI 6211.02D	*Defense Information Systems Network (DISN): Responsibilities*, 24 January 2012 http://www.dtic.mil/cjcs_directives/
(c) DoDD 8500.01E	*Information Assurance (IA)*, 24 October 2002 http://www.dtic.mil/whs/directives/
(d) DoDD O-8530.1	*Computer Network Defense,* 8 January 2001 http://www.dtic.mil/whs/directives/
(e) DoDI 8100.04	*Department of Defense (DoD) Unified Capabilities (UC)*, 9 December 2010 http://www.dtic.mil/whs/directives/
(f) DoDI 8500.2	*Information Assurance (IA) Implementation*, 6 February 2003 http://www.dtic.mil/whs/directives/
(g) DoDI 8510.01	*DoD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 November 2007 http://www.dtic.mil/whs/directives/
(h) DoDI O-8530.2	*Support to Computer Network Defense (CND),* 9 March 2001 http://www.dtic.mil/whs/directives/
(i) CJCSI 6212.02F	*Net Ready Key Performance Parameters (NR KPP)*, 21 March 2012 http://www.dtic.mil/cjcs_directives/
(j) DoDI 8551. 1	*Ports, Protocols, and Services Management*, 13 August 2004 http://www.dtic.mil/whs/directives/
(k) CNSSI 4009	*National Information Assurance Glossary*, June 2006 http://www.cnss.gov/full-index.html
(l) UCR Change III	*Department of Defense Unified Capabilities Requirements 2008*, December 2008 (signed September 2011) http://www.disa.mil/ucco/
(m) DoDD 8000.01	*Management of the Department of Defense Information Enterprise,* 10 February 2009 http://www.dtic.mil/whs/directives/
(n) DoDI 8100.4	*DoD Unified Capabilities*, 9 December 2010 http://www.dtic.mil/whs/directives/
(o) CNSSI 1253	*Security Categorization and Control Selection for National Security Systems,* October 2009 www.cnss.gov/Assets/pdf/CNSSI-1253.pdf

Reference Number	Title
(p) DoD 5220.22-M	*National Industrial Security Program Operating Manual*, 28 February 2006 www.dss.mil/isp/odaa/nispom06.html
(q) DoD CIO Office Sponsor Memorandum	*Responsibilities of DoD Components Sponsoring Mission Partner Connections to DISN-Provided Transport Infrastructure*, 11 January 2012 http://www.disa.mil/Services/Network-Services/~/media/Files/DISA/Services/DISN-Connect/Policy/DoD-CIO-Memorandum-Connection-Approval-Office.pdf
(r) NIST SP 800-37 Rev 1	*Guide for Applying Risk Management Framework to Federal Information Systems*, February 2010 http://csrc.nist.gov/publications/PubsSPs.html
(s) DoD 5220.22M	*National Industrial Security Program Operating Manual*, 28 February 2006
(t) CJCSI DoDI 4630.8	*Procedures for Interoperability and Support of Information Technology and National Security Systems*, 30 June 2004
(u) DoDI 4630.8	*Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004
(v) DoDD 8100.02	*Use of Commercial Wirelese Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2007*

APPENDIX P
ACRONYMS

Acronym	Definition
AA	Accrediting Authority
AAD	Access Approval Document
AIS	Automated Information System
APL	Approved Products List
ASN	Autonomous System Number
ATC	Approval to Connect
ATD	Authorization Termination Date
ATO	Authorization to Operate
BD	Business Development
C&A	Certification & Accreditation
CA	Certifying Authority
CAO	Connection Approval Office
CAP	Connection Approval Process
CC/S/A	Combatant Command, Service, or Agency
CCAO	Classified Connection Approval Office (now referred to as CAO)
CCSD	Command Communications Service Designator
CDA	Cross Domain Appendix
CDRB	Cross Domain Resolution Board
CDS	Cross Domain Solution
CDSAP	Cross Domain Solutions Assessment Panel
CDSE	Cross Domain Solutions Organization
CDTAB	Cross Domain Technical Advisory Board
CIO	Chief Information Officer
CND	Computer Network Defense
CNDS	Computer Network Defense Services
CNDSP	Computer Network Defense Service Provider

Acronym	Definition
COCOM	Combatant Command
CODEC	Coder-Decoder
COMSEC	Communications Security
COTS	Commercial Off-The-Shelf
CPG	Connection Process Guide
CTM	Consent to Monitor
CTO	Communications Tasking Order
DAA	Designated Accrediting Authority
DADS	DMS Asset Distribution System
DATC	Denial of Approval to Connect
DCCC	DISA Partner Contact Center
DDOE	DISA Direct Order Entry
DECC	DISA Defense Enterprise Computing Center
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISN-LES	Defense Information Systems Network - Leading Edge Services
DITPR	DoD Information Technology Portfolio Repository
DMS	Defense Messaging System
DMZ	Demilitarized Zone
DoD	Department of Defense
DREN	Defense Research and Engineering Network
DRSN	Defense Red Switch Network
DSAWG	Defense IA/Security Accreditation Working Group
DSN	Defense Switched Network
DSS	Defense Security Service
DVS	DISN Video Services
DVS-G	DISN Vide Services – Global
DVS-WS	DISN Video Services – Web Site

Acronym	Definition
EMSS	Enhanced Mobile Satellite Services
EoIP	Everything over Internet Protocol
FOUO	For Official Use Only
FRAGO	Fragmentary Order
FSO	Field Security Operations
GCA	Government Contracting Authority
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
IA	Information Assurance
IATC	Interim Approval to Connect
IATO	Interim Authorization to Operate
IATT	Interim Authorization to Test
IC	Intelligence Community
ICTO	Interim Certificate to Operate
IDS	Intrusion Detection System
IMUX	Inverse Multiplexer
INFOSEC	Information Security
IO	Interoperability
IOS	Internetworking Operating System
IP	Internet Protocol
IS	Information Systems
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISSE	Information System Security Engineering
JITC	Joint Interoperability Test Command
LAN	Local Area Network
MCU	Multipoint Control Unit
MDA	Missile Defense Agency
MHS	Military Health System

Acronym	Definition
MSL	Multiple Security Level
NA	Not Applicable
NC	Non-Compliant
NIAP	National Information Assurance Partnership
NIC	Network Information Center
NIPRNet	Non-classified Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NS/EP	National Security/Emergency Preparedness
DOD CIO	Office of the Assistant Secretary of Defense for Networks and Information Integration
OSD	Office of the Secretary of Defense
OTAR	Over The Air Rekey
OWA	Outlook Web Access
PDC	Program Designator Code
PLADS	Plain Language Address Distribution System (PLADS)
PO	Program Office
POA&M	Plan of Action & Milestones
POC	Point of Contact
PPSM	Ports, Protocols, and Services Management
RDAC	Risk Decision Authority Criteria
RFS	Request for Service
RTS	Real Time Services
SBD	Short Burst Data
SCQ	SIPRNet Connection Questionnaire
SDP	Service Delivery Point
SGS	SIPRNet GIAP System
SIP	System Identification Profile

Acronym	Definition
SIPRNet	Secret Internet Protocol Router Network
SM	Service Manager
SME	Subject Matter Expert
SME-PED	Secure Mobile Environment-Portable Electronic Device
SMO	Service Management Office
SNAP	System/Network Approval Process
SSAA	System Security Authorization Agreement
SSC	SIPRNet Support Center
SSE	System Security Engineer
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guide
TCO	Telecommunications Certification Office
TR	Telecommunications Request
TS	Top Secret
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
UC	Unified Capabilities
UCAO	Unclassified Connection Approval Office (now referred to as CAO)
UCDMO	Unified Cross Domain Management Office
USCC	USCYBERCOM
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
VOC	Video Operations Center
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VPL	Validated Product List
VPL	Virtual Private LAN
VTF	Video Teleconferencing Facility
WAN	Wide Area Network

This page intentionally left blank.

APPENDIX Q
GLOSSARY

Term	Definition
Accreditation Decision	A formal statement by a designated accrediting authority (DAA) regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO). The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD public key infrastructure (PKI)-certified digital signature. (Ref g)
Approval to Connect (ATC)	A formal statement by the Connection Approval Office granting approval for an IS to connect to the DISN. The ATC cannot be granted for longer than the period of validity of the associated ATO. An ATO may be issued for up to 3 years. An ATC will not be granted based on an IATO.
Artifacts	System policies, documentation, plans, test procedures, test results, and other evidence that express or enforce the information assurance (IA) posture of the DoD IS, make up the certification and accreditation (C&A) information, and provide evidence of compliance with the assigned IA controls. (Ref g)
Authorization to Operate (ATO)	Authorization granted by a DAA for a DoD IS to process, store, or transmit information; an ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to three (3) years. (Ref g)
Authorization Termination Date (ATD)	The date assigned by the DAA that indicates when an ATO, IATO, or IATT expires. (Ref g)
Connection Approval Process (CAP)	Packages provide the CAO the information necessary to make the connection approval decision.
Certification	A comprehensive evaluation and validation of a DoD IS to establish the degree to which it complies with assigned IA controls based on standardized procedures. (Ref g)
Certification Determination	A CA's determination of the degree to which a system complies with assigned IA controls based on validation results. It identifies and assesses the residual risk with operating a system and the costs to correct or mitigate IA security weaknesses as documented in the Information Technology (IT) Security Plan of Action and Milestones (POA&M). (Ref g)

Term	Definition
Certifying Authority (CA)	The senior official having the authority and responsibility for the certification of Information Systems governed by a DoD Component IA program.
Consent to Monitor (CTM)	This is the agreement signed by the DAA granting DISA permission to periodically monitor the connection and assess the level of compliance with IA policy and guidelines.
Connection Approval Process	Formal process for adjudication requests to interconnect information systems.
Connection Approval Office (CAO)	Single point of contact within DISA for all DISN connection approval requests.
Command Communications Service Designator (CCSD)	A unique identifier for each single service including use circuits, package system circuits, and interswitch trunk circuits.
Computer Network Defense (CND)	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.
Computer Network Defense Service Provider (CNDSP)	Required by policy to establish or provide for Computer Network Defense Services (CNDS). Support and coordinate the planning and execution of CND, develop national requirements for CND, and serve as the Accrediting Authority (AA) for the CNDS Certification Authorities (CNDS/CA).
Cross Domain Appendix (CDA)	In support of the C&A of a CDS, this appendix defines the security requirements, technical solution, testing, and compliance information applicable to the cross-domain connection.
Cross Domain Solution (CDS)	A form of controlled interface that provides the capability to manually and/or automatically access and/or transfer information between different security domains and enforce their security policies. (Ref k)
Connection Process Guide (CPG)	Step-by-step guide to the detailed procedures that Partners must follow in order to obtain and retain connections to the DISN.
Defense Information Systems Network (DISN)	DoD integrated network, centrally managed and configured to provide long-haul information transfer for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery and video teleconferencing services.

Term	Definition
Defense Information Systems Network-Leading Edge Services (DISN-LES)	Defense Information Systems Network-Leading Edge Services (DISN-LES) is a Mission Assurance Category III program designed to pass encrypted unclassified and classified traffic over the Classified Provider Edge (CPE) routers of the DISN, and provide capability for subscriber sites requiring "next generation" network, encryption, software, NETOPS, and advanced services not offered by other DISN Subscription Services (DSS). The network provides a non-command-and-control, risk aware infrastructure identical to the core DISN data services (NIPRNet and SIPRNet).
Denial of Approval to Connect (DATC)	A formal statement by the Connection Approval Office withholding (in the case of a new connection request) or rescinding (in the case of an reaccreditation connection) approval for an IS to connect (or remain connected) to the DISN.
Denial of Authorization to Operate (DATO)	A DAA decision that a DoD IS cannot operate because of an inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted. (Ref g)
Designated Accrediting Authority (DAA)	The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approving authority and delegated accrediting authority. (Ref g)
DISA Defense Enterprise Computing Center (DECC)	Services provided within a backdrop of world-class computing facilities located in both the continental United States (CONUS) and outside of the continental United States (OCONUS
Defense Information Assurance Certification and Accreditation Process (DIACAP)	The DoD processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, Federal and DoD requirements.
Defense IA/Security Accreditation Working Group (DSAWG)	Provides, interprets, and approves DISN security policy, guides architecture development, and recommends accreditation decisions to the DISN Flag panel. Also reviews and approves Cross Domain information transfers (as delegated from the DISN/GIG Flag Panel) or forwards such recommendation(s) to the Flag Panel.

Term	Definition
DIACAP Scorecard	A summary report that succinctly conveys information on the IA posture of a DoD IS in a format that can be exchanged electronically; it shows the implementation status of a DoD Information System's assigned IA controls (i.e., compliant (C), non compliant (NC), or not applicable (NA)) as well as the C&A status. (Ref g)
Demilitarized Zone (DMZ)	Physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
Defense Information Systems Agency (DISA) Direct Order Entry(DDOE)	This is the ordering tool for DISN telecommunications services.
DoD Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. It includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections. (Ref c)
DoD Partner	DoD Combatant Commands, Military Services and Organizations, Agencies, and Field Activities (CC/S/A), which are collectively referred to as DoD Components.
DoD Unified Capabilities (UC) Approved Products List (APL)	Is established in response to DoDI 8100.04 DoD Unified Capabilities (UC) and the Unified Capabilities Requirements (UCR Change III September 2011). Its purpose is to provide Interoperability (IO) and Information Assurance (IA) certified products for DoD Components to acquire and to assist them in gaining approval to connect to DoD networks in accordance with policy.
Field Security Operations (FSO)	Produces and deploys information assurance (IA) products, services, and capabilities to combatant commands, services, and agencies to protect and defend the Global Information Grid (GIG).
GIG Interconnection Approval Process (GIAP)	Electronic process to submit connection information and register a GIG connection.
Information Assurance (IA)	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Ref c)
IA Certification and Accreditation	The standard DoD approach for identifying information security requirements, providing security solutions and managing the security of DoD information systems. (Ref c)

Term	Definition
Information Systems (IS)	Computer-based information systems are complementary networks of hardware/software that people and organizations use to collect, filter, process, create, and distribute data.
Interim Approval to Connect (IATC)	Temporary approval granted by the Connection Approval Office for the connection of an IS to the DISN under the conditions or constraints enumerated in the connection approval.
Interim Authorization to Operate (IATO)	Temporary authorization granted by the DAA to operate a DoD information system under the conditions or constraints enumerated in the accreditation decision. (Ref g)
Interim Authorization to Test (IATT)	A temporary authorization to test a DoD IS in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the accreditation decision. (Ref g)
Interim Certificate to Operate (ICTO)	Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO will be made by the MCEB Interoperability Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.
Internet Protocol (IP)	Protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.
Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (Ref i)
Mission Partners	Those with whom Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments, allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.

Term	Definition
Non-DoD Partner	All organizations and entities that are not components of the Department of Defense; this includes contractors and federally funded research and development centers; other USG federal departments and agencies; state, local, and tribal governments; foreign government organizations/ entities (e.g., allies or coalition partners); non-government organizations; commercial companies and industry; academia (e.g., universities, colleges, or research and development centers); etc. (Ref a)
Plan of Action & Milestones (POA&M)	A permanent record that identifies tasks to be accomplished in order to resolve security weaknesses; required for any accreditation decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks; also used to document DAA-accepted non-compliant IA controls and baseline IA controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed. (Ref g)
Program or System Manager (PM or SM)	The individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs. (Ref g)
Request For Service (RFS)	The document, used to initially request telecommunications service, which is submitted by the requester of the service to his designated TCO.
Service Delivery Point (SDP)	The point at which a user connects to the DISN. The DISN provides IA controls up to the SDP. The Partner/user is responsible for IA controls outside of the SDP.
System Identification Profile (SIP)	A compiled list of system characteristics or qualities required to register an IS with the governing DoD Component IA program. (Ref g)
Telecommunications Certification Office (TCO)	The activity designated by a Federal department or agency to certify to DISA (as an operating agency of the National Communications System) that a specified telecommunications service or facility is a validated, coordinated, and approved requirement of the department or agency, and that the department or agency is prepared to pay mutually acceptable costs involved in the fulfillment of the requirement.
Telecommunications Service Order (TSO)	The authorization from Headquarters, DISA, a DISA area, or DISA-DSC to start, change, or discontinue circuits or trunks and to effect administrative changes.

Term	Definition
Telecommunications Service Request (TSR)	Telecommunications requirement prepared in accordance with chapter 3, DISAC 310-130-1 and submitted to DISA or DISA activities for fulfillment. A TSR may not be issued except by a specifically authorized TCO.
Unified Capabilities (UC)	The seamless integration of voice, video, and data applications services delivered ubiquitously across a secure and highly available Internet Protocol (IP) infrastructure to provide increased mission effectiveness to the warfighter and business communities. UC integrate standards-based communication and collaboration services including, but not limited to, the following: messaging; voice, video and Web conferencing; Presence; and UC clients. (Ref k)
Unified Cross Domain Management Office (UCDMO)	The UCDMO provides centralized coordination and oversight of all cross-domain initiatives across the Department of Defense and the Intelligence Community.
Virtual Private LAN (VPL)	Means to provide Ethernet-based multipoint-to-multipoint communication over IP/MPLS networks.
Wide Area Network (WAN)	A computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries).

Defense Information Systems Agency
Enterprise Connection Division (NSC)
Post Office Box 549
Fort Meade, Maryland 20755-0549
www.disa.mil/connect

http://www.disa.mil/Services/Network-Services/DISN-Connection-Process