DEFENSE INFORMATION SYSTEM NETWORK (DISN)
CONNECTION PROCESS GUIDE (CPG)

Risk Adjudication & Connection Division
Connecting the Warfighter
DISN Connection Approval
Defense Security/Cybersecurity-
Authorization Working Group (DSAWG)
Ports, Protocols, & Services Management (PPSM)

Version 6.1 August *2023*

Defense Information Systems Agency
Enterprise Integration and Innovation Center (EIIC)
Risk Management Directorate (RE)
Risk Adjudication and Connection Division (RE4)
Post Office Box 549
Fort Meade, Maryland 20755-0549
https://cyber.mil/connect/connection-approval/

UNCLASSIFED

This page intentionally left blank.

EXECUTIVE SUMMARY

The Defense Information System Network (DISN) Connection Process Guide (DCPG) implements responsibilities assigned to the Director of DISA in the Department of Defense Instruction (DoDI) 8010.01, *DODIN Transport* and DoDI 8500.01, *Cybersecurity* to oversee and maintain the DISN connection approval process. In addition, this document also provides the necessary requirements and processes established by Chairman of the Joint Chief of Staff Instruction (CJCSI) 6211.02D *Defense Information System Network (DISN) Responsibilities*, which states that all connections to the DISN shall be in accordance with (IAW) this DCPG.

DoDI 8010.01 defines DISN as:
"DoD's enterprise capability of DoD-owned and -leased telecommunications and computing subsystems, networks, and capabilities, centrally managed and configured by DISA, to provide an integrated network with cybersecurity, telecommunication, computing, and application services and capabilities (e.g., voice, video, teleconferencing, computing, imagery, satellite, and data services) for all DoD activities and their authorized mission partners."

The goal of the DCPG is to describe a process that will help the warfighter, DoD Components, and DoD Mission Partners obtain DISN services while ensuring DISA effectively tracks and securely manages connections to the DISN.

The DCPG complies with current version of the DoD policies listed in the References Section (Appendix N) and does not establish DoD policy.

The DISA Public Affairs Office approved this DCPG for public release. The current DCPG is available on the Internet from the DISA website:

https://cyber.mil/connect/connection-approval/

The instructions in this guide are effective immediately. Major updates shall be approved by DoD CIO. Interim updates to this guide (e.g., Version 6.1) shall be issued as required by the DISA Risk Management Executive/Authorizing Official.

Underlined text indicates a hyperlink to other Sections of the DCPG. To navigate a hyperlink to a reference, definition, or point of contact:

- Position your cursor over the hyperlink, press and hold the "CTRL" key on your keyboard, then click the left-mouse-button
- **To return to the text, press and hold the "ALT" key then press the left-arrow-key on the keyboard. (This makes navigating the DCPG very simple.)**

Sections 1 and 2 of the DCPG provides guidance for the end-to-end life cycle processes of the connection requirement. The Appendices provide additional detailed guidance and necessary information associated with respective portions of the life cycle of the connection requirement and allows customers to focus on those areas of the process most relevant to their needs.

Please send suggestions for improving the DCPG to the DISN Connection Approval Office (CAO).

DISN CONNECTION PROCESS GUIDE

Approvals:

____

MATTHEW A. HEIN Date

Chief, DISA Risk Adjudication and Connection
Division

____

ROGER S. GREENWELL Date

Risk Management Executive
Authorizing Official

____

JOHN B. SHERMAN Date

Principal Deputy, Department of Defense
Chief Information Officer

REVISION HISTORY

DISA will review and update this guide as directed or as needed. The revision history table reflects critical and substantive changes. The Revision History starts with Version 5.0 release.

Version	Date	Comments
5.0	November 2014	Provided connection approval requirement information related to the transition to RMF from DIACAP. Added DoD RMF terms and references. Added statement that DISN connection approval requirements will follow the DoD CIO published DIACAP to RMF timeline and instructions. Deleted Defense Red Switch Network (DRSN) now Multilevel Secure Voice. Deleted DISN Video Services (DVS). Added DODIN and DISN clarification. Added discussion on the NIPRNet Federated Gateway (NFG), Secret Internet Protocol Router Network (SIPRNet) Releasable De-Militarized Zone (REL DMZ), and SIPRNet Federal DMZ (FED DMZ). Removed previous language regarding the DISN CAO performing risk assessments. Added guidance on the requirements to update SNAP/SGS Points of Contact (POC). Updated Remote Compliance Monitoring (RCM) scanning procedures. Added DoDI 8551.01, PPSM declaration requirement. Updated references. Revised Cross Domain Solutions (CDS) appendix and process diagrams. Added the Validation Official's requirements.
5.1	May 2016	Revisions in this interim update include: ▪ Incorporates Joint Staff J6 and UCDSMO comments ▪ Reflects DISA's reorganization ▪ Aligns with terminology in recent DoD issuances ▪ Cybersecurity Service Provider Compliance ▪ Required RMF documents and artifacts ▪ Approval to Connect renewal with continuous monitoring ▪ SIPRNet FED DMZ update ▪ NFG connection process ▪ JRSS Accreditation ▪ References the DoD Cloud Computing Connection Guide ▪ Virtual Private Network (VPN) registration ▪ Initial Connection scans ▪ CDS Approval Process update ▪ References are updated ▪ Transition from legacy Time Division Multiplexing (TDM) to IP-based solutions ▪ Revised timeline for transition to RMF (DoDI 8510.01, change 1) ▪ Incorporates Defense Security/Cybersecurity Authorization Working Group (DSAWG) member recommendations

6.0	May 2021	This is a major update and includes the following changes: ▪ Incorporates guidance in DoDI 8010.01, DODIN Transport ▪ Figure 1 in Section 2 of this guide illustrates the revised procedures for registration, connection, sustainment, and discontinuation of DISN services - process variations are addressed in the appendices ▪ Incorporates the DoD CIO processes for reviewing requests for temporary exceptions to policy and for approving Mission Partner Connections to DISN (Appendices A, B, and M) ▪ Incorporates the DoD Cloud Information Technology Project (C-ITP) registration and connection process (Appendix C) ▪ Incorporates the DoD Cloud Service Offering (CSO) authorization, registration, and connection process (Appendix D) ▪ Includes a process for reviewing Point-to-Point (P2P) Cross Domain Solutions (CDS) exemption requests (Appendix G) ▪ Revised appendix on Mission Partner Gateway (e.g., SIPRNet FED DMZ and NFG) connection processes (Appendix H) ▪ Revised Section on Remote Compliance Monitoring (scanning) (Appendix J) ▪ DoD CIO approves this major update (e.g., Version 6.0) to the DCPG, and the DISA Risk Management Executive/Authorizing Official shall issue interim updates (e.g., Version 6.1) as required ▪ Includes hyperlinks to the related references, points of contact, and glossary

6.1	March 2023	This is an interim update that includes the following changes: ▪ Updated seal, DISA Office designations, version number and release year on cover page and footers. ▪ Corrected text color in footnote 1, and punctuation in footnote 3. ▪ Section 2.8, 2.10, 2.11, 2.15.3, H.2.3, H.3 - Removed references to Interim Approval to Connect (IATC) and removed the 180-day limit in Section 2.10.2 setting an ATO with conditions connectivity for up to one year ▪ Section 2.7.2 corrected spelling of register to registers ▪ Section 2.7.3 corrected PPSM references from RE42 to RE41 ▪ Section 2.8.2 corrected SNAP menu for “New Registration” ▪ Section 2.8.3.3 corrected VPN Owner to VPN Customer ▪ Section 2.9.h corrected point of contact from Compliance Monitoring Team (CMT) to Connection Approval Office (CAO) ▪ Section 2.16.2 corrected from a TSR to TSO

		Corrected links in Appendix L and Appendix N ▪ Updated and verified all references and contact information Corrected punctuation and spelling issues Clarified statements and definitions ▪ “in order to” changed to “to” ▪ “whether or not” changed to “whether” ▪ “make a decision” changed to “decide” Removed all references to the Enterprise Architecture and Services Board (EASB)

LIST OF FIGURES

LIST OF TABLES

CONTENTS

This page intentionally left blank.

1 INTRODUCTION

1.1 Purpose

Establishing and sustaining the cybersecurity of the DODIN is one of the most serious challenges facing DoD and our Mission Partners. The DISN connection approval process significantly influences the continued availability, reliability, and performance of DISN services for all DoD. The DISN Connection Process Guide (DCPG) outlines procedures DoD Components and Mission Partners follow to obtain and retain an enclave or network connection to the DISN that helps protect the DODIN as a whole. The DCPG does not establish policy, instead it is a guide for ensuring due diligence that all appropriate policies, procedures, and guidelines are followed when connecting a DoD Component or Mission Partner enclave or network to DISN.

> *"The Defense Information System Network (DISN) is the core element of DODIN transport. All connections to the DISN, including DoD Component and mission partner systems connected to DISN gateways, must be implemented and registered in the DODIN tracking and management repository in accordance with the DISN Connection Process Guide (DCPG) and DISN Cloud Connection Process Guide (DCCPG)."* DoDI 8010.01, DODIN Transport

1.2 Authorities

The DCPG implements portions of the following issuances[1] related to DISN connections:

- DoDD 5105.19, Defense Information Systems Agency
- DoDD 5144.02, DoD Chief Information Officer
- DoDI 5000.02T, Operation of the Defense Acquisition System
- DoDI 5000.74, Defense Acquisition Services
- DoDI 8010.01, DODIN Transport
- DoDI 8100.04, DoD Unified Capabilities (UC)
- DoDI 8500.01, Cybersecurity
- DoDI 8510.01, Risk Management Framework for DoD Information Technology (IT)
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- DoDI 8540.01, Cross Domain (CD) Policy
- DoDI 8551.01, Ports, Protocols, and Services Management (PPSM)
- CJCSI 6211.02D, Defense Information System Network (DISN): Responsibilities
- DoD CIO Memorandum, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services
- DoD Cloud Computing Security Requirements Guide (CC SRG)

1.3 General Guidance

The DISN Connection Process Guide (DCPG) is a living document that continues to evolve as processes are refined and as additional networks/services become available. Always check for

[1] Underlined text indicates a hyperlink to Appendix L – Points of Contact, Appendix N - References, Appendix P - Glossary. To navigate the hyperlinks: Position your cursor over the hyperlink, press and hold the "CTRL" key on your keyboard, then click the left-mouse-button. To return to the text, press and hold the "ALT" key then press the left-arrow-key on the keyboard...

the current version of the DCPG. This version of the DCPG focuses on connections to DISN services summarized below in Table 1.

DISN Services	Examples
Internet Protocol (IP)-based Data Services	Sensitive but Unclassified IP Data Service (aka NIPRNet), Secret IP Data Service (aka SIPRNet), Top Secret (TS)/Sensitive Compartmented Information (SCI) IP Data Service (aka JWICS[2])
Virtual Private Network (VPN) Services	Common Mission Network Transport (CMNT), DISN Test and Evaluation Service, Medical Community of Interest (MEDCOI) VPN, Private Data Internet Service Provider (ISP), Private IP Service
Defense Switched Network (DSN) and Unified Capabilities	Sensitive but Unclassified Voice Service, Top Secret SCI voice service, Multilevel secure voice, Public Switched Telephone Network (PSTN) Access, circuit switched or IP-based video services
Satellite Services	Distributed Tactical Communications System (DTCS), Inmarsat, Commercial Satellite Services, and Enhanced Mobile Satellite
Cross Domain Solutions	Controlled interfaces that provide the ability to manually or automatically access or transfer information between different security domains using capabilities such as file transfer, web services, Email
Joint Regional Security Stack (JRSS)	A suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, virtual routing and forwarding, and provides other network security capabilities. Centralizes security of the network into regional architectures instead of locally distributing cybersecurity suites at each military base, post, camp, or station.
DoD cloud computing services	Guidance for registration and connection of a DoD Cloud Information Technology Project or Cloud Service Offering via the DISN.

Table 1 DISN services addressed in this guide

1.4 Scope

This guide applies to all DoD Component and Mission Partner enclave owners seeking to connect to the DISN or DoD-authorized cloud computing services.

[2] DIA Directive (DIAD) 8550.500 documents the JWICS connection process.

2 DISN CONNECTION PROCESS

This version of the DCPG consolidates the connection processes for DISN and DoD cloud computing services into one document, helps customers understand connection requirements and timelines, and provides contacts for assistance throughout the process. Figure 1 depicts the DISN connection process. Where appropriate, this guide refers customers to related websites and points of contact. The connection process described in this Section of the guide applies to all DISN services. The appendices listed in Table 2 supplement Section 2 of this guide by providing supporting information and tailored guidance unique to individual DISN customers and services. Any type of connection or service that involves unified capabilities must comply with DoDI 8100.4 requirements.

Information and Tailored Guidance for:	Appendix
DoD CIO Approval of Requests for Alternatives to DISN and Cloud Enterprise Services	Appendix A
DoD CIO Approval of Mission Partner Connections to DISN	Appendix B
Cloud Information Technology Project (C-ITP) Registration and Connection Process	Appendix C
Cloud Service Offering (CSO) Registration and Connection Process	Appendix D
Topology Diagram Requirements	Appendix E
Registering Tactical, DSN, and UC Service Requirements	Appendix F
DoD Cross Domain Solution Approval Process	Appendix G
Connections to DISN Mission Partner Gateways	Appendix H
Consent to Monitor Agreement	Appendix I
Remote Compliance Monitoring (Scans)	Appendix J
Virtual Private Network (VPN) Registration (Private IP)	Appendix K
Validation Letter for Mission Partner Connections to DISN	Appendix M

Table 2 Registration and Connection Process Information and Tailored Guidance

NOTE: Proceed to Section 2.6 of this guide if renewing an existing DISN connection.

2.1 The DoD Component lead identifies the Customer and the Required Service

The DoD Component first determines the required service and if the DoD Component or the DoD Component's Mission Partner will use the service.

The DISN services catalog is the portal that lists and describes available DISN and DISA-provided services.

2.2 Is DoD CIO Approval Required?

Connections made that are not compliant with DoD policy and this guide or do not have a valid DoD CIO waiver are not authorized, will be reported to JFHQ-DODIN for disconnection, and may jeopardize approval of other complicit DISN or DODIN connections.

2.2.1 Is this a request to use a commercial alternative to DISN-provided transport, non-compliant cloud service, or unapproved cloud access point?

IAW DoDI 8010.01, DODIN Transport paragraph 4.4.a requires DoD CIO review and approval of a DoD Component request for - "commercial transport services procured as an alternative to DISN-provided transport."

In addition, paragraph 4.5 in DoDI 8010.01 requires a connection to a Cloud Service Offering (CSO) to be "implemented in accordance with the CC SRG." DoD CIO approval is required before using a cloud service that does not comply with the CC SRG or for the use of a Cloud Access Point that has not been approved by the DoD CIO.

If the desired service requires DoD CIO approval, proceed to Appendix A of this guide.

2.2.2 Is this a request for a Mission Partner[3] Connection to DISN?

DoDI 8010.01 paragraph 2.1.g states that the DoD Chief Information Officer (CIO) - "Reviews and approves DoD Component requests for mission partner connections to DISN."

If the request is for a mission partner connection to the DISN, then proceed to Appendix B of this guide that describes the DoD CIO process for approving a mission partner connection to the DISN.

2.3 Is this a request for a cloud computing connection?

DISA is currently integrating cloud computing services into the DISN provisioning process. For this version of the DCPG, proceed to Appendix C that documents the procedures for authorization, registration, connection, sustainment, and discontinuation of a Cloud Computing connection to DISN.

[3] Mission Partner – "Those with whom DoD 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." (DoDD 8000.01)

2.4 The DoD Component requests the required DISN service

Only a DoD Component can initiate a request for a DISN connection either for the DoD Component or for a Mission Partner. The DoD Component uses DISA StoreFront (DSF) to order DISN services available in DSF or use the “How to Order” link in the DISN services catalog.

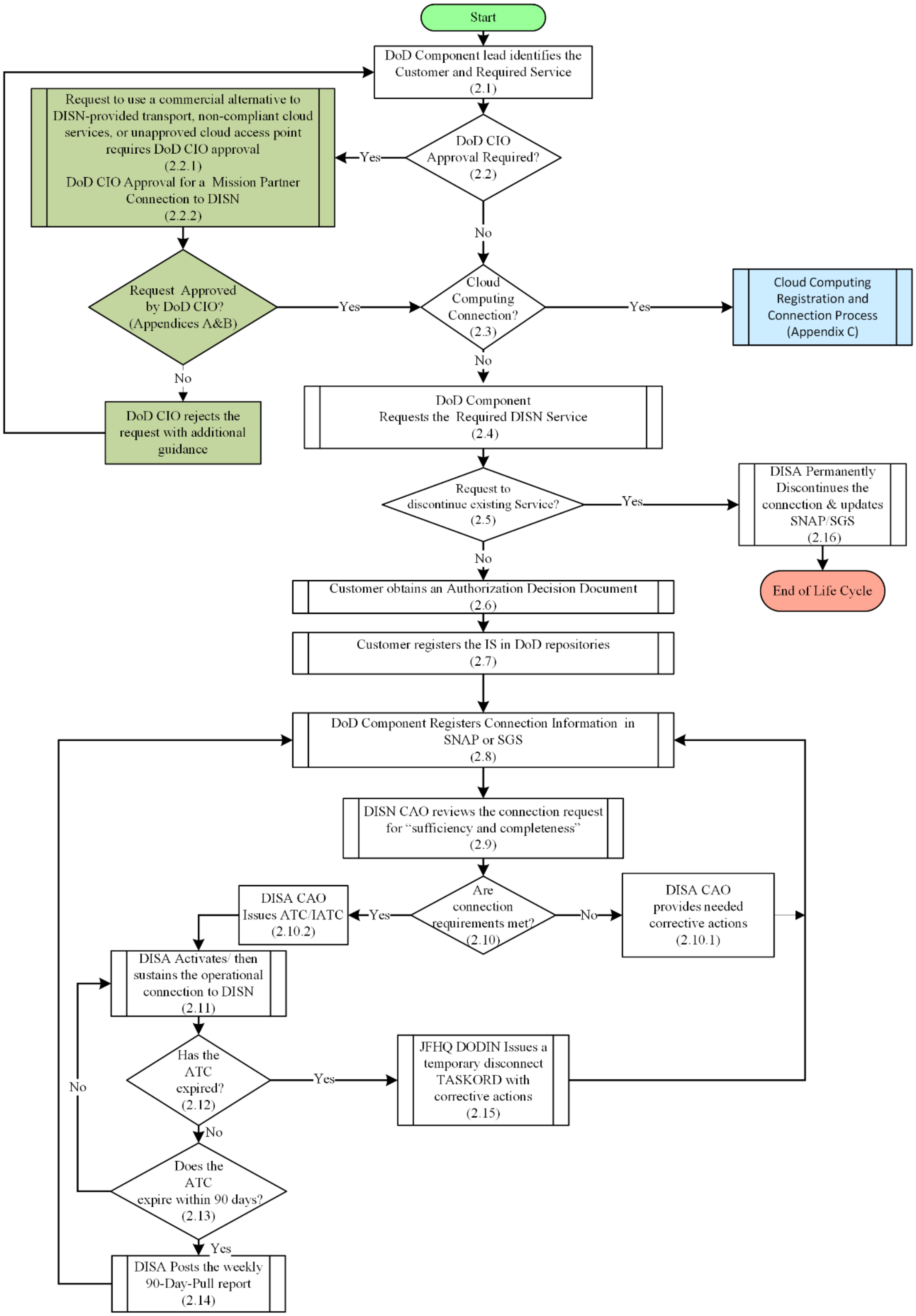

Start
DoD Component lead identifies the Customer and Required Service (2.1)
DoD CIO Approval Required? (2.2)
Yes
Request to use a commercial alternative to DISN-provided transport, non-compliant cloud services, or unapproved cloud access point requires DoD CIO approval (2.2.1)
DoD CIO Approval for a Mission Partner Connection to DISN (2.2.2)
No
Request Approved by DoD CIO? (Appendices A&B)
Yes
No
DoD CIO rejects the request with additional guidance
Cloud Computing Connection? (2.3)
Yes
Cloud Computing Registration and Connection Process (Appendix C)
No
DoD Component Requests the Required DISN Service (2.4)
Request to discontinue existing Service? (2.5)
Yes
DISA Permanently Discontinues the connection & updates SNAP/SGS (2.16)
End of Life Cycle
No
Customer obtains an Authorization Decision Document (2.6)
Customer registers the IS in DoD repositories (2.7)
DoD Component Registers Connection Information in SNAP or SGS (2.8)
DISN CAO reviews the connection request for "sufficiency and completeness" (2.9)
Are connection requirements met? (2.10)
No
DISA CAO provides needed corrective actions (2.10.1)
Yes
DISA CAO Issues ATC/IATC (2.10.2)
DISA Activates/ then sustains the operational connection to DISN (2.11)
Has the ATC expired? (2.12)
Yes
JFHQ DODIN Issues a temporary disconnect TASKORD with corrective actions (2.15)
No
Does the ATC expire within 90 days? (2.13)
No
Yes
DISA Posts the weekly 90-Day-Pull report (2.14)

Figure 1 DISN Connection Process Overview

2.4.1 The DoD Component requests the required DISN service using DSF

Use the unclassified DSF web page to request the DISN service. Do not post classified information to the unclassified DSF web page. The Classified DSF Portal is in the acquisition phase but not yet available. Currently, classified services can be ordered several different ways. If you require classified services, contact the DISA Mission Partner Engagement Office (MPEO) for assistance.

The DSF web page has descriptions of DISN services that include UC, DSN, voice, video, data, computing services[4] The DSF also describes service features, service support, billing rates, and procedures for ordering the service. The DISN Mission Partner Portal and DISA Mission Partner Engagement Office are helpful sources of additional information about DISN and cloud computing services. For Help with DSF or general order entry questions/concerns contact the GIG Service Management Organization (GSM-O) Customer Advocacy Group.

2.4.2 A TSO assigns a unique identifier for the connection

After the DoD Component has entered a DISN connection request in DSF, a Telecommunications Service Order (TSO) is issued to the DoD Component that includes a Command Communications Service Designator (CCSD) or other unique system identifier (e.g., a Virtual Private Network (VPN) Identifier, Virtual Routing and Forwarding Identifier (VRF ID)) assigned in the TSO issued for the connection. The DoD Component provides the CCSD or other unique system identifier when registering and maintaining information about their enclave connection in the SNAP or SGS as described in this guide.

2.5 Is this a DISN customer request to discontinue an existing service?

A DISN customer must submit a request via DSF to discontinue permanently an existing DISN service. When the customer submits a discontinuation request, the process proceeds to Section 2.16 of this guide that describes how DISA permanently disables the connection and ceases billing the customer for the discontinued service.

2.6 The customer obtains an Authorization Decision Document (ADD) with supporting artifacts

Customers must ensure Assessment and Authorization (A&A) of all enclaves or networks IAW the appropriate standard prior to connection to the DISN.

For reauthorization of an existing connection, the DISN customer should initiate enclave A&A and obtain an authorization decision before the Authorization Termination Date (ATD)[5] established in the ADD for the enclave/network.

For a new physical or logical connection, the DISN customer obtains an authorization decision for their enclave/network IAW the applicable A&A guidance as described in Section 2.6.1. The ADD must include the Command Communications Service Designator (CCSD), Virtual Private

[4] The DISN Subscription Services (DSS) Frequently Asked Questions (FAQS) web page provides additional information.

[5] IAW DoDI 8510.01, "An ADD/ATO authorization decision must specify an ATD [Authorization Termination Date] that is within 3 years of the authorization date unless the IS or Platform Information Technology has a system-level continuous monitoring program compliant with DoD continuous monitoring policy as issued." However, "systems that have been evaluated as having a sufficiently robust system-level continuous monitoring program may operate under a continuous reauthorization." If an enclave or network does not have a sufficiently robust system-level continuous monitoring program, it must be reviewed annually and reauthorized once every 3 years. In addition, the results of an annual review, or a significant change in the cybersecurity posture at any time, may also necessitate reassessment and reauthorization of a system.

Network (VPN) Identifier, or Virtual Routing and Forwarding Identifier (VRF ID)) assigned in the TSO issued for the connection (see Section 2.4.2), or other unique system identifier such as the Universal System Identifier (USI) assigned by SNAP when registering a DSN voice switch, or the system's DITPR ID.

The customer may leverage Type-Authorized systems as its Authorization decision as outlined in the RMF Knowledge Service provided there are no significant changes to the archetype (common) configuration, otherwise a separate authorization decision is required with associated documentation. Refer to the RMF Knowledge Service (RMF KS website) for additional guidance. DISA hosted customers must document the security control inheritance model used for authorization decisions identified on the RMF KS website. At the completion of the A&A process, the Authorizing Official (AO) for the enclave or network issues an ADD in the form of an Authorization to Operate (ATO), ATO-with-Conditions, or an Interim Authorization to Test (IATT)[6]. Note that the DoD RMF process no longer permits an "Interim Authorization to Operate."

2.6.1 Applicable Assessment and Authorization Guidance.

The appropriate standard used to A&A an enclave or network prior to connection to the DISN varies depending on the customer as described in DoDI 8500.01, DoDI 8510.01, the DoD RMF KS website, and CJCSI 6211.02D:

a. **DoD Components** authorize DoD Component and unclassified DoD Contractor enclaves or networks and prepare a Security Authorization Package IAW DoDI 8500.01 and DoDI 8510.01[7] and issue an ADD for the contractor enclave/network IAW CJCSI 6211.02D, Enclosure B, paragraph 2.C.(7).

b. **The Defense Counterintelligence and Security Agency (DCSA)**[8] (formerly the Defense Security Service (DSS)) authorizes Classified DoD Contractor Enclaves/Networks IAW DoDI 8510.01 and DoD 5220.22-M.

c. **Intelligence Community (IC) authorizes enclaves or networks** IAW Intelligence Community Directive (ICD) 503.

d. **Federal Mission Partners Authorize National Security Systems (NSS)** in accordance Committee on National Security Systems Instruction (CNSSI) No. 1253 and as stipulated in a DoD CIO agreement IAW DoDI 8010.01.

e. **Federal Mission Partner authorizes non-NSS systems** IAW National Institute of Standards and Technology (NIST) 800-37 and as stipulated in a DoD CIO agreement IAW DoDI 8010.01 as described in Appendix B of this guide.

[6] IATTs should be granted only when an operational environment with simulated-live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical), and should expire at the completion of testing (normally for a period of less than 90 days). IATTs are limited in focus and may require additional security measures for the overarching protection of the DISN or DODIN. Operation of a system under an IATT is for testing purposes only (i.e., the system will not be used for operational purposes during the IATT period) IAW DoDI 8510.01.

[7] All DoD IS and PIT systems must be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253, implement a corresponding set of security controls from NIST SP 800-53, and use assessment procedures from NIST SP 800-53A and DoD-specific assignment values, overlays, implementation guidance, and assessment procedures found on the RMF Knowledge Service (KS). – DoDI 8510.01

[8] Executive Order on Transferring Responsibility for Background Investigations to the Department of Defense, April 24, 2019

f. **Other Mission Partners** enclaves/networks connections to DISN are authorized IAW standards stipulated in a formal agreement with the DoD Component sponsor (e.g., Support Agreement, Mission Partner Environment (MPE) Joining/Membership/Exit Instruction, Memorandum of Agreement, contract, terms of reference) and validated by DoD CIO as described in Appendix B of this guide.

2.6.2 Type-Authorized Systems.

A Type-Authorized System is used to deploy identical copies of an IS or PIT system in specified environments. This method allows a single security authorization package to be developed for an archetype (common) version of a system. The system can be deployed to multiple locations with a set of installation, security control and configuration requirements, or operational security needs that will be provided by the hosting enclave. When Type Authorized Systems are implemented as the only IT system in a local enclave, the Type Authorization package can be used for the SNAP or SGS registration, but must have a topology that shows, among other things, the unique IP addresses and CCSD assigned to that enclave. If there are significant changes to the archetype (common) configuration, a separate authorization decision is required with associated documentation. When multiple IT systems reside on an enclave, the enclave authorization package is used for the SNAP or SGS registration. See the RMF Knowledge Service for additional guidance.

2.6.3 Cross Domain Solutions and the RMF Assessment and Authorization (A&A) process

Cross Domain Solutions (CDS) are IT products that do not undergo the RMF A&A process. A CDS is issued a Cross Domain Solution Authorization (CDSA) obtained IAW DoDI 8540.01 as described in Appendix G of this guide. AOs should leverage CDS risk assessments and approvals when implementing.

2.7 The customer registers the information system in DoD repositories

2.7.1 The Customer registers the Information System in the DoD IT Program Repository (DITPR), SIPRNet IT Registry (SITR), and the Defense Information Technology Investment Portal (DITIP)

DoDI 8500.01 and CJCSI 6211.02D require that DoD Components register Information Systems (IS) in the DoD Information Technology Portfolio Repository (DITPR). Use of the unclassified DITPR is preferred for registration of all ISs including classified systems. The entries for classified systems in DITPR do not include any classified information. However, a DISN customer may register an IS using the SITR if information about the system must contain classified material, or, if the organization, such as a Combatant Command, routinely uses the SIPRNet. To obtain a DITPR account, contact the DoD IT Portfolio Repository POC. For a SITR account, contact the SITR POC. Note that the DISN customer may also need to update DoD Component internal IT program registration database with system information.

IAW DoD 7000.14-R, all IT resources must be reported within investments. The Defense Information Technology Investment Portal (DITIP) provides for the entry and maintenance of common investment data elements in DITPR and Select and Native Programming Data Input System for Information Technology (SNaP-IT).

2.7.2 The customer registers a SIPRNet connection with the SIPRNet Support Center (SSC)

Register ISs connected to SIPRNet with the SSC. Refer to the SSC website on SIPRNet for details.

2.7.3 Obtain a PPSM Tracking Identifier

IAW DoDI 8551.01, Ports, Protocols, and Services Management (PPSM) DISN customers must register their system's ports and protocols in either the SIPRNet or NIPRNet version of the PPSM Registry as appropriate. DISN CAO will only approve a connection request that includes a valid PPSM Tracking Identifier. Customers may collaborate with their DoD Component's PPSM TAG representative to get ports, protocols, and services (PPS) registered in the PPSM Registry located on SIPRNet or NIPRNet. A PPSM account is required for access. Request accounts through your DoD Component PPSM TAG representative.

A customer enclave, network, or application that requires information to traverse both the NIPRNet and the Internet may need to register this requirement in the NIPRNet Demilitarized Zone (DMZ) Whitelist to ensure the DISN Internet Access Points (IAPs) are configured to permit information to flow between the Internet and NIPRNet[9]. The DISN customer should consult with their DoD Component sponsor's PPSM TAG representative to determine whether the ports, protocols and services required by the DISN customer must be registered in the NIPRNet DMZ Whitelist.

DoD IS and Platform IT (PIT) systems must have only a single valid authorization IAW DoDI 8510.01 Enclosure 5-Cybersecurity Reciprocity. Multiple authorizations indicate multiple systems under separate ownership and configuration control. PPSM registration for enterprise/core services is the responsibility of the service provider. Receiving organizations will execute a documented agreement between the provider and the receiver (e.g., memorandum of understanding (MOU), memorandum of agreement (MOA), SLA) for the maintenance and monitoring of the security posture of the system (security controls, cybersecurity service provider (CSSP), etc.).

For more information on PPSM, please refer to the DISA RE41 PPSM home page, the DISA PPSM web page, access PPSM computer based training at DISA Risk Adjudication and Connection Division's Mission Partner Training Program (MPTP), or contact the DoD PPSM team (DISA RE41).

2.7.4 Align to a DoD operations security center (OC) and supporting Cybersecurity Service Provider (CSSP)

DoDI 8530.01 requires that DoD Components align their systems with a joint or DoD Component operations center (OC) and supporting Cybersecurity Service Provider (CSSP) to allow mission operators to have confidence in the confidentiality, integrity, and availability of DoD IT and DoD information. U.S. CYBERCOM maintains a list of DoD certified and accredited CSSPs under the Cybersecurity Service Provider (CSSP) Program. The Defense Working Capital Fund (DWCF) Rate Book includes billing information for Cybersecurity services provided by the DISA CSSP Office.

[9] The IAPs are boundary protection gateways between the NIPRNet and the Internet. IAW DoDI 8010.01 paragraph 3.2.d, all traffic between NIPRNet and the Internet must be through a controlled DISN IAP.

2.8 DoD Component registers connection information in SNAP or SGS

IAW DoDI 8010.01, DoD Components must "implement and register all connections to the DISN, including DoD Component and Mission Partner systems connected to DISN gateways, in the DODIN tracking and management repository IAW the DCPG." DISA currently implements this policy using the DISA SNAP database on NIPRNet and the SGS database on SIPRNet to track connections to DISN. The SNAP database on NIPRNet has modules for registering requests for unclassified services including: DSN and UC, NIPRNet (unclassified IP-based data services), VPN services, Cloud computing connections to DISN, DoD CIO Approval of Commercial Alternatives to DISN Enterprise Services, and DoD CIO Approval of Mission Partner Connections to DISN. The SGS database on SIPRNet has modules for registering requests for classified services including VPNs, SIPRNet (Secret GENSER IP-based data services), and Cross Domain Solutions.

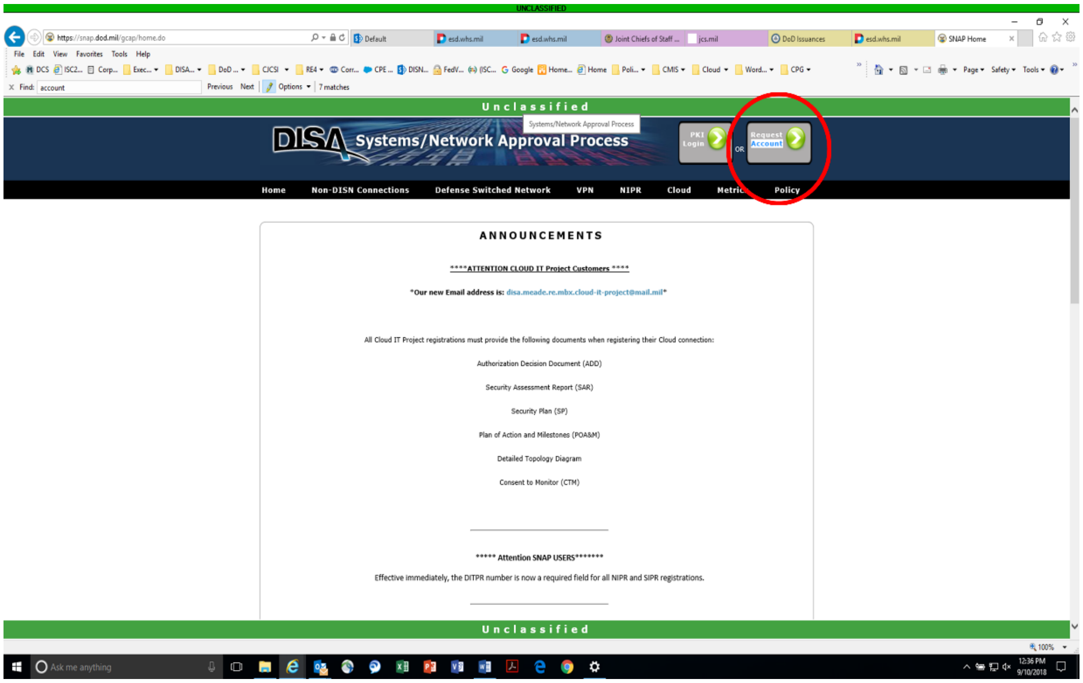
DoD Components use the modules in SNAP or SGS to register connection requests that include information needed by the DISN CAO to determine whether to issue an Approval to Connect (ATC), or a VPN Permission to Connect (PTC) to DISN.

2.8.1 DoD Component customer obtains an account on the NIPRNet SNAP database or the SIPRNet SGS database

To request a SNAP or SGS account,

- In your web browser
  - https://snap.dod.mil for NIPRNet SNAP
  - https://giap.disa.smil.mil for SIPRNet SGS
- Select the green "Request Account" as illustrated in Figure 2
- Step 1: On the "REQUEST SNAP ACCOUNT" web page:
  - Select the hyperlink for "DD Form 2875"
  - On the "REFERENCE DOCUMENTS" web page
  - Select "All Systems"

- Select “DD Form 2875” then “Download” the DD Form 2875 from SNAP and/or SGS located on the “Reference Documents” page



ANNOUNCEMENTS

****ATTENTION CLOUD IT Project Customers ****

Our new Email address is: disa.meade.re.mbx.cloud-it-project@mail.mil

All Cloud IT Project registrations must provide the following documents when registering their Cloud connection:

Authorization Decision Document (ADD)

Security Assessment Report (SAR)

Security Plan (SP)

Plan of Action and Milestones (POA&M)

Detailed Topology Diagram

Consent to Monitor (CTM)

***** Attention SNAP USERS*******

Effective immediately, the DITPR number is now a required field for all NIPR and SIPR registrations.

Figure 2 DoD Component customer obtains a SNAP/SGS Account

- Complete the form DD 2875. The user will need to provide the following information to complete the User Account Request form:
  - First and last name
  - Physical address
  - DoD component, sub agency
  - Unclassified e-mail address, commercial telephone number, DSN phone number
- In section 13 of the DD Form 2875, “Justification for Access” mark the SNAP and/or SGS module(s) you wish to access
- Upload the completed and signed DD Form 2875 SAAR on the SNAP “REQUEST SNAP ACCOUNT” web page

- Step 2 – On the “REQUEST SNAP ACCOUNT” web page
  - Provide your profile information - asterisked item are required fields
  - When Step 1 and Step 2 are completed, select the green “**Submit Request**” button at the bottom of the “REQUEST SNAP ACCOUNT” web page

- Step 3 – DISN CAO creates the SNAP Account.
  - Once the user has submitted all required information, a DISN CAO analyst will review the request for a SNAP/SGS account.
  - The user will receive an e-mail message either approving the request for a SNAP/SGS account or explaining why DISN CAO denied the request.

SNAP and SGS users must renew their accounts annually by emailing an annual Cyber Awareness Challenge training certificate of completion to the DISN CAO. Otherwise, access to SNAP/SGS will be suspended.

2.8.2 DISN Customer logs into SNAP (Unclassified) or SGS (Classified) and registers the connection request:

- Log on to SNAP for Unclassified Connections or SGS for Classified Connections.
- Hover the cursor over the applicable DISN service tab.
- Then select “New Registration” or “View/Update.”
- The customer interacts with the module to complete all “Information sections” in the NIPR/SIPR Checklist. Note that SNAP reserves sections marked with a “pad locked” icon are for use by the DISN CAO Analyst.

2.8.3 Required documents:

For either a logical enclave or physical enclave connection to DISN, the DoD Component uploads the following required documents into SNAP or SGS:

- Authorization Decision Document (ADD) prepared IAW the applicable A&A policies listed in Section 2.6 of this guide and signed by the Authorizing Official (AO)
- CSSP agreement IAW DoDI 8530.01 or as stipulated in agreements with Mission Partners.
- Topology prepared in accordance with guidance in Appendix E

- Consent to Monitor (may be included in the ADD - see the sample with instructions in Appendix I)
- DoD Component CIO concurrence memo submitted to ISRMC and DoD CIO for an ATO issued for a Component IS with a level of risk of "Very High" or "High" for a non-compliant security control IAW DoDI 8510.01 Enclosure 4 paragraph 1.b.(2). (e) and Enclosure 6 paragraphs 2.e.(4).(b) and (e).
- DoD Sponsor request for a Mission Partner connection to DISN:
  - For a DoD Contractor, Federal Department/Agency mission partner connection request, the DoD Sponsor also uploads the DoD CIO approval memo or Memorandum of Agreement (see Appendix B)
  - For a 5-Eyes, allied, or coalition mission partner connection request, the DoD Sponsor also uploads the Chairman of the Joint Chiefs of Staff approval memo IAW DoDI 5530.3 and CJCSI 6740.01C[10]

2.8.3.1 Other Supporting documents:

Recommend the customer upload the following RMF Security Package documents (prepared IAW A&A policies listed in Section 2.6 of this guide) to support Defensive Cyber Operations information sharing:

- Security Plan (SP) (optional)
- Security Assessment Report (SAR) (optional)
- Plan of Action and Milestones (POA&M) (optional)

> The SGS system is a repository for connections to SIPRNet at the Secret level. If a document or artifact associated with a system connection to SIPRNet is classified higher than Secret GENSER, please contact the DISN CAO for additional guidance.

2.8.3.2 JRSS Connection Registration

Customers must reauthorize connections moving to the DISA JRSS Stack. This only applies to NIPRNet connections at this time since SIPRNet connections are not yet moving to JRSS.

The customer uses the following procedures to create a registration in the NIPRNet module:

1. To register a JRSS connection in SNAP, in the NIPRNet module select 'New Registration'.
2. In section 0, for Circuit Type, select JRSS instead of DoD.
3. In section 1, there is a question, 'Is this systems connection type JRSS?' Select "Yes" and type in the VRF ID in the block below. (NOTE: Currently the VRF ID will not show if the customer goes to "My Entries" report. Until this is fixed, the customer will have to search by Registration ID for that registration.)

[10] Note CCMDS and other DoD Components are participating in the Joint Staff J6 Cyber Integration Workshop. The goal is to develop a "Partner Nation Systems Connection Process Guide" that integrates DoD policy and procedures to provide warfighters a 4-phased approach using the Risk Management Framework (RMF) to assess, balance mission, cybersecurity risks, and requirements of foreign partner connections to the Department of Defense.

4. Internal boundary defense equipment (firewall, IDS/IPS) is no longer required on the enclave's topology diagram since JRSS provides cybersecurity perimeter protections. The topology must show the JRSS stack as illustrated in Section E.2 of this guide.
5. The customer submits a JRSS package like any other NIPRNet Connection Approval package except that the customer identifies the JRSS by a "Virtual Routing and Forwarding Identifier (VRF ID)" rather than by a CCSD. Please remember to identify the VRF ID (and associated CCSD if applicable) in the ADD and topology. For additional information, contact the JRSS PMO.

2.8.3.3 Documentation for registering a VPN connection in SNAP/SGS:

In addition to the required documents and other supporting documents listed in Section 2.8.3 , the customer must upload the following VPN related documents:

- To establish a VPN, the **VPN Customer** registers a new VPN in SNAP/SGS, the VPN Customer must upload into SNAP/SGS the order confirmation email received from DSF that approves establishment of the VPN
- To connect to an existing VPN, the **Customer** registers a connection to an existing VPN, the VPN Customer uploads the network topology, the Authorization Decision Document (ADD) and the TSO issued by DSF that approves the VPN customer's connection to the VPN

2.8.3.4 Documentation for a Dedicated Point-to-Point Connections and DISN Backbone Connections

DoDI 8010.01, paragraph 1.2.c requires DoD Components to register all connections to the DISN in the DODIN tracking and management repository (currently SNAP/SGS). As such, dedicated point-to-point connections and DISN Backbone connections must be registered in SNAP or SGS (if classified). A Dedicated point-to-point connection uses DISN transport but does not connect to NIPRNet, SIPRNet, or DSN. A DISN Backbone Connection links DISN elements such as switches, sensors, gateways, network operations centers, and other active tools that are under the operational direction and management control of DISA. The customer uploads the required documents and other supporting documents listed in Section 2.8.3.

DISN Customer Training – The DISA Risk Adjudication and Connection Division's Mission Partner Training Program (MPTP) provides scheduled live training sessions via Defense Collaborative Service (DCS) and teleconference, 24/7 user-accessible computer based training materials, and education opportunities for DISN Connection Approval, PPSM, DSAWG, Cross Domain Solutions, and Cloud Onboarding. The Goal of the training is to reduce or eliminate processing delays caused by inaccurate or incomplete DISN connection requests. For additional information about the MPTP contact DISA's Risk Adjudication and Connection Division's Mission Partner Training Program (MPTP) or the DISN CAO.

2.8.4 The Customer submits the DISN Service Request to DISN CAO for review

When the customer has completed all SNAP/SGS Information sections and uploaded Security Package documentation, a **"SUBMIT"** button will appear at the bottom of the screen. The customer selects this button to submit the connection request to DISN CAO for review.

2.9 DISN CAO reviews the connection request for "sufficiency and completeness"

After the DISN customer submits the connection request package, a DISA analyst performs a quality review of submitted evidence registered in SNAP or SGS for "sufficiency and completeness" consistent with DoDI 8510.01 (See enclosure 5 paragraph 1.e). The DISN CAO confirms the following for a DISN connection request:

a. The AO signed the ADD and Consent to Monitor (CTM)
b. The enclave Topology was completed IAW guidance in Appendix E
c. DoD Component CIO concurrence memo submitted for a Component IS with a level of risk of "Very High" or "High" for a non-compliant security control
d. For a Mission Partner connection request, the DoD CIO approved the request as described in Appendix B
e. DoD enclaves or networks are "aligned to DoD network operations and security centers (NOSCs)" and a supporting CSSP IAW DoDI 8530.01 or as stipulated in an agreement with a Mission Partner
f. Cloud Services are approved and registered as outlined in Appendix C, paragraph C.2.
g. VPN Owner's order confirmation or VPN Member TSO confirmation (where applicable)
h. For a new SIPRNet enclave connection:
    - DISN CAO issues an Interim Approval To Test (IATT) for the connection Note: this is not the same as an Authorizing Decision Document (ADD) that may be issued by the system's AO).
    - The customer then contacts DISN Connection Approval Office (CAO) to schedule a Remote Compliance Monitoring scan of the enclave/network as described in Appendix J.

IAW DoDI 8510.01, Enclosure 4, paragraph 1.a.(2), the DISN CAO will refer all new Federal Mission Partner SIPRNet connection requests to the Defense Security/Cybersecurity Authorization Working Group (DSAWG) and Information Security Risk Management Committee (ISRMC). The DoD Component sponsor prepares a DSAWG and ISRMC presentation IAW the DSAWG briefing template. The DoD Component sponsor and Mission Partner will upload the body of evidence and security related artifacts into SGS to support the briefing to the DSAWG.

2.10 Does the connection request meet connection requirements?

2.10.1 No, DISN CAO provides needed corrective actions to the Points of Contact

The DISN CAO analyst will identify corrective actions needed for the request to obtain an ATC. SNAP/SGS will notify the customer POCs. The customer logs into SNAP/SGS, makes the needed updates, and resubmits the connection request to DISN CAO as described in Section 2.8 of this guide.

2.10.2 Yes, DISN CAO issues an ATC

The SNAP/SGS database will send an automated email to the registration point of contact as proof of registration. The email will have an ATC[11] letter attached. The approval will include an Approval Termination Date. The DISN CAO typically completes the review of a complete connection request package within five business days.

a. **Connection approval expiration date.** The Approval Termination Date for the DISA issued ATC, is usually the same as the Authorization Termination Date included in the customer's ADD. The expiration date for an ATC is also within three years unless the enclave has a system-level continuous monitoring program as described in Section 2.6 of this guide. DISN CAO may grant an ATC for up to one year consistent with DoDI 8510.01 limit on an "ATO with Conditions." DISN CAO may grant an ATC for up to one year for units deployed in the CENTCOM area of responsibility. In some instances, the risk assessment may warrant DISN CAO assigning an expiration date shorter than that of the associated ATO or IATT. The ATC for an enclave operating under an IATT is normally for a period of less than 90 days IAW DoDI 8510.01."

b. **For a Dedicated Point-to-Point Connection or DISN Backbone Connection**. DISA will email the Approval to Connect (ATC) letter to the customer. The email will indicate the status of the dedicated connection as "Operational – No ATC." The customer does not need to renew the ATC for a dedicated point-to-point connection or DISN backbone connection. DISN CAO will not report an "Operational – No ATC" connection in the 30/60/90-day report to JFHQ/DODIN. However, the office of primary responsibility for the connection must keep the connection's supporting documentation up to date in SNAP/SGS.

c. **Reissuances of an ATC:** A significant change to an enclave or network may affect the cybersecurity posture of that enclave, and consequently, the risk the enclave poses to the DISN community at large. A significant change may require the DISN customer to initiate an Assessment and Authorization before the ATC expiration date specified in the original connection approval letter. If the DISN enclave has a significant change, the DISN customer must:

- Notify the DISN CAO of significant changes effecting the enclave connection
- Update topologies and risk decision artifacts,
- Update and resubmit the SNAP/SGS registration for the connection including updated Security Package documents described in Section 2.8 of this guide

d. **Note:** The following events are not significant changes and do not require a new A&A effort and reissuance of the ATC. Instead, the DISN customer must notify the DISN CAO of the proposed change and update the network topology diagram in SNAP/SGS before deployment/implementation.

- Deployment of new VoIP phones requiring a new VLAN segment in the enclave
- Deployment of a Video Teleconference product that is on the DoD UC APL
- Changes in the IP address range assigned to the IS/enclave
- DISA transport re-homing actions that change the connection points to DISN, but the enclave remains at the same facility

[11] The DISN CAO emails a "Permission to Connect (PTC)" for approved VPN connections. Save this email, as it is proof of registration for turn- up of the VPN.

- Change in the service's bandwidth

2.11 DISA activates then sustains the operational connection to DISN

Upon receipt of the DISN CAO email containing the approval to connect (e.g., ATC) the DISA Global Operations Center (DGOC) activates the connection to the requested DISN service. The customer must work with DISA Implementation Testing and Request Fulfillment Activations team to complete the connection and satisfy the customer's operational requirement. DISA sustains the DISN connection for the period specified in the ATC. IAW DISA Circular 310-130-001, and DISA Circular 310-070-057, DISA performs Implementation, Testing, and Activation (IT&A) and Quality Management for each connection to ensure it is ready for use and has operational utility that meets the customer's stated requirements. For connection activation support, contact the DISA Implementation Testing and Request Fulfillment Activations team. For Questions regarding Provisioning (Telecommunications Service Requirements (TSR) writing), or general request fulfillment status/questions contact DISA Provisioning Customer Support. Contact the DISA Infrastructure Global Service Desk (IGSD) to report an outage or to request status of an outage.

2.11.1 IP-Based Access Connection

DoD CIO is leading efforts to terminate costly legacy network technologies and associated transport infrastructure circuits (e.g., TDM circuits) to align with Joint Information Environment (JIE) Reference and Solution Architectures and the Department of Defense Strategy for Implementing JIE by optimizing use of IP-based network infrastructure. DISA will connect customers using existing IP bandwidth at DISN Infrastructure Service (DIS) (formerly DSS) locations or using a readily available commercial IP network at non-DIS locations. For information on IP-based connection delivery timelines, contact the DISA IGSD.

2.11.2 TDM-Based Access Circuits

As stated in the DoD CIO Memo, Legacy Networking Technologies DISN customers use TDM or other legacy circuits only as a last resort when IP-based services are not available. If a TDM circuit is required, DISA Circular 310-130-001 (Tables T1.1 through T1.4) provide estimated "Lead-Times For Service" to fulfill a circuit ordered through DSF. Customers should utilize these circuit lead-times for planning purposes when ordering a physical circuit to minimize the time between delivery of circuit and activation of the circuit. A critical path action is for the customer to complete the A&A process (see Section 2.6 of this guide) and obtain an ATO for the enclave. A customer should only order a circuit when certain about completing all actions (including A&A activities) within the specified timeline to ensure best use of costly legacy circuits.[12] There is an expedited process available, for service fulfillment and connection approval of an Emergency or Essential National Security/Emergency Preparedness telecommunications service requirement. For additional information on TDM delivery timelines, contact the DISA IGSD.

[12] For information about provisioning of DISN connections, see DSF and DISA Circular 310-130-001 Communications Requirements, Submission of Telecommunications Service Requests, 19 August 2009. For information about the DISN billing process see the Defense Working Capital Fund Billing Prices for Fiscal Year 2020 Consolidated Services or contact the DoD Component's DISN Billing Support Representative. Billing for a NIPRNet or SIPRNet connection commences within 72 hours after connection delivery whether the customer has obtained an ATC required for connection activation. To avoid wasteful connection charges, the customer should order the NIPRNet/SIPRNet access connection via DSF only if all required actions described in this guide (including A&A activities) will be completed within the expected connection delivery timelines shown in DISA Circular 310-130-1 (Tables T1.1 through T1.4).

2.11.3 Mission Partner Gateway (MPGW) Connections to DISN

Mission partners connect to DISN through a MPWG IAW DoDI 8010.01 and CJCSI 6211.02D. Appendix H addresses Mission Partner Gateway (MPGW) Connections to DISN.

DoDI 8010.01 tasks DoD Component heads to - *"Leverage commercial IP network transport and cloud services available on Defense IT Contracting Organization contracts to securely connect to the DISN services if DISN service is not available at the required operating location."*

2.12 Has the ATC expired?

In accordance with JFHQ DODIN Task Order 16-0158, Connection Accreditation Enforcement Process, each week DISN CAO runs a report in SNAP or SGS that lists DISN connection with an expired ATC. The DISN CAO forwards the list of connections with an expired ATC to JFHQ DODIN for action as described in Section 2.15 of this guide.

2.13 Does the ATC expire within 90 days?

Each week, DISN CAO also runs a 90-day-pull report that builds a list of DISN connections with ATCs that expire within the next 30, 60, or 90 days.

2.14 DISA posts the weekly 90-Day-Pull Report on SIPRNet.

DISA posts the weekly report on the 90-Day-Pull Warning Order (WARNORD) web page Additionally, SNAP and SGS automatically sends email reminders to the registered points of contact for a connection reminding them to initiate actions required to renew these expiring approvals to connect to DISN.

Upon receipt of the initial 90-day expiration warning, the DISN Customer should:

- Obtain an updated ADD for the system as described in Section 2.6 of this guide.
- Update information about the system in SNAP/SGS
- Submit the updated connection renewal request as described in Section 2.8 of this guide before the connection ATC expires.

The DISN CAO will then review the request as described in Sections 2.9 through 2.11 of this guide.

The connection renewal cycle (Sections 2.8 through 2.14 of this guide) typically repeats until the DoD Component submits a request to discontinue permanently the DISN connection as described in Sections 2.5, and 2.16 of this guide.

2.15 JFHQ DODIN issues a temporary disconnect Task Order (TASKORD) with corrective actions

An expired ATC will prompt a review by Joint Force Headquarters DODIN (JFHQ DODIN) and may result in an order to disconnect the enclave/network from the DISN service in accordance with JFHQ DODIN Task Order 16-0158, Connection Accreditation Enforcement Process.

2.15.1 JFHQ DODIN Temporary Disconnection TASKORD provides corrective actions

A JFHQ DODIN Task Order (TASKORD) directs DISA to disconnect temporarily a DISN connection with an expired ATC. JFHQ DODIN posts disconnection TASKORDs on the JFHQ DODIN Notification of Non-Compliant Circuit Disconnection website on SIPRNet. The TASKORD includes guidance for the DISN customer to restore the connection.

2.15.2 DISA Implements the temporary disconnection order

JFHQ DODIN will direct DISA to disconnect temporarily the enclave's connection to DISN. The charges for the DISN connection will continue during the temporary disconnection.

2.15.3 DISN customer completes required actions

The DISN customer completes the required corrective actions, updates information about the connection in SNAP or SGS system as required, and resubmits the request as described in Section 2.8 of this guide. The DISN CAO will review the request as described in Section 2.9 of this guide. If the connection request meets all requirements described in Section 2.10 of this guide, DISN CAO issues an approval to connect (e.g., ATC) and JFHQ DODIN directs DISA to restore the connection. DISA restores the connection to sustainment status as described in Section 2.11 of this guide.

If the DISN customer determines that the connection to DISN is no longer required, the customer must submit a discontinuation request through DSF. Charges for an access circuit stop after DISA processes the customer's TSR requesting discontinuation of the enclave's connection to DISN as described in Sections 2.5 and 2.16 of this guide.

2.16 DISA Permanently Discontinues the connection and updates SNAP/SGS

2.16.1 DISA Notifies Stakeholders about Service Discontinuation.

In response to the DISN Customer request described in Section 2.5 of this guide, DISA Command Center will issue a DISA TASKORD to DISA Global to discontinue permanently the DISN connection. DISA will apprise stakeholders (e.g., VPN members and Cloud service subscribers) about discontinuation actions affecting their connections so they can take appropriate action. (If discontinuing a Cloud Service Offering (CSO), see supplemental procedures in Section D.2 of this guide.)

2.16.2 Discontinuation of a DISN Connection.

DISA Global permanently disconnects the system from DISN. For NIPRNet connections, DISA Global revises the NIPRNet DMZ Whitelist as needed. When DISA completes processing of a TSR to discontinue a physical circuit, the DSF will update the Telecommunication Inventory and Billing Information (TIBI) entry for a reimbursable service (e.g., mobility, DISN IS services). For pass-through services (e.g., DISN TDM access circuits), The Defense Information Technology Contracting Office (DITCO) will notify the commercial vendor, and manually update TIBI. The pass-through charges for the commercial circuit will stop within 30 days.[13] When the customer receives the e-mail containing the TSO that confirms the connection has been discontinued, the

[13] Currently there are no separate customer charges for logical connections (e.g., Multi-Protocol Label Switching (MPLS) VPNs)).

customer must forward the email containing the TSO to the DISN CAO. DISN CAO updates the appropriate repositories (e.g., SNAP, SGS).

The Life Cycle of a DISN Connection ends here.

Appendix A DoD CIO review and approval of requests for commercial alternatives to DISN-provided transport and non-standard cloud services, and unapproved cloud access points

This Appendix describes the process used by a DoD Component to request DoD CIO review and approval of commercial alternatives to DISN-provided transport (referred to in this appendix as a DODIN commercial connection) and non-standard cloud services, and use of Boundary Cloud Access Points (BCAP) that lack an existing DoD CIO approval.

DoD policy requires DoD components to use DISN capabilities for transport and meet DoD standards for cloud services and use only approved cloud access points:

- Per DoDI 8010.01, section 1.2, C:
  "DoD Components will use the Defense Information Systems Network (DISN) as the core element of DODIN Transport."

- Per DoDI 8010.01, section 1.2, E:
  "DoD Components will use the DISN-provided transport, when available, to satisfy DoD information transfer requirements between DoD installations and facilities…."

- Per DoDI 8010.01, section 4.5:
  "Connections to a cloud service offering (CSO), both internal and external to the DODIN, will be implemented in accordance with the DoD Cloud Computing Security Requirements Guide, the DCCPG (until integrated with the DCPG), and applicable DoD policy."

- Per DoD CIO Memo: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing:
  "Commercial cloud services used for Sensitive Data must be connected to customers through a Cloud Access Point (CAP) provided by DISA or through a CAP provided by another DoD Component."

DoD Components who have unique mission requirements that are unable to be met by the DISN or supported by DoD policy, may request authorized alternate connectivity. Per DoD policy, DoD CIO review and approval is required for DODIN commercial connections and non-standard cloud services, and unapproved cloud access points:

- Per DoDI 8010.01, section 3.2, F.2:
  "Internet traffic will flow through one of the authorized IAPs, unless the DoD CIO has authorized alternate connectivity (e.g., intelligence, law enforcement, or other specific mission requirements)."

- Per DoDI 8010.01, section 4.4, A:
  "Commercial transport services procured as an alternative to the DISN-provided transport requires compliance with this issuance or DoD CIO review and approval."

- Per DFARS, 252.239-7010 Cloud Computing Services:
  "The Contractor shall implement and maintain…in accordance with the Cloud Computing Security Requirements Guide (SRG) unless notified by the Contracting Officer that this

requirement has been waived by the DoD Chief Information Officer."

"The contracting officer may award a contract to acquire cloud computing services from a cloud service provider that has not been granted provisional authorization when-
(i) the requirement for a provisional authorization is waived by the DoD Chief Information Officer; or…."

- Per DoD CIO Memo: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing:
  "All CAPs must be approved by DoD CIO."

The missions described below in Table 3 are listed in DoDI 8010.01 paragraph 4.4 and grouped by mission types and corresponding allowable actions. These missions do not encompass all missions that may require an authorized DODIN commercial connection nor are they pre-authorized DODIN commercial connections.

All DODIN commercial connections require DoD CIO approval and are subject to Command Cyber Readiness Inspections (CCRI) and Command Cyber Operational Readiness Inspection (CCORI) to ensure conformance with DoD cybersecurity requirements and compliance with DoDI 8510.01, DoDI 8530.01, and other DoD cybersecurity policies and guidance.

Table 3 Description of unclassified DODIN commercial connections referenced by DoDI 8010.01, paragraphs 4.4.f through 4.4.i

Authorized Mission	Description
Connections to Temporary Facilities	Provisional commercial connections installed to support temporary facilities due to DoD employee relocation caused by military construction, natural disaster, or unforeseeable events where DODIN Transport is not available or would be cost-prohibitive to install due to the temporary nature of the need. *Per DoDI 8010.01, paragraph 4.4f: May be used to transmit Controlled Unclassified Information.*
Infrastructure Non-availability	Interim commercial connections installed to support DoD IT requirements due to loss of telecommunication infrastructure (e.g., outside plant cabling system, communication nodes) caused by natural disaster, significant equipment refresh, repairs, or unforeseeable events where the DODIN Transport is not available or would be cost-prohibitive to install due to the temporary nature of the need. *Per DoDI 8010.01, paragraph 4.4f: May be used to transmit Controlled Unclassified Information.*
Urgent and Ad hoc Mission Connections	These commercial connections are temporary (up to 90 days). The Commanding General of the Major Command or Senior Executive approves the personnel and equipment selected for the mission and provides funding for the commercial connections.

Authorized Mission	Description
	Per DoDI 8010.01, paragraph 4.4f: May be used to transmit Controlled Unclassified Information.
Temporary Training Connections	Temporary commercial training connections are used to exercise COOP, military operations, or contingency plans, or as a secondary communication link for force protection exercises. These connections are normally short (fewer than 90 days) and the requirement for the connection noted in a formal document. A permanent connection maintained for one or more annual exercises requires the DoD CIO approval. *Per DoDI 8010.01, paragraph 4.4f: May be used to transmit Controlled Unclassified Information.*
Connections to non-DoD Locations	Locations outside of DoD facilities (e.g., a recruiting station renting commercial office space, satellite health clinics, etc.) where the location, low number of users, or need for mobility make it cost prohibitive to procure anything but commercial connections. Information systems using these commercial connections must comply with all DoD cybersecurity policies. *Per DoDI 8010.01, paragraph 4.4f: May be used to transmit Controlled Unclassified Information.*
Enduring Training and Education	Enduring commercial training connections used to support DoD educational institutions such as the Military Academies and training institutions or DoDEA schools. Connections are typically permanent and are used to access educational resources that may not be reachable via the NIPRNET due to DoD policies (e.g., Dependent children, foreign students, and visiting professors without CACs). AOs must consider the Family Educational Rights and Privacy Act (FERPA), Children’s Online Privacy Protection Act (COPPA), the Privacy Act, and other applicable policies when applying cybersecurity controls to these connections. *Per DoDI 8010.01, paragraph 4.4g: Supports unique information systems and missions and requires appropriate DoD cybersecurity controls applied by the DoD Component AO*
Missions requiring managed attribution	Missions requiring non-attribution. *Per DoDI 8010.01, paragraph 4.4g: Supports unique information systems and missions and requires appropriate DoD cybersecurity controls applied by the DoD Component AO*
Support to Civil-Military Operations in accordance with DoDI 8220.02, DoDI	Per DoDI 8220.02, United States task forces may support civil-military partners with unclassified data and voice services in support of stabilization and reconstruction, disaster relief, and humanitarian and civic assistance. These operations may include DoD Components, U.S. departments and agencies, foreign governments

Authorized Mission	Description
3000.05, and DoDI 3003.01	and security forces, international organizations, nongovernmental organizations (NGOs), and members of the private sector to facilitate the sharing and integrating of stabilization and reconstruction, disaster relief, and humanitarian and civic assistance information across various portal instantiations. To ensure security of the DODIN, these connections will normally be commercial in nature. Examples include Wireless Access Points (WAPs), SATCOM links, or terrestrial connections on foreign telecommunication infrastructure for emergency response trucks/trailers and mobile emergency operations centers. DoDI 3000.05 directs DoD entities to assist other U.S. Government agencies in identifying and developing strategies for the use of information and communications technology capabilities to enable civil-military interaction, information sharing, and accelerating stability and reconstruction activities. Per DoDI 3003.01, when possible, support civil agency efforts to improve the capabilities of communications and information management systems, and of personnel location and identification technologies, for civil search and rescue (SAR). *Per DoDI 8010.01, paragraph 4.4g: Supports unique information systems and missions and requires appropriate DoD cybersecurity controls applied by the DoD Component AO*
Force protection and public safety in accordance with DoDD 3020.44, 3025.13, and 3025.18 and DoDI 5535.10 and 6055.17	Mission requirements include: • DoDDs 3020.44, 3025.13, and 3025.18 and DoDIs 5535.10 and 6055.17 direct DoD entities to support interagency efforts with the Department of Homeland Security (DHS) and other Federal, State, and local law enforcement agencies to combat threats to U.S. Forces and the homeland • Coordination and information sharing with civil First Responders in an accessible information environment when necessary to protect and defend hosts and tenant, on and adjacent to DoD Installations to enable emergency management activities *Per DoDI 8010.1, section 4.4h: May be used to transmit data*
Civil authority database in accordance with Directive-type Memorandum 09-012 (This DTM shall expire effective February 28, 2019, and shall be incorporated into	This DTM establishes DoD access control policy and the minimum DoD security standards for controlling entry to DoD installations and stand-alone facilities. Installations are directed to procure an electronic physical access control system (PACS) that provides the capability to rapidly and electronically authenticate credentials and individual's authorization to enter an installation. The PACS must support a DoD-wide and federally interoperable access control capability that can authenticate USG physical access credentials and support access enrollment, authorization processes, and securely share information. *Per DoDI 8010.1, section 4.4h: May be used to transmit data*

Authorized Mission	Description
DoD 5200.08-R and DoDI 5200.08)	
Payment card in accordance with DoDD 5400.11	DoD organizations processing Automatic Teller Machine (ATM) or Point of Sale (POS) transactions must connect to civilian financial institutions and credit card companies to process these requests. These are enduring commercial connections that have standards and mandates levied by commercial and State entities. The Payment Card Industry Security Standards Council (PCI SSC) governs the security of sensitive cardholder data. It produces cybersecurity standards for the PCI that are law in many States. *Per DoDI 8010.1, section 4.4h: May be used to transmit data*
Community relations events in accordance with DoDI 5410.19	Temporary connections to support events held to extend good will to communities located adjacent to DoD Installations require temporary commercial connections due to the unique mission-set associated with hosting these affairs. Examples of community events include the Marine Corps Marathon and United States Air Force Thunderbirds air demonstrations. DoDI 5410.19 provides further guidance on types of applicable community relations and restrictions on use of government capabilities to support these types of activities. *Per DoDI 8010.1, section 4.4i: non-DISN requirement that processes, stores, and transmits publicly releasable DoD data requires DoD Component AO to tailor appropriate security controls*
Non-Appropriated Fund Instrumentalities (NAFI) in accordance with DoD 7000.14-R and DoDIs 1015.10 and 1015.15	Non-DISN commercial connections are procured and funded with NAFI due to the policies within DoD 7000.14-R, DoDI 1015.10, and DoDI 1015.15 that include guidance on the level and types of support that DoD Components may provide to NAFIs using appropriated funds. *Per DoDI 8010.1, section 4.4i: non-DISN requirement that processes, stores, and transmits publicly releasable DoD data requires DoD Component AO to tailor appropriate security controls*
Morale, Welfare, and Recreation (MWR) activities in accordance with DoDI 8550.01	Commercial internet services for military exchanges, internet cafes, and lodging programs, provided by MWRs, for use by authorized patrons IAW guidance contained in DoDI 8550.01. Examples include Wounded Warrior housing, hospitals/clinics, Wounded Warrior fund raising events, etc. *Per DoDI 8010.1, section 4.4i: non-DISN requirement that processes, stores, and transmits publicly releasable DoD data requires DoD Component AO to tailor appropriate security controls*

Table 3 Description of unclassified DODIN commercial connections referenced by DoDI 8010.01, paragraphs 4.4.f through 4.4.i

The DoD CIO review and approval process of DODIN commercial connections and non-standard cloud services is depicted in Figure 3 and described subsequently below.

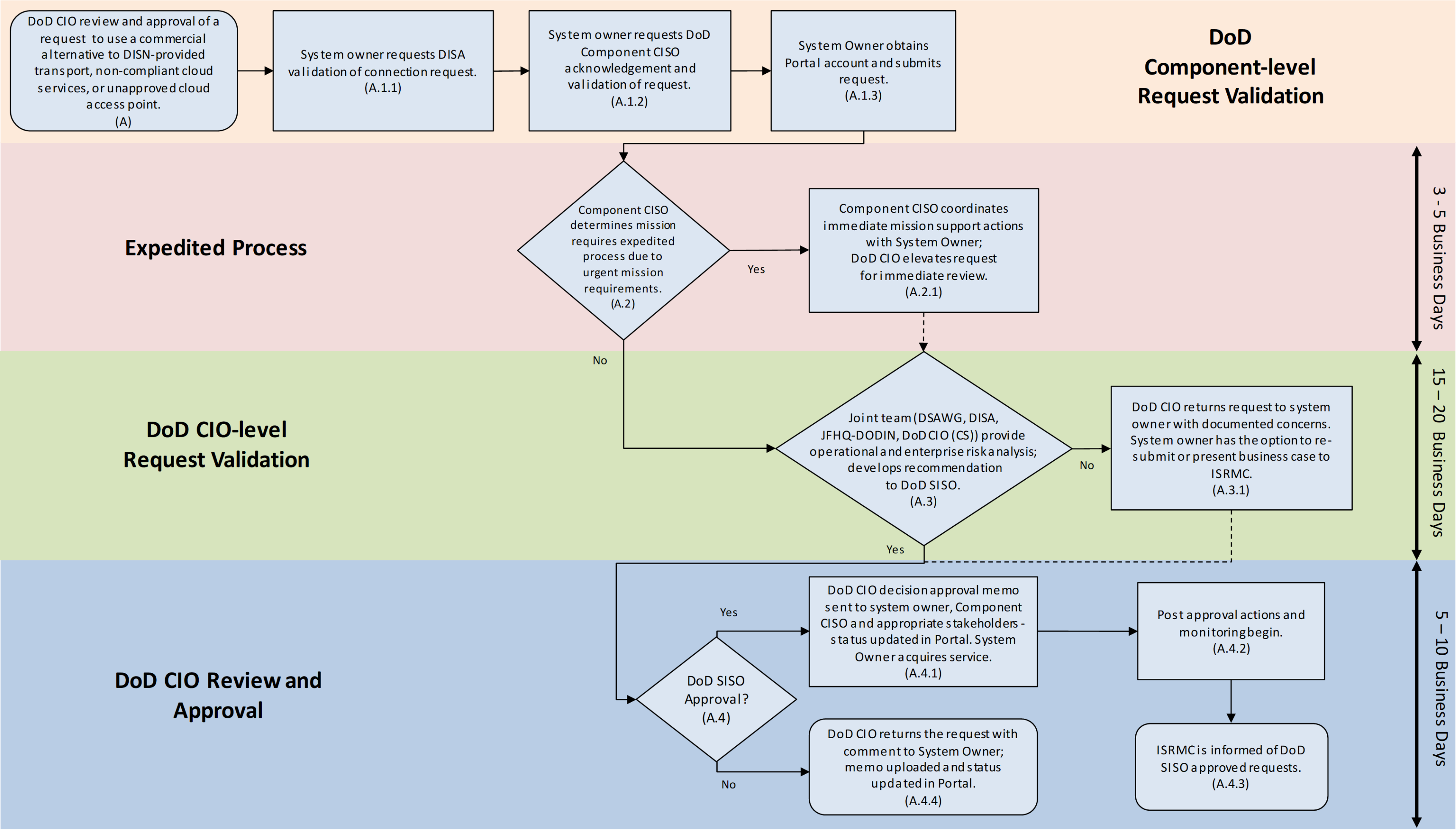

DoD CIO review and approval of a request to use a commercial alternative to DISN-provided transport, non-compliant cloud services, or unapproved cloud access point. (A)
System owner requests DISA validation of connection request. (A.1.1)
System owner requests DoD Component CISO acknowledgement and validation of request. (A.1.2)
System Owner obtains Portal account and submits request. (A.1.3)
DoD Component-level Request Validation
Expedited Process
Component CISO determines mission requires expedited process due to urgent mission requirements. (A.2)
Yes
Component CISO coordinates immediate mission support actions with System Owner; DoD CIO elevates request for immediate review. (A.2.1)
3 - 5 Business Days
No
DoD CIO-level Request Validation
Joint team (DSAWG, DISA, JFHQ-DODIN, DoD CIO (CS)) provide operational and enterprise risk analysis; develops recommendation to DoD SISO. (A.3)
No
DoD CIO returns request to system owner with documented concerns. System owner has the option to re-submit or present business case to ISRMC. (A.3.1)
15 – 20 Business Days
Yes
DoD CIO Review and Approval
Yes
DoD SISO Approval? (A.4)
No
DoD CIO decision approval memo sent to system owner, Component CISO and appropriate stakeholders - status updated in Portal. System Owner acquires service. (A.4.1)
Post approval actions and monitoring begin. (A.4.2)
DoD CIO returns the request with comment to System Owner; memo uploaded and status updated in Portal. (A.4.4)
ISRMC is informed of DoD SISO approved requests. (A.4.3)
5 – 10 Business Days

Figure 3 DoD CIO review and approval workflow for commercial alternatives to DISN-provided transport and non-standard cloud services and unapproved cloud access points

A.1. DoD CIO review and approval of requests for DODIN commercial connections and non-standard cloud services

A.1.1. System Owner requests DISA validation of connection request:

- Missions listed in Table 3 do not require DISA validation as they are validated for unclassified commercial connections per DoD policy.
- DISA reviews request and validates inability of an enterprise capability to meet mission requirements.
- If DISA can provide capability and it meets mission requirements, request is rejected. If requestor disagrees that DISA can provide capability, decision is elevated to DSAWG/ISRMC for review.

A.1.2. System Owner requests DoD Component Chief Information Security Officer (CISO) acknowledgment and validation of request:

- CISO (or deputy CISO if necessary) acknowledges the request complies with the component CIO policy and has an operational requirement.
- CISO office conducts initial review of the request and determines if the submission is valid, complete, and technically adequate. If the CISO non-concurs with the system owner's request, the CISO returns the package to the system owner with documented concerns.
- CISO will provide risk perception of request to DoD CIO. Requests will only be elevated to DoD CIO for review and approval following CISO review and concurrence.
- If the DoD Component does not have a CISO, the DoD CIO will coordinate the request with a representative of the DoD Component's CIO or senior IT official.

A.1.3. System owner obtains a SNAP account as described in Section 2.8 of this guide and submits a request for a DODIN commercial connection and cloud service under the "non-DISN Connections" module in SNAP.

- SNAP Portal URL: https://snap.dod.mil
  SNAP User Guide URL: https://snap.dod.mil/gcap/user-guide.do

- The system owner initiates DoD CIO review and approval of request by uploading the DoD CIO request template and required artifacts in SNAP. The intent of the registration is to capture the following key information, to include information to address conditions as outlined in DoDI 8010.01, section 4.4, E:

  - A Memo signed by DISA validating request (if request does not support a mission listed in Table 3)
  - A Memo signed by the DoD Component's CISO that acknowledges request and validates completeness of package.
  - Business case for request of Approved Alternate Connection (AAC), to include purpose or mission directive
  - Type of request: Temporary or Permanent/Enduring Mission Support
  - The sensitivity of the data being processed, stored, and transmitted

  - Plan for annual review of need for connection and compliance
  - Equipment used by the DoD Component on the DoD Approved Products List
  - Architecture and detailed topology diagram
  - Physical and/or logical separation (specify any requirement to connect to DISN)
  - Transition plan to DISN
  - Cybersecurity Service Provider (CSSP) Narrative
    - CSSP Alignment (Yes/No)
    - CONOPS (Incident Response, System Recovery, Vulnerability Management, Configuration Management)
    - If there is not a CSSP alignment, provide cybersecurity activities/defensive measures in response to vulnerabilities and threats as outlined in DoDI 8530.01
  - Business case cost analysis

- Templates for required artifacts can be found on the SNAP portal.

- This process is completely dependent on universal use of SNAP for processing of requests to include notifications, review, tracking, and approval. All required artifacts must be uploaded in SNAP portal.

> DODIN commercial connections are required to be logically and physically isolated from the DISN. Any exceptions that require configurations with any type of connectivity to DISN to support mission requirements must be implemented via a NIPRNet Federated Gateway (NFG) and must be approved by DoD CIO as illustrated in Figure 4.

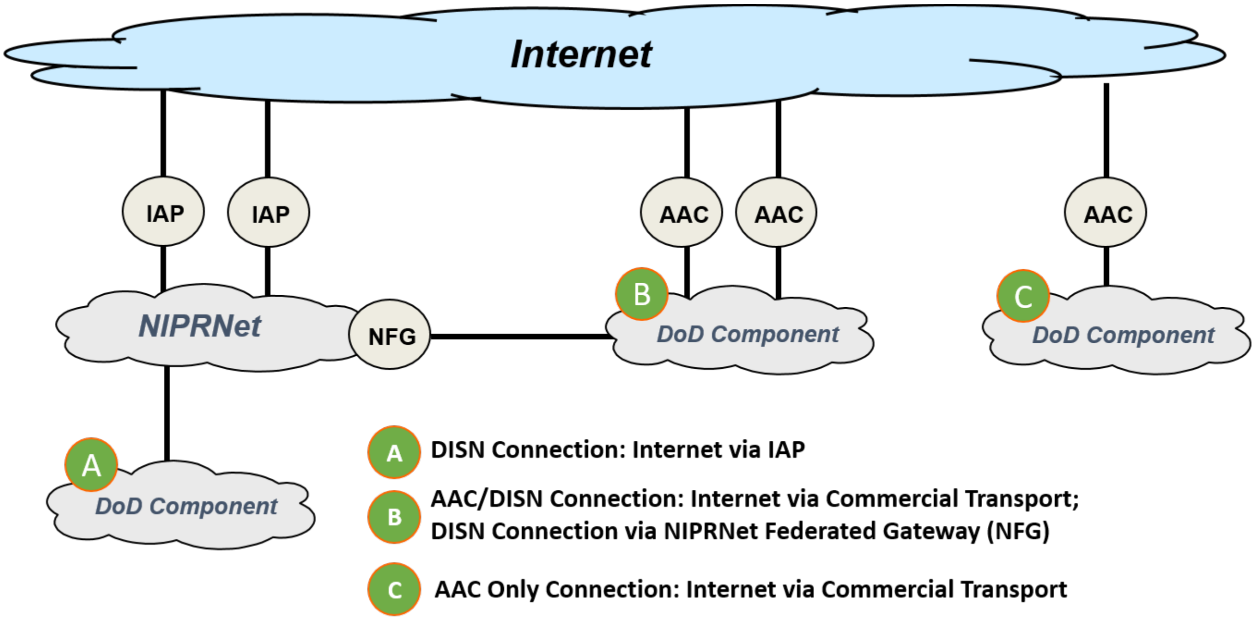

Internet
IAP
IAP
AAC
AAC
AAC
NIPRNet
NFG
B
DoD Component
C
DoD Component
A
DoD Component
A DISN Connection: Internet via IAP
B AAC/DISN Connection: Internet via Commercial Transport; DISN Connection via NIPRNet Federated Gateway (NFG)
C AAC Only Connection: Internet via Commercial Transport

Figure 4 DODIN Internet Gateways: Internet Access Points (IAP) and Authorized Alternate Connections (ACC) Connection Types

A.2. The DoD Component CISO determines request requires an expedited process due to urgent mission requirements.

- If an operational case exists with a need for immediate mission support with temporary requirements (less than 90 days), the request can be expedited. Expedited requests must be validated with DoD Component GO/FO level approval.

A.2.1. Service CISO coordinates immediate support actions: DoD CIO elevates request

- Component CISO acquires GO/FO validation, mission requirements, and coordinates immediate actions necessary to support system owner. DoD CIO moves request for immediate review and approval (five business days).

A.3. Joint Team Engineering Review and Analysis

- The office of the DoD Deputy CIO for Cybersecurity (DCIO CS) will act as the primary point of contact and will collaborate with the joint team consisting of the DSAWG Chair (represents and coordinates with voting members), DISA, JFHQ-DODIN to determine whether business case submission is valid, complete, and technically adequate. The joint team produces a report and submits a recommendation to the Principal Deputy (PD) CIO for Cybersecurity for approval or non-approval by the DoD CISO.

A.3.1 DoD CIO returns request to the system owner with documented concerns.

- If the request is determined not to be valid or complete, DoD CIO returns request package to the system owner with documented concerns.
- System owner has the option to address concerns and re-submit or present business case to ISRMC.

A.4. DoD CISO Approval

- DoD CISO reviews request package with corresponding recommendations from PD CIO for CS, the joint team, and the Component CISO.
- DoD CISO focus points include, but are not limited to:
    - Level of Sensitivity of Data Protected
    - Foreign Nationals
    - Physical and Logical Isolation from DISN
    - Strong Authentication
    - Device Hardening
    - Reduced Attack Surface
    - Alignment to Cybersecurity Service Provider
    - United States Cyber Command Responsiveness

A.4.1. DoD CISO Approves request and signs approval memo

- DoD CIO decision approval memo sent to system owner, Component CISO, and appropriate stakeholders - status is updated in SNAP accordingly.
- The system owner may then acquire the commercial connection in accordance with the approved Business Case Analysis.

Note that DoD Component orders for connections via DoD-approved Federal contracts (e.g., NETWORX) must come through DITCO as the mandated DoD ordering agency. DoD Components must attain DoD CIO approval for ALL commercial connections procured via DITCO. Ordering commercial circuits via DITCO does not exempt DoD CIO approval.

If the Component CIO determines that the DoD Component's alternate solution is more cost/mission effective than the DITCO solution, then the customer may choose their best option for ordering the service.

- For an approved cloud, service request, upon receipt of the approval notification, registers the use of the Cloud service as described in Appendix C of this guide.
- For an approved DoD Component Boundary Cloud Access Point (BCAP) or alternate CSO, the DoD CIO will send a copy of the approval notification to DISA Secure Cloud Computing Architecture (SCCA) PMO. The DISN CAO will add the approved Component BCAP or alternate CSO to SNAP as valid selections.
- For an approved Cloud Information Technology Project (C-ITP), the Mission Owner will upload the approval notification when registering the C-ITP in the SNAP Cloud C-ITP module as described in Section 2.8 of this guide.

DISA, DoD CIO, and U.S. CYBERCOM use entries in the SNAP "non-DISN Connections" module to identify emerging requirements that may lead to development of new or lower cost capabilities such as the DISN Private Data Internet Service Provider VPN service.

A.4.2. Post approval actions and monitoring begin

- Per DoDI 8010.01, section 4.4 C:
  "Authorized commercial connections are subject to CCRIs to ensure conformance with DoD cybersecurity requirements consistent with DoDI 8510.01, DoDI 8530.01, and other DoD cybersecurity policies and guidance."
- DoD CIO memo approvals will be tracked and monitored for expiration and compliance with caveats/directives specified in the memo.
- All DoD Components are required to comply with the standards and conditions set forth in the decision memo. Deviation or non-compliance at any point during the duration of the approval will be considered means for disconnection. Decision memos must be tracked by the DoD Component and maintained in a current status. Renewal requests are subject to full compliance of previous decision memos.

A.4.3. ISRMC is informed monthly of DoD CISO approved and returned requests.

A.4.4. DoD CISO returns request

- DoD CIO returns the request with comment to the DoD Component System Owner; memo is uploaded to portal and status is updated in portal.

END OF PROCESS. Process Duration: 30-45 Days

Appendix B Mission Partner Connections to DISN

DoDI 8010.01 paragraph 2.1.g states that the DoD Chief Information Officer (CIO) - "Reviews and approves DoD Component requests for mission partner connections to DISN." This Appendix describes the process illustrated in Figure 5 for a DoD Component request to connect a Mission Partner's enclave or network to the DISN.

Mission Partner Connections (MPC) are DISN connections for DoD Contractors; Federal Partners; or Allied/Coalition Partners. A DoD Component sponsor is required for DoD Contractors with a valid contract. A DoD CIO Memorandum of Agreement is required (IAW DoDI 8010.01) for a Federal Department/Agency Mission Partner connections to the DISN. A Joint Staff validated requirement is required for Allied and Coalition Partners for connection to the DISN. Federal Partners and Allied/Coalition Partners are connected through a Mission Partner Gateway, described in Appendix H of this guide.

B.1. The DoD Component sponsor submits a formal Mission Partner Connection (MPC) request to the DISN Service Manager.

B.1.1. For a DoD Contractor Connection:

When a DoD Component has a requirement for a DoD contractor connection to DISN, the DoD Component sponsor prepares a Validation Letter for Mission Partner Connections to DISN and a DoD Mission Partner Connection Briefing as described in Appendix M of this guide following the process identified in Figure 5. An O-6 equivalent or higher DoD Component sponsor must digitally sign the Validation Letter with the attached briefing and email the request to the appropriate DISN Service Manager (i.e., the SIPRNet Service Manager or NIPRNet/Virtual Private Network (VPN) Service Manager).

B.1.2. For a Federal Department or Agency Mission Partner Connection:

In general, the DoD Deputy CIO for Cybersecurity is the sponsor. A Memorandum of Agreement is entered into between DoD CIO and that Federal Department/Agency CIO IAW DoDI 8010.01. The MOA establishes the framework of cooperation between DoD and the Federal Partner. There can be special cases where a specific DoD organization may be the sponsor for a Federal Partner connection.

B.1.3. For an Allied and Coalition Mission Partner Connection:

When a Combatant Commander (COCOM) has a requirement to connect a Coalition partner to the DISN, the DoD Component sponsor prepares a Validation Letter for Mission Partner Connections to DISN and a DoD Mission Partner Connection Briefing as described in Appendix M of this guide. An O-6 equivalent or higher DoD Component sponsor must digitally sign the Validation Letter with the attached briefing and email the request to the appropriate DISN Service Manager (i.e., the SIPRNet Service Manager or NIPRNet/Virtual Private Network (VPN) Service Manager).

B.2. DISA Service Manager reviews/validates the service request

Either the DISN NIPRNet/VPN Service Manager or the SIPRNet Service Manager validates whether DISN can support the requested service. In most cases, this is a simple determination of whether the type of connection is appropriate and available. Some validations may require the DISN Service Manager to propose a different type of connection. An example of this may be proposing the use of a Demilitarized Zone connection (e.g., SIPRNet Federal DMZ), instead of a direct connection to the SIPRNet. If the request is validated, the DISN Service Manager digitally signs the formal request, and provides a validation number. The DISN Service manager then emails the validation or rejection of the request to the DoD Component CISO for review.

B.3. The DoD Component CISO Reviews the DoD Component request

B.3.1. For a DoD Contractor, Allied, or Coalition Partner Connection:

The Component CISO[14] reviews the DoD Component request for adequacy, and completeness of the cybersecurity requirements. For Allied and Coalition Partner connections Joint Staff J6 CISO Rep performs this function. If the DoD Component CISO rejects the request, the CISO will provide additional guidance to the submitting organization for revising and resubmitting the request. If the request meets the cybersecurity requirements, the DoD Component CISO digitally signs the request and forwards the request to DoD CIO.

B.3.2. For a Federal Department or Agency Mission Partner Connection:

DoD CIO OPR works with the Federal Partner to develop a Memorandum of Agreement (MOA) IAW Figure 6. The MOA is reviewed by both parties, to include a General Council review. The DoD CISO is the sponsor for Federal Department and Agency Mission Partner Connections, and they are signed by the DoD CIO and the Federal Department or Agency CIO.

B.4. DoD CISO reviews the DoD Component request

DoD CISO staff reviews the DoD Component request for cybersecurity requirements. To be approved the DoD Component must execute an agreement with a qualified Cybersecurity Service Provider.

B.4.1. DoD CISO rejects the request for a Mission Partner Connection

If the request does not meet cybersecurity requirements, DoD CISO will send a rejection notification with additional guidance to the DoD Component sponsor organization that originated the request with copies to the DoD Component CISO, DCSA, US Cyber Command, and others for situational awareness. The DoD Component sponsor may then resubmit the request as described in Section B.1 of this guide.

B.4.2. DoD CISO approves the request for a Mission Partner Connection

If the request meets the cybersecurity requirements, the DoD Chief Information Security Officer (CISO) signs an approval memorandum with caveats. Approval caveats must be achieved to maintain DoD CISO approval for connection. DoD CIO OPR sends the DoD CISO approval Memorandum to the DoD Component sponsor organization that originated the request with copies to the DoD Component CISO, DISA, DCSA, US Cyber Command, and others for situational awareness. The DoD CISO approval shall be valid for up to three years and shall be reviewed annually to determine if the sponsor is maintaining the mission partner connection within the risk appetite of the DoD CISO.

[14] Click here for the link to the DoD Component CISO List. The Joint Staff CISO reviews COCOM requests to connect an Ally or Coalition partner network or information system to DISN.

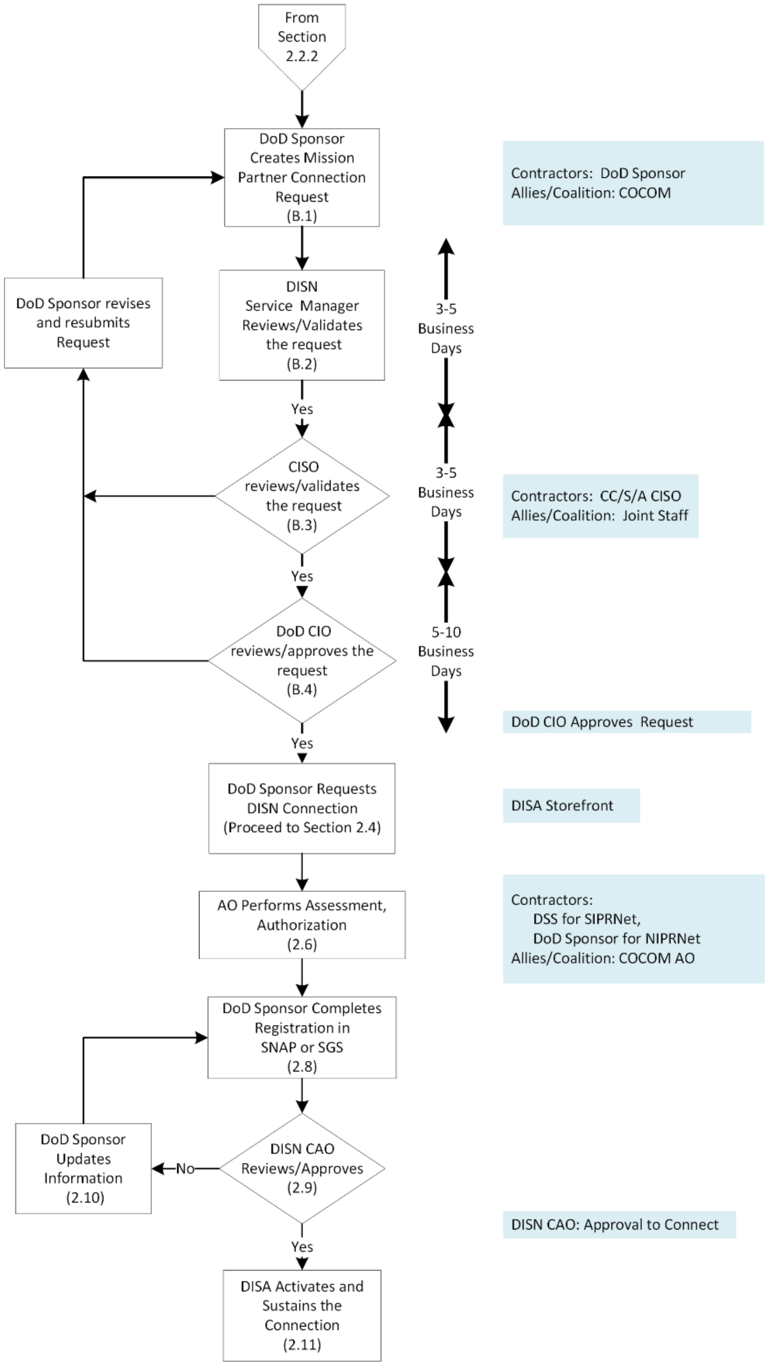

From Section 2.2.2
DoD Sponsor Creates Mission Partner Connection Request (B.1)
Contractors: DoD Sponsor
Allies/Coalition: COCOM
DoD Sponsor revises and resubmits Request
DISN Service Manager Reviews/Validates the request (B.2)
3-5 Business Days
Yes
CISO reviews/validates the request (B.3)
3-5 Business Days
Contractors: CC/S/A CISO
Allies/Coalition: Joint Staff
Yes
DoD CIO reviews/approves the request (B.4)
5-10 Business Days
DoD CIO Approves Request
Yes
DoD Sponsor Requests DISN Connection (Proceed to Section 2.4)
DISA Storefront
AO Performs Assessment, Authorization (2.6)
Contractors:
DSS for SIPRNet,
DoD Sponsor for NIPRNet
Allies/Coalition: COCOM AO
DoD Sponsor Completes Registration in SNAP or SGS (2.8)
DoD Sponsor Updates Information (2.10)
No
DISN CAO Reviews/Approves (2.9)
DISN CAO: Approval to Connect
Yes
DISA Activates and Sustains the Connection (2.11)

Figure 5 DoD Mission Partner Connections to DISN

For a Federal Department or Agency Mission Partner Connection, DoD CIO and the Federal Partner agree to an MOA, and both parties sign the MOA. The MOA shall be valid for up to nine years and shall be reviewed annually.

When registering a Mission Partner connection request in SNAP or SGS, the DoD Component Sponsor must also upload the DoD CISO approval memo into the SNAP/SGS entry and select the “OSD Approved” option.

Once the DoD Component sponsor receives DoD CISO approval memo (or signed MOA), the DoD Component sponsor can initiate a DISN connection request as described starting at Section 2.4 of this guide. Note: When registering the connection request in SNAP/SGS as described in Section 2.8 of this guide, the DoD Component sponsor must also upload the DoD CISO approval memo into the SNAP/SGS entry and select the “OSD Approved” option.

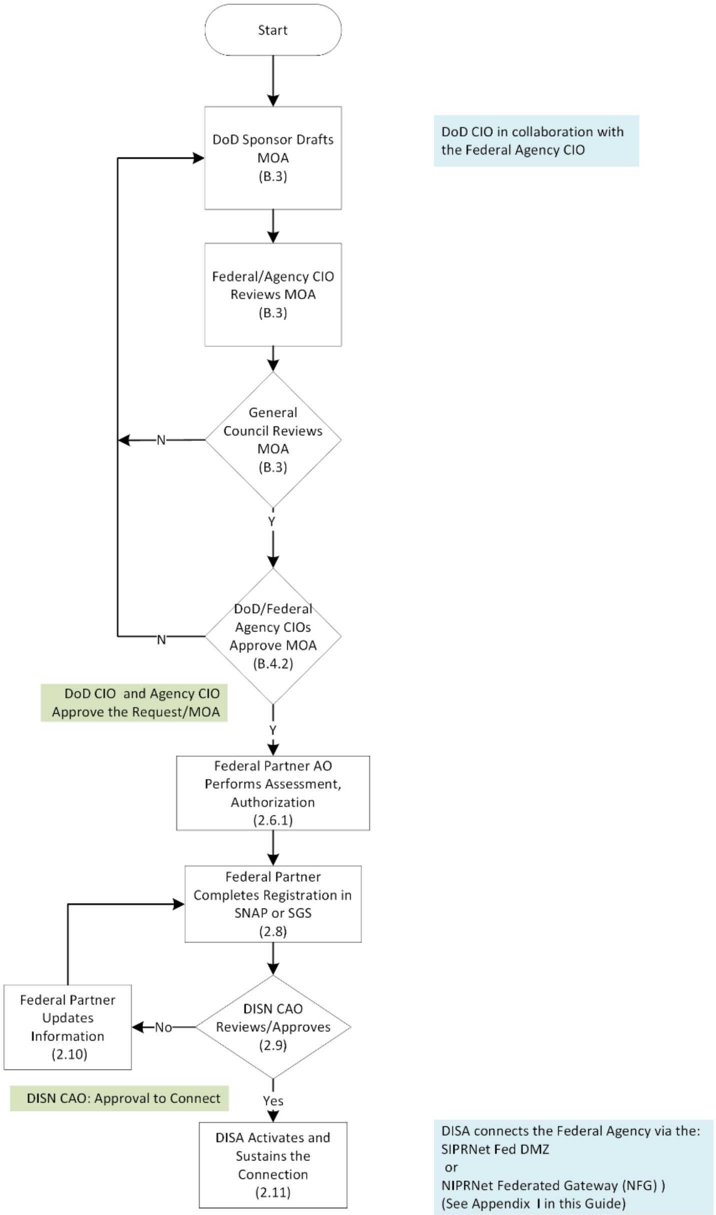

Start
DoD Sponsor Drafts MOA (B.3)
DoD CIO in collaboration with the Federal Agency CIO
Federal/Agency CIO Reviews MOA (B.3)
General Council Reviews MOA (B.3)
N
Y
DoD/Federal Agency CIOs Approve MOA (B.4.2)
N
DoD CIO and Agency CIO Approve the Request/MOA
Y
Federal Partner AO Performs Assessment, Authorization (2.6.1)
Federal Partner Completes Registration in SNAP or SGS (2.8)
DISN CAO Reviews/Approves (2.9)
No
Federal Partner Updates Information (2.10)
DISN CAO: Approval to Connect
Yes
DISA Activates and Sustains the Connection (2.11)
DISA connects the Federal Agency via the:
SIPRNet Fed DMZ
or
NIPRNet Federated Gateway (NFG))
(See Appendix I in this Guide)

Figure 6 DoD CIO MOA for a Federal Mission Partner Connection to DISN

Appendix C Cloud Information Technology Project (C-ITP) Registration and Connection Process

This appendix describes the process used by a DoD Mission Owner to register and connect a Cloud Information Technology Project (C-ITP) to the DISN. IAW the DoD Cloud Computing Security Requirements Guide (CC SRG), "All Mission Owners are required to register all Cloud based systems/applications, their CSP/CSO, MCD [i.e., Mission Cyberspace Defense (MCD) provider], and connection method in the DISA Systems/Network Approval Process (SNAP) database Cloud Module."

Note: This appendix addresses the registration and connection of a Mission Owner's Cloud IT Project (C-ITP) to a Cloud Service Offering (CSO) via the DISN[15]. It assumes that the Mission Owner has an existing communications connection to the DISN. Instructions for obtaining a communications connection to the DISN are provided in Section 2 of this guide.

Figure 7 and Sections C.1 through C.9 describe the process used by a Mission Owner (a Cloud Consumer) to register, connect via the DISN, and onboard a C-ITP to a CSO that has an appropriate DoD Provisional Authorization (DoD PA). A computer-based presentation of the process for registration and connection of a C-ITP is available on the DISA's Risk Adjudication and Connection Division's Mission Partner Training Program (MPTP) website.

C.1. Mission Owner Initiates a Cloud Information Technology Project

For the purpose of this guide, a DoD C-ITP is a software application or information service implemented (or onboarded) into a DoD provisionally authorized CSO.

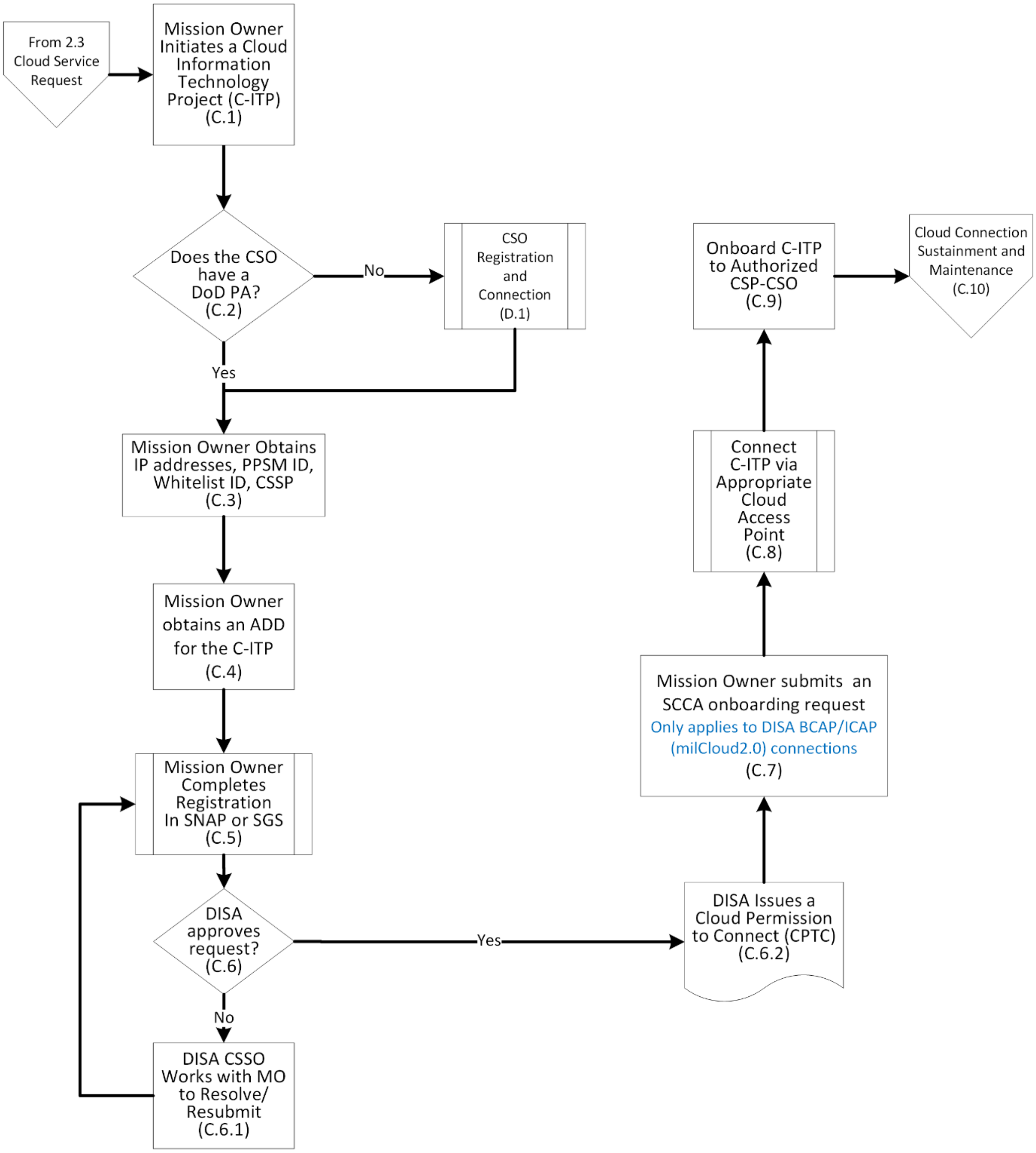
The DoD Component Cloud Migration Offices listed in Appendix L will assist their Mission Owners tasked with initiating a C-ITP and selecting an appropriate CSO. Mission Owners that do not have a Component Cloud Migration Office listed in Appendix L should contact their DoD Component CIO. Mission Owners may also contact the DISA Mission Partner Engagement Office for general assistance with DISA Cloud authorization, registration, connection, and

> DISA wrote the Best Practices Guide for Department of Defense Cloud Mission Owners who are planning to migrate (or onboard) an existing information system from a physical environment to a virtualized cloud environment. This guide is not DoD policy. Instead, it documents best practices discovered during DoD CIO Cloud implementation efforts. Additionally, the DISA Risk Adjudication and Connection Division's Mission Partner Training Program (MPTP) provides scheduled live training sessions via Defense Collaborative Service (DCS) and teleconference, 24/7 user-accessible computer-based training materials, and education opportunities for cloud onboarding. For additional information about the MPTP contact DISA's Risk Adjudication and Connection Division's Mission Partner Training Program (MPTP) or the DISN CAO. Another useful reference is the DoD CIO Enterprise Cloud Community website.

[15] This version of the DCPG describes the process used by a DoD Mission Owner to register and connect a Cloud Information Technology Project (C-ITP) that is transitioning from a legacy data center environment to a virtual cloud computing environment. There are ongoing efforts to update the Cloud registration and connection process to include Enterprise General Purpose Cloud computing services delivered under the recently awarded JEDI contract as well as basic use of Cloud computing services that require on-demand-self-service, rapid elasticity, and measured service as defined in NIST 800-145. Registration and connection procedures for these Cloud services will be included in updates to this guide.

onboarding processes. When selecting a CSO, the Mission Owner should also consider the most appropriate Cloud Deployment Model, and the most appropriate Cloud Service Model. For details, see NIST Special Publication 800-146.

Figure 7   C-ITP Registration and Connection


From 2.3 Cloud Service Request
Mission Owner Initiates a Cloud Information Technology Project (C-ITP) (C.1)
Does the CSO have a DoD PA? (C.2)
No
CSO Registration and Connection (D.1)
Yes
Mission Owner Obtains IP addresses, PPSM ID, Whitelist ID, CSSP (C.3)
Mission Owner obtains an ADD for the C-ITP (C.4)
Mission Owner Completes Registration In SNAP or SGS (C.5)
DISA approves request? (C.6)
Yes
No
DISA CSSO Works with MO to Resolve/ Resubmit (C.6.1)
DISA Issues a Cloud Permission to Connect (CPTC) (C.6.2)
Mission Owner submits an SCCA onboarding request
Only applies to DISA BCAP/ICAP (milCloud2.0) connections
(C.7)
Connect C-ITP via Appropriate Cloud Access Point (C.8)
Onboard C-ITP to Authorized CSP-CSO (C.9)
Cloud Connection Sustainment and Maintenance (C.10)

C.2. Does the selected CSO have an appropriate DoD Provisional Authorization (DoD PA)?

The Mission Owner must determine the Impact Level (IL) of the C-ITP using guidance provided in paragraph 3 of the DoD CC SRG. After determining the IL of the C-ITP, the Mission Owner must determine if the desired CSO for hosting C-ITP is authorized and registered. The Mission Owner should review the FedRAMP Marketplace for an approved IL2 CSO and verify if the CSO is registered in the SNAP database. For IL4, IL5, and IL6 CSOs, a DoD Provisional Authorization is required. Current and candidate CSOs at IL4, IL5, and IL6 are listed in the DoD Cloud Authorization Services (DCAS) portal and current CSOs are registered in SNAP (IL4 and IL5) or SGS (IL6). Candidate CSOs will be registered in SNAP or SGS once the DoD PA is issued. If the CSO is registered in the DISA SNAP or SGS systems, the Mission Owner can proceed to Section C.3 of this Appendix.

If the selected CSO **is not** listed or is not authorized at the required IL, then the Mission Owner may:

- If the desired IL2 CSO is FedRAMP approved but is not registered in SNAP, contact the CAO Cloud Team for assistance. Download the IL2 Moderate reciprocity memo from the Current CSOs tab on the DCAS portal for use as the CSO authorization.
- If the desired IL2 CSO is not FedRAMP approved, contact the DCAS Team.
- Proceed to Appendix D and sponsor the CSO for an appropriate DoD PA for IL4, IL5, and IL6 requirements.
- Proceed to Appendix A to request DoD CIO approval for an exception to policy

C.3. Mission Owner obtains IP addresses, PPSM ID, Whitelist ID, and aligns with a Cybersecurity Service Provider (CSSP)

The Mission Owner obtains information needed to complete registration and connection of the C-ITP.

C.3.1. Mission Owner Obtains IP Addresses

If the selected CSO (e.g., milCloud 2.0) is in the DISA SNAP for IL4, IL5 CSOs, or SGS for IL6 CSOs and has the appropriate IL DoD PA, the DoD Mission Owner obtains IP addresses required to use the Provisionally Authorized CSO.

- For an **IaaS** or **PaaS** CSO, the Mission Owner enters the IP addresses assigned to the C-ITP by the NIC
- For a **SaaS** CSO, the Mission Owner enters the Government enclave IP address ranges the Mission Owner wants DISN to advertise to the SaaS CSO provider

DoDI 8410.01 requires DoD to conduct public and private Internet-based communications (e.g., electronic mail and Web operations) under the “*.mil”* Top Level Domain. (Some IL 4 or 5 CSOs are approved to use **commercial IP addressing**. A VPN is required to connect with these CSOs[16]). The Mission Owner is responsible for obtaining required IP addresses for a C-ITP or

[16] Mission Owners planning to connect to an IL 4 or 5 CSO that uses commercial IP addresses:

for a sponsored CSO. The CC SRG (paragraph 5.10.4) stipulates requirements for IP Addressing and Domain Name Services (DNS) and provides guidance for situations in which DoD Network Information Center (NIC) assigns DoD IP addresses and those situations where the CSP provides commercial IP addresses. The SCCA Knowledge Center also includes a tab for "Obtaining Cloud IP Space."

Note that the NIC has allocated IP address space for CSOs to the DoD Component Cloud Migration Offices. The NIC website identifies DoD Component points of contact (POC) for the assigned IP address. Access the NIC website as follows:

a. Log into https://www.nic.mil

b. Select "Whois Search."

c. Type in: **CLOUD***

d. Under the column labeled "Network Name," find the desired CSO aligned with your DoD Component (e.g., "CCSNET-AF-SAAS-ORACLE," "CCSNET-ARMY-IAAS-AWS_WEST").

e. Double click on the associated "handle" to identify the DoD Component POC to contact for additional direction.

If none of the listed "Network Names" supports your requirement, contact the DoD Component Cloud Migration Office, DISA SCCA PMO, or NIC for guidance to obtain needed IP addresses.

The DoD Network Information Center (NIC) Registry Protocol 9802 provides the Mission Owner additional information on assignment and registration of DoD IP address space and IP numbered resources.

The SCCA Mission Partner Home website contains information Mission Owners may use as a guide when working with their Component and DISA subject matter experts to develop a formal cloud transition plan.

C.3.2. Mission Owner obtains a PPSM Tracking Identifier

IAW DoDI 8551.01, Ports, Protocols, and Services Management (PPSM) DISN customers must register their system's ports and protocols in either the SIPRNet or NIPRNet version of the PPSM Registry as appropriate. DISN CAO will only approve a connection request that includes a valid PPSM Tracking Identifier. Customers may collaborate with their DoD Component's PPSM TAG representative to get ports, protocols, and services (PPS) registered in the PPSM Registry located on SIPRNet or NIPRNet. A PPSM account is required for access. Request accounts through your DoD Component PPSM TAG representative.

For more information on PPSM, please refer to Section 2.7.3 of this guide, the DISA RE4 PPSM home page, the DISA PPSM web page, or contact the DoD PPSM team (DISA RE4).

- Contact your DoD Component Migration Office for guidance since your DoD Component may have established a VPN for the desired CSO, also DISA established a Cloud VPN Community of Interest (VPN ID: DKL30035)
- Submit a request for a VPN connection to the CSO IAW the process starting at Section 2.4 in this guide as supplemented with information in Appendix K, VPN Registration. In parallel with the VPN request, continue the process in Section C.3.2 for also requesting to use the CSO.

C.3.3. Mission Owner Obtains NIPRNet DMZ Whitelist registration ID

A Mission Owner’s C-ITP that requires information to traverse both the NIPRNet and the Internet may need to register this requirement in the NIPRNet DMZ Whitelist located on SIPRNet. Registration may be required to ensure the DISN Internet Access Points (IAPs) are configured to permit information to flow between the Internet and NIPRNet. The Mission Owner should consult with their DoD Component’s PPSM TAG representative to determine whether the ports, protocols and services required by the C-ITP must be registered in the NIPRNet DMZ Whitelist. See “DoD Whitelist” in the CC SRG.

C.3.4. Mission Owner aligns the C-ITP with a Security Operations Center (SOC) supported by a Cybersecurity Service Provider (CSSP)

DoDI 8530.01 and the CC SRG require all DoD Information systems to align with a SOC supported by a CSSP. The DWCF Rate Book includes billing information for DISA provided CSSP subscription services. U.S. CYBERCOM maintains a list of DoD certified and accredited CSSPs under the Cybersecurity Service Provider (CSSP) Program. The Defense Working Capital Fund (DWCF) Rate Book includes billing information for Cybersecurity services provided by the DISA CSSP Office.

C.4. Mission Owner obtains an Authorization Decision Document (ADD) for the C-ITP to operate within the CSO

IAW DoDI 8510.01 and the CC SRG , the Mission Owner must categorize, assess, and authorize the C-ITP to operate within the provisionally authorized CSO. Section 2.6 of this guide describes this process. The Mission Owner must obtain an Authorization to Operate (ATO) or Interim Approval to Test (IATT) to register and connect the C-ITP to a provisionally authorized CSO via the DISN. The C-ITP must have an ATO to operate in the cloud before going operational.

> *“Prior to operational use, all cloud services must have an Authority to Operate granted by the PM/FSM’s Authorizing Official. PMs/FSMs that acquire or use cloud services remain responsible for ensuring that end to end security and computer network defense requirements are met.”* DoDI 5000.74

C.5. Mission Owner Completes Registration of the C-ITP in DISA SNAP or SGS

DoD uses the DISA SNAP or SGS registration process to initiate, track, and manage C-ITPs connections to CSOs via DISN. As stated in the CC SRG , a Mission Owner must register an IL2, IL4,or IL5 (unclassified) C-ITP in the DISA SNAP database or an IL6 (secret) C-ITP in the DISA SGS database consistent with DoDI 8010.01, DoDI 5000.74, and CJCSI 6211.02D.[17] The “Mission Owner (Cloud IT Project)” module in the DISA SNAP database provides workflow status, and a place for the Mission Owner to store required documentation and artifacts.

[17] Note: A single C-ITP registration is sufficient for a family of applications that share the same DoD Component owner, the same Cloud Service Offering, the same Cloud Service Model (i.e., IaaS, PaaS, SaaS), and the same Impact Level.

C-ITP Naming Convention:

- When registering the C-ITP in SNAP or SGS, recommend that the Mission Owner use the same name as the Unique Investment Identifier (UII)/Investment Name used in DITIP, SNaP-IT, DITPR, or SITR and be identified on the Authorization Decision Document for the C-ITP.
- The DoD FY20XX IT-1 Report is a Microsoft Excel spreadsheet listing unclassified UIIs. These reports are hosted on the CAPE web page.

IP addresses for the C-ITP

SNAP/SGS requires the Mission Owner to enter:

- For an **IaaS** or **PaaS** CSO, the Mission Owner enters the IP addresses assigned to the C-ITP by the NIC (see Section C.3 of this guide).
- For a **SaaS** CSO, the Mission Owner enters the Government enclave IP address ranges the Mission Owner wants DISN to advertise to the SaaS CSO provider.

C.5.1. **Mission Owner logs into SNAP or SGS and enters required information**

Section 2.8 of this guide describes the steps for obtaining an account and registering connection information in SNAP or SGS. When logged into SNAP or SGS, the C-ITP Mission Owner selects the “Mission Owners (Cloud IT Project)” module, enters the required information, and uploads documents as described in Section 2.8.3 of this guide.

When the Mission Owner has completed all SNAP/SGS information sections and uploaded Security Package documentation, a “SUBMIT” button will appear at the bottom of the screen. The Mission Owner selects this button to submit the connection request to DISN CAO for review.

C.6. Does DISN CAO approve the connection request submitted in SNAP or SGS?

The DISN CAO reviews the Mission Owner’s request for connection to a provisionally authorized CSO as described in Section 2.9 of this guide and additionally determines whether:

- The C-ITP connects to a CSO with an appropriate DoD PA. (If not, the Mission Owner must upload a DoD CIO approval memo obtained using the process described in Appendix A of this guide)
- The C-ITP connects to the CSO via a DoD CIO-approved Cloud Access Point (CAP)

C.6.1. **DISN CAO works with the Mission Owner to resolve issues.**

The DISN CAO analyst will not issue a Cloud Permission to Connect (CPTC) for a C-ITP connection request if the Mission Owner’s submission is incomplete, or if there is an issue that the Mission Owner needs to address (see Section 2.9 of this guide for DISN CAO review criteria). The DISN CAO analyst will identify corrective actions needed for the C-ITP to obtain a CPTC. SNAP/SGS will notify the Mission Owner POCs identified in the connection request about the needed corrective actions. The Mission Owner logs into SNAP/SGS, makes the needed updates, and resubmits the connection request to DISN CAO as described in Section C.5 of this guide.

C.6.2. DISN CAO approves the C-ITP connection request and issues a CPTC

C.6.2.1. CPTC for Connections via a DISA Boundary Cloud Access Point (BCAP) or Internal Cloud Access Point (ICAP). When DISN CAO approves the connection request, SNAP/SGS will issue a CPTC for the C-ITP to the points of contact registered in SNAP or SGS. The DISN CAO will notify the SCCA PMO when issuing a CPTC for a DISA BCAP or ICAP connection. The DISA SCCA PMO requires a CPTC for connections to the DISA BCAP or ICAP (serving milCloud 2.0). (See paragraph 5.10.1 of the CC SRG for the explanation of BCAP, ICAP, and IAP.)

The DISN CAO analyst will also approve a CPTC for a C-ITP that has an Interim Approval To Test (IATT) issued by its AO. For example, a Mission Owner may need to connect via the DISA BCAP to develop and test interoperability with the Virtual Data Center Security Stack (VDSS). The CPTC will permit a connection to the DISA BCAP for up to 90-days. IAW DoDI 8510.01, the IATT issued by the AO will be for testing purposes only and not for operational purposes. The Mission Owner must obtain an ATO to operate in the cloud before the 90-day CPTC expires. Otherwise, the DISN CAO will collaborate with the DISA SCCA PMO and the Mission Owner to determine if DISN CAO should allow the CPTC to expire or extend it for an additional 90 days. If allowed to expire, DISN CAO will notify the Mission Owner and the DISA SCCA PMO will discontinue the C-ITP's connection to the DISA BCAP. The DISN CAO will issue a 90-day CPTC for testing purposes if the AO has issued an IATT for the C-ITP. Proceed to **Section C.7**.

C.6.2.2. CPTC for Connections to Impact Level 2 CSOs or milCloud 1.0. The CPTC issued by SNAP/SGS simply acknowledges successful registration of the IL2 C-ITP. Proceed to **Section C.8.**

C.6.2.3. CPTC for Connections via a DoD Component (non-DISA) BCAP or ICAP. A CPTC issued by SNAP/SGS simply acknowledges that the C-ITP has successfully registered in SNAP/SGS. The CPTC issued by SNAP/SGS does not authorize the C-ITP to connect via a DoD Component BCAP or ICAP. The owning DoD Component decides whether to permit a C-ITP to connect via that DoD Component's BCAP or ICAP. Proceed to **Section C.8.**

C.7. Mission Owner submits an SCCA onboarding service request for connections via a DISA BCAP or ICAP (milCloud 2.0)

This step only applies to Mission Owners requesting a connection via a DISA BCAP or ICAP (serving milCloud 2.0). (See paragraph 5.10.1 of the CC SRG for the explanation of BCAP, ICAP, and IAP).

Once DISN CAO issues the Cloud Permission to Connect (CPTC) the DISA SCCA PMO works to engineer the connection of an IL4 or IL5 C-ITP to a DISA BCAP or ICAP (serving milCloud 2.0). To start the process, the Mission Owner uses their browser to access the Secure Cloud Computing Architecture (SCCA) Onboarding web page and completes the SCCA Onboarding

> There is no separate cost to connect to the DISA BCAP or ICAP. These costs are included in the DISN rates.
>
> The cost of optional SCCA services (VDSS, VDMS) is in the Defense Working Capital Fund (DWCF) Rate Book (See CS-ES-10).

service request form. The SCCA PMO uses this information to manage and implement applicable services for the DISA BCAP or ICAP (milCloud 2.0), Virtual Datacenter Security Stack (VDSS), and Virtual Datacenter Management Services (VDMS). See the SCCA Knowledge Center for details about the DISA BCAP, ICAP and SCCA onboarding.

C.7.1. DISA Conducts Periodic Deep Dive Meetings for connections via the DISA BCAP

DISA SCCA PMO may host a series of deep dive technical and/or policy centric meetings with the Mission Owner and other stakeholders to exchange detailed information that supports the registration and connection via a DISA BCAP or ICAP. See the DISA SCCA PMO website for additional information about deep dive meetings.

C.8. Connect a C-ITP to a Provisionally Authorized CSO via an appropriate CAP

Once the Mission owner has registered the C-ITP in the SNAP or SGS databases, and the DISN CAO has issued the a CPTC, the next steps to activate the connection will depend upon the IL of the C-ITP and the CAP (BCAP, ICAP, IAP) the Mission Owner will use to connect to the CSO as illustrated in Figure 8.

C.8.1. An Impact Level 2 C-ITP connection to an off-premises Impact Level 2 CSO via an Internet Access Point (IAP)

An IL2 C-ITP connects to an off-premises IL2 CSO via a NIPRNet Internet Access Point (IAP). Once the DISN CAO issues the CPTC, the Mission Owner in coordination with the DoD Component Cloud Migration Office may contact the CSP to commence onboarding of the C-ITP using the provisionally authorized CSO. The Mission Owner may need to work with their DoD Component PPSM TAG representative to determine if the C-ITP's IP addresses, ports, protocols and services used to access the CSO must be registered in the NIPRNet DMZ Whitelist to enable connection between the CSO and C-ITP via the NIPRNet IAP.

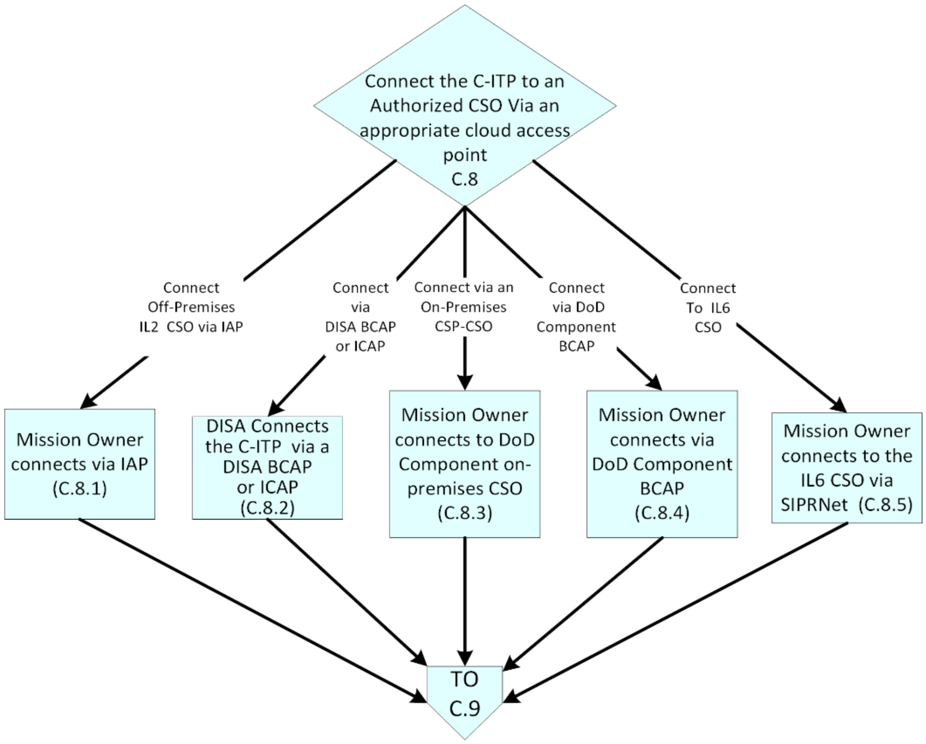
> DoD CIO Memo - Treatment of Personally Identifiable Information within Impact Level 2 Commercial Cloud Services for the Department of Defense" establishes Cloud Security IL2 as the minimum cybersecurity requirement for DoD applications/systems containing low confidentiality impact level Personally Identifiable Information (PII), as determined IAW NIST SP 800-122.

C.8.2. DISA Connects a C-ITP to a Provisionally Authorized CSO via a DISA BCAP or ICAP

DISA SCCA PMO uses the information submitted by the Mission Owner via the SCCA Onboarding Service Request and gathered in deep dives meetings (see Section C.7 of this guide) to implement the C-ITP connection to the provisionally authorized CSO via a DISA BCAP or ICAP.

If the C-ITP will be accessed by users connecting via the Internet, then Mission Owners may need to work with their PPSM TAG representative to determine if the C-ITP's IP addresses, ports, protocols and services need to be registered in the NIPRNet DMZ Whitelist to enable connections to the C-ITP via the NIPRNet IAP.

Figure 8 C-ITP Connection to a Provisionally Authorized CSO via the appropriate CAP


Connect the C-ITP to an Authorized CSO Via an appropriate cloud access point C.8
Connect Off-Premises IL2 CSO via IAP
Connect via DISA BCAP or ICAP
Connect via an On-Premises CSP-CSO
Connect via DoD Component BCAP
Connect To IL6 CSO
Mission Owner connects via IAP (C.8.1)
DISA Connects the C-ITP via a DISA BCAP or ICAP (C.8.2)
Mission Owner connects to DoD Component on-premises CSO (C.8.3)
Mission Owner connects via DoD Component BCAP (C.8.4)
Mission Owner connects to the IL6 CSO via SIPRNet (C.8.5)
TO C.9

C.8.2.1. **Mission Owner Onboarding a C-ITP to DISA milCloud 2.0**. The DISA milCloud 2.0 portal has instructions for onboarding to this cloud service. The DWCF Rate Book includes subscription rates for milCloud 2.0 services.

C.8.2.2. **Mission Owner Onboarding a C-ITP to a Commercial off-premises CSO**. The Mission Owner may contact the CSP to commence onboarding of the C-ITP using the selected CSO in coordination with the DoD Component Cloud Migration Office.

C.8.3. Mission Owner connects a C-ITP to a DoD Component's on-premises CSO

A C-ITP connects to a DoD Component's on-premises CSO via an ICAP (see the CC SRG paragraph 5.10.1.2) owned and operated by the hosting DoD Component and not via a DISA CAP. The Mission Owner then may contact the owning DoD Component to commence connection and onboarding of the C-ITP using the selected CSO in coordination with the Mission Owner's DoD Component Cloud Migration Office.

C.8.4. Mission Owner Connects a C-ITP to a Provisionally Authorized CSO via a DoD CIO-approved DoD Component (non-DISA) BCAP[18]

Normally all IL4 and IL5 CSOs connect to the DISN via a DISA BCAP. However, a CSO may connect to a DoD CIO-approved DoD Component (non-DISA) BCAP.[19] The Department of the Navy Cloud Service Management Organization (Cloud SMO) operates a DoD CIO Approved DoD Component BCAP. DISN CAO will issue a CPTC for the connection to acknowledge that the C-ITP is registered in SNAP or SGS.

Requirements for a DoD Mission Owner to Connect a C-ITP to **DoD Component (non-DISA) BCAP** are:

- The Mission Owner obtains concurrence from the DoD Component BCAP office
- The C-ITP has an ATO issued by the C-ITP AO
- The C-ITP is registered in the DISA SNAP or SGS Databases
- The CSO has a DoD PA for the appropriate IL. See Para C.2 if the DoD PA is not available.

C.8.5. A C-ITP connection to an Impact Level 6 (Secret-level) CSO

C-ITPs must connect to an authorized IL4/IL5 CSO via an appropriate DoD CIO-approved CAP listed in SNAP/SGS. Appendix A of this guide outlines the process for a DoD Component to request DoD CIO approval of a DoD Component BCAP.

DoD authorizes an IL6 CSO to accommodate classified national security information. The classification determination is pursuant to (i) Executive Order 13526, *Classified National Security Information* (December 29, 2009), or (ii) pursuant to the Atomic Energy Act of 1954, as amended, (Public Law 83-703)16 to be Restricted Data (RD).

An on-premises or off-premises IL6 CSO currently connects directly to SIPRNet as explained in the CC SRG (see paragraph 5.10.1.3). The Mission Owner may contact the CSP to commence implementation of the C-ITP using the selected CSO in coordination with its DoD Component Cloud Migration Office. DISA's milCloud 1.0 offers a SECRET IaaS/PaaS CSO connected to SIPRNet. The DISA milCloud website has instructions for registration, connection, and onboarding to this cloud service.

[18] *"Commercial cloud services hosting controlled unclassified information or non-publicly releasable information outside of the Department's security boundary must be connected to the Department of Defense Information Network (DODIN) through a Cloud Access Point that has been approved by the Information Security Risk Management Committee and the DoD CIO, in accordance with connection approvals in the Chairman of the Joint Chiefs of Staff Instruction 6211.02D."*-- DoDI 5000.74, Defense Acquisition Services

[19] *"Commercial cloud services used for Sensitive Data must be connected to customers through a Cloud Access Point (CAP) provided by DISA or through a CAP provided by another DoD Component. All CAPs must be approved by DoD CIO. The current Navy CAP is an example of an approved provisional cloud access point. In the future, to standardize cyber defenses, our goal is that all DoD access to commercial cloud services be via a DISA provided CAP."*-- DoD CIO Memo, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services.

C.8.5.1. Onboarding to an IL6 CSO. The Mission Owner works with the CSP to onboard the C-ITP to the IL6 CSO. The IL6 CSO's entry in the DoD Approved Cloud Service Offerings Catalog includes a link to the CSO's DoD PA. The DoD PA provides CSP contact information.

(NOTE: DISA is currently implementing SIPRNet CAPs. Once operational, on-premises and off-premises IL6 CSOs must utilize them or another DoD CIO-approved DoD Component SIPRNet CAP.)

A Mission Owner must register an IL6 (secret) DoD Cloud IT Project in the SIPRNet GIAP System (SGS). CSOs and C-ITPs running at classification levels above SECRET are outside the scope of this guide.

C.9. The Mission Owner onboards the C-ITP to a Provisionally Authorized CSO

After DISA makes a CSO accessible to users, a Mission Owner may then work with the CSP to complete activities necessary to onboard a C-ITP onto the Provisionally Authorized CSO. There are several resources available to help Mission Owners plan the transition to a cloud environment.

C.9.1. **Onboarding to DISA milCloud 1.0.**

The DISA milCloud 1.0 is an Infrastructure as a Service (IaaS) solution that leverages a combination of mature Commercial off the Shelf (COTS) and Government developed technology to deliver cloud services tailored to needs of the DoD. It operates within a DISA DECC that is directly accessible via NIPRNet, so a DISA BCAP is not involved in the connection. Once the CPTC is issued, the Mission Owner may work with their Component Cloud Migration Office and the DISA milCloud 1.0 office to connect and onboard a C-ITP into milCloud 1.0. Information about connection and onboarding to milCloud 1.0 is available on the DISA milCloud website. The DWCF Rate Book includes subscription rates for “milCloud” services.

Prior to ordering new or modifying existing milCloud 1.0 services, Mission Partners are encouraged to visit the DISA milCloud 2.0 portal or reach out to the milCloud 2.0 Program Management Office (PMO) to determine their ability to support specific cloud service requirements and implementation timelines. Although customers can still order/modify milCloud 1.0 services, be aware that milCloud 2.0 is the replacement service for milCloud 1.0.

C.9.2. **Onboarding guidance for DoD Cloud Mission Owners.**

The following sources provide information helpful for connection and onboarding of a C-ITP to an approved CSO:

- Best Practices Guide for Department of Defense Cloud Mission Owners planning to migrate an existing information system from a physical environment to a virtualized cloud environment covering assessment and authorization, IP standards, Domain Name Service availability, and cloud email
- DISA milCloud website milCloud is an Infrastructure as a Service (IaaS) solution that leverages a combination of mature Commercial off the Shelf (COTS) and government developed technology to deliver cloud services tailored to needs of the DoD.
- DISA milCloud 2.0 portal: milCloud® 2.0 connects commercial cloud service offerings to Department of Defense (DoD) networks, in a private deployment model to provide DISA mission partners the latest cloud technology at competitive prices without compromising security or performance.

- DISA Mission Partner Engagement Office Website provides access to Reports, available DISA services, service requests, technical support, billing POCs, DWCF Rate Book, and Frequently Asked Questions, and MPEO points of contact for additional information and assistance.
- DISA SCCA PMO website descriptions of CAP, VDSS, VDMS, list of on-premises and off-premises CSOs connected to DISA CAP and SCCA offerings.
- DoD Cloud Acquisition Guidebook (DoD Acquisition University) is a comprehensive online resource with chapters designed to provide specific and tailored information for PMs, Contracting personnel, Engineers/IT Technical personnel, Financial Managers, Attorneys, and Cybersecurity personnel.
- DoD CIO Memo, DoD Cybersecurity Activities Performed for Cloud Service Offerings expands upon DoDI 8530.01 to address the engagement in Defensive Cyber Operations as DoD networks transition data, applications, capabilities and services to DoD and commercial cloud capabilities and services.
- DoD Cloud Computing Security Requirements Guide (CC SRG) outlines the security model by which DoD will leverage cloud computing along with the security controls and requirements necessary for using cloud-based solutions
- DoD Cloud Computing Security Website the online library of DoD Cloud Computing Security documents and web links.
- DoD Cloud Cyberspace Protection Guide defines a set of reporting and incident handling procedures for the organizations that will protect the DODIN in the cloud as specified in the DoD CC SRG section on cyberspace protection and incident response.
- DoD Cloud Strategy Deputy Secretary of Defense issuance that identifies strategic objectives to address DoD mission requirements through a multi-cloud, multi-vendor strategy that incorporated General Purpose cloud and Fit For Purpose cloud capabilities.

C.10. Cloud Connection Sustainment and Maintenance

Figure 9 illustrates the requirements for sustaining and maintaining a C-ITP or CSO connection to the DISN via the DISA BCAP and includes:

C.10.1. **Meet all contract requirements.**

A DoD Mission Owner C-ITP using a CSO and the Cloud Service Provider of the CSO must continue to meet all obligations within their contract including those specified in the 80 FR 51739, Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018).

C.10.2. **Comply with requirements in the CC SRG, ADD, or DoD PA.**

Mission Owners and CSPs and must continuously monitor their system's compliance with conditions specified in the CC SRG and the associated DoD PA or ATO. This includes submitting timely renewal request prior to the expiration date specified in the C-ITP's ATO and the CSO's DoD PA, conducting Continuous Monitoring, Cyberspace Defense and Incident response, and Change Control following procedures in the CC SRG paragraph 5.3.

C.10.3. Comply with USCYBERCOM and JFHQ DODIN operational orders (OPORDS).

In the case that a USCYBERCOM or JFHQ DODIN operational order affects a CSO or C-ITP, the Cybersecurity Services Provider and Contract Officer are responsible for providing the unclassified portion of the OPORD to the CSP and ensuring compliance. CSPs and DoD Mission Owners must ensure their systems comply with applicable operational orders

C.10.4. Maintain Accurate Information in SNAP or SGS and other repositories.

Mission Owners update C-ITP information in SNAP and SGS particularly personnel contact information that is vital to timely notification. DISN CAO assisted by CSPs will ensure that CSO records in SNAP/SGS are kept current.

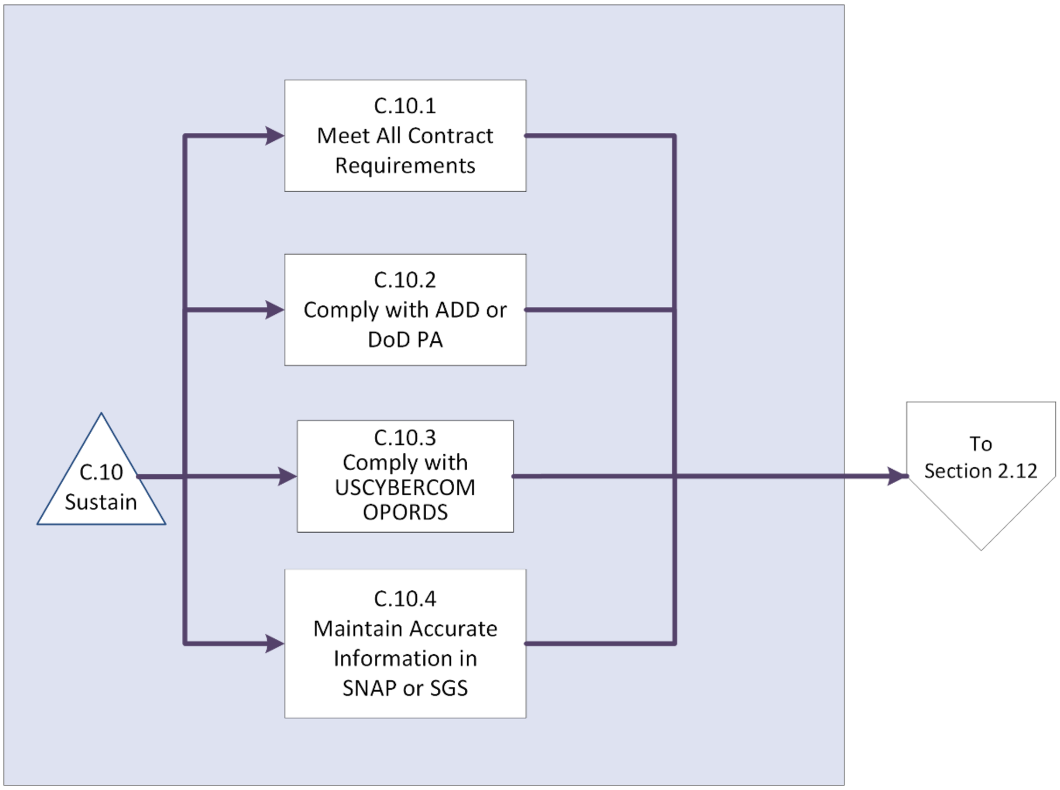

C.10.1
Meet All Contract Requirements
C.10.2
Comply with ADD or DoD PA
C.10
Sustain
C.10.3
Comply with USCYBERCOM OPORDS
To Section 2.12
C.10.4
Maintain Accurate Information in SNAP or SGS

Figure 9 Cloud Connection Sustainment and Maintenance Process

Section 2.12 through Section 2.15 of this guide describe the processes for renewing an approval to connect to DISN and for handling temporary disconnections from DISN. DISA will notify registered Mission Owners and CSPs having dependencies in the event there are issues concerning a CSO's DoD PA such as issuance of a FedRAMP Corrective Action Plan.

C.11. Permanent discontinuation of a C-ITP connection from DISN

Sections 2.5 and 2.16 of this guide describe the process for permanently discontinuing a C-ITP connection to the DISN.

During the sustainment and maintenance process, the JFHQ DODIN may order DISA to disconnect temporarily a C-ITP or CSO from DISN due to non-compliance. Reasons may include:

- The ATO or CPTC for a C-ITP may expire
- The FedRAMP PA, DoD PA, or CATC for a CSO may be placed in remediation status, be revoked, or may expire

JFHQ DODIN will order DISA to reconnect a C-ITP or CSO after the non-compliance issue is resolved. (See Section 2.15 of this guide for details.)

The life cycle of the C-ITP connection ends here.

Appendix D Cloud Service Offering (CSO) Authorization, Registration, and Connection

D.1. CSO Authorization, Registration, and Connection Overview

This Section describes processes illustrated in Figure 10 for authorization, registration, and connection of a Cloud Service Provider (CSP) - Cloud Service Offering (CSO) to the DISN, in compliance with DoD policies and standards.

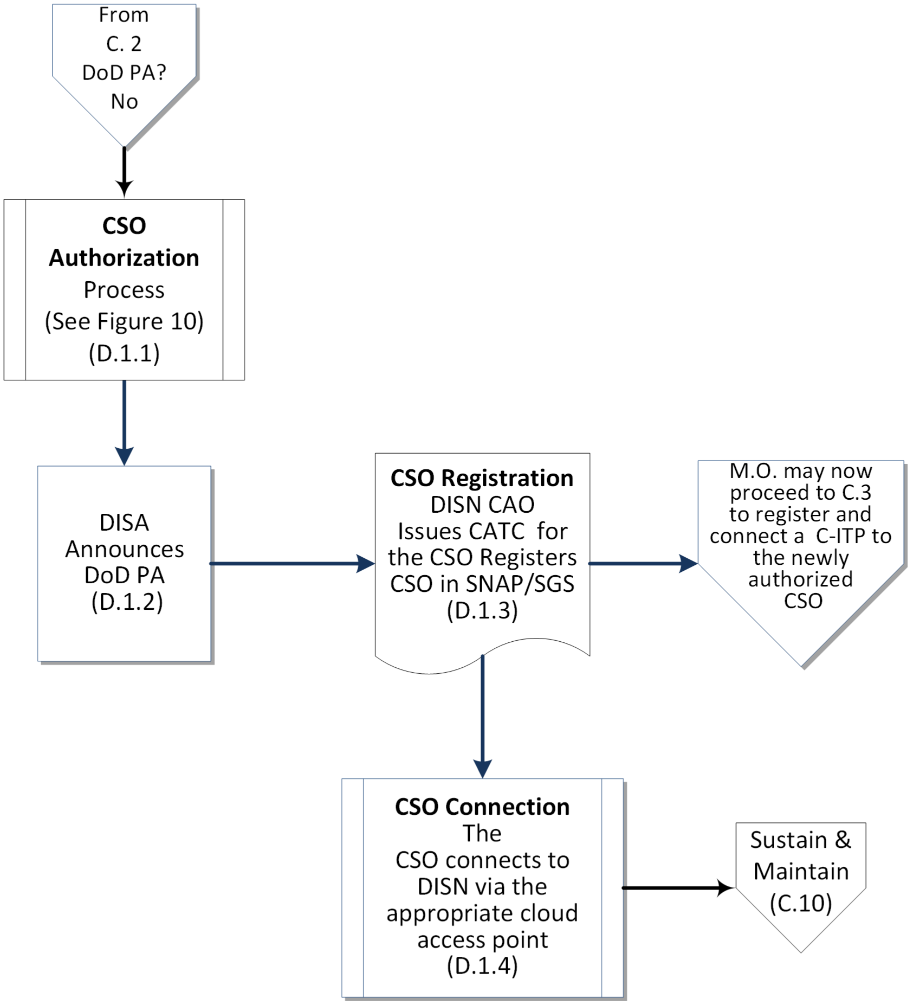


Figure 10 CSO Authorization, Registration, and Connection Process

D.1.1. Cloud Service Offering (CSO) Authorization Process

The DoD Cloud Authorization Services (DCAS) Team provides support to DoD component sponsors through the pre-screening, assessment, coordination with Third Party Assessor Organizations (3PAOs), validation, and Provisional Authorization (PA) process outlined on the DCAS portal for IL4, IL5, and IL6 CSO requirements.

D.1.2. DISA announces DoD PA and updates pertinent repositories with CSO Information

Once the DISA AO issues the DoD PA, the DCAS Team will work with the DISA Public Affairs Office to issue a public announcement that an IL4 or above CSO has received a DoD PA. In addition, the CSO will be added to the "Current DoD CSOs" on DCAS. The DCAS Team will provide information needed by the DISN CAO to register the CSO and any dependencies in DISA SNAP/SGS. The CSO will then be available in SNAP/SGS for selection by DoD Mission Owners as described starting in
Section C.3 of this guide. The DISN CAO will upload the following documents into the DISA SNAP or SGS system CSO module:

- DoD Provisional Authorization
- DoD RMF Authorization Decision Document (ADD) – An ADD is only required for an on-premises CSO IAW the CC SRG (paragraph 4.5)

The DISN CAO will continue to work with the DCAS Team, the CSP and the DoD Component sponsor to update the CSO entry in SNAP or SGS annually or as required.

D.1.3. CSO Registration

DISN CAO issues a Cloud Approval to Connect (CATC) and registers the CSO in SNAP (IL2-IL5) or SGS (IL6). The DISN CAO will notify both the DoD Component sponsor and the SCCA PMO when issuing a CATC for a CSO connection to the DISA BCAP or ICAP.

Once a CSO has obtained the requested DoD PA, the DoD Component sponsor may begin the process of registering and connecting a Cloud Information Technology Project (C-ITP) to the newly Provisionally Authorized CSO as described starting in Section C.3 of this guide.

D.1.4. CSO Connection

Once registered in the SNAP or SGS, the next steps to implement the CSO connection will depend upon the IL of the CSO, and which CAP the CSO will use. The implementation of the CSO connection to the DISN via an appropriate cloud access point is similar to the manner in which C-ITPs connect to the CSO as described in Section C.8 and illustrated in Figure 8 of this guide.

A. **Connection via a DISA BCAP or ICAP**. If an off-premises CSO is connecting via the DISA BCAP and is not collocated with a DISA BCAP Meet-Me-Point, then the CSP must obtain, fund, and sustain a connection between CSP enclave hosting the CSO and the DISA BCAP Meet-Me Point. Figure 11 illustrates the process DISA uses to activate a CSO connection via a DISA BCAP or ICAP.

> DoDI 8010.01 and CJCSI 6211.02D require a DoD Component to sponsor a CSO's connection to the DISN. Consequently, DISA SCCA PMO will only activate the CSO BCAP connection when a DoD Mission Owner receives a CPTC to connect a Cloud IT Project (C-ITP) to the CSO as described starting in Section C.1 of this guide.

B. **Connection via a DoD Component CAP (non-DISA CAP).** When connecting an off-premises CSO via a DoD Component BCAP or connecting an on-premises CSO via a DoD Component ICAP, the DoD Sponsor works with the responsible DoD Component to engineer and implement the CSO connection IAW the CC SRG (see paragraph 5.10.1.3).

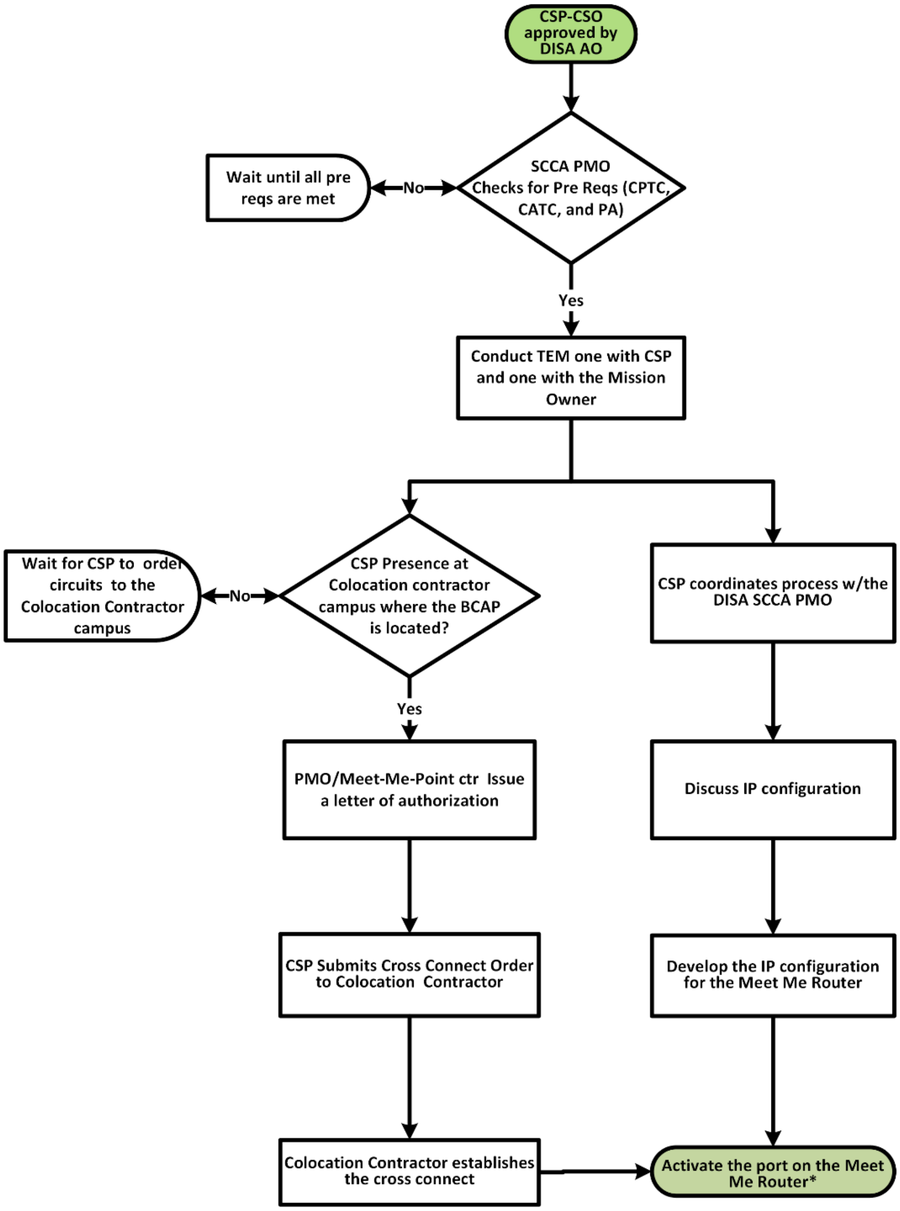

CSP-CSO approved by DISA AO
SCCA PMO Checks for Pre Reqs (CPTC, CATC, and PA)
No
Wait until all pre reqs are met
Yes
Conduct TEM one with CSP and one with the Mission Owner
CSP Presence at Colocation contractor campus where the BCAP is located?
No
Wait for CSP to order circuits to the Colocation Contractor campus
Yes
PMO/Meet-Me-Point ctr Issue a letter of authorization
CSP Submits Cross Connect Order to Colocation Contractor
Colocation Contractor establishes the cross connect
CSP coordinates process w/the DISA SCCA PMO
Discuss IP configuration
Develop the IP configuration for the Meet Me Router
Activate the port on the Meet Me Router*

Figure 11 Activating the CSO Connection to the DISA BCAP/ICAP

C. **Connection to an Impact Level 6 (Secret-level) CSO**. Currently, an IL6 CSO connects directly to SIPRNet and not through a DISA BCAP. However, once DISA's SIPRNet CAPs are operational, on-premises and off-premises IL6 CSOs must utilize them or another DoD CIO-approved DoD Component SIPRNet CAP. Once the DISN CAO registers the IL6 CSO in SGS, the DoD Component Sponsor requests the CSO connection to SIPRNet following the procedures in Section 2 of this guide.

The CSO connection now enters the sustainment and maintenance described in Section C.10 until end of life as described in Sections 2.5, 2.16, and D.2.

D.2. Permanent discontinuation of a CSO connection from DISN

Sections 2.5 and 2.16 of this guide describe the process for permanently discontinuing a connection to the DISN. However, since permanent discontinuation of a CSO from DISN can affect any Mission Owner using that CSO, the discontinuation process for a CSO involves the following additional actions as illustrated in Figure 12:

D.2.1. DISA Notifies Stakeholders about CSO Service Discontinuation.

DISA Command Center will issue a DISA TASKORD and DISA Global will permanently discontinue the connection to the CSO. The DCAS Team and CAO Cloud Team will apprise Mission Owners or CSPs with dependencies on the discontinued CSO so they can take appropriate action (e.g., Mission Owners off-boarding their C-ITP and data).

D.2.2. DISA Closes CSO registrations and Discontinues the CSO Connection

DISA Global executes the DISA TASKORD by permanently discontinuing the CSO's DISN connection and revising the NIPRNet DMZ Whitelist as needed. The DCAS Team marks the entry in DoD Approved Cloud Service Offerings Catalog as "Closed" and notifies the DISN CAO that the CSO is discontinued. DISN CAO marks the CSO's SNAP/SGS entry as "Closed" and uploads the DCAS discontinuation notification to SNAP/SGS. Closing the SNAP/SGS entry removes the CSO from the list of available CSOs on SNAP/SGS and deletes any Whitelist entries in the DISA IAPs. Mission Owners will no longer be able to select the CSO for a new C-ITP connection.

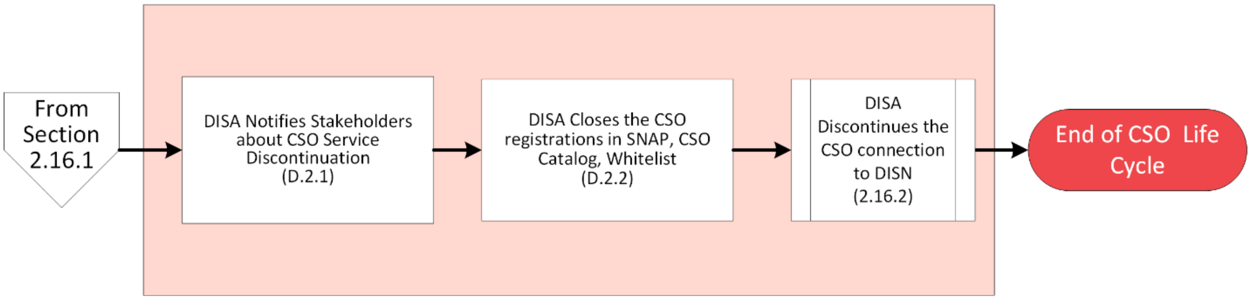

From Section 2.16.1
DISA Notifies Stakeholders about CSO Service Discontinuation (D.2.1)
DISA Closes the CSO registrations in SNAP, CSO Catalog, Whitelist (D.2.2)
DISA Discontinues the CSO connection to DISN (2.16.2)
End of CSO Life Cycle

Figure 12 Permanently Discontinue a CSO Connection to DISN

Appendix E Topology Diagram Requirements

E.1. Topology Diagram/System Design Document

The network topology diagram depicts the physical or logical configuration and security posture of the various elements (links, nodes, etc.) a computer enclave or network connection to DISN. The topology diagram illustrates the "System Enterprise and Information Security Architecture" cited in the DoD RMF Security Plan.

Figure 13 through Figure 16 in this appendix depict the network configuration and security posture of various types of DoD Component enclave or network connections to DISN.

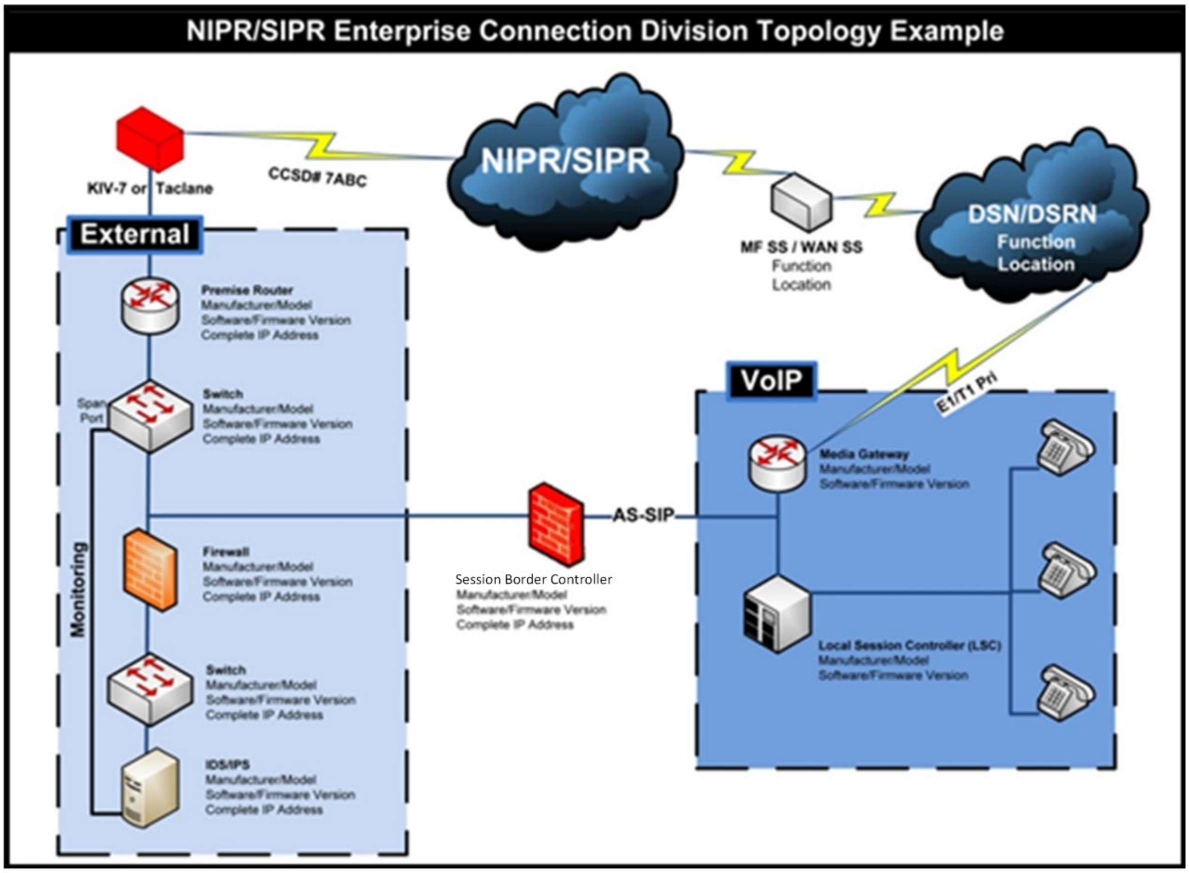


Figure 13 NIPR/SIPR Customer Network Enclave Topology Sample

As shown in Figure 13 Topology diagrams must:

- Be dated
- Clearly delineate authorization boundaries
- Identify the CCSDs of all connections to the DISN
- Identify equipment inventory (equipment make, model, most recent configuration including any enclave boundary firewalls, Intrusion Detection System (IDS)/Intrusion Protection System (IPS), premise router, routers, switches, backside connections, IP addresses (obtain IP address space from the NIC), encryption devices, CDS, software versions, and IP address ranges of the devices on the diagram; (DISN CAO confirms

that equipment and OS version are on the Approved Products List Tracking System or National Information Assurance Partner (NIAP) Evaluated Products)

- Show other NIPRNet or SIPRNet connections (access points); the flow of information to, from, and through all connections, host IP addresses, and CCSD number must be shown
- Identify all cybersecurity or cybersecurity-enabled products deployed in the enclave
- Identify any connections to other systems/networks/enclaves to include:
  - The name of the organization that owns the other enclave
  - The connection type (e.g., wireless, dedicated point-to-point connection, etc.)
  - IP addresses for all devices within the other enclave (IP addresses may be obtained from the NIC)
  - The organization type (e.g., DoD, federal agency, contractor, etc.)
- Identify the Internetworking Operating System (OS) version
- Show actual and planned interfaces to internal and external Local Area Networks (LANs) or Wide Area Networks (including backside connections)
- Note on the topology if the enclave is protected by a gateway (e.g., Navy Marine Corps Internet or Air Force Block 30)
- Appropriately classify the topology diagram for SIPRNet enclaves, or cloud services using DISA Circular 300-115-3 DISN SIPRNet Security Classification Guide

The DoD Network Information Center (NIC) Registry Protocol 9802 provides additional information on assignment and registration of DoD IP address space and IP numbered resources.

*** DISA Authorizing Official approval is required to use Private IP addresses (non-routable) space (RFC 1918) on SIPRNet. All RFC 1918 requests must be submitted to the DSAWG Secretariat for DISA AO approval. ***

E.2. Customer Network Enclaves Connection via JRSS

The topology diagram for customer network enclaves that connect via the JRSS must include a JRSS topology overlay as shown in the Figure 14. The JRSS topology overlay also must identify the make/model/IP address/software version of the JRSS equipment in use.

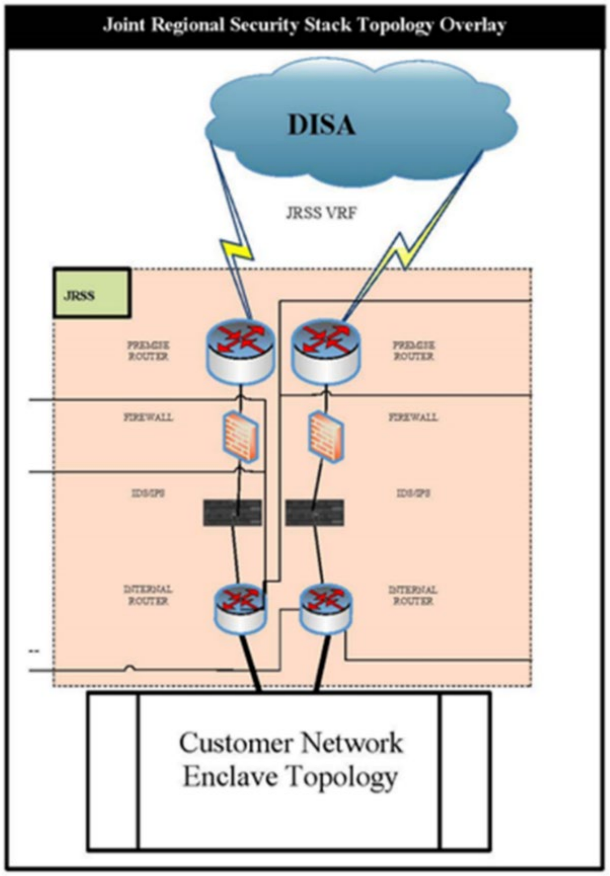


Figure 14 JRSS Security Stack Topology Overlay

E.3. TDM/IP DSN topologies

All TDM/IP DSN topologies illustrated in Figure 15 and Figure 16 must include:

- Topology date
- Function, vendor, model, and software version of the voice switch (preferably near the voice switch)
- All Customer Edge router or Terminating type equipment used behind the voice switch (Analog, Digital, VoIP, Video Teleconference, NE, 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 Channel Associated Signaling (CAS), Integrated Services Digital Network, etc.)

Addenda for a voice switch connection to an Assured Services Local Area Networks (ASLAN):

- 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 Customer Edge Router

Addendum for voice softswitch or session controller connections to the DISN:

- Depict the function and location of the source softswitch or session controller providing connection to the DISN backbone (preferably near the DISN cloud)

- Depict function, vendor, model, software version and IP address of all Session Border Controllers
- Depict NIPRNet CCSD(s) providing the Ethernet/IP connection within the enclave (preferably near the customer edge router)
- Select connection type “backbone” if DISA manages the softswitch or session controller and provides UC services for multiple DoD and Mission Partners.

All Cybersecurity and cybersecurity-enabled products must comply with the evaluation and validation requirements of DoDI 8500.01 and DoDI 8100.04.

“DoD Components are required to acquire or operate only UC products listed on the UC APL” IAW DoDI 8100.04, Unified Capabilities. Cloud services are considered UC if they traverse DoDIN.

It is important to note that IAW DoD and DISA guidance, firewalls, Intrusion Detection Systems (IDSs), and Wireless-IDSs (where applicable) are required on all partner enclaves. Indicate and label all the devices, features, or information. The minimum diagram size is 8.5" x 11

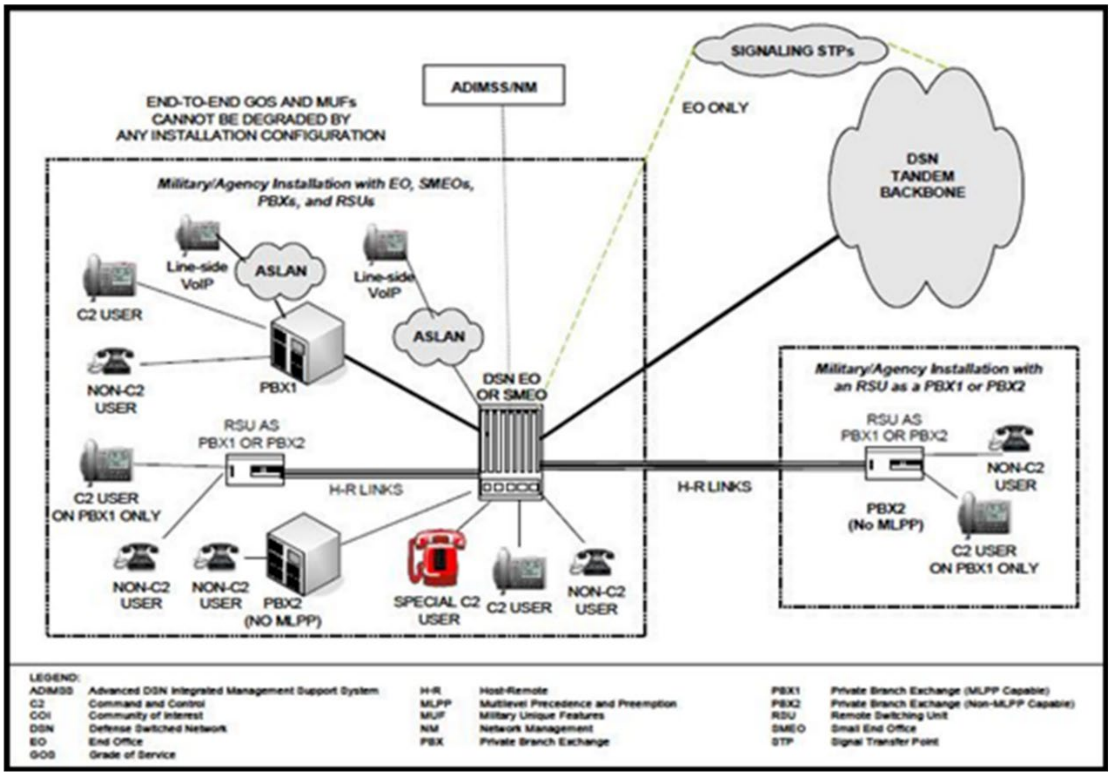
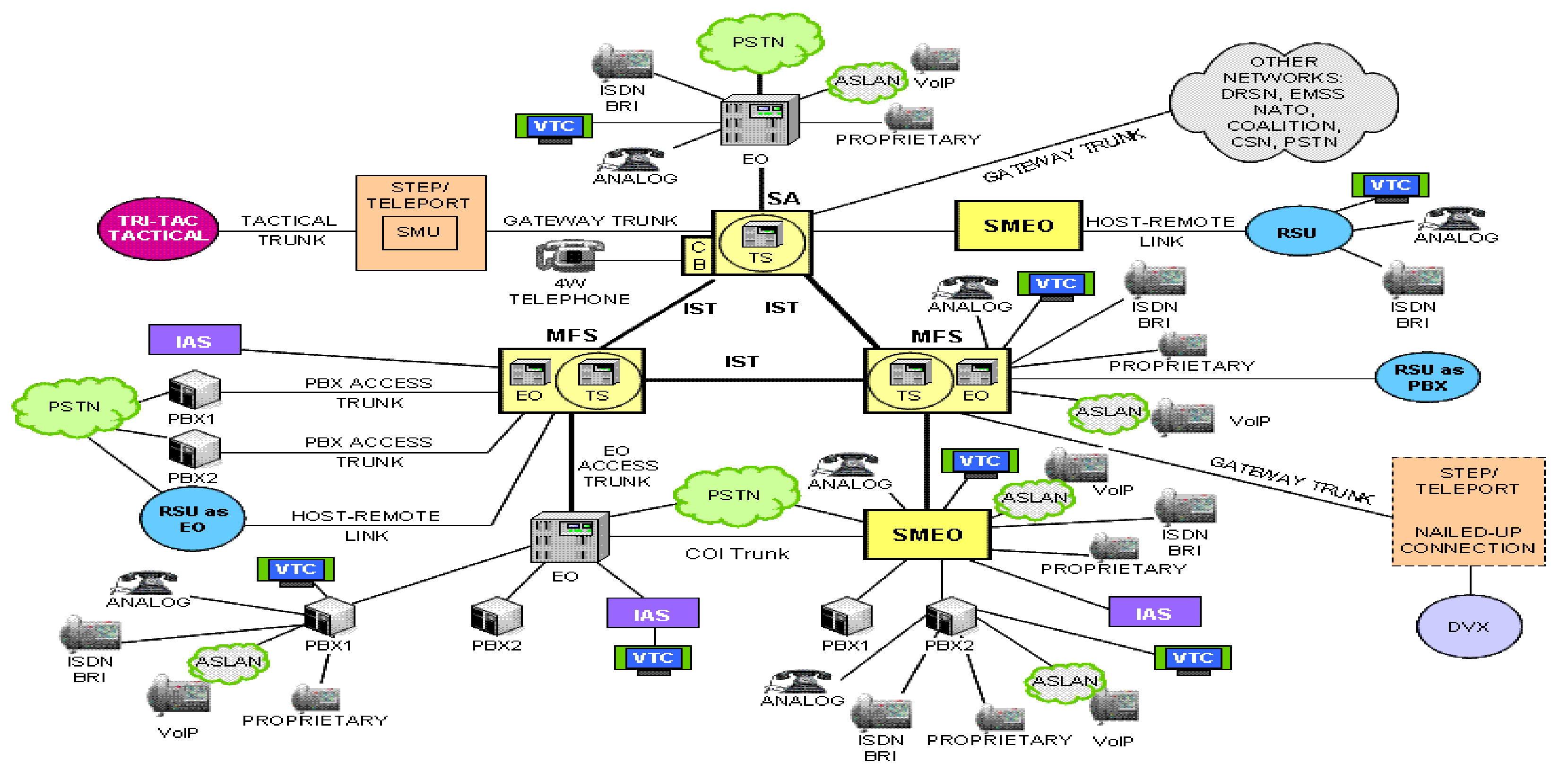

SIGNALING STPs
ADIMSS/NM
EO ONLY
END-TO-END GOS AND MUFs
CANNOT BE DEGRADED BY
ANY INSTALLATION CONFIGURATION
DSN
TANDEM
BACKBONE
Military/Agency Installation with EO, SMEOs, PBXs, and RSUs
Line-side VoIP
ASLAN
Line-side VoIP
ASLAN
C2 USER
NON-C2 USER
PBX1
DSN EO OR SMEO
RSU AS PBX1 OR PBX2
H-R LINKS
C2 USER ON PBX1 ONLY
NON-C2 USER
NON-C2 USER
PBX2 (NO MLPP)
SPECIAL C2 USER
C2 USER
NON-C2 USER
H-R LINKS
Military/Agency Installation with an RSU as a PBX1 or PBX2
RSU AS PBX1 OR PBX2
NON-C2 USER
PBX2 (No MLPP)
C2 USER ON PBX1 ONLY
LEGEND:
ADIMSS Advanced DSN Integrated Management Support System
C2 Command and Control
COI Community of Interest
DSN Defense Switched Network
EO End Office
GOS Grade of Service
H-R Host-Remote
MLPP Multilevel Precedence and Preemption
MUF Military Unique Features
NM Network Management
PBX Private Branch Exchange
PBX1 Private Branch Exchange (MLPP Capable)
PBX2 Private Branch Exchange (Non-MLPP Capable)
RSU Remote Switching Unit
SMEO Small End Office
STP Signal Transfer Point

Figure 15 Sample DSN Topology



LEGEND:

4W	4-Wire Subscriber Line
BRI	Basic Rate Interface
CB	Channel Bank
COI	Community of Interest
CSN	Canadian Switched Network
DRSN	Defense RED Switch Network
DVX	Deployable Voice Exchange
EMSS	Enhanced Mobile Satellite System
EO	End Office
IAS	Integrated Access Switch
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
MFS	Multifunction Switch
MLPP	Multilevel Precedence and Preemption
NATO	North American Treaty Organization
PBX1	Private Branch Exchange (MLPP Capable)
PBX2	Private Branch Exchange (Non-MLPP Capable)
PSTN	Public Switching Telephone Network
RSU	Remote Switching Unit
SA	Stand-Alone Switch
SMEO	Small End Office
SMU	Switch Multiplex Unit
STEP	Standard Tactical Entry Point
Tri-Tac	Tri-Service Tactical
TS	Tandem Switch
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing

Figure 16 Example Installation Topology

This Page Intentionally Left Blank.

.

Appendix F Registering Tactical, DSN, and UC Service Requirements

F.1. Supplemental Guidance for Tactical Exercise or Tactical Mission TELEPORT Connection Registration

The customer will submit a connection request using the SIPRNET GIAP module in the SGS system. The customer completes section 0 of the GIAP record to identify points of contact for the connection and posts a modified connection security package that includes:

- ATO/ADD
- Topology

The customer will then submit the package to the CAO.

The DISN CAO will review the registration information and will issue an ATC for the duration of the ATO upon successful and complete registration. The ATC will show the Registration ID number for the record. DISN CAO will post the ATC under section 10.1 of the SGS system and email the ATC to the POCs in section 0.

For an ATC that expires within the next 30, 60, or 90 days SGS automatically sends email reminders to the registered points of contact reminding them to initiate actions required to renew the ATC.

F.2. Supplemental Guidance for Defense Switched Network (DSN) and UC Connection Registration

Connection of a DSN telecommunication switch or Unified Capabilities (UC) product to the DISN requires procurement of interfacing hardware and/or software elements identified on the DoD UC Approved Products List (UC APL). DoD UC is "the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. DISA's Joint Interoperability Test Center (JITC) or other authorized Component test center ensures certifies products on the UC APL for interoperability and tests products for Cybersecurity IAW DoDI 8100.04, Unified Capabilities. UC products from the UC APL include circuit switched, and IP-based devices that have undergone interoperability and Cybersecurity assessment. Addition to the APL involves end device-to-end device security, authentication, and non-repudiation to support mission assurance objectives. The customer uses the UC Reference Architecture in conjunction with all relevant DoD security requirements and DoD Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs). Operational deployment of the UC APL product must be compliant with all Conditions of Fielding and risk mitigations identified in the Cybersecurity recommendation and the APL approval memorandum.

F.2.1. **Before purchasing a product not on the UC APL, the customer must:**

- Work with the JITC to have the product tested and certified for Interoperability and cybersecurity and placed on the UC APL.
- Alternatively, obtain a DoD CIO review and approval IAW DoDI 8100.04, Unified Capabilities.

F.2.2. The following additional guidance applies:

- Voice soft switches or session controllers connected to the DISN shall be registered in SNAP using the DSN module and obtain connection approval as described in Section 2 of this guide.
- IAW DoDI 8010.01 and CJCSI 6211.02D, the user must "register all connections to the DISN" to include all TDM/DSN[20] voice switches and TDM-based video service connected to the DSN as a servicing voice switch using the DSN module as described in Section 2 of this guide.
- The user will register all TDM/DSN voice switches (e.g., PBX1, NE-SHOUTS, Switch Multiplex Unit, and Inverse Multiplexer (IMUX)) that connect via a tandem/nodal connection to the Multifunction Switch (MFS) in SNAP using the DSN module. The user will also obtain a DoD CIO review and approval IAW DoDI 8010.01 and Appendix A of this guide or have a completed Tailored ISP for connection approval.
- New/additional TDM trunk connections to an operational legacy DSN switch for growth requirements will be allowed, but the legacy switch must be registered in SNAP using the DSN module and obtain connection approval, as described in Section 2 of this guide if they have not previously obtained formal connection approval.
- If a legacy switch is on the UC APL End of Sale list or has fallen off the UC End of Sale list, then the Customer must register the voice switch in SNAP using the DSN module. The customer request must be approved by DoD CIO IAW DoDI 8100.04 in order to obtain a connection approval as described in Section 2 of this guide.
- TDM/DSN voice switches or VoIP capable soft switches [e.g., PBX1[21], PBX2, Network Element (NE) SHOUTS, Remote Switching Unit (RSU), Switch Multiplex Unit, Inverse Multiplexer (IMUX)), IP-based video service connected behind the local user's installation DSN End Office (EO)/Small End Office (SMEO)] must be connected IAW the connection approval process stipulated by the hosting DoD Component. These connections do not require a SNAP registration or DISA connection approval unless directed as a MAJCOM, Combatant Command, or Theater Command requirement. Instead, the user must register the hosting installation's connection to DISN in SNAP

[20] Commercial vendors are rapidly phasing out Low Speed Time Division Multiplexing (LSTDM) technologies reaching End of Life and End of Service support. As a result, the DoD CIO Memo, Circuit Optimization directs efforts to terminate costly legacy network technologies and associated transport infrastructure circuits (e.g., TDM circuits) to align with JIE objectives by optimizing use of Ethernet and IP-based network infrastructure. DoD CIO Memo, Legacy Networking Technologies tasks all DoD Components to eliminate all non-Internet Protocol network technologies by FY23. Additionally, the DoD UC Master Plan (see section 5.d. (1) (h) and (i); Pg. 28, 29) states that, circuit switch-based services shall begin migrating to IP-based non-assured/assured services over DoD Component ASLAN Intranets and UC transport using products from the DoD UC APL. Time Division Multiplexing (TDM)/IP hybrid technologies shall provide both converged and non-converged UC during this implementation timeframe. The Voice-Over-Secure-IP, DVS, Standard Tactical Entry Point/Teleport, and deployable programs shall upgrade respective infrastructures using products from the DoD UC APL.

DISA hosts quarterly TDM Technical Interchange Meetings to bring the DoD Communications Community together to discuss and exchange information relating to requirements for TDM elimination. This includes approaches to migrating from TDM to IP-based solutions and meeting requirements in DoD CIO Memo, Legacy Networking Technologies.

Note that Quality of Service (QoS) is not a service but a required feature of DISA's MPLS transport that is applied to defined customers delivery of a service. Currently, this feature is a manual process accomplished by DISA Engineers through customer engagement. As DISA evolves QoS and the ordering process, DISA will give MPLS customers the ability to specify QoS management requirements according to the customer wishes. For assistance with MPLS QoS, contact the DISA MPEO.

[21] PBX1 is a PBX with Multi-Level Precedents and Preemption (MLPP) capability needed for Command and Control applications. PBX2 designates a PBX without MLPP capability.

using the DSN module and these types of switches and depict them in the topology diagram of the host installation.

For information on UC APL, products and the process for getting equipment added to the UC APL refer to the UC APL website and the DISA UC Approved Products Certification Office.

Appendix G DoD Cross Domain Solution Approval Process

A Cross Domain Solution (CDS) is a form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. This appendix provides the steps necessary to obtain a Cross Domain Solution Authorization (CDSA). A CDSA is the official document authorizing operational use of a CDS. A CDSA will not be issued for dates beyond the Approval to Connect (ATC) expiration date for the enclave in which it resides.

> IAW DoDI 8540.01, paragraph 3.g, it is DoD Policy that "*the DoD-level risk decision on use of a CDS to access or transfer information between different interconnected security domains must be made by the designated DoD risk executive as a CDS authorization (CDSA) ….*"
>
> IAW DoDI 8540.01, Enclosure 2, paragraph 8.u.(1) DoD Component Heads shall:" Require *the issuance of a DoD ISMRC [sic] or DSAWG CDSA before allowing a CDS to access or transfer information between different interconnected security domains. A CDSA is required for use of a CDS."*

A customer desiring to implement a CDS must first contact their respective Cross Domain Support Element (CDSE) to discuss the requirement, receive guidance on the CDS process, and receive their recommended way forward. If you do not know your CDSE point of contact information, you may contact DSAWG Secretariat (CDTAB Support) to receive that contact information.

G.1. DoD CDS Approval Process Scope, Applicability and Exclusions

The DoD CDS approval process covers CDS connections to networks classified Top Secret and below, including standalone, isolated, and test networks. This includes IC-owned CDSs that connect to DoD networks. CDS devices with connection to networks classified Top Secret–Sensitive Compartmented Information (SCI) and above follow different approval processes as determined by Director of National Intelligence (DNI) policy and guidance. If an Intelligence Community (IC) approved CDS connects to SIPRNet, an IC Registration needs to be created in the SGS system (see Section G.8 of this guide). Programs with strict OPSEC requirements needing to utilize a CDS will also go through the CDS approval process. The process will be adapted to ensure the need-to-know requirements are met IAW paragraph 7.2.5 in the DSAWG Charter.

> DISA's Risk Adjudication and Connection Division's Mission Partner Training Program (MPTP) provides an overview of DSAWG and CDS processes.

G.2. Categories of Cross Domain Solutions

The two main categories of Cross Domain Solutions (CDS) are enterprise CDS and Point-to-Point CDS. Within these broad categories are an Access CDS, Transfer CDS, or Multi-level CDS types. An Enterprise CDS is a CDS approved for use by an enterprise cross-domain service provider. A Point-to-Point CDS is a CDS purchased, implemented, and managed within the authorization boundary of the organization's own network. A Point-to-Point CDS is unable to use an ECDSP. Details of each type of CDS are described below.

G.2.1. Enterprise Cross Domain Solution (Enterprise CDS)

An **Enterprise Cross Domain Service (ECDS)** provides automated capabilities available to end users and hosted mission applications within an enterprise environment for information sharing across-and-among security domains utilizing one or more CDSs. There are two classes of enterprise CD services:

- General Purpose (GP) enterprise cross domain service is available to all authorized users of connected networks and supports a broad range of data types.
- Mission Specific (MS) enterprise cross domain service is available to a select community [e.g., signals intelligence (SIGINT), geospatial intelligence (GEOINT), Maritime] with a limited set of data types and domains.

An enterprise-CD-service may qualify as one or both types of cross domain service.

a. Enterprise CDS Candidate: This term refers to an organization with CDS requirements in negotiation with an Enterprise Cross Domain Service Provider (ECDSP) which will be brought through the CDS Phase 1 just as a point-to-point CDS. Once the DSAWG approves the Phase 1 requirement, the DSAWG Secretariat (CDTAB Support) will document the DSAWG approval of the requirement for ECDSP implementation in SGS and then close the original CDS Request in SGS. The requirement will be implemented on an Enterprise CDS under an Enterprise CDS Ticket number.

b. Enterprise CDS Ticket or Request. An enterprise CDS Ticket or Request is a CDS sponsored by an ECDSP that supports multiple organizations.

Per DoDI 8540.01, *"DoD will employ existing enterprise CD service provider's (*ECDSP*'s) enterprise CD service or enterprise-hosted CDS when their use satisfies the CD mission requirements of DoD Components. Leveraging another operational CDS, deployment of a* CDS baseline list *point-to-point CDS or development of a new CD technology will be considered as alternative solutions only when an enterprise solution cannot meet the CD capability requirements."*

G.2.2. Point-to-Point Cross Domain Solution (CDS):

A Cross Domain Solution purchased, implemented, and managed within the authorization boundary of the organization's own network. Point-to-Point CDS are CDS that are owned and operated by an organization that cannot use an ECDSP. A particular P2P CDS may be categorized as an Access CDS, Minimal (Community) Impact CDS, Tactical CDS or a P2P CDS that requires an exemption.

a. **Minimal (Community) Impact CDSs (formerly referred to as "For Tracking Purposes Only (FTPO)")** presents a minimal community risk in terms of DoD information security. A Minimal (Community) Impact CDS must be registered in SGS, the "designated repository," in IAW DoDI 8540.01 enclosure 3, paragraph 4.a. If the CDS meets the Minimal Community Impact Criteria – they do not need to complete the P2P Approval Process (or associated documentation). The CDTAB determines whether a CDS fits one of the following four cases of Minimal (Community) Impact CDSs:

i. **Completely Isolated**: The networks connected to the CDS are completely isolated.

ii. **A Controlled Interface of Interest** is a CDS connected to two networks of the same security classification that have different Administrative Domains. In such cases, the controlled interface at each network boundary satisfies both parties' security requirements.

iii. **Very Low Risk (VLoR)**: A VLoR CDS meets VLoR assertions in the VLoR Process Implementation Guide (see paragraph 5). A VLoR CDS is a transfer CDS architecture/system in which the low side system(s) provide minimal threat to the high side network, and its connected enclaves present minimal risk to the High side enclave(s). VLoR review process is designed to assess the risk for systems such as Global Positioning Satellites (GPS), Network Time Protocol (NTP) and sensors isolated from general network traffic.

iv. **Cyber Situational Awareness (SA) Taps**: Cyber Situational Awareness Taps are one-way CDS devices that forward network traffic into a closed collection enclave for analysis. In such cases, the CDSE and DSAWG Secretariat (CDTAB Support) will review the test evidence verifying the one-way-ness of the proposed CDS device and the network architecture and protections of the collection enclave to ensure isolation.

The *DoD CIO and USD(A&S) Memorandum, Suspension of new Point-to-Point Cross Domain Solutions* issued October 10, 2018, directs use of enterprise cross domain services to the max extent possible and immediately suspends acquisition, procurement, or implementation of new Point-to-Point CDS implementations. The exemption process is outlined in the memo. The P2P CDS Exemption process is illustrated in **Figure 19** and detailed in Section G.3.4.c of this guide

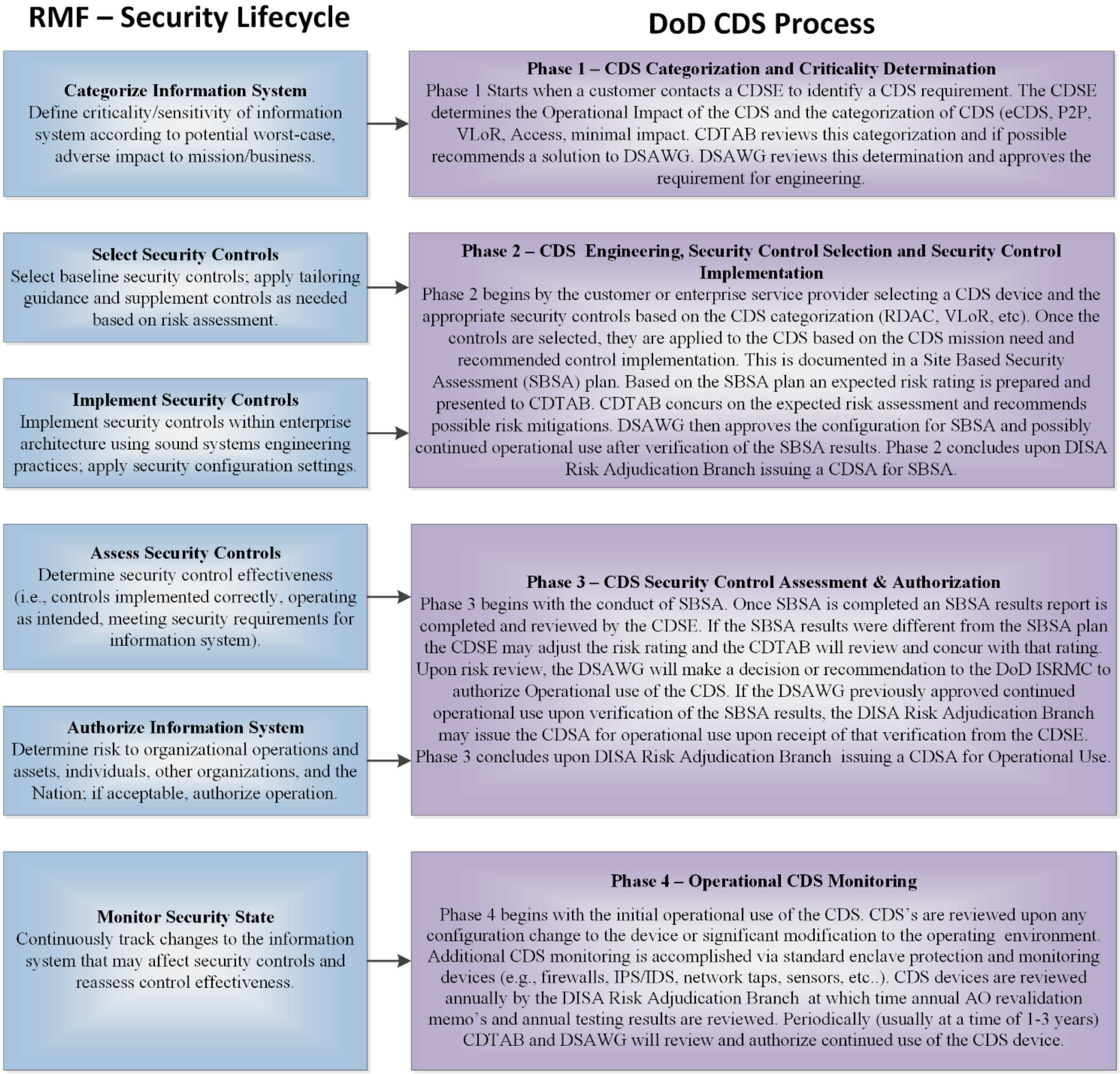
b. **Tactical CDS.** A Tactical CDS deployment operates in austere environmental conditions, or, where terrestrial communications are not possible, reliable, or survivable. Austere environmental conditions include combat and related land, sea, or air vehicles. If the CDSE' determines the CDS is tactical, it will not require submission to an ECDSP for review or require a P2P CDS Exemption memorandum as illustrated in Figure 18. The P2P CDS must meet all the Tactical Criteria defined in the NCDSMO document available on the P2P CDS supporting documentation web page - select "*ECDS P2P Tactical Criteria 20190603 V1.0*.". Otherwise, the P2P CDS also will require a Plan of Action and Milestones (POA&M) signed by the Program/Project Manager or the individual responsible for maintaining and monitoring overall execution of the POA&M.

c. **Other types of Point-to-Point CDS**

A P2P CDS that is not an Access/Tactical/MCI CDS must follow the P2P CDS Exemption Process IAW DoD CIO and USD (A&S) Memorandum, Suspension of New P2P CDSs that states that DoD Components must use enterprise CDS services to the maximum extent possible and immediately suspend acquisition, procurement, or implementation of new P2P CDS implementations. The memo outlines an exemption process clarified in an NCDSMO document available on the P2P CDS supporting documentation web page - select "*DoD P2P CDS Memo Implementation Guidance 20190603 V1.0.*" Procedures for requesting a P2P CDS exemption review and approval are illustrated in Figure 19 and described in Section G.3.4.c of this guide.

G.2.3. **IC Owned Cross Domain Solution.**

An IC Owned CDS is a CDS that an intelligence agency owns, approves, and manages. Only IC CDSs connected to DoD networks are referenced in this connection process guide for visibility and reciprocity purposes. (See Section G.8 of this guide for registration procedures.)



RMF – Security Lifecycle

DoD CDS Process

Categorize Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

Phase 1 – CDS Categorization and Criticality Determination
Phase 1 Starts when a customer contacts a CDSE to identify a CDS requirement. The CDSE determines the Operational Impact of the CDS and the categorization of CDS (eCDS, P2P, VLoR, Access, minimal impact. CDTAB reviews this categorization and if possible recommends a solution to DSAWG. DSAWG reviews this determination and approves the requirement for engineering.

Select Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

Implement Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

Phase 2 – CDS Engineering, Security Control Selection and Security Control Implementation
Phase 2 begins by the customer or enterprise service provider selecting a CDS device and the appropriate security controls based on the CDS categorization (RDAC, VLoR, etc). Once the controls are selected, they are applied to the CDS based on the CDS mission need and recommended control implementation. This is documented in a Site Based Security Assessment (SBSA) plan. Based on the SBSA plan an expected risk rating is prepared and presented to CDTAB. CDTAB concurs on the expected risk assessment and recommends possible risk mitigations. DSAWG then approves the configuration for SBSA and possibly continued operational use after verification of the SBSA results. Phase 2 concludes upon DISA Risk Adjudication Branch issuing a CDSA for SBSA.

Assess Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

Authorize Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

Phase 3 – CDS Security Control Assessment & Authorization
Phase 3 begins with the conduct of SBSA. Once SBSA is completed an SBSA results report is completed and reviewed by the CDSE. If the SBSA results were different from the SBSA plan the CDSE may adjust the risk rating and the CDTAB will review and concur with that rating. Upon risk review, the DSAWG will make a decision or recommendation to the DoD ISRMC to authorize Operational use of the CDS. If the DSAWG previously approved continued operational use upon verification of the SBSA results, the DISA Risk Adjudication Branch may issue the CDSA for operational use upon receipt of that verification from the CDSE. Phase 3 concludes upon DISA Risk Adjudication Branch issuing a CDSA for Operational Use.

Monitor Security State
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Phase 4 – Operational CDS Monitoring
Phase 4 begins with the initial operational use of the CDS. CDS's are reviewed upon any configuration change to the device or significant modification to the operating environment. Additional CDS monitoring is accomplished via standard enclave protection and monitoring devices (e.g., firewalls, IPS/IDS, network taps, sensors, etc..). CDS devices are reviewed annually by the DISA Risk Adjudication Branch at which time annual AO revalidation memo's and annual testing results are reviewed. Periodically (usually at a time of 1-3 years) CDTAB and DSAWG will review and authorize continued use of the CDS device.

Figure 17 RMF Lifecycle

G.3. Cross Domain Solution (CDS) Authorization Process

This Section includes the CDS authorization process for all categories except the IC CDS Registration process that is described in Section G.8 of this guide.

Figure 17 cross-references the RMF process steps to the various CDS phases and provides detail for each of the phases. The four phases are:

- **Phase 1**: CDS Categorization and Criticality Determination
- **Phase 2**: CDS Engineering, Security Control Selection and Security Control Implementation
- **Phase 3**: CDS Security Control Assessment & Authorization
- **Phase 4:** Operational CDS Monitoring

Figure 18 illustrates the CDS Connection Process. In each phase, the DSAWG makes recommendations to the ISRMC regarding CDS requests or makes decisions on CDS requests IAW authorities delegated to the DSAWG by the ISRMC (see Section G.9.1 of this guide).

G.3.1. **Phase 1: CDS Categorization and Criticality Determination**

Phase 1 of the CDS process is illustrated in

Figure 18. Any exceptions to the CDS process must be coordinated with the DoD Component's CDSE and the DSAWG Secretariat (CDTAB Support). It will also likely require approval of the CDTAB/DSAWG/DoD ISRMC boards.

G.3.1.1. The CDS organization must coordinate with their respective CDSE representatives to determine and document the information transfer and mission requirements. This is to support the CDSE's CDS Categorization and enable him to identify the respective processes and artifacts needed to proceed.

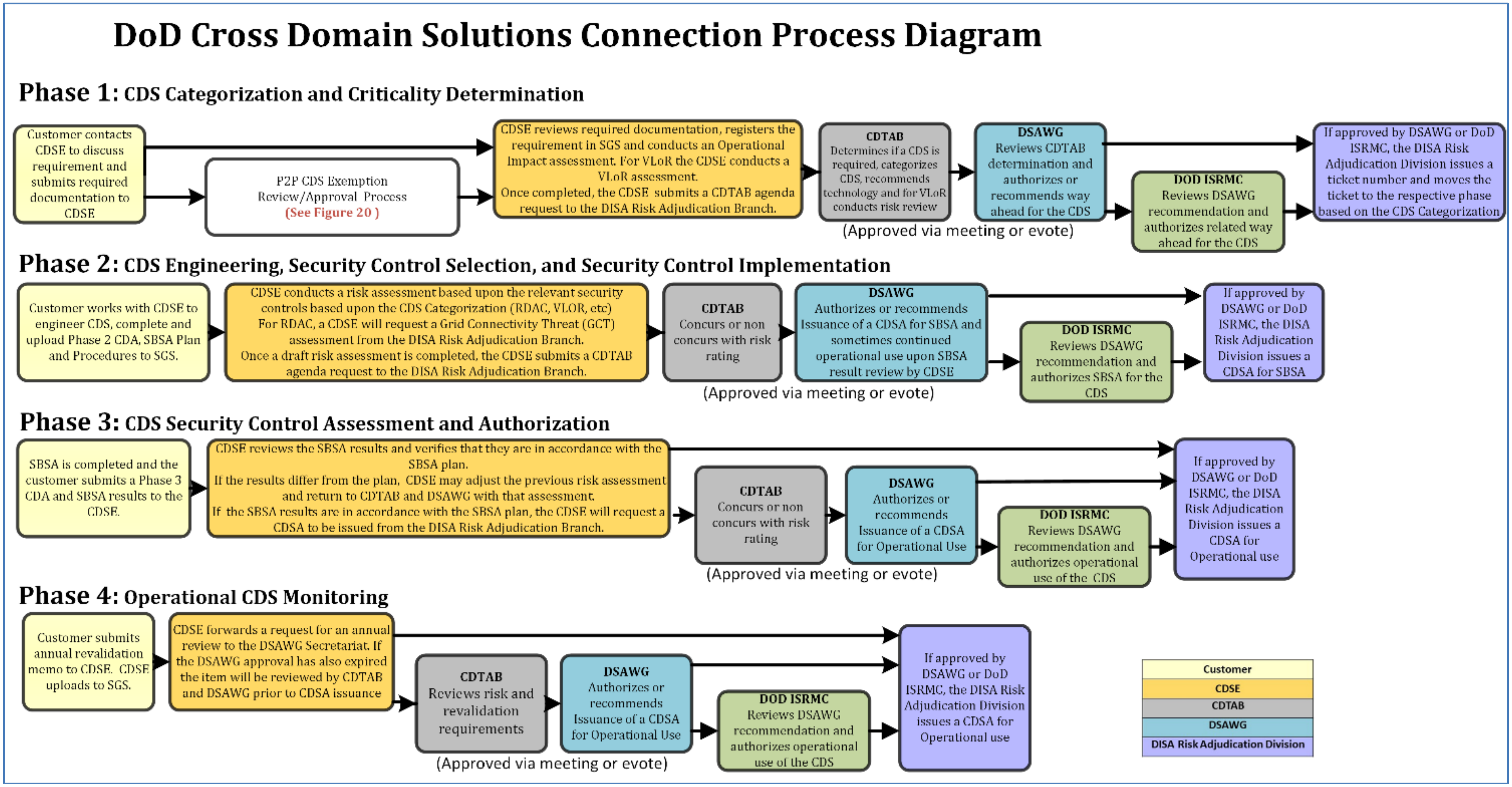
Please review DoDI 8540.01 Enclosure 5 *CD and RMF Roles,* paragraph 4, if you would like to review the roles of a CDSE. If you do not know your CDSE POC, the DSAWG Secretariat (CDTAB Support) can assist in providing that information.

> Per DoDI 8540.01 Enclosure 5, paragraph 4.g. CDSE provides CD support to Combatant Commands and other organizations IAW DoDD 5100.03, *Support of the Headquarters of Combatant and Subordinate Joint Commands.*

G.3.1.2. The CDSE logs into the SGS system and opens a new CDS request filling out all applicable database fields, and uploads all of the following Phase 1 required documents:

a) Validation Memorandum, signed by an O-6 or civilian equivalent that has authority to release funds.

b) Cross Domain Appendix (CDA) with section 1.0 completed and with the Designated Command Representative signature required in phase 1 – the CDA template is available on the NIPRNet CDTAB website under the "Shared Documents" tab and the "new_cds-customer-docs" folder.



DoD Cross Domain Solutions Connection Process Diagram

Phase 1: CDS Categorization and Criticality Determination

Customer contacts CDSE to discuss requirement and submits required documentation to CDSE

P2P CDS Exemption Review/Approval Process (See Figure 20)

CDSE reviews required documentation, registers the requirement in SGS and conducts an Operational Impact assessment. For VLoR the CDSE conducts a VLoR assessment. Once completed, the CDSE submits a CDTAB agenda request to the DISA Risk Adjudication Branch.

CDTAB Determines if a CDS is required, categorizes CDS, recommends technology and for VLoR conducts risk review

DSAWG Reviews CDTAB determination and authorizes or recommends way ahead for the CDS

(Approved via meeting or evote)

DOD ISRMC Reviews DSAWG recommendation and authorizes related way ahead for the CDS

If approved by DSAWG or DoD ISRMC, the DISA Risk Adjudication Division issues a ticket number and moves the ticket to the respective phase based on the CDS Categorization

Phase 2: CDS Engineering, Security Control Selection, and Security Control Implementation

Customer works with CDSE to engineer CDS, complete and upload Phase 2 CDA, SBSA Plan and Procedures to SGS.

CDSE conducts a risk assessment based upon the relevant security controls based upon the CDS Categorization (RDAC, VLOR, etc) For RDAC, a CDSE will request a Grid Connectivity Threat (GCT) assessment from the DISA Risk Adjudication Branch. Once a draft risk assessment is completed, the CDSE submits a CDTAB agenda request to the DISA Risk Adjudication Branch.

CDTAB Concurs or non concurs with risk rating

DSAWG Authorizes or recommends Issuance of a CDSA for SBSA and sometimes continued operational use upon SBSA result review by CDSE

(Approved via meeting or evote)

DOD ISRMC Reviews DSAWG recommendation and authorizes SBSA for the CDS

If approved by DSAWG or DoD ISRMC, the DISA Risk Adjudication Division issues a CDSA for SBSA

Phase 3: CDS Security Control Assessment and Authorization

SBSA is completed and the customer submits a Phase 3 CDA and SBSA results to the CDSE.

CDSE reviews the SBSA results and verifies that they are in accordance with the SBSA plan. If the results differ from the plan, CDSE may adjust the previous risk assessment and return to CDTAB and DSAWG with that assessment. If the SBSA results are in accordance with the SBSA plan, the CDSE will request a CDSA to be issued from the DISA Risk Adjudication Branch.

CDTAB Concurs or non concurs with risk rating

DSAWG Authorizes or recommends Issuance of a CDSA for Operational Use

(Approved via meeting or evote)

DOD ISRMC Reviews DSAWG recommendation and authorizes operational use of the CDS

If approved by DSAWG or DoD ISRMC, the DISA Risk Adjudication Division issues a CDSA for Operational use

Phase 4: Operational CDS Monitoring

Customer submits annual revalidation memo to CDSE. CDSE uploads to SGS.

CDSE forwards a request for an annual review to the DSAWG Secretariat. If the DSAWG approval has also expired the item will be reviewed by CDTAB and DSAWG prior to CDSA issuance

CDTAB Reviews risk and revalidation requirements

DSAWG Authorizes or recommends Issuance of a CDSA for Operational Use

(Approved via meeting or evote)

DOD ISRMC Reviews DSAWG recommendation and authorizes operational use of the CDS

If approved by DSAWG or DoD ISRMC, the DISA Risk Adjudication Division issues a CDSA for Operational use

Figure 18 CDS Connection Process

c) P2P Exemption Memorandum – (Not required for Access, ECDSP Sponsored Systems, or Minimal Community Impact, Access)

i. Required if an ECDSP states they can support, and customer does not intend to migrate if NCDSMO determines that an Exemption Memorandum is required or if ECDSP states they cannot support the requirement but the customer also does not meet the P2P criteria (See Figure 19).

d) POA&M - If a CDS Does not meet the Tactical, P2P or ECDSP criteria (respectively as applicable to the CDS categorization of the request) as defined in *Criteria for Determination of Enterprise Cross Domain Service Provider, Point-to-Point Deployment, and Tactical Deployment Status* and POA&M must be provided to meet the relevant criteria based on the CDS categorization.

e) Additional Phase 1 Requirements for a VLoR CDS:

i. CDA section 2.0 Completed (section 2.1 not required)

ii. Site Based Security Assessment (SBSA) Plan [22] (detailed procedures not required)

iii. VLoR Assertions Response Completed

f) Additional Phase 1 requirements for Repeatable Accreditation/Authorization CDS are:

i. Complete the DSAWG Criteria for Repeatable Accreditation of CDS checklist (section 2.0)

ii. Planned Repeatable Inventory Template

iii. Document the requirement for Repeatable Accreditation/Authorization within section 1.0 of the CDA

> Per DoDI 8540.01, Enclosure 3, paragraph 4.b.(4) *"The DoD Component CDS owner must establish a tracking process approved by the CDSE and must track [repeatable] instantiations to include CDS number; unique CDS identifiers, such as hardware serial number or asset tag; location; deployment dates; local points of contact; and the Command Communications Service Designator. The DoD Component CDS owner or manager will forward this information to the CDSE monthly or when changes occur for uploading the information into the designated repository."*

G.3.1.3. The organization's respective CDSE POC reviews the required artifacts and assigns an Operational Impact to the requirement by updating the "Channels" section in the SGS system for the respective request. The CDSE POC then submits an agenda request form to the DSAWG Secretariat (CDTAB Support). The CDSE ensures all required artifacts are uploaded into SGS prior to requesting the item to be reviewed by the CDTAB. If the CDSE determines that the CDS request is for an Access CDS, Minimal Community Impact, or ECSDP Sponsor System Ticket, then the respective CDSE must submit an agenda request form (select the "Template" tab on the SIPRNet CDTAB website) to the DSAWG Secretariat (CDTAB Support 14 calendar days prior to the next CDTAB meeting. The CDTAB and DSAWG meet once per month but, after review, DISA RE42 may determine to process your request electronically via an "evote" versus presenting at the CDTAB meeting. The CDTAB/DSAWG yearly schedule is located on the DSAWG website. Regarding CDS matters, the DSAWG Secretariat (CDTAB Support) will only accept agenda requests from an organization's CDSE.

[22] A copy of the Site Based Security Assessment (SBSA) Plan template is posted on the CDTAB website.

The DSAWG Secretariat (CDTAB Support) will verify receipt of all required items and notify the CDSE if additional items are required.

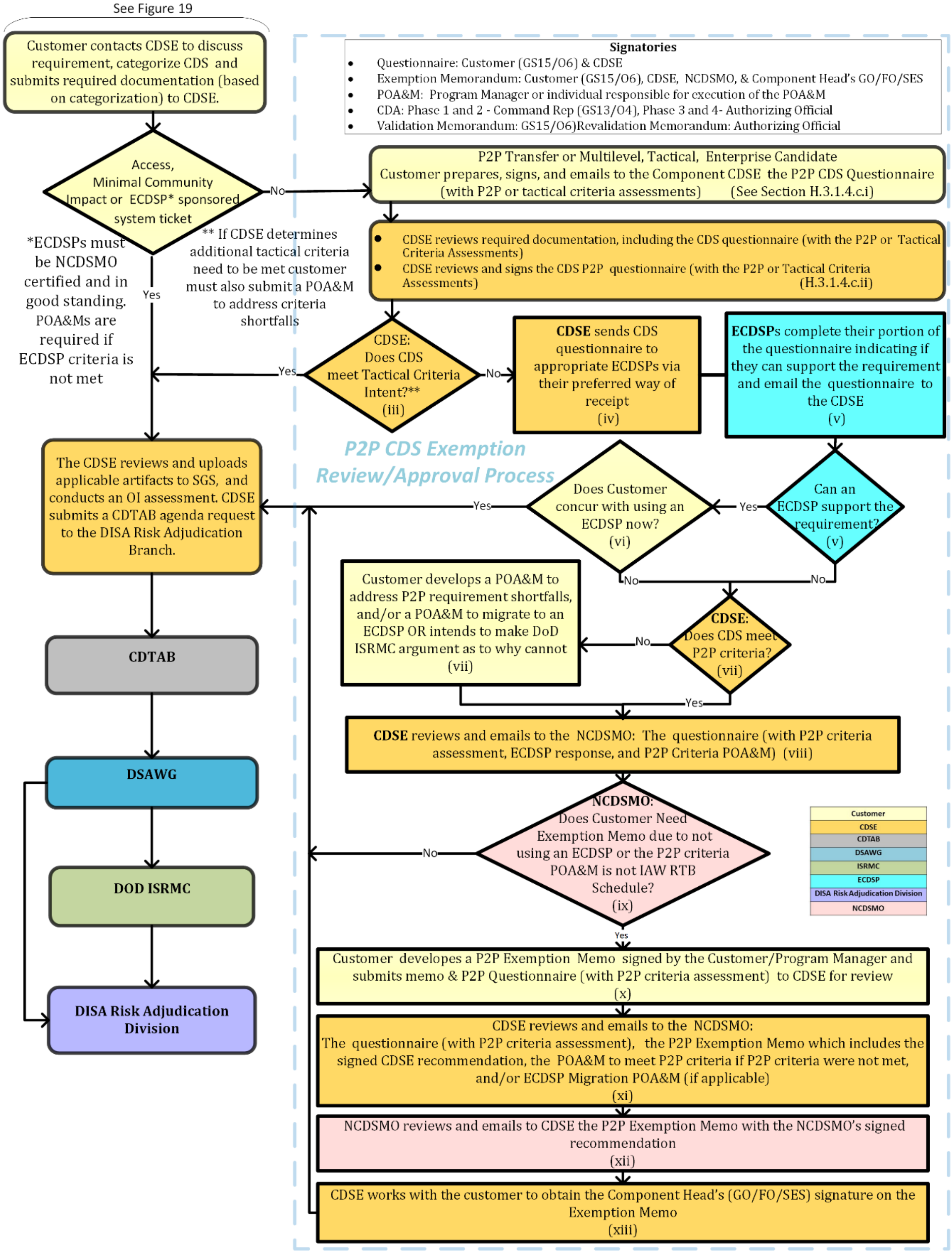

See Figure 19
Customer contacts CDSE to discuss requirement, categorize CDS and submits required documentation (based on categorization) to CDSE.
Access, Minimal Community Impact or ECDSP* sponsored system ticket
No
Yes
*ECDSPs must be NCDSMO certified and in good standing. POA&Ms are required if ECDSP criteria is not met
** If CDSE determines additional tactical criteria need to be met customer must also submit a POA&M to address criteria shortfalls
Signatories
• Questionnaire: Customer (GS15/O6) & CDSE
• Exemption Memorandum: Customer (GS15/O6), CDSE, NCDSMO, & Component Head's GO/FO/SES
• POA&M: Program Manager or individual responsible for execution of the POA&M
• CDA: Phase 1 and 2 - Command Rep (GS13/O4), Phase 3 and 4- Authorizing Official
• Validation Memorandum: GS15/O6)Revalidation Memorandum: Authorizing Official
P2P Transfer or Multilevel, Tactical, Enterprise Candidate Customer prepares, signs, and emails to the Component CDSE the P2P CDS Questionnaire (with P2P or tactical criteria assessments) (See Section H.3.1.4.c.i)
• CDSE reviews required documentation, including the CDS questionnaire (with the P2P or Tactical Criteria Assessments)
• CDSE reviews and signs the CDS P2P questionnaire (with the P2P or Tactical Criteria Assessments) (H.3.1.4.c.ii)
CDSE: Does CDS meet Tactical Criteria Intent?** (iii)
Yes
No
CDSE sends CDS questionnaire to appropriate ECDSPs via their preferred way of receipt (iv)
ECDSPs complete their portion of the questionnaire indicating if they can support the requirement and email the questionnaire to the CDSE (v)
P2P CDS Exemption Review/Approval Process
Can an ECDSP support the requirement? (v)
Yes
No
Does Customer concur with using an ECDSP now? (vi)
Yes
No
The CDSE reviews and uploads applicable artifacts to SGS, and conducts an OI assessment. CDSE submits a CDTAB agenda request to the DISA Risk Adjudication Branch.
CDTAB
DSAWG
DOD ISRMC
DISA Risk Adjudication Division
Customer develops a POA&M to address P2P requirement shortfalls, and/or a POA&M to migrate to an ECDSP OR intends to make DoD ISRMC argument as to why cannot (vii)
CDSE: Does CDS meet P2P criteria? (vii)
No
Yes
CDSE reviews and emails to the NCDSMO: The questionnaire (with P2P criteria assessment, ECDSP response, and P2P Criteria POA&M) (viii)
NCDSMO: Does Customer Need Exemption Memo due to not using an ECDSP or the P2P criteria POA&M is not IAW RTB Schedule? (ix)
No
Yes
Customer
CDSE
CDTAB
DSAWG
ISRMC
ECDSP
DISA Risk Adjudication Division
NCDSMO
Customer developes a P2P Exemption Memo signed by the Customer/Program Manager and submits memo & P2P Questionnaire (with P2P criteria assessment) to CDSE for review (x)
CDSE reviews and emails to the NCDSMO: The questionnaire (with P2P criteria assessment), the P2P Exemption Memo which includes the signed CDSE recommendation, the POA&M to meet P2P criteria if P2P criteria were not met, and/or ECDSP Migration POA&M (if applicable) (xi)
NCDSMO reviews and emails to CDSE the P2P Exemption Memo with the NCDSMO's signed recommendation (xii)
CDSE works with the customer to obtain the Component Head's (GO/FO/SES) signature on the Exemption Memo (xiii)

Figure 19 P2P CDS Exemption Review/Approval

G.3.1.4. **CDTAB Phase 1 Review**. During the CDTAB review, the CDTAB will:

a. Determine if a CDS is required to meet the mission requirement**.**

b. Recommend a NCDSMO baseline solution to meet the requirement.

The following abbreviated summary of the requirements described in the DoD CIO and USD(A&S) memo, "*Suspension of New P2P CDS Implementations and Changes to Existing Point-to-Point Cross Domain Solutions Implementations*,:" October 10, 2018, and described in detail in the DOD ISRMC approved (2 Jun 2019) "NCDSMO *Implementation Guidance for Department of Defense (DOD) Suspension of Point-to-Point Cross Domain Solution (CDS) and Migration to Enterprise Cross Domain Services."* If the guidance is updated to articulate requirements different than explained below – the Implementation Guidance is the authoritative document defining the requirements and must be followed IAW DoD ISRMC guidance.

c. **P2P CDS Exemption Review/Approval Process**. For a P2P CDS that is not an Access CDS[23] or MCI CDS: Ensure the applicable P2P Implementation Guidance Process and Artifacts have been completed (See P2P CDS Exemption Review/Approval Process) and make a recommendation to DSAWG on approval or disapproval of a point-to-point solution to meet the mission requirement. The following P2P CDS Exemption Review and Approval Process is illustrated in Figure 19.

i. For a P2P Transfer or Multilevel, Tactical, server-based Access CDS, or Enterprise Candidate P2P CDS the Customer works with the CDSE to complete the CDS questionnaire that includes the P2P and/or Tactical criteria assessments. The customer (GS15/O6) signs and forwards the P2P CDS questionnaire to the DoD Component's CDSE POC.

ii. The Component's CDSE reviews the required documentation including the P2P CDS questionnaire (with P2P and tactical criteria assessments) and signs the questionnaire.

iii. If the CDSE determines the CDS meets the tactical intent, then the CDSE notes this in the comment section of the CDS questionnaire and no additional P2P Implementation Guidance Processes or artifacts are required prior to CDTAB review. The CDSE emails notification to NCDSMO that tactical questionnaire has been completed and uploaded to SGS two weeks prior to the CDTAB decision request. The CDSE does not have to wait for a NCDSMO response to proceed.

If however the CDS does not meet all tactical criteria at the present time according to the development & deployment timeline requirements found in the *"Cross Domain Solution (CDS) Design and Implementation Requirements: 2018 Raise the Bar (RTB) Baseline Release,"* then a POA&M to meet those criteria will be required that is signed by the Program/Project Manager or the individual responsible for maintaining and monitoring overall execution of the POA&M.

[23] Note: Access CDS (e.g., Virtual Data Center, M-DRIVE) used to host multiple domains (e.g., via technologies like Virtualization) need to complete the P2P CDS Exemption Process. Access CDS used directly by users to access two or more domains from a single workstation and MCI CDS do not have to complete the P2P CDS Exemption Process. ...

iv. If the P2P CDS request does not meet tactical criteria intent, the CDSE sends the P2P CDS questionnaire (with the P2P CDS criteria assessment) to the appropriate ECDSPs for review via the ECDSP's preferred way of receipt.

v. Each ECDSP completes its portion of the CDS questionnaire indicating if the ECDSP can support the requirement. The ECDSP emails the updated questionnaire to the CDSE and the customer.

vi. If an ECDSP asserts within their section of the CDS questionnaire that it CAN support the CDS requirement, and the Customer CONCURS no additional P2P Implementation Guidance Processes or artifacts are required prior to CDTAB review.

vii. If an ECDSP asserts within their section of the CDS questionnaire that it CANNOT support the CDS requirement, or if an ECDSP states they CAN but the customer NON-CONCURS with utilizing an ECDSP, then the CDSE reviews the P2P Criteria responses in the CDS Questionnaire and determines if the customer meets the P2P Criteria.

- If the P2P CDS request does not meet the P2P criteria, the CDSE works with the customer to develop a POA&M that addresses the P2P CDS requirement shortfalls. The customer may also have to develop a POA&M to migrate to an ECDSP or indicate the customer's intent to provide a justification to the DoD ISRMC (post CDTAB and DSAWG) for not migrating to an ECDSP.

viii. The CDSE emails to the NCDSMO the CDS Questionnaire (which includes P2P criteria assessment and ECDSP response) as well as the POA&M (if required) with required signatures completed.

ix. NCDSMO reviews the P2P CDS questionnaire, the CDSE's P2P CDS assessment criteria assessment and the P2P CDS Criteria POA&M (if required). The NCDSMO will then determine if the P2P CDS request requires a P2P CDS Exemption Memo due to not using an ECDSP or if the P2P CDS criteria shortfall POA&M is not in accordance with the Raise the Bar (RTB) schedule requirements.

- If the NCDSMO notifies the CDSE that a P2P CDS Exemption Memo is NOT required, the CDSE uploads into SGS the P2P CDS questionnaire (with the P2P CDS criteria assessment) and POA&M (if required). After this, no additional P2P Implementation Guidance Processes or artifacts are required prior to CDTAB review.

x. If the NCDSMO notifies the CDSE and customer that a P2P CDS Exemption Memo IS required, the customer develops a P2P CDS Exemption Memo signed by the customer/program manager and submits P2P CDS Exemption Memo, the P2P CDS Questionnaire (with P2P CDS criteria assessment), and any POA&Ms to CDSE for review.

xi. CDSE reviews then emails to the NCDSMO: the P2P CDS questionnaire (with P2P criteria assessment), the P2P Exemption Memo that includes the signed CDSE recommendation, the POA&M to meet P2P criteria if P2P criteria were not met, and/or the POA&M for migrating to an ECDSP (if applicable).

xii. NCDSMO reviews and emails the P2P CDS Exemption Memo with the NCDSMO's signed recommendation to the CDSE.

xiii. CDSE works with the customer to obtain the Component Head's (GO/FO/SES) signature on the Exemption Memo before meeting with the DSAWG. The CDSE uploads into SGS the P2P CDS questionnaire (with the P2P CDS criteria assessment), the signed P2P CDS Exemption Memo, and POA&Ms (if any). After this, no additional P2P Implementation Guidance Processes or artifacts are required prior to CDTAB review.

d. **For an Enterprise CDS Candidate** where the Enterprise CD Service Provider (ECDSP) has responded they can meet the requirement and the organization intends to utilize the ECDSP: Ensure there is a valid mission requirement for the proposed solution and that a CDS is required to meet the mission requirements.

e. **For an ECDSP System CDS Request:** Review the proposed system architecture and the DSAWG approved customer requirements (specific organization requests approved by DSAWG for Enterprise CDS implementation) and make any comments/suggestions regarding the technology selection.

f. **For a Minimal Community Impact CDS (non-VLOR) request:** Determine if the criteria for a Minimal (Community) Impact CDS has been met.

g. **For Minimal Community Impact-VLoR:** Conduct a Risk Review of the VLoR assertions and decide if the CDTAB determines the requirement meets the intent of VLoR.

h. **For a Repeatable Accreditation Candidate CDS:** Review the architecture, CDS, and data flows and provide comments to DSAWG. For a Repeatable Accreditation/Authorization Candidate: Determine if Repeatable Accreditation/Authorization Requirements are met.

G.3.1.5. **DSAWG Phase 1 Review**: The DSAWG will review the CDTAB's recommendation and comments and decide (or recommendation to DoD ISRMC) based on the following categories of CDS.

> The following listed decisions are standard decisions based on the category of CDS listed. The DSAWG may make modified approval decisions or recommendations to the DoD ISRMC as they see fit.

a. **For a point-to-point CDS**: Approval for ticketing and phase 2 analysis OR direction that an ECDSP must be utilized.

b. **For a Minimal Community Impact (non-VLOR) request**: Approval for 3 years of operational use. SBSA approval is within AO purview and does not require separate DSAWG approval

c. **Minimal Community Impact VLoR**: Conduct a Review of the CDTAB's VLoR determination and approve for SBSA and continued operational use for 3 years contingent upon the CDSE review of the SBSA results

d. **For an Enterprise CDS Candidate** where the ECDSP has responded that they could meet the requirement and the organization intends to utilize the ECDSP: approval for Enterprise CDS Implementation.

G.3.1.6. **DoD ISRMC Phase 1 Review** (may not be required - see Section G.9.1 of this guide): The DoD ISRMC will review the DSAWG's recommendation and comments and decide. Per the DoD CIO and USD(A&S) Memorandum, *"Suspension of New Point-to-Point Cross Domain Solutions and Changes to Existing Point-to-Point Cross Domain Solutions Implementations"* and the DoD P2P CDS Memo Implementation guidance – the DoD ISRMC will need to make the decision on all new P2P guards that require exemptions – that is, a P2P CDS that is not a Tactical CDS, Minimal (Community) Impact CDS, Access CDS, or a scenario where the ECDSP was unable to support).

G.3.2. Phase 2: CDS Engineering, Security Control Selection & Security Control Implementation

This phase applies only to point-to-point CDS and Enterprise CDS that are required to receive a RDAC/Cross Domain Risk Model (CDRM)[24] analysis. Minimal Community Impact Tickets usually skip this phase.

G.3.2.1. The organization works with their respective CDSE POC (and the ECDSP where applicable) to engineer the CDS, and to complete and upload the following into SGS:

a) Documentation Requirements

- Phase 2 CDA, section 2.0 completed
- SBSA Plan and Procedures
- CDS Risk Assessment Reports (RAR) template. The CDS RAR template is located on the SIPRNet CDTAB website
- Note, the designated entities complete the draft risk analysis under RDAC, the CDSE usually provides the Data Risk and all portions of the Attack Risk, except the Partner Type provided by the Defense Intelligence Agency (DIA), and the Grid Connectivity Threat (GCT) provided by the DISA Risk Adjudication. The CDSE ensures all required artifacts are loaded into SGS prior to requesting the item to be reviewed by the CDTAB.

G.3.2.2. The respective CDSE submits a CDTAB agenda request to the DSAWG Secretariat (CDTAB Support) 14 calendar days prior to the next CDTAB meeting. The DSAWG Secretariat (CDTAB Support) will not accept any late submissions. The DSAWG Secretariat (CDTAB Support) will only accept agenda requests from an organization's CDSE. If the CDSE and DSAWG Secretariat (CDTAB Support) determines the decision will be non-controversial, they can request a CDTAB evote be conducted electronically.

G.3.2.3. CDTAB Phase 2 Review: The voting members will review the information provided from the organization's CDA and the compiled risk rating and will provide a vote of concur or non-concur with the risk rating and adjust the assigned risk ratings as necessary. They will also review and/or provide recommended risk mitigations, if needed.

G.3.2.4. DSAWG Phase 2 Review: The ticket is then presented to the DSAWG with the CDTAB's risk rating and recommended risk mitigations, if needed. The DSAWG will decide (or recommendation to the DoD ISRMC) regarding whether to approve a CDSA for SBSA based on the following scenarios:

[24] For information about the Cross Domain Risk Model (CDRM), see the Shared Documents folder on the CDTAB website.

- If the organization intends (or is directed) to apply CDTAB recommended mitigations prior to SBSA or if the technology is being deployed for the first time in DoD, then SBSA approval will be granted for 2 weeks within a 90-day window. Note that organizations may request additional time for SBSA if needed. After SBSA, the organization will proceed to Phase 3.
- If no additional mitigations need to be applied and if the technology is not being deployed for the first time in DoD: SBSA approval for 2 weeks within a 90-day window and continued operational use upon CDSE review of the SBSA results will be granted. This process is a compressed process for Phase 3 and does not require a Phase 3 CDTAB or DSAWG review.
- Need for Immediate Operational Use upon SBSA completion. On occasion, the DSAWG grants approval for 30 days Immediate Operational Use upon conclusion of the SBSA prior to CDSE review of the SBSA results. This is usually done for tickets that are upgrades or configuration changes to already operational systems so as not to cause a lapse in service. An example DSAWG approval in this case would be “approval for 2 weeks within 90 days for SBSA with 30 days immediate operational use. DSAWG also approves 1 year of operational use upon successful review of the SBSA results by the CDSE.”

G.3.2.5. DoD ISRMC Phase 2 Review (may not be required): The ticket is then presented to the DoD ISRMC with the CDTAB’s risk rating and recommended risk mitigations, as well as the DSAWG recommendation. If needed, the DoD ISRMC will decide regarding whether to approve a CDSA for SBSA and/or CDSA for operational use.

G.3.2.6. Based on the DSAWG (or DoD ISRMC) decision, DISA Risk Adjudication will update SGS milestones and take the following actions based on the approval that was given: (see CDSA Issuance Section G.4 of this guide).

G.3.3. **Phase 3: CDS Security Control Assessment & Authorization**

This phase applies only to P2P CDSs and Enterprise CDSs that are required to receive a risk analysis. Minimal Community Impact Tickets usually skip this phase.

G.3.3.1. The organization works with their respective CDSE (and ECDSP if applicable) to conduct SBSA, to review the SBSA results, and to complete and upload the following into SGS:

a) Required Documentation

- SBSA results
- Updated Phase 3 CDA to include identification of IP addresses for the Guards and administrative server on the topology diagram.

G.3.3.2. The respective CDSE will review the SBSA results to verify no changes exist between the Draft Risk Analysis and the actual test results. If there are no changes and the DSAWG already approved operational use upon CDSE review of the SBSA results, then the CDSE must document this SBSA result in the SGS sections 6.9, 6.10 and 6.11, and notify the DISA Risk Adjudication requesting issuance of the CDSA. (Proceed to step 4) If the CDSE discovers that the SBSA results differ from the SBSA plan expected results, or if DSAWG otherwise requires the ticket to return to DSAWG for operational use, continue the steps below. The CDSE will revise the risk rating and request other entities, which provide the risk rating to revise it, based on the SBSA results as necessary. Once the revised ratings are provided, the

CDSE will submit an agenda request[25] to the DSAWG Secretariat (CDTAB Support) 14 calendar days prior to the next CDTAB meeting or request an evote.

G.3.3.3. CDTAB Phase 3 Review: CDTAB voting members will review the post SBSA risk ratings and provide a vote of concur or non-concur with the risk rating and comments, if necessary.

G.3.3.4. DSAWG Phase 3 Review: The ticket will be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will decide (or recommendation to DoD ISRMC) whether to approve a CDSA for Operational Use.

G.3.3.5. DoD ISRMC Phase 3 Review (may not be required): The ticket will be presented to the DoD ISRMC with the CDTAB's risk rating and comments and the DSAWG recommendation. The DoD ISRMC will decide whether to approve a CDSA for Operational Use

G.3.3.6. Based on the DSAWG decision, the DISA Risk Adjudication will update SGS milestones and take the actions described in Section G.4 of this guide based on the DSAWG's approval.

G.3.4. **Phase 4: Operational CDS Monitoring**

CDSs can receive approval for up to 3 years of operational use from the DSAWG or DoD ISRMC. This means that they do not need to return to CDTAB/DSAWG/DoD ISRMC for 3 years. However, the CDS (unless a Minimal Community Impact CDS) still requires an annual review by the CDSE and the DSAWG Secretariat (CDTAB Support).[26] The process described below describes actions necessary for an annual review when CDTAB/DSAWG/DoD ISRMC review is required as well as an annual review where CDTAB/DSAWG review is not required.

G.3.4.1. The organization contacts CDSE, submits required documentation, and updates SGS as follows:

- **CDS Revalidation Memorandum**. A CDS revalidation memo from the AO stating that the CDS is still required, the CDS configuration has not changed, and has been tested. For an Enterprise CDS: the revalidation memorandum is split into multiple revalidation memorandums. A revalidation memorandum that revalidates the mission requirement for the CDS is required from each organizations' AO. The AO of the ECDSP must provide an additional revalidation memorandum that verifies the unchanged configuration and testing of the system.
- **CDS Annual Self-Assessment Report**. IAW DoDI 8540.01, Enclosure 5, paragraph 8.k the IS owner assesses the protection mechanisms and security controls implemented to protect CD activities. The assessment will:
    - Review the security relevant configuration, operation, and administration of the CDS in its operational environment.
    - Verify that the CDS is utilized per the approved security relevant configuration and documentation requirements.

[25] A mission owner may not submit an agenda request directly to the DSAWG Secretariat (CDTAB Support). Only an organization's CDSE POC can submit an agenda request.

[26] DoDI 8540.01, Enclosure 3, paragraph 4.a.(4)

    - Identify possible security vulnerabilities.
    - Document findings in an assessment report and updated IS POA&M to support annual CDSA revalidation.

- **Repeatable Accreditation/Authorization**. The owner must submit to the CDSE an updated CDS tracking spreadsheet of the repeatable CDS inventory that the organization's CDSE uploads into SGS.
- POA&M **(if required)** uploaded to SGS: If the CDS fits any of the following conditions, the IS Owner must submit via their CDSE a POA&M detailing their schedule to migrate to a new solution or for applying other mitigations within the architecture.
    - The IS Owner is using a non-baseline CDS device
    - An ECDSP has stated they can meet the requirement
    - DSAWG or DoD ISRMC directs improvements to the current system being deployed.

> DoDI 8540.01, Enclosure 5 "*CD and RMF Roles*," paragraph 9 "*Information Owner"*
>
> e. Coordinates with the IS owner to support the DoD Component CDS risk assessment by providing the level of impact (i.e. harm) to the organization due to a threat event causing an unauthorized disclosure, unauthorized modification, unauthorized destruction, or the loss information in support of DoD Component CDS risk assessment consistent with [NIST 800-30].

G.3.4.2. CDSE must review the updated annual review artifacts and advise if the previously assessed risk assessment has change due to newly discovered threats and/or vulnerabilities. CDSE must notify the DSAWG Secretariat (CDTAB Support) of these completed actions. If the DSAWG/DoD ISRMC approved operational period has not expired, the DSAWG Secretariat (CDTAB Support) will proceed to step 5. If the ticket needs an extended operational approval, the DSAWG Secretariat (CDTAB Support) will schedule the CDS for CDTAB review. The DSAWG Secretariat (CDTAB Support) will only accept agenda requests from an organization's CDSE. The respective CDSE must submit all agenda requests to the DSAWG Secretariat (CDTAB Support) 14 calendar days prior to the next CDTAB meeting. If the CDSE and DSAWG Secretariat (CDTAB Support) determines the decision will be non-controversial, they can request a CDTAB evote be conducted electronically.

G.3.4.3. CDTAB Phase 4 Review: The CDTAB voting members will review the CDS Annual Review required documents, any additional information provided/extracted from the organization's CDA, and the previous risk rating prior to providing a concur or non-concur vote with the risk rating and any associated comments/ recommendations to DSAWG.

G.3.4.4. DSAWG Phase 4 Review: The ticket will be presented to the DSAWG with the CDTAB's risk rating, recommendation, and comments. The DSAWG will decide whether to extend the operational approval for the ticket.

G.3.4.5. DoD ISRMC Phase 4 Review (may not be required): The ticket will be presented to the DoD ISRMC with the CDTAB's risk rating, recommendation, and comments and the DSAWG's recommendation. The DoD ISRMC will decide whether to extend the operational approval for the ticket.

G.3.4.6. Based on the DSAWG/DoD ISRMC decision, the DSAWG Secretariat (CDTAB Support) will update SGS milestones and take the actions described in Section G.5 of this guide based on the DSAWG's approval.

G.4. Post DSAWG/DoD ISRMC Actions and Cross Domain Solution Authorization Issuance

G.4.1. Based on the DSAWG decision, the DSAWG Secretariat (CDTAB Support) will update SGS milestones and take the following actions based on the approval that was given:

a) If ticketing was approved for a point-to-point CDS or an enterprise owned system, a CDS ticket number will be assigned

b) If ticketing was approved by the DSAWG and an ECDSP can meet the requirement, the request number will be closed. The ECDSP will notify the customer of the ticket number for the system they intend to use to meet the customer's requirement in Phase 2. The original request number will always be used to reference the customer's requirement and DSAWG approval of the requirement for the Enterprise CDS implementation.

c) If SBSA was approved, the DISA Risk Adjudication will review the documentation requirements for issuance of a CDSA for SBSA which include:

i. Notification of SBSA dates from CDSE at least 2 weeks prior to the start of SBSA.

ii. A Phase 2 CDA (meaning sections 1.0 and 2.0 completed), which references the CCSD and is signed by the AO. (If not signed by an AO, then a separate ATO signed by the AO that authorizes the specific CDS ticket numbers will be accepted). This must show the complete CDS Ticket Number/s.

iii. SBSA Plan and Procedures.

iv. A valid ATC (signed and current) for the CCSD's connection to the CDS. (A CDSA for SBSA or Operational Use will not be issued past a CCSD expiration date)

v. An updated Enclave topology with the CDS must be uploaded to the respective CCSD in section 10.2 (topology) of the SGS GIAP module and show the CDS and CDS ticket number to include identification of IP addresses for the Guards and administrative server on the topology diagram. The CDS Ticket number must be accurate within the first two sections of the ticket number. Examples of accepted ticket number depictions are 1234-0001-xxx or 1234-0001-001 (Applies to SIPR connected CDSs only)

vi. Section 4 of the SGS GIAP for the hosting CCSD must be updated stating that a CDS resides in the enclave and referencing the CDS Ticket Number/s. The CDS Ticket number must be accurate within the first two sections of the ticket number. Examples of accepted ticket number depictions are 1234-0001-xxx or 1234-0001-001 (Applies to SIPR connected CDSs only)

> An SGS GIAP record must be unlocked before it can be updated. The owner of the SGS record must first send an email asking DISN CAO to unlock the SGS record. After the owner completes updating the SGS record, the owner must send an email asking DISN CAO to lock the SGS record

d) If Operational Use was approved, the DISA Risk Adjudication will review the documentation requirements for issuance of a CDSA for Operational Use which include:

i. A Phase 3 CDA (meaning sections 1.0, 2.0, and 3.0 completed), which references the CCSD and is signed by the AO. (If not signed by an AO, then a separate ATO signed by the AO which authorizes the specific CDS ticket numbers will be accepted)

ii. A valid ATC for the CCSD's connection to the CDS. (A CDSA for SBSA or Operational Use will not be issued past a CCSD expiration date)

iii. An updated Enclave topology with the CDS must be uploaded to the respective CCSD in section 10.2 (topology) of the SGS GIAP module and show the CDS and CDS ticket number to include identification of IP addresses for the Guards and administrative server on the topology diagram. The CDS Ticket number must be accurate within the first two sections of the ticket number. Examples of accepted ticket number depictions are 1234-0001-xxx or 1234-0001-001 (Applies to SIPR connected CDSs only)

iv. Section 4 of the SGS GIAP for the hosting CCSD must be updated stating that a CDS resides in the enclave and referencing the CDS Ticket Number/s. The CDS Ticket number must be accurate within the first two sections of the ticket number.

v. Examples of accepted ticket number depictions are 1234-0001-xxx or 1234-0001-001 (Applies to SIPR connected CDSs only)

vi. SBSA Results (If SBSA was required)

vii. Uploaded verification of CDSE review of the SBSA results (If SBSA was required)

G.4.2. If the documentation requirements are not sufficient for a CDSA to be issued at the time of the DSAWG or DoD ISRMC, decision the DISA Risk Adjudication will notify the CDSE of the missing requirements. In order to obtain a CDSA once the documentation requirements are completed, a CDSA request form (see the "Template" tab on the SIPRNet CDTAB website) must be submitted to the DISA Risk Adjudication.

G.4.3. CDSAs for operational use will not be issued which would expire within two weeks of the date the CDSA request form received due to ATO expiration, ATC expiration or DSAWG/DoD ISRMC Approval Window Expiration.

G.4.4. If the DSAWG or the DoD ISRMC approved more than 1 year of operational use, then a CDSA will be issued for a maximum of 1 year and will be reissued when the annual review is conducted. (See Operational CDS Monitoring, Section G.3.4). If the CDS was approved as a Minimal (Community) Impact CDS, then a CDSA can be issued not to exceed three years from the date of the DSAWG or DoD ISRMC review. CDSAs will not be issued past AO authorization for the CDS.

G.4.5. If the ticket is a repeatable authorization/accreditation ticket, the CDSA for SBSA and/or "Operational Use" it will specifically reference the number of CDSs authorized by the DSAWG or DoD ISRMC. If the organization needs to operate additional instantiations, it is necessary to return to DSAWG with mission justification for approval.

G.4.6. The CDS device is marked operational in SGS upon the initial issuance of a CDSA by the DISA Risk Adjudication) following a DSAWG or DoD ISRMC approval. It remains operational until the DISA Risk Adjudication receives evidence in the form of either an email or memo from the organization's respective CDSE that the device is non-operational.

G.5. Configuration Changes to Operational CDSs

Planned changes to the configuration of the CDS including patches and upgrades must be coordinated with the organization's respective CDSE and entered into the SGS as Phase I requests (unless CDTAB has approved an exception due to patch being minor in which case SGS just needs to be updated and DSAWG Secretariat (CDTAB Support) notified). If the change is a patch (determined by CDTAB to be applied in the form of a new ticket), software upgrade, or other configuration change such as adding a channel or network, the DSAWG Secretariat (CDTAB Support) will administratively move the request to Phase 2. The DSAWG Secretariat (CDTAB Support) will then issue a new CDS ticket number provided the phase 1 documentation requirements (including a CDS Questionnaire, exemption memorandum and POA&M if applicable) and SGS updates have been completed. The CDS ticket will proceed to CDTAB in Phase 2 to complete the normal CDS approval process.

The CDS ticket will not be administratively moved to Phase 2 if the request is for a change in technology. Instead, the CDS ticket follows the normal Phase 1 process.

G.6. Closure of a CDS Requirement

If for any reason it becomes necessary to discontinue use of a CDS or an organization is no longer continuing their mission, the respective CDSE must submit a closure request to stop tracking 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." If the CDS device connects to SIPRNet, the related CCSD sections 4 (Classified Network Information) and 10.2 (Topology) of the SGS GIAP module must be updated by the customer as well to remove the CDS.

G.7. Process for Approving an ECDSP System for Streamlined Onboarding of new customer

The DoD ISRMC approved the ECDSP Streamlined Onboarding (SO) Process on 25 Jun 2019.

G.7.1. Criteria

This process allows for an abbreviated A&A process for ECDSPs to onboard customers to ease and expedite DoD Components transition to ECDSPs when the following criteria are met:

a. An ECDSP has brought an initial solution/filter forward for SO to CDTAB for a risk rating and DSAWG/DoD ISRMC for approval

b. Evidence of AO approval for SO required.

c. The filter should be given a unique name/identifier and incremented version number

d. Additional customer(s) deployed to use the solution/filter must be deployed on an operational ECDSP CDS with the same filter that was previously approved by DSAWG/DoD ISRMC

   i. SO Channels should represent less than or equal to the amount of risk as the initial approval.

e. The new channel(s) for SO shall be the same as the initially approved channels in the following manner:

   i. Transfer data between the same network pairs as the initial approval

ii. Fielded on the same guard

iii. Pass the same data type(S)

iv. Employ the same filter name/version

v. Have the same auditing/logging mechanism in place and send the same information to the ECDSP CNDSP

f. All changes to the solution/filter require a new brief to CDTAB for an updated risk rating and DSAWG/DoD ISRMC for approval for SBSA and operational use.

g. ECDSP must provide Due Diligence to CDTAB/DSAWG/DoD ISRMC monthly or (as requested)

h. ECDSP filter is provided to NCDSMO for the Cross Domain Threat Assessment Enclave. (TAE) (after approval for CDSA for operational use)

G.7.2. **Process for on boarding a new customer to an ECDSP approved for Streamlined Onboarding**

After an ECDSP system is approved to use the Streamlined Onboarding Process (see Section G.7.1), the process for onboarding a new customer to the approved ECDSP will occur depending on the Phase:

G.7.2.1. Phase 1:

- CDS approval for an ECDSP would proceed as normal

G.7.2.2. Phase 2:

- During the initial approval for the enterprise CDS - In addition to normal phase 2/3 CDS process the following will occur:
- An ECDSP brings forward a filter for SO with initial customer to phase 2/3 approval
- The CDSE provides SO recommendation (prior to CDTAB)
- CDTAB will make a SO recommendation
- DSAWG or DoD ISRMC would approve the ticket and the use of SO

G.7.2.3. Phase 3:

- DISA Risk Adjudication would issue CDSA for SBSA
- ECDSP would review SBSA report and if acceptable request CDSA for operational use

G.7.2.4. Phase 4:

- DISA Risk Adjudication would issue the CDSA for operational use that would reference the SO approval.

G.7.2.5. After the ECDSP system is approved for SO the onboarding process as illustrated in Figure 20 to add a customer channel would be as follows:

a. ECDSP has new customer requirements (customer request has already completed phase 1 of the CDS process as an ECDS candidate and has been approved by DSAWG for ECDSP implementation)

b. ECDSP updates Phase 2/3 for proposed channels

c. ECDSP/ECDSP CDSE enter in process channels to include A/R date in SGS (channels marked as in process)

d. ECDSP CDSE evaluates Phase 2/3 SO requirements

e. ECDSP CDSE determines SO requirements met or not.

f. If not, SO process does not apply and ticket number and the filter must be incremented and proceed to standard phase 2/3 process

g. If ECDSP CDSE determines SO requirements were met and the risk rating is equivalent or less, the ECDSP uploads the concurrence to the SGS and notifies DISA RE42

h. DISA RE42 would verify the artifacts to include the evidence of ECDSO AO's approval for SO. If acceptable the secretariat would issue a new updated CDSA and mark the channels approved in SGS under the respective ticket number

i. ECDSP would proceed to add the new flow to the CDS

j. ECDSP tracks configuration management tool

k. ECDSP CDSE receives CM evidence as requested

l. ECDSP/ECDSP CDSE provide Due Diligence brief to the CDTAB/DSAWG monthly or as requested

m. ECDSP/ECDSP CDSE align SO channels with Annual Review

n. New Channels documented annually in the Annual Review slides

G.8. IC CDS Registration Process

As illustrated in Figure 21, the DoD ISRMC requested that all IC owned CDSs that connect to DoD Networks are registered in SGS. Having all CDSs which connect to DoD Networks registered in one central location aids the CDTAB, DSAWG and DoD ISRMC by maintaining an accurate depiction of DoD network environments and interconnections to facilitate rapid incident response.

G.8.1. **Step 1: Obtain and Complete an IC CDS Registration Form**

To obtain an IC CDS Registration form template, contact the DSAWG Secretariat (CDTAB Support). The form is also posted on both the CDTAB website and DSAWG SIPR Intelink Sites. The IC registration form contains all the data necessary to complete an SGS database registration.

G.8.2. **Step 2: SGS Entry and IC Registration Form Review**

Once the IC registration form is completed, the IC Component or CDSE will register the CDS in the SGS database and upload the IC registration form as an attachment.

Access to the SGS database on SIPRNet and select “request an account.” The CDSE will be required to upload a completed DD 2875. A template is on the entry page of the website. Once the registration is complete, the IC component or CDSE will notify the DSAWG Secretariat (CDTAB Support) of a completed registration. The DSAWG Secretariat (CDTAB Support) will review the registration, generate a CDS Ticket Number, and notify the submitting IC Component and/or CDSE of the CDS Ticket Number.

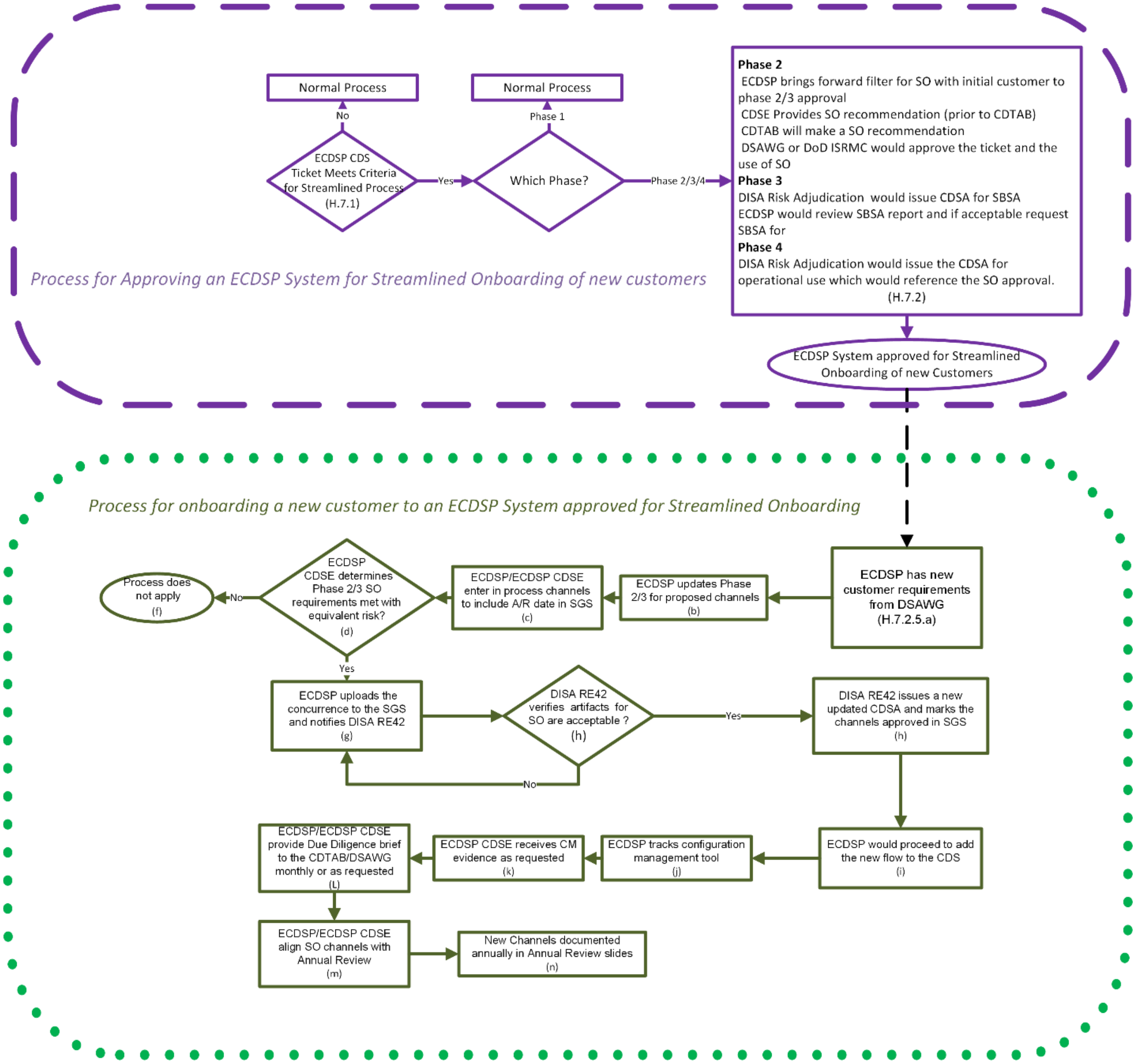

Normal Process
Normal Process
No
Phase 1
ECDSP CDS Ticket Meets Criteria for Streamlined Process (H.7.1)
Yes
Which Phase?
Phase 2/3/4
Phase 2
ECDSP brings forward filter for SO with initial customer to phase 2/3 approval
CDSE Provides SO recommendation (prior to CDTAB)
CDTAB will make a SO recommendation
DSAWG or DoD ISRMC would approve the ticket and the use of SO
Phase 3
DISA Risk Adjudication would issue CDSA for SBSA
ECDSP would review SBSA report and if acceptable request SBSA for
Phase 4
DISA Risk Adjudication would issue the CDSA for operational use which would reference the SO approval.
(H.7.2)
Process for Approving an ECDSP System for Streamlined Onboarding of new customers
ECDSP System approved for Streamlined Onboarding of new Customers
Process for onboarding a new customer to an ECDSP System approved for Streamlined Onboarding
ECDSP has new customer requirements from DSAWG (H.7.2.5.a)
ECDSP updates Phase 2/3 for proposed channels (b)
ECDSP/ECDSP CDSE enter in process channels to include A/R date in SGS (c)
ECDSP CDSE determines Phase 2/3 SO requirements met with equivalent risk? (d)
No
Process does not apply (f)
Yes
ECDSP uploads the concurrence to the SGS and notifies DISA RE42 (g)
DISA RE42 verifies artifacts for SO are acceptable ? (h)
No
Yes
DISA RE42 issues a new updated CDSA and marks the channels approved in SGS (h)
ECDSP would proceed to add the new flow to the CDS (i)
ECDSP tracks configuration management tool (j)
ECDSP CDSE receives CM evidence as requested (k)
ECDSP/ECDSP CDSE provide Due Diligence brief to the CDTAB/DSAWG monthly or as requested (L)
ECDSP/ECDSP CDSE align SO channels with Annual Review (m)
New Channels documented annually in Annual Review slides (n)

Figure 20 Streamlined Onboarding Process for an ECDSP

G.8.3. Step 3: Submission of Requested Documentation for Reciprocity Acceptance

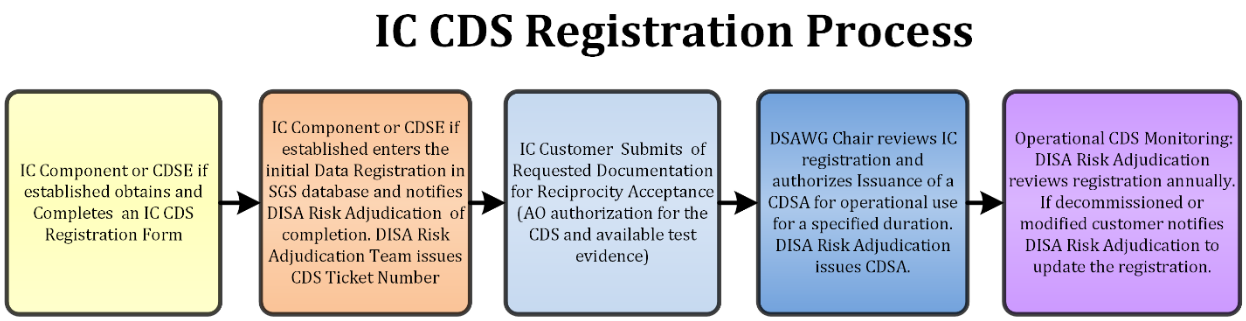
The IC component or CDSE will upload a copy of the signed AO authorization for the CDS and the SBSA evidence for the CDS to the SGS database under the respective SGS record. Once uploaded, the IC component or CDSE will notify the DSAWG Secretariat (CDTAB Support) that all documents have been submitted. The DSAWG Secretariat (CDTAB Support) will send notification of a completed IC CDS registration to the DSAWG Chair.

G.8.4. Step 4: CDSA Issuance

Upon review of the notification of IC registration, the DSAWG Chair will authorize the DISA Risk Adjudication to issue a CDSA for operational use for a specified duration.

G.8.5. Step 5: Operational CDS Monitoring

Annually, the DSAWG Secretariat (CDTAB Support) will request the IC POC to verify if the CDS is still operational. Any time that the devices are modified in a manner that requires the IC registration to be updated, the IC agency should provide that update to the DSAWG Secretariat (CDTAB Support). If the device is decommissioned, the IC agency provides a signed memo or digitally signed e-mail to the DSAWG Secretariat (CDTAB Support), which will close the registration in SGS.



IC CDS Registration Process

IC Component or CDSE if established obtains and Completes an IC CDS Registration Form

IC Component or CDSE if established enters the initial Data Registration in SGS database and notifies DISA Risk Adjudication of completion. DISA Risk Adjudication Team issues CDS Ticket Number

IC Customer Submits of Requested Documentation for Reciprocity Acceptance (AO authorization for the CDS and available test evidence)

DSAWG Chair reviews IC registration and authorizes Issuance of a CDSA for operational use for a specified duration. DISA Risk Adjudication issues CDSA.

Operational CDS Monitoring: DISA Risk Adjudication reviews registration annually. If decommissioned or modified customer notifies DISA Risk Adjudication to update the registration.

Figure 21 IC CDS Registration Process

G.9. Frequently Asked Questions

G.9.1. Q: What CDS decisions has the DoD ISRMC delegated to the DSAWG?

A: The DoD ISRMC Decision Ballot on “Delegation to DSAWG of Decision Authority on CDS Tickets, 24 April 2018 is as follows:

- Tickets inside of the RDAC risk range based on tech, data, and mission
- Tickets 1 step out of the RDAC risk range with due diligence to DoD ISRMC
- Exercise CDS tickets
- For Minimal (Community) Impact CDS Tickets [formerly “Tracking Purposes Only (FTPO) Tickets”] which meet on of the following criteria: completely isolated connecting enclaves, VLoR or controlled interfaces
- Cyber TAPS utilizing approved one-way solution in DoD ISRMC approve Cyber SA enclave
- Annual review of impacted tickets. If CDS vendor and customer are actively working to resolve the issues, as per DoD CIO policy memo and NSA guidelines
- Annual review of previously approved DoD ISRMC CDS ticket, with no change in previous risk rating and complying with DSAWG/DoD ISRMC directed constraints and directives for Contractor Facility CDS & Continued use of a Sunset CDS

Note: New P2P CDS requests must go to the ISRMC unless they are for an Access CDS or MCI CDS per *the Implementation Guidance for Department of Defense (DoD) Suspension of Point-to-Point Cross Domain Solution (CDS) and Migration to Enterprise Cross Domain Services* .

G.9.2. **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 it is being used for load balancing?**

A: A separate request/ticket is required for each CDS device/distribution console if there are any configuration differences or if they are deployed at different locations. A separate request is not needed for a cold spare, but the cold spare must go through SBSA with the primary and evidence of the SBSA results must be uploaded under the SGS. In the event the cold spare is utilized, the CDSE and the DSAWG Secretariat (CDTAB Support) must be notified, and a new request must be opened.

- The example of this is if the ticket is an ECDSP ticket or a Repeatable Accreditation/Authorization ticket. Another example is if multiple identically configured guards are going to be deployed at the same location at the same time and SBSA will be conducted at the same time. In these scenarios, the “Instantiations” field of SGS will be updated to reflect the number of instantiations a single CDS ticket represents. All documentation (CDA/CDSA/Briefing Slides) will be maintained under that single CDS ticket number in SGS and will list the ticket numbers as if they existed in the database (Ex: 1234-1/2/3/4/5-001).

G.9.3. Q: What is the significance of the three partitions of a CDS ticket number?

A: Once a point-to-point CDS or enterprise owned CDS Request (ex: R0001111) is approved at DSAWG, it is assigned a ticket number that is formatted in three partitions (ex: 1234-0001-001). The significance of these partitions is as follows:

- **First partition (*1234*-0001-001):** The first partition represents the organization’s configuration. If this is a new organization configuration, the request will receive a ticket number with a unique first partition. The second and third partitions will be numbered ”0001-001”
- **Second partition (1234-*0001*-001):** The second partition represents the instantiation of the CDS device. For example, if three identically configured CDS devices were needed at three different locations the ticket numbers would be 1234-0001-001, 1234-0002-001, and 1234-0003-001. The configuration and organization requirement are the same, but there are three devices meeting this requirement at three different locations.
- **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 elements. 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. Once the new ticket is operational, the previous iteration -001 will be closed in SGS.

G.9.4. Q**:** What is the difference between a CDSA and an ATC?

A: Once a Security Authorization Package is submitted, reviewed, and accepted by the DISN CAO, then 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 or DoD ISRMC approval of a CDS contingent upon all required paperwork being submitted to DISA RE42. A DSAWG or DoD ISRMC Ballot is not community authorization to utilize a CDS. Per 8540.01, a CDSA is required.

> IAW DoDI 8540.01, paragraph 3.g, it is DoD Policy that "*the DoD-level risk decision on use of a CDS to access or transfer information between different interconnected security domains must be made by the designated DoD risk executive as a CDS authorization (CDSA) ….*"
>
> IAW DoDI 8540.01, Enclosure 2, paragraph 8.u.(1) DoD Component Heads shall:" Require *the issuance of a DoD ISMRC [sic] or DSAWG CDSA before allowing a CDS to access or transfer information between different interconnected security domains. A CDSA is required for use of a CDS."*

Other Policy and Guidance for Cross Domain Solutions and Services
CDTAB Charter - Establishes the CDTAB to assess community[27] risks IAW the RDAC and make recommendations to the DSAWG and the DISA Authorizing Official on the connections of implementations to community networks.
CJCSI 6211.02D - Updates Unified Cross Domain Services Management Office (NCDSMO) roles and responsibilities. Adds guidance on prioritization of CD requirements. Directs CC/S/As to use Enterprise CD services and only use point-to-point CDS services when enterprise-CD-services don't meet the operational mission requirements
DoD CIO and Office of the Director of National Intelligence Memorandum, (U) Unified Cross Domain Services Management Office Disestablishment and Functional Transition to the National Cross Domain Strategy and Management Office Establishes the NCDSMO as the CD services requirements and engineering manager to expedite progress toward Enterprise CD services and improve coordination across the federal government.
DoDI 8510.01 - The RMF requires an AO responsible for an Information System or Platform Information Technology (PIT) system to consider the security impact of the CDS operation in the overall authorization decision.
DoDI 8540.01, Cross Domain Policy - Establishes policy, assigns responsibilities, and identifies procedures for the interconnection of information systems (ISs) of different security domains using CD solutions (CDSs).
RDAC 2.3
VLoR Assertions
P2P CDS Supporting Documentation: • **Implementation Guidance for Department of Defense (DoD) Suspension of Point-to-Point Cross Domain Solution (CDS) and Migration to Enterprise Cross Domain Services** - provides implementation guidance for the *DoD CIO and USD (A&S) Memorandum, Suspension of New Point-to-Point Cross Domain Solutions and Changes to Existing Point-to-Point Cross Domain Solutions Implementations*. • **Enterprise CDS, Point-to-Point CDS, or Tactical CDS Deployment Status** - provides the criteria for defining what constitutes an Enterprise CDS, Point-to-Point CDS, or Tactical CDS deployment and outlines the requirements to establish and sustain an Enterprise Cross Domain Service Provider • **Development & Deployment Timeline Requirements for the “Cross Domain Solution (CDS) Design and Implementation Requirements: 2018 Raise the Bar (RTB) Baseline Release** - Establishes development and deployment guidance on how to apply the NCDSMO Cross Domain Solution (CDS) Design and Implementation Requirements: 2018 Raise the Bar (RTB) Baseline Release (NCDSMO-R-00008-001_03) • **Plan of Action and Milestones (POA&M) for Transitioning P2P CDS to an ECDSP** – Template • **Template for P2P Exemption**

Table 4 Other Policy and Guidance for Cross Domain Solutions

[27] The community is defined as the transport, network management, and network segments of the DISN for the Department of Defense (DoD) Global Information Grid (GIG)

This page intentionally left blank.

Appendix H Connection to DISN Mission Partner Gateways (MPGW)

H.1. Mission Partner DMZ or Gateway Connections

This Appendix supplements information provided in Section 2.11 of this guide with additional information on DISN MPGW connections. DISN MPGWs provide support for DoD Contractors, Federal Partners, and Allied/Coalition Partners with connections approved by DoD CIO as described in Appendix B.

The NIPRNet Federated Gateway (NFG) supports unclassified Mission Partner connections to NIPRNet, the SIPRNet FED DMZ supports classified U.S. Mission Partner connections to SIPRNet, and the SIPRNet REL DMZ supports classified coalition connections to SIPRNet.

IAW DoDI 8010.01 and CJCSI 6211.02D, DoD Mission Partner (non-DoD organizations) enclave connections (including a contractor's enclave connection) to DISN-provided transport must be through an established DISN DMZ and will follow DISN DMZ security requirements. In certain limited special use cases, the DoD CIO has approved some non-DoD Federal Agency direct connections to the NIPRNet and SIPRNet; however, this is not the norm. DISN DMZs/NFG access connections can be either physical or logical (see Figure 22). Mission Partners will work with the NIPRNet NFG Office or the SIPRNet FED and REL DMZ Office to initiate their respective MPGW connections.

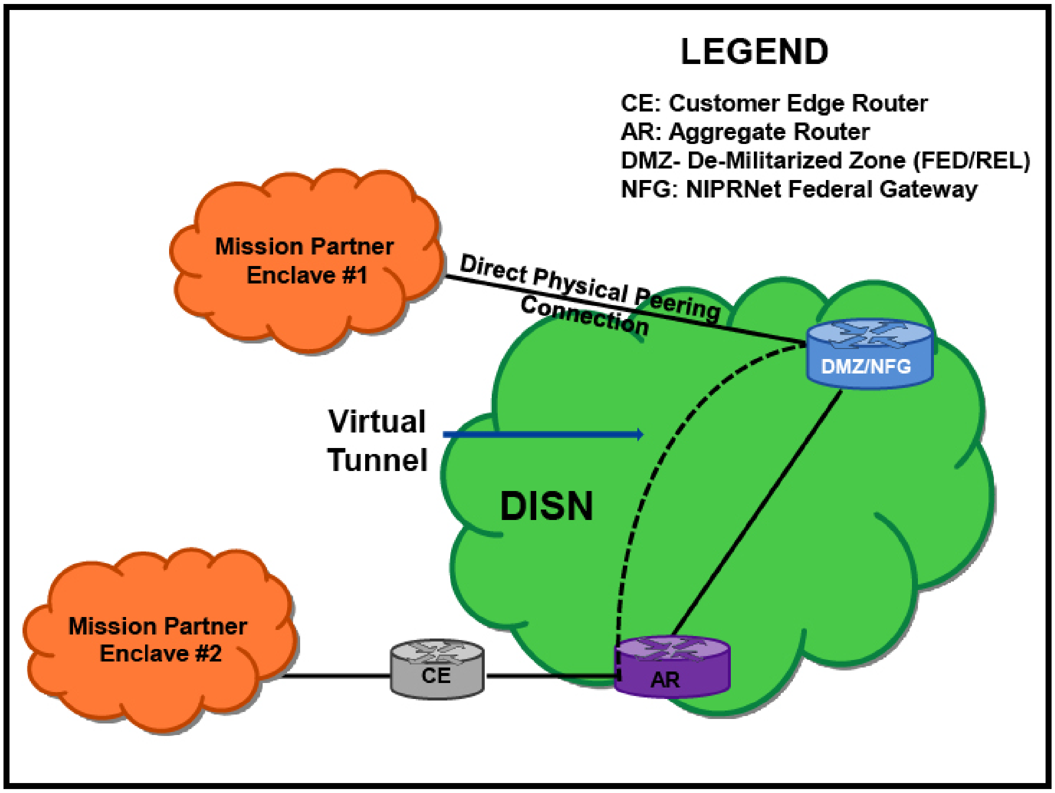

LEGEND
CE: Customer Edge Router
AR: Aggregate Router
DMZ- De-Militarized Zone (FED/REL)
NFG: NIPRNet Federal Gateway
Mission Partner Enclave #1
Direct Physical Peering Connection
DMZ/NFG
Virtual Tunnel
DISN
Mission Partner Enclave #2
CE
AR

Figure 22 Generic DISN DMZ and Gateway Connections

All Mission Partner NIPRNet/SIPRNet connections require DoD CIO Approval, a formal agreement (e.g., Contract, MOA, or MOU) and DoD Component sponsor to validate DoD mission need for Mission Partner access to the DISN (See Appendix B for details). DoD

Component sponsors must understand and agree to their responsibilities as summarized in the DoD CIO sponsor Responsibilities Memorandum, applicable issuances, and the Defense Finance and Accounting Regulations (DFAR). DoD Component sponsors must codify responsibilities for DISN connection in an appropriate agreement (e.g., MOA, MOU, or contract). The DoD CIO establishes agreements with federal departments and agencies, consistent with DoDI 8010.01 and guidance in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47.

H.2. NFG

The NFG (aka Mission Partner Gateway (MPG) for JIE) provides a secure, robust, and scalable means for non-DoD Federal Agencies, Mission Partners, and contractor connections to connect to the Unclassified but Sensitive IP Router Network (NIPRNet). In addition to the requirements listed in this Appendix, DoD Sponsors and Mission Partners must complete a NIPRNet Federated Gateway Policy Spreadsheet and Questionnaire. The NFG Spreadsheet and Questionnaire provides baseline data for NFG engineering team to work with Mission Partner while the NFG Policy Spreadsheet identifies the firewall posture of the NFG that will support the Mission Partner. The customer must notify the NIPRNet NFG Office of the PPSM Tracking Identifier, in addition to the above referenced documentation. The NIPRNet NFG Office works with the DISA Web Content Filtering team provide the applicable firewall rulesets to the DISA Command Center. The DISA Command Center issues a DISA Task Order (DTO) containing the firewall ruleset. The DISA Global Operations Center (DGOC) implements the firewall rule set IAW the DTO (See Figure 23 and Figure 24). The customer must identify PPSMs so DISA can configure the firewall rules to allow the enclave to use the corresponding services. The NFG supports both logical and physical connections. Figure 23 illustrates the NFG Connection Process, Use the zoom feature to improve legibility.

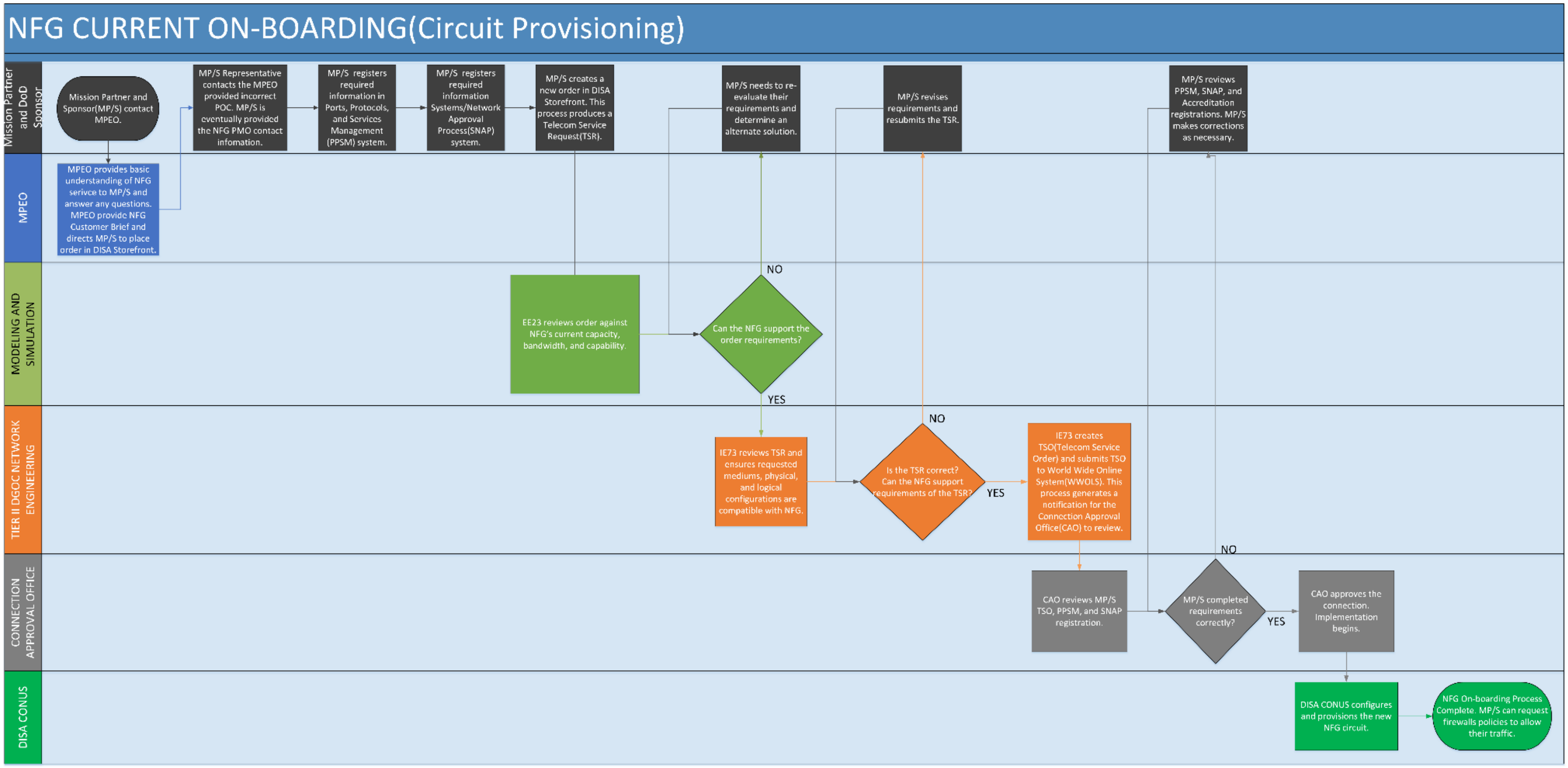

NFG CURRENT ON-BOARDING(Circuit Provisioning)
Mission Partner and DoD Sponsor
MPEO
MODELING AND SIMULATION
TIER II DGOC NETWORK ENGINEERING
CONNECTION APPROVAL OFFICE
DISA CONUS
Mission Partner and Sponsor(MP/S) contact MPEO.
MPEO provides basic understanding of NFG serivce to MP/S and answer any questions. MPEO provide NFG Customer Brief and directs MP/S to place order in DISA Storefront.
MP/S Representative contacts the MPEO provided incorrect POC. MP/S is eventually provided the NFG PMO contact infomation.
MP/S registers required information in Ports, Protocols, and Services Management (PPSM) system.
MP/S registers required information Systems/Network Approval Process(SNAP) system.
MP/S creates a new order in DISA Storefront. This process produces a Telecom Service Request(TSR).
EE23 reviews order against NFG's current capacity, bandwidth, and capability.
Can the NFG support the order requirements?
NO
MP/S needs to re-evaluate their requirements and determine an alternate solution.
YES
IE73 reviews TSR and ensures requested mediums, physical, and logical configurations are compatible with NFG.
Is the TSR correct? Can the NFG support requirements of the TSR?
NO
MP/S revises requirements and resubmits the TSR.
YES
IE73 creates TSO(Telecom Service Order) and submits TSO to World Wide Online System(WWOLS). This process generates a notification for the Connection Approval Office(CAO) to review.
CAO reviews MP/S TSO, PPSM, and SNAP registration.
MP/S completed requirements correctly?
NO
MP/S reviews PPSM, SNAP, and Accreditation registrations. MP/S makes corrections as necessary.
YES
CAO approves the connection. Implementation begins.
DISA CONUS configures and provisions the new NFG circuit.
NFG On-boarding Process Complete. MP/S can request firewalls policies to allow their traffic.

Figure 23 The NFG Connection Process

H.2.1. NFG Logical Connections

DISA may extend existing Mission Partner connections to NIPRNet to the NFG point of presence without installing new physical circuits. DISA accomplishes this by provisioning logical tunnels over the DISN. These tunnels extend existing Mission Partner connection(s) to the NFG, and the traffic will flow to the NFG via the logical connection. Encryption is also available for logical connections if required by the Mission Partner. Mission Partners are required to maintain a direct physical connection to a DISN node to be eligible for a logical connection. DoD policy prohibits logical connections to DISN via DoD Component sponsor enclave (backside connections). Logical connection use cases are as follows:

1. A commercial circuit extends from the customer to the DISN node. At the DISN router, the customer logically connects to the NFG via the MPGW/NFG Community of Interest (MPG/NFG COI) Level-3 VPN service (VPN ID DKL300249).
2. Mission Partners currently having a direct connection to a NIPRNet router for NIPRNet access will be re-routed to NIPRNet via the MPG/NFG COI VPN service.

H.2.2. NFG Physical Connections

Physical connections terminate on the NFG using up to OC-12 SONET 1 Giga Byte (Gb) and 10 Gb Ethernet (copper or fiber) connections. A non-DoD organization such as a Federal Department/Agency, DoD contractor, or other Mission Partners may connect to the NFG router via third-party leased circuit or DISN transport in consonance with a formal agreement (e.g., contract, MOU, MOA, etc.). In cases where the Mission Partner equipment is collocated with an NFG site, the Mission Partner Customer Edge router can connect to the NFG using a direct cable connection without a leased circuit and/or DISN transport.

Physical connection use cases are as follows:

1. A commercial carrier extends a circuit from the Mission Partner service point to the NFG site.
2. A commercial carrier extends a circuit from the Mission Partner service point to DISN physical transport for a dedicated circuit to an NFG site.
3. A Mission Partner plugs directly into DISN transport for a dedicated circuit to an NFG site.

H.2.3. NFG Connection Approval Requirements

NFG connections whether logical or physical require a modified Connection Approval Process package as illustrated below. NFG connections will be annotated in SNAP database as “NIPR FED GW.” Qualified NFG connections will receive an ATC and be reviewed IAW the established agreement (e.g., MOA/MOU/SLA). Section 2.8.3 of this guide lists the attachments, documents, and artifacts required for a Non-DoD U.S. Government unclassified enclave or network connection to the NFG.

H.2.4. Ordering NFG Connections

The customer orders NFG connections via the DSF:

1. Mission Partners must collaborate with their DoD Component sponsoring organization to order a connection to the NFG. The DoD Component sponsor will use DSF to generate a TSR for connection to the NFG. Refer to the DSF website for information on the connection ordering process.
   a. For logical connections, the VPN Identification (ID) number for the NFG Community of Interest (COI) service is DKL300249
   b. DSF assigns the VPN ID to all Mission Partners requesting NFG COI Service
2. The TSR initiates the process in DISA for identifying Mission Partner requirements and provisioning the new NFG connection paths based on the approved engineering design and connection approval package.
3. To revise approved connections, Mission Partners must update the approved connection approval package or submit a new package based on the approved engineering solutions.
4. Mission Partners must obtain and complete the NIPRNet Federated Gateway Policy Spreadsheet and Questionnaire. The applicable PPSM must be identified so the corresponding services may be made available. This may require the Mission Partner/sponsor to submit firewall rule requests to support the customer's requirements as illustrated in Figure 24.

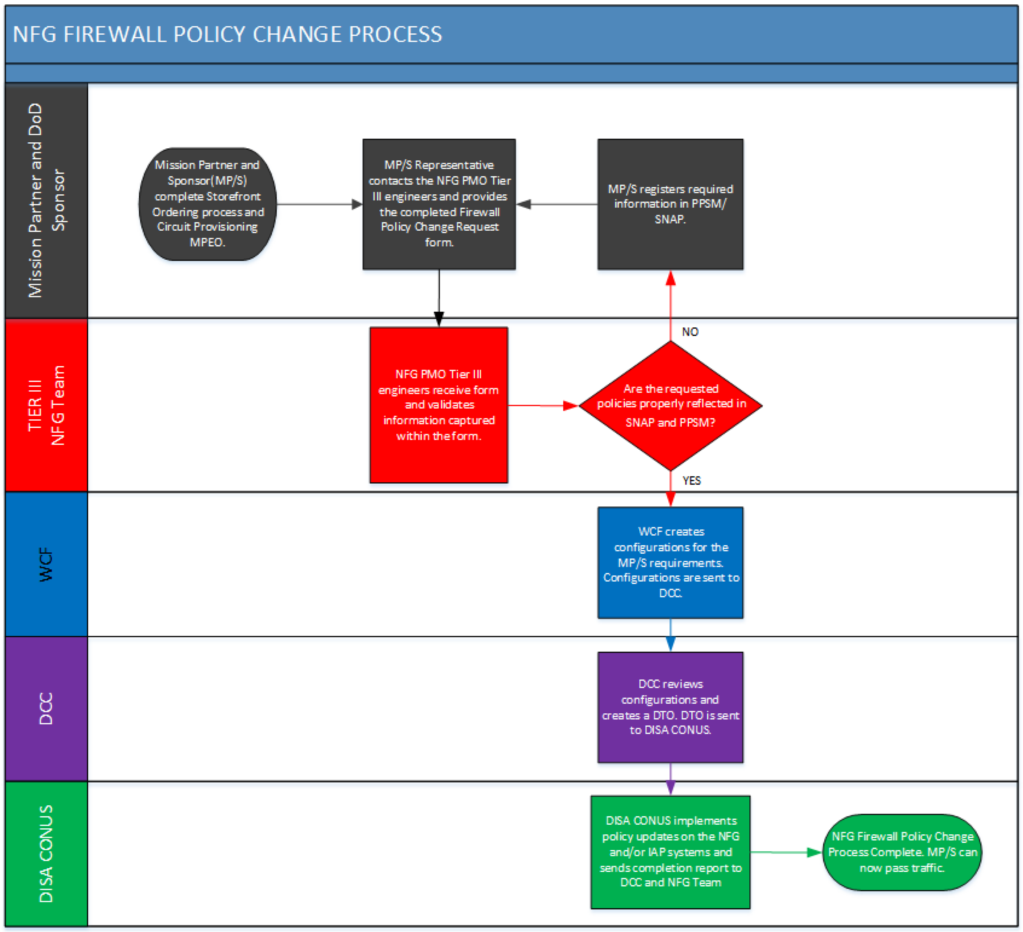

NFG FIREWALL POLICY CHANGE PROCESS
Mission Partner and DoD Sponsor
TIER III NFG Team
WCF
DCC
DISA CONUS
Mission Partner and Sponsor(MP/S) complete Storefront Ordering process and Circuit Provisioning MPEO.
MP/S Representative contacts the NFG PMO Tier III engineers and provides the completed Firewall Policy Change Request form.
MP/S registers required information in PPSM/ SNAP.
NFG PMO Tier III engineers receive form and validates information captured within the form.
Are the requested policies properly reflected in SNAP and PPSM?
NO
YES
WCF creates configurations for the MP/S requirements. Configurations are sent to DCC.
DCC reviews configurations and creates a DTO. DTO is sent to DISA CONUS.
DISA CONUS implements policy updates on the NFG and/or IAP systems and sends completion report to DCC and NFG Team
NFG Firewall Policy Change Process Complete. MP/S can now pass traffic.

Figure 24 NFG Firewall Policy Change Process

H.3. Mission Partner SIPRNet FED DMZ Connections

Figure 25 illustrates the Mission Partner SIPRNet FED DMZ connection process. DoD CIO must approve a DoD Component sponsor's request to connect a Mission Partner to the DISN as described in Appendix B. Mission Partner connections to SIPRNet are through either the SIPRNet FED-DMZ, or the SIPR REL DMZ. In rare cases, the DoD CIO may approve Mission Partner direct SIPRNet connection. Applicable Mission Partner connections must adhere to DoDI 8110.01 applicable A&A standards (See Section 2.6 of this guide) and CJCSI 6290.01, *Requirements Management Process for Mission Partner Environment* as part of the MPE and Joining, Membership, and Exiting Instructions (JMEI) policy requirements. Like Mission Partner NFG connections, Mission Partner SIPRNet FED DMZ and SIPRNet REL DMZ connections can be either physical or logical. Physical connections are directly homed to the SIPRNet FED DMZ (e.g., point-to-point connections between the DMZ and a Mission Partner's network). Logical connections are physically homed to a SIPRNet router and connected to the SIPRNet FED DMZ / SIPRNet REL DMZ via an encapsulated tunnel. SIPRNet FED DMZ and SIPRNet REL DMZ connections require a modified Connection Approval Process package as illustrated below. Qualified SIPRNet FED DMZ and SIPRNet REL DMZ connections will receive an ATC and be reviewed IAW the established agreement (e.g., Inter Agency Agreement/MOA/MOU/Service Level Agreement). Section 2.8.3 of this guide lists the network connection to the SIPRNet FED DMZ and SIPRNet REL DMZ.

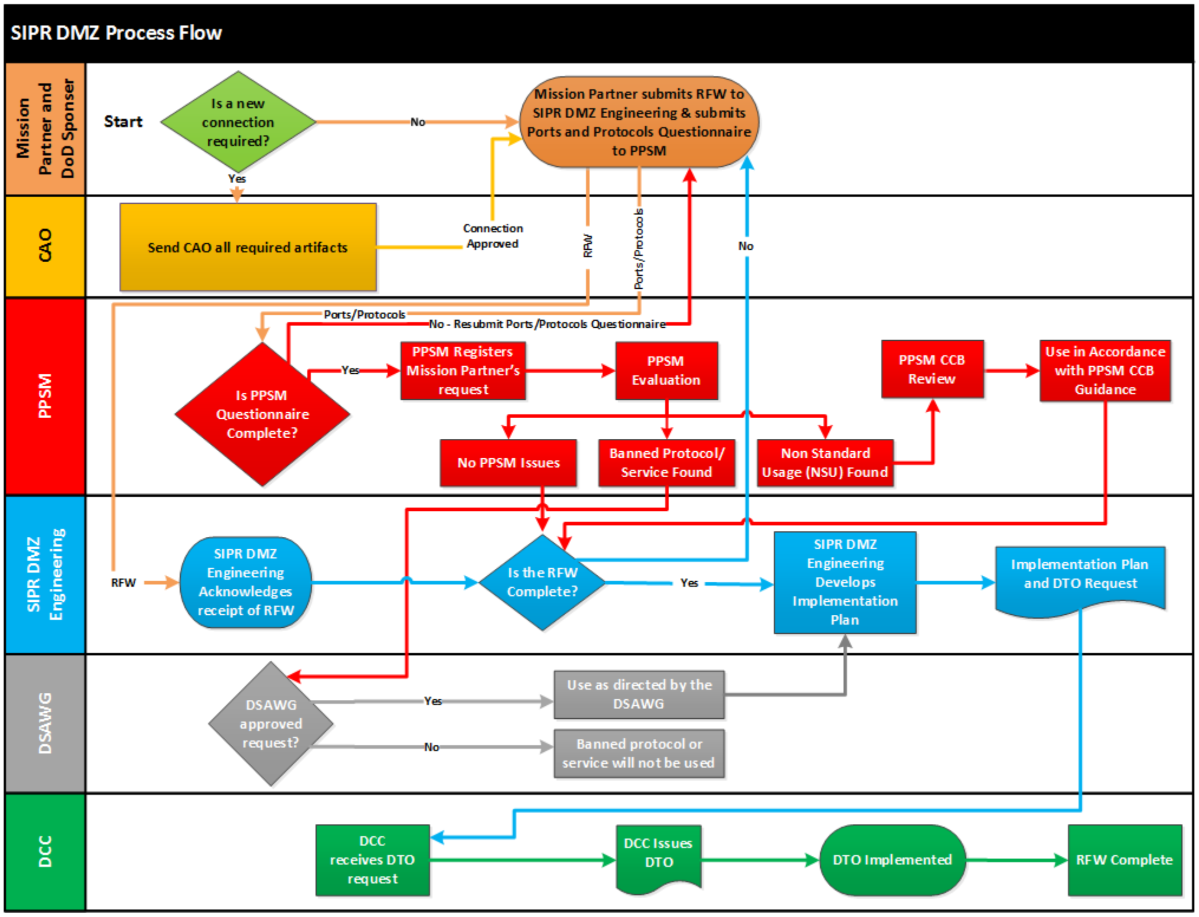

SIPR DMZ Process Flow
Mission Partner and DoD Sponsor
CAO
PPSM
SIPR DMZ Engineering
DSAWG
DCC
Start
Is a new connection required?
No
Yes
Mission Partner submits RFW to SIPR DMZ Engineering & submits Ports and Protocols Questionnaire to PPSM
Send CAO all required artifacts
Connection Approved
RFW
Ports/Protocols
No
Ports/Protocols
No - Resubmit Ports/Protocols Questionnaire
Is PPSM Questionnaire Complete?
Yes
PPSM Registers Mission Partner's request
PPSM Evaluation
PPSM CCB Review
Use in Accordance with PPSM CCB Guidance
No PPSM Issues
Banned Protocol/ Service Found
Non Standard Usage (NSU) Found
RFW
SIPR DMZ Engineering Acknowledges receipt of RFW
Is the RFW Complete?
Yes
SIPR DMZ Engineering Develops Implementation Plan
Implementation Plan and DTO Request
DSAWG approved request?
Yes
No
Use as directed by the DSAWG
Banned protocol or service will not be used
DCC receives DTO request
DCC Issues DTO
DTO Implemented
RFW Complete

Figure 25 The SIPRNet FED DMZ Connection Process

Appendix I Consent to Monitor Agreement (Sample)

++++++++++++++++++++++++ SAMPLE BEGINS HERE ++++++++++++++++++++++

<Date>

SUBJECT: Consent to Monitor for <CCSD, VPN ID, VRF Identifier, Cloud Service Offering name, or Cloud IT Project Name>

1. IAW the requirements of Chairman Joint Chief of Staff Instruction (CJCSI) 6211.02D, Defense Information System Network (DISN) Responsibilities, 24 January 2012, and Unclassified Connection Approval Office Requirements, I acknowledge that the Defense Information Systems Agency will conduct periodic monitoring of the NIPRNet/IP Core/DATMS-U circuits. I acknowledge and consent to DISA conducting initial and periodic unannounced vulnerability assessments on our connected host system to determine the security features in place to protect against unauthorized access or attack.

____

Authorizing Official

+++++++++++++++++++++++++++ SAMPLE ENDS HERE +++++++++++++++++++++++++++

The DISN customer must submit a signed CTM signed by the Authorizing Official to Defense Information Systems Agency via SNAP or SGS to obtain approval to connect to DISN. The CTM may be included within the ADD.

- Copy and paste the sample text above either into the ADD or onto Organization Letterhead.
- Be sure to provide the CCSD, VPN ID, Cloud Service Offering, or C-ITP names as appropriate.
- When complete, upload the CTM statement into the SNAP registration package.

Direct questions about the CTM to the DISN Connection Approval Office.

This page intentionally left blank.

Appendix J Remote Compliance Monitoring

J.1. Vulnerability Scanning

The DISN Connection Approval Office (CAO) is the point of contact for requesting remote compliance scans. There are three types of scan requests:

- IATT scan required for new SIPRNet connection
- Ad Hoc requested by a customer

J.2. Scan Types

J.2.1. Perimeter Defense Test Scans

These scans test the connection's perimeter defenses to assess the perimeter security device's ability to deny intrusion from an unknown source IP

- Performed from a scanning server which uses an unknown IP, to ascertain the defense in depth stance by simulating a probe from an unknown attacker
- The network enclave passes when the scan does not identify any devices within the internal network. Should any devices be identifiable within the internal network, it will be considered a failure of the perimeter defense test
- DISA will forward results to POCs listed in SNAP/SGS or to stakeholder requesters in the event of a failed penetration test.

J.2.2. Vulnerability Compliance Scans

These scans are coordinated with the CCSD enclave owner to allow a known or "trusted" IP address to scan for vulnerabilities

- The POC(s) listed in SNAP/SGS will coordinate with the Scan Team to establish the Access Control Lists on the network security devices to allow the IP Address to access the designated CCSD enclave. A pass rating is attained when no RMF critical/very high/high vulnerabilities are found IAW current DoD STIGs and ACAS\NESSUS vulnerability assessment
- Inspectors assign a "failed" rating when finding RMF critical/very high/high vulnerabilities or the vulnerability compliance scan cannot access the connection. Inspectors will upload results into SNAP/SGS and send them to the POCs listed in SNAP/SGS or stake holder requesters for review and mitigation

J.3. Types of Scan Requests

J.3.1. IATT Scans

DISA RE41 initiates these scans for all new SIPRNet enclave connection requests. The scan begins after the 72- hour burn in or when subsequently requested by the enclave owner. IATT scans are required to complete the Connection Approval Process:

- IATT scans are announced vulnerability compliance scan assessments
- IATT Scans are a requirement for an ATC to SIPRNet

- IATT scans are conducted the same as a Vulnerability Compliance Scan
- DISA RE4 or DISA SE711 provides a report of results from the vulnerability scan to the SGS POCs on the details of all scan results, and therefore it is crucial for AOs' and enclave owners to keep POC information in the SGS registration(s) current under their area of responsibility.
- 8 lists prerequisites for an initial SIPRNet IATT scan.

	Steps To be Completed PRIOR to an Initial SIPRNet Scan for ATC Issuance:
1	Equipment installed, configured, and turned on.
2	72-hour burn-in completed by the DISA Implementation Testing and Activation team.
3	At least one (1) server, workstation, or laptop with at least one (1) port, protocol, or service enabled. (Please refer to PPSM Registry for allowed ports and protocols or contact DoD PPSM Team (DISA/RE4)).
4	For the initial scan or CMT "Vulnerability Compliance Scan" the IP Address needs to be added to the Host Based Security System (HBSS), firewall(s); IDS/IPS, Access Control Lists.

Table 5 Initial SIPRNet Scan Prerequisites

J.4. Follow-up after a Failed Scan

Following a failed scan do the following:

- For a failed perimeter defense scan, the enclave owner reviews and locks down the boundary protection systems as much as possible
- For a failed vulnerability compliance scan, review the RMF critical/very high/high vulnerability findings and fix/mitigate them
- The enclave owner contacts the Compliance Monitoring Team to schedule a re-scan after resolving issues

This page intentionally left blank.

Appendix K VPN Registration (Private IP)

This Appendix supplements information provided in Section 2 of this guide with additional information on DISN VPN connection requirements.

DISN VPN services provide an enterprise-wide solution to all DISN customers who need to segment their IP traffic from that of other customers. NIPRNet offers these capabilities as transport-only services using Multi-Protocol Label Switching (MPLS) to create VPNs. As such, the connection process differs slightly from that usually required for connection to NIPRNet/SIPRNet. For VPN services, the VPN owner is required to register each VPN in the SNAP/SGS systems as described in Section 2.8 of this guide. The VPN owner is responsible for ensuring that the appropriate Cybersecurity services, capabilities, and measures are in place on the system/network associated with the VPN.

DISN capabilities can be used to isolate Communities of Interest (COIs) as separate enclaves and segregate test traffic from the operational network using MPLS, VPN tunnels, approved Type I encryption devices, and/or other approved solutions as needed.

For example, the DISN Test and Evaluation Service is hosted as a Layer 3 VPN (L3VPN) across the DISN IP core, providing IP transport-only service for test and evaluation (T&E) and test and development (T&D) COIs.

U.S. Cyber Command (USCYBERCOM) distributed TASKORD 12-0371 instructing DoD Components to transition all Unrestricted and Restricted public facing applications into a DMZ Extension. The NIPRNet Internet Access Point (IAP)-DMZ-VPN Community of Interest Network (COIN) improves security posture to protect DoD assets by isolating public facing Internet applications traffic flows from the NIPRNet flows.

DoD Component network administrators who are responsible for providing the routing policy on the customer premise routers can use the Internet Access Point Demilitarized Zone Virtual Private Network Community of Interest Customer User's Guide. The guide supplements the VPN User Guides and Tutorials and provides additional information to assist customers in ordering the IAP-DMZ-VPN service via DSF and ensuring the DMZ extensions are compliant with the DoD Internet-NIPRNet DMZ Security Technical Implementation Guide (STIG) requirements. For assistance with VPN services, contact the NIPRNet/VPN Service Manager or the DISA IGSD.

The process for ordering and registering a VPN connection begins at Section 2.4 of this guide. The DSF website has VPN Tutorials with instructions on how to establish a new VPN and for connection to an existing VPN. However, fewer documents are required when a VPN Owner registers a new VPN in SNAP/SGS and when a VPN Member registers a VPN connection in SNAP/SGS. The required documents are described in Section 2.8.3.3 of this guide. The DISN CAO issues a Permission to Connect (PTC) for Level 3 VPNs.

This page intentionally left blank.

Appendix L Points of Contact

DISA is in the process of reorganizing the “disa.mil” web presence. DISA web pages listed in this Appendix may move to other locations such as “storefront.disa.mil” or “cyber.mil.” DISN CAO will post an Addendum to this Appendix on the Miscellaneous references web page.

Note some web pages posted to “storefront.disa.mil” may take a minute or so to fully display.

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
Cloud Migration Office: Defense Logistics Agency, DISA Liaison and Hosting Office Supporting Defense Logistics Agency (DLA)		EnterpriseHosting@dla.mil		✓
Cloud Migration Office: Department of the Air Force, Cloud Computing Environment (CCE) Cloud Transition Team (formerly MSO)			(CAC login required): https://info.cloudone.af.mil/	✓
Cloud Migration Office: Department of the Army, Army Application Migration Business Office (AAMBO)		usarmy.belvoir.peo-eis.mbx.army-app-migration-office@mail.mil (Emails to this address automatically creates Remedy ticket – intended for Army application owners migrating to approved hosting environment or seeking general info about ECOCS functions)	https://ecosc.army.mil https://asc.army.mil/web/news-a-map-to-migration/ https://disa.deps.mil/ext/CloudServicesSupport/Lists/Announcements/Attachments/11/CloudStrategy_Army.pdf https://army.deps.mil/army/cmds/hqda_ciog6_Project/ADCCP/CloudDocRepository/Documents/1604194822%20Signed%20SECARMY%20Army%20Directive%202016-38.pdf https://disa.deps.mil/ext/CloudServicesSupport/CCPG/AAMBO%20Introduction%20(AUGUST2015).pdf	✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
Department of the Navy Cloud Management Organization: (PMW270)	619-524-2021	CSMOSupport.fct@us.navy.mil	https://digital.navy.mil/cloudsmo (Chrome works best)	✓
Cloud Migration Office: USMC HQMC C4	703-693-3488	HQMC_C4_MCCLOUD@usmc.mil		✓
Cloud: DISA Cloud Authorization Services (DCAS) Team		disa.meade.re.mbx.cloud-team@mail.mil	(CAC required) https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/SitePages/CASHome.aspx	✓
Cloud: DISA Stratus	Stratus Service Desk 301-225-7878	disa.cst@mail.mil DISA-CloudUserGroup@groups.mail.mil If an incident occurs, hosted programs should report occurrences to Columbus Net Assurance (COLS-NA) at: disa.columbus.eis.mbx.cols-esdna@mail.mil or 614-692-5600	https://stratus.mil/ DISA Hosting and Compute Center DISA HaCC https://www.hacc.mil (CAC required. Works best with Chrome or Firefox web browsers.) User Group Briefing Link available upon request to disa.cst@mail.mil	✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
Cloud: DISA Mission Partner Engagement Office (MPEO)	Global Service Desk (GSD) 844-DISA-HLP 844-347-2457	**DoD, OSD, Federal Agency, USCG, IC:** disa.cst@mail.mil **CCMD, Joint Staff, MILDEPs:** **International Relations and Engagements:** **General Mission Partner Support:** disa.cst@mail.mil disa.mpeo@mail.mil	https://services.disa.mil/csm	✓
Cloud: DISA Secure Cloud Computing Architecture (SCCA) PMO		disa.meade.re.mbx.cloud-team@mail.mil disa.meade.id.list.cap-pmo@mail.mil	**SCCA Mission Partner Portal:** https://disa.deps.mil/ORG/SD/SD8/SCCA/MissionPartners/SitePages/Secure%20Cloud%20Computing%20Architecture.aspx **SCCA Knowledge Center:** https://disa.deps.mil/ORG/SD/SD8/SCCA/MissionPartners/SitePages/SCCA%20Knowledge%20Center.aspx	✓
Cloud: Office of the Secretary of Defense/Joint Staff National Capital Region, Joint Service Provider (JSP) Pentagon Service Desk (For C-ITPs using the JSP-AWS Gov Cloud)	703-571-4577	Unclassified Email: osd.pentagon.jsp.mbx.jsp-service-desk@mail.mil	https://jsp.sp.pentagon.mil/Pages/Home.aspx	✓
Compliance Monitoring Team (CMT)	301-225-2902 DSN 312-375-2902	Unclassified email: disa.meade.re.mbx.caoscans@mail.mil Classified email: disa.meade.ns.mbx.caoscans@mail.smil.mil		✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
Defense Counterintelligence and Security Agency (formerly DSS)	888-282-7682	Unclassified email: dss.quantico.dss-hq.mbx.disn@mail.mil	www.dcsa.mil or, https://www.dcsa.mil/mc/isd/locations/ (To obtain contact information for the appropriate DCSA Field Office)	✓
DISA Assessment and Authorization Division (RE5)			NIPRNET: https://disa.deps.mil/org/RE5/default.aspx https://dod365.sharepoint-mil.us/sites/DISA-Assessment-And-Authorization-External/	✓
DISA Cross Domain Enterprise Services		disa.meade.id.list.cdes-aa@mail.mil	**NIPRNet:** https://public.cyber.mil/cdes/ or, https://cyber.mil/cdes/ **SIPRNet:** http://intelshare.intelink.sgov.gov/sites/cdes/	✓
DISA Cloud Assessment Division (RE2)		DISA (RE2) Cloud Team disa.meade.re.mbx.cloud-team@mail.mil DISA (RE2) eMASS Team disa.meade.re.mbx.disa-cloud-emass-team@mail.mil	https://dod365.sharepoint-mil.us/sites/DISA-Cloud-Assessment/?e=1%3A5c6e141cfdd24b249949fef06d52a40	✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
DISA Joint Operations Center Cyber Security Service Provider (CSSP)	Comm 301-225-3505 DSN 312-375-3505	NIPR disa.meade.ops.mbx.dcc-bc@mail.mil SIPR disa.meade.ops.mbx.dcc-bc@mail.smil.mil	https://disa.deps.mil/ext/cop/cdsp/	✓
DISA Global Operations Center (DGOC)	618-418-8626		https://www.disa.mil/DGOC/GNSC	✓
DISA Implementation Testing and Request Fulfillment Activations team	618-418-8627			✓
DISA Infrastructure Global Service Desk (IGSD) (24x7) (Formerly DCCC)	844-347-2457, Option 2 or, 614-692-0032, DSN 850-0032 Option 2	Unclassified Email disa.global.servicedesk.mbx.infrastructure-ticket-request@mail.mil Classified Email: Disa.global.servicedesk.mbx.infrastructure-ticket-request@mail.smil.mil		✓
DISA Provisioning Customer Support	614-692-1428			✓
DISA Unified Capabilities Approved Products Certification Office		disa.meade.ie.list.approved-products-certification-office@mail.mil		✓
DISA Web Content Filtering Office		disa.meade.ma.list.wcftieriii@mail.mil		✓
DISA's Risk Adjudication and Connection Approval Division's Mission Partner Training Program (MPTP)	301-225-4330 DSN 312-375-4330	disa.meade.re.mbx.mptp@mail.mil	https://cyber.mil/connect/mptp/ https://public.cyber.mil/connect/mptp/	✓
DISN Billing Support Representatives		disa.letterkenny.eis.list.ocf4-team-leads@mail.mil		✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
DISN CAO	301-225-2900/2901 or DSN 312-375-2900/2901	Unclassified Email: disa.meade.re.mbx.ucao@mail.mil disa.meade.re.mbx.cloud-it-project@mail.mil disa.meade.re.mbx.ucao-vpn@mail.mil Classified Email: disa.meade.ns.mbx.ucao@mail.smil.mil	https://cyber.mil/connect/connection-approval/	✓
DISN CAO for Classified Connections	301-225-2900/2901 or DSN 312-375-2900/2901	Unclassified Email: disa.meade.re.mbx.ccao@mail.mil Classified Email: disa.meade.ns.mbx.ccao@mail.smil.mil		✓
DISN CAO for DSN Connections	301-225-2900, 301-225-2901 DSN 312-375-2900, 312-375-2901	Unclassified Email: disa.meade.re.mbx.cao-dsn@mail.mil		✓
DoD CIO OPR		osd.pentagon.dod-cio.mbx.dcio-cs-ae@mail.mil		✓
DoD Component Chief Information Security Officer (CISO) – Contact List			Log into SNAP using your CAC card at: https://snap.dod.mil/ Hover your cursor over “Policy,” then Select: “Reference Documents” > “Waiver” >”Temporary Exception to Policy (TEP) SRO Contacts”>”Download” (OPEN the PDF that downloads to your desktop) (Note: Organizations that do not have an SRO listed must have the request validated by their DoD Component CIO or senior IT official.)	✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
DoD Cross Domain Support Element (CDSE) Points of Contact List		If your CDSE POC is not listed contact DISA RE42 at: 301-225-2903 DSN 312-375-2903 Unclassified email: disa.meade.re.mbx.cdtab@mail.mil Classified email: disa.meade.ns.mbx.cdtab@mail.smil.mil	**NIPRNet:** https://intellipedia.intelink.gov/wiki/IA32_Cross_Domain_Solutions#Cross_Domain_Support_Element_POCs **SIPRNet:** https://intelshare.intelink.sgov.gov/sites/ncdsmo/_layouts/15/start.aspx#/Lists/CDSE%20Contact%20List/Allitems.aspx https://intelshare.intelink.sgov.gov/sites/ucdsmo/Lists/CDSE%20Contact%20List/Allitems.aspx	✓
DoD Information Technology Portfolio Repository (DITPR) POC		osd.mc-alex.dod-cio.mbx.ditpr-support-team@mail.mil	https://ds-itsmweb.dc3n.navy.mil/kinetic/DisplayPage?name=DITPR_Request	✓
DoD PPSM Team (DISA/RE41)	301-225-2904	NIPRNet: disa.meade.re.mbx.dod-ppsm@mail.mil dod.ppsm@mail.mil SIPRNet: disa.meade.ns.mbx.ppsm@mail.smil.mil	**NIPRNet:** https://dod365.sharepoint-mil.us/Sites/DISA-Ports-Protocols-Services-Management https://intelshare.intelink.gov/sites/ppsm/ **SIPRNet:** https://intelshare.intelink.sgov.gov/sites/dod-ppsm/ https://intelshare.intelink.sgov.gov/sites/dod-ppsm/SitePages/Home.aspx	✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
DSAWG Secretariat (DISA Risk Adjudication)	**CDTAB Support:** 301-225- 2903 DSN 312-375-2903 **DSAWG Support:** 301-225- 2905 DSN 312-375-2905	**CDTAB Support/DISA Risk Adjudication:** Unclassified email: disa.meade.re.mbx.cdtab@mail.mil Classified email: disa.meade.ns.mbx.cdtab@mail.smil.mil **DSAWG Support:** Unclassified email: disa.meade.re.mbx.dsawg@mail.mil Classified email: disa.meade.ns.mbx.dsawg@mail.smil.mil	**CDTAB Support/DISA Risk Adjudication:** **NIPRNet:** https://intelshare.intelink.gov/sites/cdtab **SIPRNet:** https://intelshare.intelink.sgov.gov/sites/cdtab/SitePages/Home.aspx **DSAWG Support:** **NIPRNet**: https://cyber.mil/connect/dsawg/ https://cyber.mil/connect/faq-dsawg https://intelshare.intelink.gov/sites/dsawg/default.aspx **SIPRNet:** https://intelshare.intelink.sgov.gov/sites/dsawg	✓
Global Information Grid (GIG) Service Management Operations (GSM-O) Customer Advocacy Group	618-418-9922			✓
Information Security Risk Management Committee (ISRMC)			https://intellipedia.intelink.sgov.gov/wiki/Information_Security_Risk_Management_Committee	✓
Joint Interoperability Test Center (JITC)			https://storefront.disa.mil/kinetic/disa/service-catalog#/category/testing	✓
JRSS PMO		Disa.meade.id.mbx.jrss-jmt-gov-leads@mail.mil	https://disa.deps.mil/ext/cop/mae/cop_mae/JRSS/SitePages/Home.aspx	✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
Mission Partner Engagement Office (MPEO)		disa.meade.bd.mbx.bdm4-mpeo-support@mail.mil	https://disa.deps.mil/ext/cop/mpp/index.aspx https://services.disa.mil/csm	✓
National Cross Domain Strategy and Management Office (NCDSMO)	240-373-0796	NIPRNet: ncdsmo@nsa.gov SIPRNet: ncdsmo@nsa.smil.mil	**NIPRNet:** https://intelshare.intelink.gov/sites/ncdsmo **SIPRNet:** https://intelshare.intelink.sgov.gov/sites/ncdsmo	✓
Network Information Center (NIC)	Phone: 844-347-2457, Option 2; 614-692-0032, Option 2; DSN: 312-850-0032, Option 2	For unclassified connections contact the NIC through the DISA IGSD at: disa.global.servicedesk.mbx.infrastructure-ticket-request@mail.mil	https://www.nic.mil	✓
NIPRNet NFG Office		disa.meade.id.list.nfg-pmo@mail.mil	https://dod365.sharepoint-mil.us/sites/disa-id5/ID52/NFG/SitePages/Home.aspx	✓
NIPRNet/VPN Service Manager	301-225-2388 DSN 375-2388	karen.l.neal11.ctr@mail.mil		✓
PPSM Configuration Control Board (CCB) or Technical Advisory Group (TAG) DoD Component Contact List			https://dl.cyber.mil/ppsm/pdf/contacts_list_poc_current.pdf (In the left-hand margin select: “DoD Component Contact List”)	✓
SIPRNet Information Technology Registry (SITR) POC		Unclassified Email: osd.mc-alex.dod-cio.mbx.ditpr-support-team@mail.mil (Include 'SIPR IT Registry' in the subject line)		✓

POINTS OF CONTACT	PHONE	EMAIL	WEBSITES	Verified
SIPRNet REL-DMZ SIPRNet FED DMZ Office		Unclassified email: disa.meade.id.list.sipr-dmz-eng-team@mail.mil Classified email: disa.meade.id.list.sipr-dmz-eng-team@mail.smil.mil		✓
SIPRNet Service Manager	301-225-4998 DSN: 375-4998	Unclassified email: disa.meade.ie.mbx.siprnet-pmo-ie1@mail.mil		✓
SIPRNet Support Center (SSC) Website	844-347-2457 Option 1-Option 5		NIPRNet: https://services.disa.mil/sp	✓
TDM Technical Interchange Meetings		disa.werx@mail.mil	https://www.disa.mil/en/About/DISAWERX/TEM	✓

Appendix M Validation Letter for Mission Partner Connections to DISN

DoDD 8000.1 defines a "Mission Partner" as - "Those with whom DoD 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." DoDI 8010.01 paragraph 2.1.g states that DoD CIO reviews and approves DoD Component [sponsor] requests for mission partner connections to the DISN.

The DoD Component sponsor must submit a Validation Letter for Mission Partner Connections to DISN and a DoD Mission Partner Connection Briefing to request a new Mission Partner connection to DISN. The DoD Component sponsor staffs the Validation Letter and briefing through the appropriate DISN Service Manager (NIPRNet/VPN Service Manager, or SIPRNet Service Manager) and the DoD Component CISO.[28] The DoD Component sponsor then emails the validation letter endorsed by the DoD Component CISO and DISA Service Manager to the DoD CIO OPR for final approval.

The DoD Component sponsor must submit a new validation letter for DoD CIO approval if any of the following significant changes occur:

- The date of the DoD CIO Approval letter is past the stated expiration date in the DoD CIO Approval memo or more than 3 years past the last DoD CIO approval
- A change in DoD Component sponsor
- New Contract Vendor
- Change of Location
- Change in Mission
- Change in topology that affects the cybersecurity posture/authorization of Mission Partner's enclave

This following is the only acceptable template for the Validation letter.

Click here for a link to templates for the Validation Letter for Mission Partner Connections to DISN and the DoD Mission Partner Connection Briefing

[28] Organizations that do not have a DoD Component CISO listed must have the request validated by their DoD Component CIO or senior IT official. (Click here for the link to the DoD Component CISO List)

****

Validation Letter for Mission Partner (Non-DoD) Connections to DISN (Template)

****

Package #________________
[Provided by DISA]

COCOM/Service/Agency/Field Activity Letterhead

From: DoD organization sponsor Date: DoD Sponsor Letter signed

Memorandum For: Defense Information Systems Agency (Attn: IE1, RE4)
{DoD Component CISO[29] *[example: Department of the Army, Chief Information Security Officer (Attn: Name]}*
DoD CIO

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

1. OPERATIONAL REQUIREMENT: (Must answer all sections/questionnaires)
   a. Operational need for connection:
      i. State the DoD mission, program, or project to be supported by this connection
      ii. Describe specifically how the connection will support the DoD sponsor organization and contractor or other Mission Partner entity mission tasks
   b. Classification/Type of work to be conducted by the contractor or other Mission Partner entity:
      i. Specify Classified or Unclassified and/or level, e.g. (Unclassified//for official use only (U//FOUO) – Secret and Top Secret.
      ii. 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 Mission Partner 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 e-mail/classified e-mail/phone number)
   c. Mission Partner's on-site Cybersecurity Individual responsible for this connection: (name/title/unclass e-mail/classified e-mail/phone number)

[29] The DoD Component Chief Information Security Officer (CISO) (Click here for the link to the DoD Component CISO List). Organizations that do not have a DoD Component CISO listed must have the request validated by their DoD Component CIO or senior IT official.

d. Cybersecurity Service Provider (CSSP):
e. DoD Sponsor Cybersecurity Representative for Combatant Command/Service/Agency/Field Activity (CC/S/A):
f. Mission Partner Entity/Contractor/Corporate name (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. Contractor Info: Contract Number, expiration date, contracting officer name, and phone number
j. DoD Contractor Security FSO:

3. CONNECTION DETAILS:
a. Connection location addresses (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:
f. The topology should annotate all devices and connections in the enclave to include routers, IA equipment (firewalls/IDS/etc.), servers/data storage devices/workstations/etc., all connections, to include enclave entry and exit connections, and security classification of environment

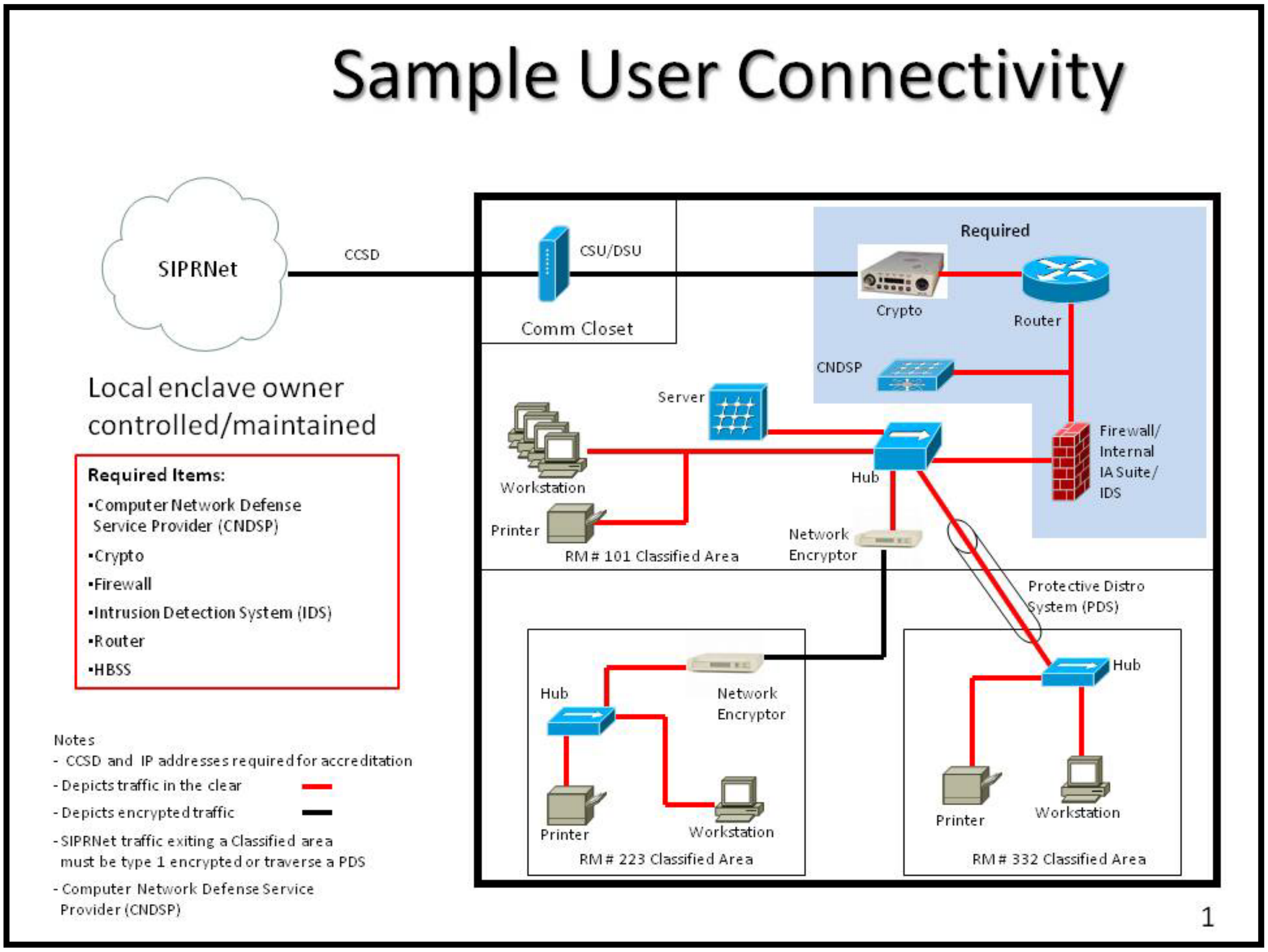
As the DoD Sponsor, I must ensure connectivity requirements are properly coordinated, periodic inspections are conducted, and adequate controls are in place in accordance with:

- DoDI 8010.01, Department Of Defense Information Network (DODIN) Transport, 10 September 2018
- DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*
- DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)* for connections between DoD and contractor information systems
- DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*
- DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations*
- CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities*, 24 January 2012
- DISN Connection Process Guide (https://public.cyber.mil/connect)
- DoD CIO Memorandum, Responsibilities of DoD Components Sponsoring Mission Partner Connections to DISN-Provided Transport Infrastructure, 14 August 2012

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

Attachments:

1. **{Sample of an IT Topology Diagram}**
   ILAP Domain Configuration @ ABCDEF Systems
2. **{Request for Mission Partner Connection Briefing}**



Sample User Connectivity

Local enclave owner controlled/maintained

Required Items:
- Computer Network Defense Service Provider (CNDSP)
- Crypto
- Firewall
- Intrusion Detection System (IDS)
- Router
- HBSS

Notes
- CCSD and IP addresses required for accreditation
- Depicts traffic in the clear 🟥
- Depicts encrypted traffic ⬛
- SIPRNet traffic exiting a Classified area must be type 1 encrypted or traverse a PDS
- Computer Network Defense Service Provider (CNDSP)

Attachment 1: Sample User IT Topology Diagram

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. Tunneling SIPRNET traffic through NIPRNET/Corporate network requires DSAWG review approval in accordance with CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities*, 24 January 2012.)

I reviewed/discussed this connection request with the DoD Component/

Mission Partner's sponsor - Concur or non-concur.

1st Endorser ______________________________ Date

SIGNATURE
DISN Validation Official[30]

I have reviewed the DoD Sponsor's request for [Mission Partner entity] to have a DISN connection. Recommend DoD CIO approve this connection.

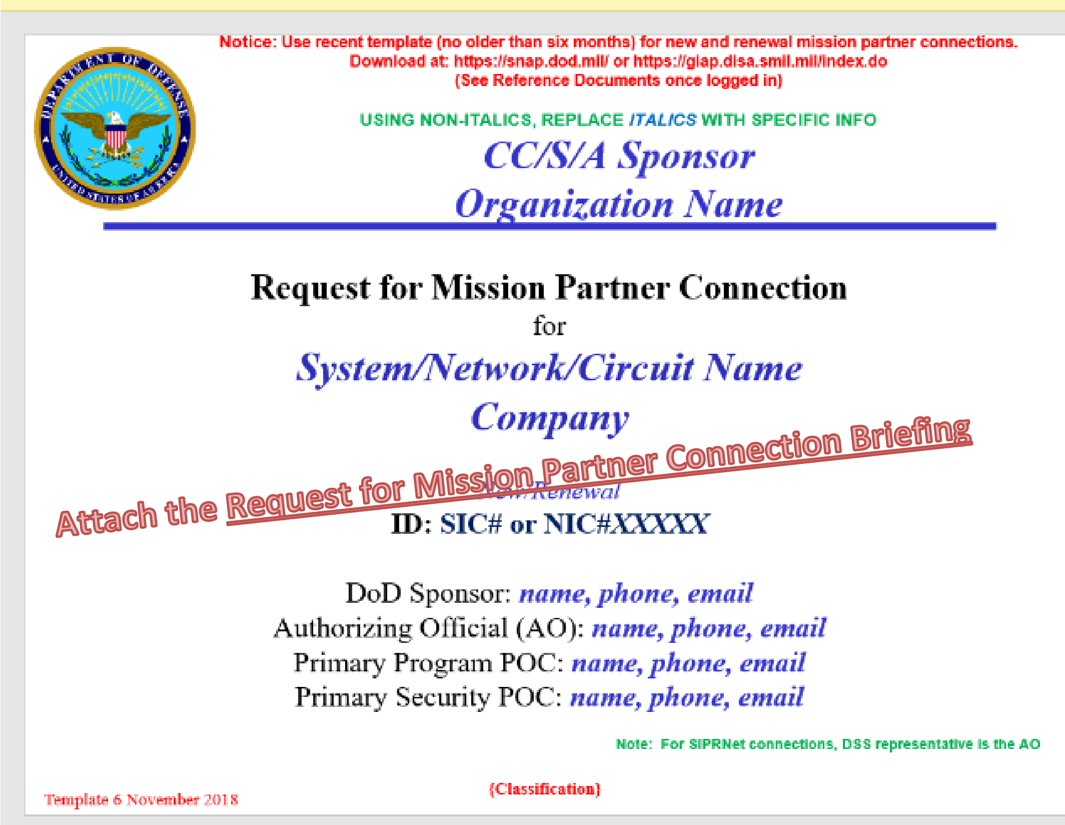
2nd Endorser ______________________________ Date

SIGNATURE

CC/S/A/FA Validation Official[31]

[30] The NIPRNet/VPN Service Manager or the SIPRNet Service Manager (as appropriate) is the "DISN Validation Official" and "1st Endorser."

[31] The DoD Component Chief Information Security Officer (CISO) or designated representative is the "CC/S/A/FA Validation Official" and "2nd Endorser" for this validation letter. (Click here for the link to the DoD Component CISO List). Organizations that do not have a DoD Component CISO representative listed must have the request validated by their DoD Component CIO or senior IT official.



Notice: Use recent template (no older than six months) for new and renewal mission partner connections.
Download at: https://snap.dod.mil/ or https://giap.disa.smil.mil/index.do
(See Reference Documents once logged in)

USING NON-ITALICS, REPLACE *ITALICS* WITH SPECIFIC INFO

CC/S/A Sponsor
Organization Name

Request for Mission Partner Connection
for
System/Network/Circuit Name
Company

Attach the Request for Mission Partner Connection Briefing

New/Renewal

ID: SIC# or NIC#*XXXXX*

DoD Sponsor: ***name, phone, email***
Authorizing Official (AO): ***name, phone, email***
Primary Program POC: ***name, phone, email***
Primary Security POC: ***name, phone, email***

Note: For SIPRNet connections, DSS representative is the AO

(Classification)

Template 6 November 2018

Attachment 2: Request for Mission Partner Connection Briefing

****

The Template for the Mission Partner Validation Letter ends here.

Appendix N References

DoDI 8170.01 Disclaimer - The appearance of hyperlinks does not constitute endorsement by the Defense Information Systems Agency of non-U.S. Government sites, or the information, products, or services contained therein. Although the Defense Information Systems Agency may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all the information that you may find at these locations. Such hyperlinks are provided consistent with the stated purpose of this guide.

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
10 United States Code (U.S.C), Section 2222.(i).(1).(A) (Defines – "Defense Business System")	http://uscode.house.gov/view.xhtml?req=(title:10%20section:2222%20edition:prelim)	✓
3PAO SAR briefing template	Contact the DCAS Team	✓
40 U.S.C., Section 11101 (6) (Definitions – "Information Technology")	https://www.govinfo.gov/content/pkg/USCODE-2011-title40/pdf/USCODE-2011-title40-subtitleIII-chap111-sec11101.pdf	✓
40 U.S.C., Section 1401 (3) (Definitions – "Information technology")	https://www.govinfo.gov/content/pkg/USCODE-1998-title40/pdf/USCODE-1998-title40-chap25-sec1401.pdf	✓
44 U.S.C., Section 3502, (8) (Definitions – "information system")	https://www.govinfo.gov/content/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapI-sec3502.pdf	✓
44 U.S.C., Section 3542 (b) (2) (Definitions – "national security system")	https://www.govinfo.gov/content/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf	✓
80 FR 51739, Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), August 26.2015	https://www.govinfo.gov/content/pkg/FR-2015-08-26/pdf/2015-20870.pdf	✓
90-Day-Pull WARNORD	SIPRNet: https://intelshare.intelink.sgov.gov/SITES/DCC/WEEKLY%20EXPIRING%20CIRCUITS/FORMS/ALLITEMS.ASPX	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
Army Enterprise Cloud Computing Reference Architecture (AECCRA) Version 1.0, September 2014	https://army.deps.mil/army/cmds/hqda_ciog6_Project/ADCCP/CloudDocRepository/default.aspx	✓
Army Standards Profile Guidance in support of Common Operating Environment (COE)	https://army.deps.mil/army/cmds/hqda_ciog6/AO/AOD/architecture/SitePages/Home.aspx?RootFolder=%2Farmy%2Fcmds%2Fhqda%5Fciog6%2FAO%2FAOD%2Farchitecture%2FShared%20Documents%2FCOE%20Standards%20View%201%20for%20COE%203%5F0&FolderCTID=0x012000D1ECE38A76B6574AA4C47BD731F587F6&View=%7BF660F86E%2DDB2D%2D4AE7%2D97F7%2DC53A91572089%7D	✓
Assessment and Authorization Division (RE5) website	https://disa.deps.mil/org/RE5/default.aspx https://dod365.sharepoint-mil.us/sites/DISA-Assessment-And-Authorization-External/	✓
Assessment and Authorization Requests Tracking System (RTS)	https://disa.deps.mil/org/RMED/rts2e/SitePages/Home.aspx https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/rts2e/sitepages/home.aspx	✓
Best Practices Guide for DoD Cloud Mission Owners	https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/unclass-best_practices_guide_for_dod_cloud_mission_owners_FINAL.pdf or https://cyber.mil/dccs/dccs-documents/ (Navigate the web page to select the document)	✓
CDTAB Website	NIPRNet: https://intelshare.intelink.gov/sites/cdtab SIPRNet: https://intelshare.intelink.sgov.gov/sites/cdtab	✓
CJCSI 6211.02D, Defense Information System Network (DISN) Responsibilities, 4 August 2015	https://www.jcs.mil/Library/CJCS-Instructions/ (Use the search window)	✓
CJCSI 6290.01, Requirements Management Process for Mission Partner Environment, 17 September 2019	https://www.jcs.mil/Library/CJCS-Instructions/ (Use the search window)	✓
CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 Jun 2015	https://www.jcs.mil/Library/CJCS-Instructions/ (Use the search window)	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
CJCSI 6740.01C, Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations, 17 June 2019	https://www.jcs.mil/Library/CJCS-Instructions/ (Use the search window)	✓
Cloud System Security Plan (SSP) addendum template	https://cyber.mil/dccs/dccs-documents/ (Enter "SSP" into the Search window.) or Contact the DCAS Team	✓
CNSSI No. 4009, National Information Assurance Glossary, April 6, 2015,	https://www.cnss.gov/CNSS/issuances/Instructions.cfm (Scroll down to find the document)	✓
Command Cyber Readiness Inspection (CCRI)	SIPRNet: https://intelshare.intelink.sgov.gov/sites/jfhq-dodin/JD/SitePages/CCRI%20Program.aspx	✓
Committee on National Security Systems Instruction (CNSSI) No. 1253, Security Categorization and Control Selection for National Security Systems, 27 March 2014	https://www.cnss.gov/CNSS/issuances/Instructions.cfm (Scroll down to find the document)	✓
Cross Domain Technical Advisory Board (CDTAB) Charter,	(CAC and an account are required for access. Email the DSAWG Secretariat (CDTAB Support) to request an account) https://intelshare.intelink.gov/sites/cdtab/default.aspx	✓
CSO architecture briefing template	Contact the DCAS Team	✓
CSO Initial Contact Form	https://disa.deps.mil/org/RMED/cas/SitePages/CASHome.aspx https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/sitepages/cashome.aspx (Select "Sponsor CSO") or, Contact the DCAS Team	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
CSP Security Package Documentation Checklist (current version)	https://cyber.mil/dccs/dccs-documents/ (This web page contains several cloud computing security documents. Scroll down to find “Documentation Checklist,” or Contact the DCAS Team	✓
Cyber Awareness Challenge	https://cyber.mil/training/cyber-awareness-challenge/	✓
Defense Information Technology Investment Portal (DITIP)	https://snap.cape.osd.mil/ITPortal/PortalHome	✓
Defense Security/Cybersecurity Authorization Working Group (DSAWG) Charter, 16 Aug 21	(To access, copy and paste the following link into a web browser then log into your NIPRNet INTELINK account) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fdsawg%2FShared%20Documents%2FDSAWG%5FCharter&FolderCTID=0x012000CC2A7A98C1295C45AFD9DAC8E15A4267&View=%7BEC1D88D1%2DBA36%2D4AA1%2D98FD%2D1D47AEB1CEF1%7D (Select the “New DSAWG Charter – 16 August 2021” tab)	✓
Defense Switched Network (DSN) Services and Capabilities	https://storefront.disa.mil/kinetic/disa/service-catalog#/category/voice	✓
Defense Working Capital Fund Billing Prices for Fiscal Year 2023 – Consolidated Services, 1 October 2022	https://services.disa.mil/csm (Search “Rate Books”)	✓
Department of Defense Strategy for Implementing the Joint Information Environment (JIE)	https://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf	✓
DFARS Subpart 239.7401	https://www.acq.osd.mil/dpap/dars/dfars/html/current/239_74.htm	✓
DIA Directive 8550.500, JWICS Connection Approval (“DIA IA Front Door” website)	(To access, copy and paste the following link into a web browser then log into your NIPRNet INTELINK account) https://intelshare.intelink.gov/sites/diaia/_layouts/15/start.aspx#/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fdiaia%2FShared%20Documents%2FJWICS%20Connection%20Approval%20Program%20%28JCAP%29%20Artifacts&FolderCTID=0x012000A0C87F6814C8C743999C955F11915DC7&View=%7B0646F3EE%2DB8A4%2D4F5E%2D9FB3%2D78BA67B32FF9%7D (Select the “Documents” tab. Select “JWICS Connection Approval Program (JCAP) Artifacts” folder)	

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DISA Advisory Message (DAM) 17-047, Modernization Consolidation (PEMC) Efforts, TSO Elimination, and WWOLS Retirement, Phase 1, 28 July 2017	https://disa.deps.mil/ext/cop/ns-extranet/PMCWG/Documents/References/(U)%20DAM%2017-047%20-%20PEMC%20Efforts%20TSO%20Elimination%20WWOLS%20Retirement%20Phase%201%20(U).pdf#search=DISA%20Advisory%20Message%20%28DAM%29%2017-047	
DISA Circular 300-115-3, Defense Information Systems Network (DISN), Secret Internet Protocol Routing Network (SIPRNet) Security Classification Guide	https://dod365.sharepoint-mil.us/:w:/r/Sites/DISA-Risk-Adjudication/Shared%20Documents/DISA%20RE42%20SCG%20Duties/DISA%20SCGs/DISAC_300-115-3_-_DISN_SIPRNet_SCG_(15Mar2013).docx?d=w42d1d500fe7d42469106f0fbcf181c88&csf=1&web=1&e=H6w4ad	✓
DISA Circular 310-070-057, DISN Quality Management Program, 22 December 2014	https://disa.deps.mil/ext/resource/disa_publications_issuances/DISA_Publications/Forms/AllItems.aspx?RootFolder=%2Fext%2Fresource%2Fdisa%5Fpublications%5Fissuances%2FDISA%5FPublications%2F300%20%2D%20Global%20Information%20Grid%2F310%20%E2%80%8BGIG%20Operations%2FIssuances https://dod365.sharepoint-mil.us/sites/DISA-SO/SO4/DA/DISA%20Circulars/Forms/AllItems.aspx (Scroll down to find the document)	✓
DISA Circular 310-130-001, Communications Requirements, Submission of Telecommunications Service Requests, 19 August 2009	https://disa.deps.mil/ext/resource/disa_publications_issuances/DISA_Publications/Forms/AllItems.aspx?RootFolder=%2Fext%2Fresource%2Fdisa%5Fpublications%5Fissuances%2FDISA%5FPublications%2F300%20%2D%20Global%20Information%20Grid%2F310%20%E2%80%8BGIG%20Operations%2FIssuances https://dod365.sharepoint-mil.us/sites/DISA-OP4/CircWG/default.aspx (Scroll down to find the document)	✓
DISA Circular 310-65-1, Circuit and Trunk Table Management for the Defense Information Systems Network (DISN), 27 July, 2018	https://www.disa.mil/-/media/Files/DISA/About/Publication/Circular/dc3106501.pdf (Scroll down to find the document)	✓
DISA Cross Domain Enterprise Services (CDES) Customer Requirements Questionnaire	https://intellipedia.intelink.gov/wiki/IA32_Cross_Domain_Solutions#Cross_Domain_Support_Element_POC.27s (Scroll down to find: “New Customer Questionnaire and CDES Overview Documents”)	✓
DISA JRSS Portal	https://disa.deps.mil/ext/cop/mae/cop_mae/JRSS/SitePages/Home.aspx	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DISA milCloud Website (aka milCloud 1.0)	https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/milcloud-10 For more information email: disa.meade.bd.mbx.bdm4-mpeo-support@mail.mil	✓
DISA PPSM web pages	**NIPRNet:** **PPSM Home:** https:/cyber.mil/PPSM **DISA RE4:** https://dod365.sharepoint-mil.us/sites/DISA-Ports-Protocols-Services-Management **SIPRNet** **PPSM Home:** https://cyber.smil.mil/connect/ppsm/ **PPSM Registry Database:** https://pnp.cert.smil.mil	✓
DISA RE41 PPSM Home Page	NIPRNet: https://dod365.sharepoint-mil.us/sites/DISA-Ports-Protocols-Services-Management SIPRNet: https://intelshare.intelink.sgov.gov/sites/dod-ppsm/SitePages/Home.aspx	✓
DISA Services and Capabilities Catalog	https://storefront.disa.mil/kinetic/disa/service-catalog#/ **DISA Capabilities Brochure:** https://www.disa.mil/-/media/Files/DISA/Fact-Sheets/DISA-Capabilities.ashx?la=en&hash=058FFF28911BFA504B699B2D3642AB82C292F482 (Open the document after it downloads to your desktop)	✓
DISA StoreFront (DSF)	(CAC and an account are required for access) https://storefront.disa.mil/	✓
DISA's Risk Adjudication and Connection Division's Mission Partner Training Program (MPTP)	https://cyber.mil/connect/mptp https://cyber.mil/connect/faq-mptp **Computer-based training is located at:** **https://cyber.mil/connect/mptp/** https://www.youtube.com/playlist?list=PLRPVoCgP5zRYqzNJ5FS5FBuPG6eH7vr6i	✓
DISN Connection Process Guide (DCPG), (Current Version)	https://cyber.mil/connect/connection-approval/ (Scroll down to find the document.)	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DISN Connection Reference Library	https://snap.dod.mil/gcap/reference-docs.do	✓
DISN services catalog	https://storefront.disa.mil/kinetic/disa/service-catalog#/category/services-and-capabilities	✓
DISN Subscription Service (DSS) Frequently Asked Questions (FAQs)	https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/dss-faqs	✓
DISN/GIG Flag Panel Decision Ballot – Cloud Security Model v2.0D, 12 Dec 2013	SIPRNet: https://intellipedia.intelink.sgov.gov/wiki/Information_Security_Risk_Management_Committee (In the “CONTENTS” window select “2013 DISN/GIG Flag Panel” Scroll down to “Decision Ballot – Cloud Security Model v2.0D”)	✓
DoD 5220.22-M, National Industrial Security Program Operating Manual,	The National Industrial Security Program Operating Manual (NISPOM) is now Part 117 of Title 32, Code of Federal Regulations https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117?toc=1 https://www.esd.whs.mil/Directives/issuances/dodm/ (Use the search window)	✓
DoD 7000.14-R, Department of Defense Financial Management Regulation (DoD FMR)	https://comptroller.defense.gov/FMR.aspx For SNaP-IT guidance, download Volume 2B, Chapter 18 at: https://comptroller.defense.gov/Portals/45/documents/fmr/current/02b/02b_18.pdf	✓
DoD Approved Cloud Service Offerings Catalog	For IL4, IL5 and IL6 CSOs see: https://disa.deps.mil/org/RMED/cas/SitePages/CSOCatalog.aspx Also see: DISA SNAP for all authorized IL2, IL4 and IL5 CSOs DISA SGS for all authorized IL6 CSOs	✓
DoD CIO and Office of the Director of National Intelligence Memorandum, (U) Unified Cross Domain Services Management Office Disestablishment and Functional Transition to the Nation al Cross Domain Strategy and Management Office, February 2019	https://intelshare.intelink.gov/sites/ncdsmo/Shared%20Documents/Policies/ODNI%20Memo%202017-7048.pdf (Select the desired document.)	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DoD CIO and USD (A&S) Memorandum, Suspension of New Point-to-Point Cross Domain Solutions and Changes to Existing Point-to-Point Cross Domain Solutions Implementations, October 10, 2018	(To access, copy and paste the following link into a web browser then log into your NIPRNet INTELINK account) https://intelshare.intelink.gov/sites/ncdsmo/Shared%20Documents/Policies/DoD%20Memo_Suspension%20of%20P2P%20CDS.PDF	✓
DoD CIO JRSS website	https://www.milsuite.mil/wiki/JRSS or Log in using your CAC at: www.milsuite.mil/wiki (Enter "jrss" in the '*Search milWiki*' search window)	
DoD CIO Memorandum, Circuit Optimization, May 5, 2016 (DoD CIO Briefing)	https://dodcio.sp.pentagon.mil/sites/Collaboration/JIEIntegration/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/Collaboration/JIEIntegration/Shared%20Documents/Circuit%20Optimization%20Task%207-7-16.pptx&action=default&DefaultItemOpen=1 https://dodcio.sp.pentagon.mil/sites/Collaboration/SitePages/Home.aspx	✓
DoD CIO Memorandum, DoD Cybersecurity Activities Performed for Cloud Service Offerings, Nov 15, 2017	https://dl.cyber.mil/cloud/pdf/DoD-CIO-Memo-CS-Activities-Perf-for-Cloud-Serv-Activ-Offerings.pdf or, https://cyber.mil/dccs/dccs-documents/ (Scroll down to find the document)	✓
DoD CIO Memorandum, Improving Security of Federal Department and Agency Connections to the Department of Defense Secret Internet Protocol Router Network, August 9, 2013	https://dodcio.sp.pentagon.mil/SiteCollectionDocuments/Improving%20Security%20of%20Fed%20Dept%20Agency%20Connections%20to%20DoD%20SIPRNet%20(Final).pdf#search=Improving%20security%20of%20Federal%20Department	✓
DoD CIO Memorandum, Legacy Networking Technologies, July 27, 2017	https://disa.deps.mil/ext/cop/ns-extranet/NS1/Shared%20Documents/TDM_TIM/TDM-TIM-2018-March-06-07/CIO%20Signed%20Memo%20Legacy%20Networking%20Technologies.pdf	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DoD CIO Memorandum, Responsibilities of DoD Components Sponsoring Mission Partner Connections to DISN-Provided Transport Infrastructure, 14 August 2012	Miscellaneous References web page (Scroll down to find the document.)	✓
DoD CIO Memorandum, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 December 2014	https://dodcio.sp.pentagon.mil/SiteCollectionDocuments/DoD%20CIO%20-%20Updated%20Guidance%20-%20Acquisition%20and%20Use%20of%20Commercial%20Cloud%20Services_20141215.pdf#search=Updated%20guidance%20on%20acquisition	✓
DoD Cloud Acquisition Guidebook	https://www.dau.edu/tools/t/DoD-Cloud-Acquisition-Guidebook	✓
DoD Cloud Authorization Process web page	https://disa.deps.mil/org/RMED/cas/SitePages/CSOAuthReqs.aspx	✓
DoD Cloud Computing Security Requirements Guide (CC SRG), current version	https://public.cyber.mil/dccs/dccs-documents/ (Scroll down to find the “Cloud Computing SRG v1r4” or the current version)	✓
DoD Cloud Computing Security website	https://public.cyber.mil/dccs/dccs-documents/ (Scroll down to find the desired document)	✓
DoD Cloud Cyberspace Protection Guide	https://public.cyber.mil/dccs/dccs-documents/ (Navigate the web page to find the current version of the document.)	✓
DoD Cloud Strategy (Deputy Secretary of Defense), December 2018	https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF	✓
DoD Dictionary of Military and Associated Terms, as of October 2022	https://www.jcs.mil/Doctrine/DOD-Terminology-Program/	✓
DoD Enterprise Information Technology Standard Business Case Analysis	DoD CIO Memo is at: https://dodcio.defense.gov/Portals/0/Documents/Use%20ofEnterprise%20Information%20Technology%20Standard%20Business%20Case.pdf Template is at: https://dodcio.defense.gov/Portals/0/Documents/BPSR/TEMPLATE%20-BCA.pdf?ver=2018-07-26-113256-063	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DoD FY20XXXX IT-1 Report (unclassified investments)	https://www.cape.osd.mil/ Follow the above link, select Public Reports, select the desired FY20XX IT President’s Budget Request Reports, select the IT-1 Report listed	✓
DoD Information Technology Program Repository (DITPR)	(CAC and DITPR account required for access) https://ditpr.dod.mil	✓
DoD Information Technology Standards Registry (DISR)	(CAC and DISR account required for access) https://gtg.csd.disa.mil/disr/	✓
DoD Internet-NIPRNet DMZ STIG- Current Version	https://cyber.mil/stigs/downloads (Search for: “DoD Internet-NIPRNet DMZ STIG”)	✓
DoD Mandated Cloud Computing Standards	(CAC and DISR account required for access) https://gtg.csd.disa.mil/disr/standards/search/simple.html?searchText=cloud&baseline=&status=120&intelStatus=&search=Search	✓
DoD Network Information Center (NIC) Registry Protocol 9802	https://www.nic.mil/webmenu/docfiles/registry_protocol_9802.pdf	✓
DoD RMF Authorization Decision Document (ADD)	https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/AuthDecision.aspx To navigate to the page: https://rmfks.osd.mil/rmf/Pages/default.aspx and login via CAC Mouse over “Controls and Authorization”, then hover over “Security Authorization Package” in the drop-down selection, a side bar expands, and you select “Authorization Decision Document.”	✓
DoD RMF Plan of Action and Milestones (POA&M)	https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/POAM.aspx To navigate to the page: https://rmfks.osd.mil/rmf/Pages/default.aspx and login via CAC Mouse over “Controls and Authorization”, then hover over “Security Authorization Package” in the drop-down selection, a side bar expands, and you select “POA&M.”	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DoD RMF Risk Assessment Report (RAR)	For DISN Telecommunication connections use: https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/RiskAssessment.aspx To navigate to the page: https://rmfks.osd.mil/rmf/Pages/default.aspx and login via CAC Mouse over "Controls and Authorization", then hover over "Security Authorization Package" in the drop-down selection, a side bar expands, and you select "Risk Assessment Report" For Cloud connections use DoD FedRAMP+ RAR template at: https://dl.dod.cyber.mil/wp-content/uploads/cloud/doc/DoD_RAR_template_DRAFT_%28002%29.doc	✓
DoD RMF Security Assessment Report	https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SAR.aspx To navigate to the page: https://rmfks.osd.mil/rmf/Pages/default.aspx and login via CAC Mouse over "Controls and Authorization", then hover over "Security Authorization Package" in the drop-down selection, a side bar expands, and you select "Security Assessment Report"	✓
DoD RMF Security Plan	https://rmfks.osd.mil/rmf/ControlsandAuthorization/SecAuthPackage/Pages/SecurityPlan.aspx To navigate to the page: https://rmfks.osd.mil/rmf/Pages/default.aspx and login via CAC Mouse over "Controls and Authorization", then hover over "Security Authorization Package" in the drop-down selection, a side bar expands, and you select "Security Plan"	✓
DoD Secure Cloud Computing Architecture (SCCA) Functional Requirements (FR) (current version)	https://disa.deps.mil/ORG/SD/SD8/SCCA/MissionPartners/SitePages/Secure%20Cloud%20Computing%20Architecture.aspx	✓
DoD Security Technical Implementation Guides (STIGs)	https://cyber.mil/stigs/downloads/	✓
DoDD 5100.03, Support of the Headquarters of Combatant and Subordinate Unified Commands, (Change 1), September 7, 2017	https://www.esd.whs.mil/Directives/issuances/dodd/ (Use the search window)	✓
DoDD 5105.19, Defense Information Systems Agency, July 25, 2006	https://www.esd.whs.mil/Directives/issuances/dodd/ (Use the search window)	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DoDD 5144.02, DoD Chief Information Officer, Change 1, September 19, 2017	https://www.esd.whs.mil/Directives/issuances/dodd/ (Use the search window)	✓
DoDI 5530.03, International Agreements, December 4, 2019	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDD 8000.01, Management of the Department of Defense Information Enterprise, July 27, 2017	https://www.esd.whs.mil/Directives/issuances/dodd/ (Use the search window)	✓
DoDI 1015.10, Military Morale, Welfare, and Recreation (MWR) Programs	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 1015.15, Establishment, Management, and Control of Non-Appropriated Fund Instrumentalities and Financial Management of Supporting Resources	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 5000.02T, Operation of the Defense Acquisition System, Change 6, January 23, 2020	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 5000.74, Defense Acquisition Services, January 20, 2020	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 5000.76, Accountability and Management of Internal Use Software (IUS), CH 2 June 7, 2019	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 5400.11, DoD Privacy and Civil Liberties Programs, January 29, 2019	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8010.01, DODIN Transport, September 10, 2018	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8100.04, DoD Unified Capabilities (UC), December 9, 2010	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8110.01, Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD, November 25, 2014	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DoDI 8115.02, Information Technology Portfolio Management Implementation, October 30, 2006	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8170.01, Online Information Management and Electronic Messaging, January 2, 2019	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS), Change 2, December 11, 2019	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8410.01, Internet Domain Name Use and Approval, December 4, 2015	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8440.01, DoD Information Technology (IT) Service Management (ITSM), December 24, 2015	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8500.01, Cybersecurity, October 7, 2019	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), Change 2, July 28, 2017	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, Change 1, July 25, 2017	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8540.01, Cross Domain Policy, Change 1, August 28, 2017	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), Change 1, July 27, 2017	https://www.esd.whs.mil/Directives/issuances/dodi/ (Use the search window)	✓
DSAWG briefing template	https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fdsawg%2FShared%20Documents%2FDSAWG%5FMeeting%5FBriefing%5FToolkit&FolderCTID=0x012000CC2A7A98C1295C45AFD9DAC8E15A4267&View=%7BEC1D88D1%2DBA36%2D4AA1%2D98FD%2D1D47AEB1CEF1%7D	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
DSAWG Criteria for Repeatable Accreditation of Cross Domain Solutions	https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fdsawg%2FShared%20Documents%2FCDS%2FRepeatable%5FAccreditation%5FCriteria&FolderCTID=0x012000CC2A7A98C1295C45AFD9DAC8E15A4267&View=%7BEC1D88D1%2DBA36%2D4AA1%2D98FD%2D1D47AEB1CEF1%7D	✓
eMASS Computer Based Training	https://www.cdse.edu/Training/eLearning/DISA-100/	✓
eMASS Frequently Asked Questions (FAQ), System Administrator POCs, and URLs	https://disa.deps.mil/ext/cop/iase/emass/Documents/eMASS_FAQ_6.pdf or, https://dl.cyber.mil/emass/pdf/unclas-emass_faq.pdf	✓
eMASS Mission Assurance Support Service	https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/enterprise-mission-assurance-support-service or email: disa.meade.re.mbx.emass-account-request@mail.mil	✓
eMASS Overview (RMF KS website)	https://rmfks.osd.mil/rmf/HelpandResources/eMASS/Pages/What%20is%20eMASS.aspx or https://safe.menlosecurity.com/doc/docview/viewer/docN93ECAC74469447f18fe115b8ccaf2488f182a935bd65fdef10a69e6149fae8c91a3dfbc4c9df	✓
Enterprise Cloud Computing website	https://intelshare.intelink.gov/Term%20Stores/dod-enterprise-cloud-community	✓
Enterprise Mission Assurance Support System (eMASS) Account	https://cyber.mil/emass/ or, disa.meade.re.mbx.emass-account-request@mail.mil or, disa.meade.id.mbx.emass-tier-iii-support@mail.mil	✓
Federal Risk Authorization and Management Program (FedRAMP)	https://www.fedramp.gov https://www.fedramp.gov/faqs/	✓
FedRAMP 3PAO requirements	https://www.fedramp.gov/updated-3PAO-obligations-and-performance-standards-document/	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
FedRAMP Marketplace website (FedRAMP Provisionally Authorized CSO products)	https://www.fedramp.gov/ Select the “**Marketplace**” tab	✓
Intelligence Community Directive 503, Information Technology Systems Security Risk Management, Certification and Accreditation, Effective, 15 September 2008	https://www.dni.gov/files/documents/ICD/ICD_503.pdf	✓
Internet Access Point Demilitarized Zone Virtual Private Network Community of Interest Customer User’s Guide	https://disa.deps.mil/org/ID5/ID23/CentralLibrary/_layouts/15/WopiFrame.aspx?sourcedoc=/org/ID5/ID23/CentralLibrary/Documents/COI/IAP%20DMZ%20COI%20Connection%20Guide%20v34.docx&action=default&DefaultItemOpen=1	✓
JFHQ DODIN Notification of Non-Compliant Circuit Disconnection Website	SIPRNet: https://intelshare.intelink.sgov.gov/sites/jfhq-dodin/J3/JDOC/Orders/Forms/DTD.aspx	✓
JFHQ DODIN Task Order 16-0158, Connection Accreditation Enforcement Process, 011753 DEC 16	SIPRNet: https://intelshare.intelink.sgov.gov/sites/jfhq-dodin/J3/JDOC/SitePages/Orders-Dashboard.aspx *Use the search bar in the upper right or filter bar near the center of page to filter for 16-0158 to find more easily. **In the “search this site” box enter:** “SUBJ/(U) JFHQ-DODIN TASKORD 16-0158 JFHQ-DODIN CONNECTION” then scroll down to find the TASKORD)	✓
JIE Reference and Solution Architectures	NIPRNet: https://wmaafip.js.mil/home SIPRNet: https://wmaafip.js.smil.mil	✓
Joint Staff J6 Cyber Integration Workshop (“Partner Nation Systems Connection Process Guide”)	NIPRNet: https://intelshare.intelink.gov/sites/js-j6/DCD SIPRNet: https://conference.apps.smil.mil/webconf/ciwg	
Mission Partner Portal	https://services.disa.mil/csm	✓
National Cross Domain Strategy and Management Office (NCDSMO) Baseline List	**SIPRNet:** https://intelshare.intelink.sgov.gov/sites/ncdsmo/ (Requires an account.)	✓
National Information Assurance Partner (NIAP) Evaluated Products	https://www.niap-ccevs.org/Product/	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
Navy Acquisition and Use of Commercial Cloud Computing Services	http://www.doncio.navy.mil/TagResults.aspx?ID=104	✓
NFG Connection Process Chart	Contact the NIPRNet NFG Office for a more readable version of the chart.	✓
NIPRNet DMZ Whitelist (current version)	SIPRNet: https://niprdmzwhitelist.csd.disa.smil.mil/	✓
NIPRNet Federated Gateway (NFG) Policy Spreadsheet & Questionnaire	https://dod365.sharepoint-mil.us/sites/disa-id5/ID52/NFG/SitePages/Home.aspx	✓
NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find 800-122)	✓
NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find “800-145”)	✓
NIST SP 800-146, Cloud Computing Synopsis and Recommendations, May 2012	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find NIST SP “800-146”)	✓
NIST SP 800-18, Rev 1, Guide for Developing Security Plans for Federal Information Systems, February 2006	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find 800-18)	✓
NIST SP 800-30, Rev 1, Guide for Conducting Risk Assessments, September 2012	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find 800-30)	✓
NIST SP 800-37, Rev 2, Risk Management Framework for Information Systems and Organizations, December 2018	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find 800-37) (Note Rev 1 will be withdrawn on Dec 20, 2019, and superseded by SP 800-37 Rev 2)	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
NIST SP 800-39, Managing Information Security Risk: Organization, Mission and Information System View, current edition	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find 800-39)	✓
NIST SP 800-53, Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, current edition	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find 800-53)	✓
NIST SP 800-53A, Rev 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, current version	https://csrc.nist.gov/publications/search?requestserieslist=1&requeststatuslist=1,3&requestdisplayoption=brief&itemsperpage=all&requestsortorder=5 (Use the search bar to find 800-53A)	✓
OMB FY14 Guidance on Exhibits 53 and 300- Information Technology and E-Government	https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fy14_guidance_on_exhibits_53_and_300.pdf	✓
Open Cloud Computing Interface - Core, Open Grid Forum, GFD-P-R.183 7 Apr 2011	https://www.ogf.org/documents/GFD.183.pdf	✓
Open Cloud Computing Interface – RESTful HTTP Rendering, Open Grid Forum, GFD-P-R.185 June 21, 2011	https://www.ogf.org/documents/GFD.185.pdf	✓
P2P CDS Supporting Documentation web page	SIPRNet: https://intelshare.intelink.sgov.gov/sites/cdtab/default.aspx/home.aspx/ (The SIPRNet CDTAB website has a folder that contains the P2P CDS Supporting Documentation. When connecting to the CDTAB website select the link for "P2P Implementation Guidance" then select the desired document by title)	✓
PPSM Category Assurance List (CAL)	https://dod365.sharepoint-mil.us/:b:/r/Sites/DISA-Ports-Protocols-Services-Management/External/Knowledge_Service/Vulnerability_Assessment/Category%20Assurance%20List/CAL_by_Service-20221227.pdf?csf=1&web=1&e=BF2VfP (Note: PKI is required for access.)	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
PPSM Registry	For the **PPSM-Secret (PPSM-S) Registry**: Enter the following link into the **SIPRNet** web browser https://pnp.cert.smil.mil/pnp/ For the **PPSM-Unclassified (PPSM-U) Registry**: Enter the following link into the **NIPRNet** web browser: https://pnp.cert.mil/pnp/ (NOTE: PKI/SIPRNet Token and PPSM account are required for access – request an account through your CC/S/A PPSM Technical Advisory Group (TAG) representative).	
Private Data Internet Service Provider	https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/private-data-internet-service-provider	✓
RFC 1918 Guidance Memo,	(To access, copy and paste the following link into a web browser then log into your NIPRNet INTELINK account) https://intelshare.intelink.gov/sites/dsawg/RFC_1918/Forms/AllItems.aspx (Open the document after it downloads to your desktop)	✓
Risk Decision Authority Criteria (RDAC) Version 2.3	https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fdsawg%2FShared%20Documents%2FCDS%2Frisk%5Fassessment%5Fmethodolgies%2FRDAC&FolderCTID=0x012000CC2A7A98C1295C45AFD9DAC8E15A4267&View=%7BEC1D88D1%2DBA36%2D4AA1%2D98FD%2D1D47AEB1CEF1%7D	✓
Risk Management Framework (RMF) Knowledge Service	https://rmfks.osd.mil/rmf/Pages/default.aspx	✓
Secure Cloud Computing Architecture (SCCA) Knowledge Center	https://disa.deps.mil/ORG/SD/SD8/SCCA/MissionPartners/SitePages/SCCA%20Knowledge%20Center.aspx	✓
Secure Cloud Computing Architecture (SCCA) Mission Partner Home web page	https://go.usa.gov/xycHD Or, https://disa.deps.mil/ORG/SD/SD8/SCCA/MissionPartners/SitePages/Secure%20Cloud%20Computing%20Architecture.aspx	✓
Secure Cloud Computing Architecture (SCCA) Onboarding web page	https://disa.deps.mil/ORG/SD/SD8/SCCA/MissionPartners/SitePages/Secure%20Cloud%20Computing%20Architecture%20(SCCA)%20Onboarding.aspx	✓
Select and Native Programming Data Input System for Information Technology (SNaP-IT)	Request access via the DITIP portal at: https://snap.cape.osd.mil/ITPortal/PortalHome	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
SIPRNet GIAP System (SGS)	SIPRNet: https://giap.disa.smil.mil	✓
SIPRNet IT Registry (SITR)	SIPRNet: https://dodcio.osd.smil.mil/itregistry (A SITR account is required for access – contact the SIPRNet IT Registry POC)	
SNAP Reference Documents	https://snap.dod.mil/ Hover your cursor over "Policy," then, *Select*: "Reference Documents"	✓
System Network Approval Process (SNAP)	https://snap.dod.mil/index.do (Requires a CAC and a SNAP account see Section 2.8 of this guide)	✓
Telecommunication Services Enterprise Acquisition Services (TSEAS) Inventory and Billing Information (TIBI)	https://tibi.csd.disa.mil/	✓
Temporary Exception to Policy Template	Log into your SNAP account using your CAC card at: https://snap.dod.mil/ Hover your cursor over "Policy," then *select:* *"Reference Documents"* > *"Waiver"* > *"DODIN Commercial Connection Request for Temporary Exception to Policy"*> "Download"	✓
Training Management System (TMS)	https://disa.deps.mil/org/RMED/tms/SitePages/home.aspx	✓
Unified Capabilities (UC) Master Plan, October 2011	http://www.disa.mil/Network-Services/UCCO/~/media/Files/DISA/Services/UCCO/APL-Process/Unified_Capabilities_Master_Plan.pdf	✓
Unified Capabilities (UC) Reference Architecture,	http://dodcio.defense.gov/Library/DoD-Architecture-Framework/	✓
Unified Capabilities Approved Products List (UC APL)	https://aplits.disa.mil/processAPList	✓

REFERENCES	ONLINE LINK (Access to some links may require a Common Access Card (CAC) and a user account)	Verified
Unified Capabilities Requirements (UCR) 2013, change 2, September 2017	https://aplits.disa.mil/docs/UCR-2013-Change2.pdf	✓
Validation Letter for Mission Partner Connections to DISN and Request for Mission Partner Connection Briefing Template	https://rmfks.osd.mil/dode2p https://rmfks.osd.mil/dode2p/Pages/Resources.aspx Select: _DoD Mission partner Connection_Template	✓
Very Low Risk (VLoR) Assertions, version 2.4, 13 July 2013	(To access, copy and paste the following link into a web browser then log into your NIPRNet INTELINK account) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/CDS/risk_assessment_methodolgies/VLOR/VLoR_Process_Guidance_v2.4.docx (See section 5 of the VLoR Assertions document)	✓
Very Low Risk (VLoR) Process Implementation Guide, version 2.4 13 July 2013	(To access, copy and paste the following link into a web browser then log into your NIPRNet INTELINK account) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/CDS/risk_assessment_methodolgies/VLOR/VLoR_Process_Guidance_v2.4.docx	✓
Virtual Data Center Security Stack (VDSS)	https://www.disa.mil/NewsandEvents/2018/Secure-Cloud-Computing-Architecture	✓
VPN User Guides and Tutorials (Current Version)	**The guide for registering a VPN in SNAP can be found by logging into SNAP using your CAC card at:** https://snap.dod.mil/ Hover your cursor over "Policy," then, *Select:* "Reference Documents" > "VPN" **A Tutorial for using DISA Storefront to order a VPN is at:** https://ddsf.disadirect.disa.mil/kinetic/themes/ddsf/training/DISA%20Storefront_Establish%20VPN_Overview.pdf The VPN customer ordering guides are also posted on the Miscellaneous References web page. See: "1- CustOrdGuide-EstablishVPN" "2- CustOrdGuide-ConnecToVPN" "3 - VPN-Registration in SNAP"	✓

Appendix O Acronyms

ACRONYM	TERM
3PAO	Third Party Assessor Organization
A&A	Assessment and Authorization
ADD	Authorization Decision Document
AO	Authorizing Official
APL	Approved Products List
ATC	Approval to Connect
ATO	Authorization to Operate
BCAP	Boundary Cloud Access Point
CAC	Common Access Card
CAO	Connection Approval Office
CATC	Cloud Approval to Connect
CC SRG	DoD Cloud Computing Security Requirements Guide
CCORI	Command Cyber Operational Readiness Inspection
CCRI	Command Cyber Readiness Inspection
CCSD	Command Communications Service Designator
CDA	Cross Domain Appendix
CDES	Cross Domain Enterprise Services (also see "DISA CDES")
CDS	Cross Domain Solution
CDSA	Cross Domain Solution Authorization
CDSE	Cross Domain Support Element
CDTAB	Cross Domain Technical Advisory Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer

ACRONYM	TERM
SISO	Senior Information Security Officer
C-ITP	Cloud Information Technology Project
CMT	Compliance Monitoring Team
CNSS	Committee on National Security Systems
CPTC	Cloud Permission to Connect
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CSSP	Cybersecurity Service Provider
CTM	Consent to Monitor
DCPG	DISN Connection Process Guide
DCSA	Defense Counterintelligence and Security Agency (DCSA) (formerly the Defense Security Service (DSS))
DFARS	Defense Federal Acquisition Regulation Supplement
DIS	DISN Infrastructure Service
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITCO	Defense Information Technology Contracting Office
DITPR	DoD Information Technology Portfolio Repository
DMZ	Demilitarized Zone
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DODIN	Department of Defense Information Networks
DSAWG	Defense Security/Cybersecurity Authorization Working Group
DSF	DISA StoreFront
DSN	Defense Switched Network

ACRONYM	TERM
DSS	Defense Security Service (now DCSA) Or, DISN Subscriber Service (now DIS)
ECDSP	Enterprise Cross Domain Service Provider
FedRAMP	Federal Risk and Authorization Management Program
FTPO	For Tracking Purposes Only
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
IAP	Internet Access Point
IATT	Interim Authorization to Test
IAW	In accordance with
IC	Intelligence Community
ICAP	Internal Cloud Access Point
ICD	Intelligence Community Directive
IDS/IPS	Intrusion Detection System/Intrusion Prevention System
IGSD	DISA Infrastructure Global Service Desk
IP	Internet Protocol
IS	Information Systems
ISO/IEC	International Standards Organization/International Electrotechnical Commission
ISP	Internet Service Provider
ISRMC	Information Security Risk Management Committee
IT	Information Technology
JIE	Joint Information Environment
JRSS	Joint Regional Security Stack

ACRONYM	TERM
JSP	Joint Services Provider (Pentagon)
JWICS	Joint Worldwide Intelligence Communications System
MPE	Mission Partner Environment
MPEO	Mission Partner Engagement Office (DISA)
MPLS	Multi-Protocol Label Switching
NCDSMO	National Cross Domain Strategy and Management Office
NFG	NIPRNet Federated Gateway
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
OC	Operation Center
OGF	Open Grid Forum
PA	Provisional Authorization
POA&M	Plan of Action & Milestones
POC	Point of Contact
PPSM	Ports, Protocols, and Services Management
PTC	Permission To Connect (issued by the DISN CAO for Level 3 VPNs connected via DISN see Appendix K)
RDAC	Risk Decision Authority Criteria
RMF	Risk Management Framework
SAR	Security Assessment Report
SBSA	Site Based Security Assessment
SCCA	Secure Cloud Computing Architecture

ACRONYM	TERM
SGS	SIPRNet GIAP System
SIPRNet	Secret Internet Protocol Router Network
SNAP	System/Network Approval Process
SNaP-IT	Select and Native Programming Data Input System for Information Technology (SNaP-IT)
SRG	Security Requirements Guide
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TIBI	Telecommunication Services Enterprise Acquisition Services (TSEAS) Inventory and Billing Information
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
UC	Unified Capabilities
USCYBERCOM	United States Cyber Command
USI	Universal System Identifier
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRF ID	Virtual Routing and Forwarding Identifier

This page intentionally left blank.

Appendix P Glossary

TERM	DEFINITION
3PAO	A Third-Party Assessor (3PAO) is an organization that has been accredited to help cloud service providers and government agencies meet FedRAMP compliance regulations. The American Association for Laboratory Accreditation (A2LA) accredits a 3PAO that meets FedRAMP 3PAO requirements.
Access CDS	A type of cross domain solution (CDS) that provides access to a computing platform, application, or data residing on different security domains from a single device. (CNSSI 4009)
Application	The system or problem to which a computer is applied. (DoD Dictionary of Military and Associated Terms)
Approval to Connect (ATC)	A formal statement by the appropriate CAO granting approval for an information system to connect to a DoD network. (DoDI 8330.01)
Artifacts	System policies, documentation, plans, test procedures, test results, and other evidence that express or enforce the cybersecurity posture of the DoD IS, make up the A&A documentation (for RMF packages), and provide evidence of compliance with the assigned cybersecurity controls.
Authorization Decision Document (ADD)	An ATO, and IATT, or a DATO
Authorization Termination Date (ATD)	The date assigned by the AO that indicates when an ATO or IATT expires.
Authorization To Operate (ATO)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (CNSSI 4009)
Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (CNSSI 4009)

TERM	DEFINITION
Backside connection	An indirect physical extension of DODIN services, across a separate and distinct intermediate accreditation boundary, to a third party. (DoDI 8010.01)
Boundary Cloud Access Point (BCAP)	Boundary CAP (BCAP) is required to connect off-premises commercially owned and operated CSOs to the DISN (or another network). A BCAP will interconnect the network it protects with multiple CSP networks that offer private connectivity services. (See paragraph 5.10.1 of the CC SRG for the explanation of BCAP, ICAP, and IAP.) (CC SRG) DISN perimeter gateway that provides a barrier of protection between the DISN and the CSO. (DoD Cloud Cyberspace Protection Guide)
Circuit	Any line, conductor, or other conduit by which information is transmitted and represents the complete path between two terminals or users over which one-way or two-way communications may be provided. A dedicated circuit, private circuit, or leased line is a line that is dedicated to only one use or service (i.e., data, voice, video, etc.).
Cloud Access Point (CAP)	A capability that provides access to the commercial cloud, interface translations necessary for CSO compatibility, and supports boundary cyber defense by protecting the DISN from the commercial cloud. (DoDI 8010.01) A system of network boundary protection and monitoring devices (e.g., firewall, IPS, IDS, proxy, etc.), otherwise known as a Cybersecurity or IA stack, through which CSP infrastructure and networks will connect to the network the CAP protects. (CC SRG) "BCAP" and "ICAP" are each a type of Cloud Access Point.
Cloud Approval to Connect (CATC)	A formal statement by the DISN CAO that grants approval for a provisionally authorized CSO to connect to the DISN via a DISA BCAP. For a CSO that does not connect via the DISA BCAP the CATC serves as an acknowledgement that the CSO is registered in SNAP or SGS.

TERM	DEFINITION
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-145)
Cloud Deployment Model	A cloud computing system may be deployed privately or hosted on the premises of a cloud customer, may be shared among a limited number of trusted partners, may be hosted by a third party, or may be a publicly accessible service, i.e., a public cloud. Depending on the kind of cloud deployment, the cloud may have limited private computing resources, or may have access to large quantities of remotely accessed resources. The different deployment models present several tradeoffs in how customers can control their resources, and the scale, cost, and availability of resources. (NIST SP 800-146)
Cloud Information Technology Project (C-ITP)	An information technology project that uses a Cloud Service Offering to implement a DoD mission owner's information system, enclave, application, Defense Business System, National Security System, data set, or other information technology solution. (When registering the C-ITP in SNAP or SGS, recommend that the Mission Owner use the same name as the Unique Investment Identifier (UII)/Investment Name used in DITIP, SNaP-IT, DITPR, or SITR.) (Also see footnote 17)
Cloud Permission To Connect (CPTC)	A formal statement by the DISN CAO granting approval for a Mission Owner to connect a C-ITP to a provisionally authorized CSO via a DISA BCAP. The CPTC may be granted no longer than the period of validity of a C-ITP's ATO or ADD. Note: For a C-ITP connection to an IL2 CSO or DoD Component BCAP, the CPTC simply acknowledges that the C-ITP was successfully registered in SNAP or SGS.
Cloud Service Models	A cloud can provide access to software applications such as email or office productivity tools (the Software as a Service, or SaaS, service model), or can provide an environment for customers to use to build and operate their own software (the Platform as a Service, or PaaS, service model), or can provide network access to traditional computing resources such as processing power and storage (the Infrastructure as a Service, or IaaS, service model). (NIST SP 800-146)

TERM	DEFINITION
Cloud Service Offering (CSO)	Refers to a CSP's product or service offering. In other words, a CSO is the actual Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) solution available from a CSP. (CC SRG) The actual Infrastructure as a Service, Platform as a Service, or Software as a Service solution available from a CSP. (DoDI 8010.01)
Cloud Service Provider (CSP)	An organization, commercial or Private, that offers/provides Cloud Services. Unqualified use of the term refers to any or all Cloud Service Providers, DoD, or non-DoD. (CC SRG) Any or all DoD or non-DoD entities that offer one or more cloud services in one or more deployment models. A CSP might leverage or outsource services of other organizations and other CSPs (e.g., placing certain servers or equipment in third party facilities such as data centers, carrier hotels or collocation facilities, and internet network access points). CSPs offering Software as a Service may leverage one or more third party CSPs (e.g., for Infrastructure as a Service or Platform as a Service) to build out a capability or offering. (DoDI 8010.01)
Command Communications Service Designator (CCSD)	A unique identifier for each single DISN service including use connections, package system connections, inter-switch trunk connections, and VPN connections.
Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off-premises. (NIST SP 800-146)

TERM	DEFINITION
Conditional Provisional Authorization	A Conditional DoD PA includes conditions for using a CSP-CSO, for example: • A requirement to use a CSP-CSO in conjunction with another CSP-CSO(s). • A requirement to use the CSP-CSO only in a specific environment or configuration.
Connection	A physical (i.e., circuit) or logical (e.g., VPN) telecommunications path by which information is transmitted.
Connection Approval Process	Formal process for adjudication requests to interconnect ISs.
Consent to Monitor (CTM)	This is the agreement signed by the AO granting DISA permission to periodically monitor the connection and assess the level of compliance with cybersecurity policy and guidelines.
Continuous Monitoring	(1) Maintaining ongoing awareness to support organizational risk decisions. (2) Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions (CNSSI 4009)
Cross Domain Appendix (CDA)	In support of the A&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 ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)
Customer	There are two general types of DISN customers/partners: DoD and non-DoD customers. DoD customers are DoD Combatant Commands, Military Services and Organizations, and Agencies (DoD Component/), collectively referred to as “DoD Components.” Non-DoD customer include 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. and are collectively referred to as “Mission Partners.”

TERM	DEFINITION
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DoDI 8500.01)
Defense Business System	1. An information system, other than a national security system, operated by, for, or on behalf of the DoD, including financial systems, mixed systems, financial data feeder systems, and IT and cybersecurity (formerly IA) infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. (DoDI 8330.01) (10 U.S.C §2222.(i).(1).(A))
Defense Information Systems Network (DISN)	DoD's enterprise capability of DoD-owned and -leased telecommunications and computing subsystems, networks, and capabilities, centrally managed and configured by DISA, to provide an integrated network with cybersecurity, telecommunication, computing, and application services and capabilities (e.g., voice, video, teleconferencing, computing, imagery, satellite, and data services) for all DoD activities and their authorized Mission Partners. (DoDI 8010.01)
Defense Information Technology Investment Portal (DITIP)	A centralized location for IT investment portfolio data, is the authoritative data source for DoD IT Header information, and aligns IT systems information in the Defense IT Portfolio Registry (DITPR) with budget information in the Select and Native Programming Data Input System for IT (SNaP-IT). DITIP provides for the entry and maintenance of common DITPR and SNaP-IT data elements and supports the CMO defense business system (DBS) certification. Access to the Portal requires User registration and authentication. (Defense Information Technology Investment Portal (DITIP))
Defense Security/Cybersecurity Authorization Working Group (DSAWG)	The community forum for reviewing and resolving authorization issues related to the sharing of community risk. The DSAWG develops and provides guidance to the AOs for IS connections to the DoD Information Enterprise. (DoDI 8510.01)

TERM	DEFINITION
Demilitarized Zone (DMZ)	1. Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. 2. A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. 3. An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. (CNSSI 4009)
Denial of Approval to Connect (DATC)	A formal statement by the DISN C withholding (in the case of a new connection request) or rescinding (in the case of an existing connection) approval for an IS to connect (or remain connected) to the DISN.
Denial of Authorization to Operate (DATO)	An ADD issued if the AO determines the risk associated with an enclave is unacceptable.
DISA Risk Adjudication (DISA RE42)	The office in DISA that has authority to issue a CDSA or GCT, and to conduct risk assessments. Personnel in DISA Risk Adjudication also provide administrative support to the CDTAB and staff the DSAWG Secretariat.
DISN Backbone Connections	A connection, such as a trunk, between DISN elements that are under the operational direction and management control of DISA.
DISN CAO	Single point of contact within DISA for DISN connection approval requests.
DoD Component	The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense agencies, Department of Defense field activities, and all other organizational entities in the Department of Defense. (DoD Dictionary of Military and Associated Terms)

TERM	DEFINITION
DODIN	The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (DoD Dictionary of Military and Associated Terms)
Enclave	A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (CNSSI 4009) Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (DoDI 8330.01)
enterprise Cross Domain service (enterprise CD service)	An automated capability available to end users and hosted mission applications within an enterprise environment for information sharing across and among security domains utilizing one or more CDSs. (DoDI 8540.01)
Enterprise Cross Domain Service Provider (ECDSP)	An organization that establishes, manages, and maintains the overall infrastructure and security posture offering automated capabilities to users and applications within an enterprise environment for information sharing across and among security domains. (DoDI 8540.01)
Enterprise Cross Domain Solution (Enterprise CDS)	An Enterprise Cross Domain Solution (CDS) is a form of controlled interface device approved for use as a General Purpose or Mission Specific enterprise cross-domain services.
Enterprise Cross Domain Solutions (ECDS) Ticket or Request	An Enterprise CDS Ticket or Request is a CDS that represents a centrally managed service that supports multiple DoD Components.

TERM	DEFINITION
Enterprise Service	A service that is offered on a communications network by a single provider to all entities in the DoD Enterprise and is characterized by function performed, service provider, specific service offering, and scope of the enterprise served. (DoDI 8440.01)
FedRAMP	The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves cost, time, and staff required to conduct redundant Agency security assessments. (FedRAMP FAQs)
FedRAMP+	FedRAMP+ is the concept of leveraging the work done as part of the FedRAMP assessment and adding specific security controls and requirements necessary to meet and assure DoD's critical mission requirements. (CC SRG)
For Tracking Purposes Only (FTPO)	See "Minimal (Community) Impact"
General Purpose enterprise CDS	An enterprise-CDS available to all authorized users of connected networks with support for a broad range of data types.
GIG Interconnection Approval Process (GIAP)	Electronic process to submit connection information and register a DODIN connection.
IC Owned Cross Domain Solution	An IC Owner CDS is one that an intelligence agency owns, approves, and manages. Only IC CDSs connected to DoD networks that do not also connect to a TS-SCI network are referenced in this connection process guide for visibility and reciprocity purposes.
Information Assurance (IA)	Superseded by "Cybersecurity" IAW DoDI 8500.01
Impact Level	Cloud security impact levels are defined by the combination of 1) the sensitivity or confidentiality level of information (e.g., public, private, classified, etc.) to be stored and processed in the CSP environment; and 2) the potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information. (See CC SRG paragraph 3 for details)

TERM	DEFINITION
Impact Level 2	**Non-Controlled Unclassified Information** Level 2 includes all data cleared for public release (i.e., as well as some low confidentiality unclassified information NOT designated as Controlled Unclassified Information (CUI) or critical military/contingency operations mission data, but the information requires some minimal level of access control (e.g., user ID and password). Access to the CSO is via the Internet. (See CC SRG for details)
Impact Level 4	**Controlled Unclassified Information:** Level 4 accommodates CUI and/or other mission critical data to include that used in direct support of military or contingency operations. (See CC SRG for details)
Impact Level 5	**Controlled Unclassified Information:** Level 5 accommodates CUI that may require a higher level of protection than that afforded by Level 4 as deemed necessary by the information owner, public law, or other government regulation. The determination if CUI fits this category is up to the AO responsible for categorizing the information and choosing the Cloud Impact Level. (See CC SRG for details)
Impact Level 6	**Classified Information up to SECRET:** Level 6 accommodates information that has been determined: "(i) pursuant to EO 12958, *Classified National Security Information* (April 17, 1995) as amended by EO 1329227, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, (P.L. 83-703)28 to be Restricted Data (RD)." (See CC SRG for details)
Information Security Risk Management Committee (ISRMC)	This body, supported by the DSAWG, is the DoD "risk executive (function)" as described in NIST SP 800-37 and NIST SP 800-39. (DoDI 8510.01)
Information System (IS)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C. Sec 3502) Note: ISs also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (CNSSI 4009)

TERM	DEFINITION
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. ((CNSSI 4009; 40 U.S.C. Sec. 11101-adapted; 40 U.S.C. Sec. 1401-(adapted))
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (NIST SP 800-145)
	IATC Removed
Interim Approval to Test (IATT)	Temporary authorization to test an information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization. (CNSSI 4009)

TERM	DEFINITION
Internal Cloud Access Point (ICAP)	An ICAP is a DISN boundary consisting of a Cybersecurity stack which protects the DISN (or other network) or the datacenter network to which the CSO is connected (inside / protected side of the boundary) from, and provides detection of, unauthorized network access from the CSP's infrastructure (outside / unprotected side of the boundary), externally connected CSO management plane, CSP corporate networks, CSP connections to the Internet, and from compromised Mission Owner systems/applications and virtual networks. Typically, one ICAP is required for each physical CSO infrastructure instance. Impact Levels 2/4/5: Internal CAPs (ICAPs) will be implemented for on-premises commercially owned and operated CSO connectivity to the DISN, if the CSO management plane has connectivity to external networks that bypasses native NIPRNet enclave and external boundary protections. (CC SRG) (See paragraph 5.10.1 of the CC SRG for the explanation of BCAP, ICAP, and IAP.)
Internet Access Point (IAP)	Approved connections from the internet to the NIPRNet that provides common enterprise security services for all DoD Components, including Enterprise Email Security Gateway, access controls, network firewall protections, intrusion detection sensors, and other transport-layer security services. (See paragraph 5.10.1 of the CC SRG for the explanation of BCAP, ICAP, and IAP.) (DoDI 8010.01)
Internet Protocol (IP)	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (CNSSI 4009)
Investment	With the exception of Defense Business Systems, Major Automated Information Systems, Approved Data Services, and programs, projects and activities exempted by DoD 7000.14-R, investments can be systems, programs, projects, organizations, activities, or grouping of systems with related functionality. (DoD 7000.14-R DoD Financial Management Regulation)

TERM	DEFINITION
Joint Worldwide Intelligence Communications System (JWICS)	Provides a secure high-speed multimedia communication service between TS/SCI users designed to support the DoD Intelligence Information System community through the Defense Intelligence Agency (DIA) Regional Support Center and supports DoD's efficiency initiatives using an IP-based infrastructure. The DISA TS/SCI IP Data Service provides wide area network transport services for JWICS. (See the Defense Intelligence Agency, "Network Connection Policy for Joint Worldwide Intelligence Communications System," January 1995.)
Long-Haul Telecommunications	All general and special purpose long-distance telecommunications facilities and services (including commercial satellite services, terminal equipment, and local circuitry supporting the long-haul service) to or from the post, camp, base, or station switch and/or main distribution frame (except for trunk lines to the first-serving commercial central office for local communications services) (DFARS Subpart 239.7401)
Meet-Me Point	A DISN Point-of-Presence (PoP) located in a carrier agnostic commercial network interconnection facility or commercial carrier's collocation facility. This PoP minimally consists of a high-capacity router but may include DISN boundary protection capabilities that constitute all or part of the BCAP Cybersecurity stack. The purpose of the BCAP Meet-Me Point is to facilitate the interconnection of the DISN BCAP with multiple CSP networks. (CC SRG)
milCloud 2.0	milCloud® 2.0 connects commercial cloud service offerings to Department of Defense (DoD) networks, in a private deployment model to provide DISA mission partners the latest cloud technology at competitive prices without compromising security or performance. milCloud 2.0 Portal
Minimal (Community) Impact CDS	A CDS that poses a minimal risk to DODIN. For example, a CDS with no DODIN connectivity, encrypted tunneling, or data flow isolation may have Minimal (Community) Impact. (DoDI 8540.01)
Mission Owner (MO)	Entities such as IT system/application owner/operators or program managers within the DoD Components/Agencies responsible for instantiating and operating one or more ISs and applications who may leverage a CSP's CSO in fulfilment of IT missions. (CC SRG)

TERM	DEFINITION
Mission Partner	Those with whom DoD 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. (DoDD 8000.01)
Mission specific enterprise-CDS	A CDS deployment that is available to a select community [e.g., signals intelligence (SIGINT), geospatial intelligence (GEOINT), Maritime] with a limited set of data types and domains. An enterprise-CD-service may qualify as one or both types of cross domain service
Multi-level CDS	A type of cross domain solution (CDS) that uses trusted labeling to store data at different classifications and allows users to access the data based upon their security domain and credentials. (CNSSI 4009)
National Cross Domain Strategy and Management Office (NCDSMO)	Office for centralized coordination and oversight of all cross-domain initiatives across the DoD and the IC.
National Security System	(A) Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which— (I) involves intelligence activities. (II) involves cryptologic activities related to national security. (III) involves command and control of military forces. (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B) Subparagraph (A) (i) (V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (CNSSI 4009 and 44 U.S.C. SEC 3542 (b)(2))

TERM	DEFINITION
Off-Boarding	The set of activities that take place when a Mission Owner terminates use of a CSO. This process is required when a Mission Owner migrates to a new cloud service, a mission reaches end of life, a contract ends, or a CSO ceases operations. The off-boarding process is split into two stages: 1- data retrieval/migration and 2- data sanitization or destruction. (CC SRG)
off-premises	A facility (building/container) or IT infrastructure is off-premises if it is NOT physically or virtually on DoD owned or controlled property (i.e., on-premises physically or virtually). (CC SRG)
Onboarding	Onboarding is the set of activities that take place when a Mission Owner migrates a C-ITP to a provisionally authorized CSO.
on-premises	A facility (building/container) or IT infrastructure is on-premises if it is physically on DoD owned or controlled property. That is, it is within the protected perimeter (walls or "fence line") of a DoD installation (i.e., Base, Camp, Post, or Station (B/C/P/S) or leased commercial space) which is under the direct control of DoD personnel and DoD security policies. (CC SRG)
Plan of Action & Milestones (POA&M)	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (CNSSI 4009)
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (NIST SP 800-145)
Platform Information Technology	IT, both hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems. (DoDI 8500.01)

TERM	DEFINITION
Platform Information Technology System	A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. (DoDI 8500.01)
Point-to-Point CDS	A Cross Domain Solution purchased, implemented, and managed within the authorization boundary of the organization's own network. Point-to-Point CDS are CDS that are owned and operated by an organization that cannot use an ECDSP.
Point-to-Point Connection	A dedicated circuit that uses DISN transport but does not connect to NIPRNet, SIPRNet, or DSN
PPSM Category Assurance List	Summary reference used for implementing and promoting the standardization and management of PPS used on DODIN (DoDI 8551.01)
Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple Mission Owner s (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on-premises or off-premises. (NIST SP 800-145)
Program Manager	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (CNSSI 4009)
Provisional Authorization (PA)	A pre-acquisition type of Risk Management Framework IS authorization used by DoD and FedRAMP to pre-qualify Commercial CSOs to host Federal Government and/or DoD information and ISs. PAs are to be used by Federal and DoD Cloud Mission Owners during source selection and subsequent system authorization under RMF. (CC SRG)
Reciprocity	Mutual agreement among participating enterprises to accept each other's security assessments to reuse information system resources and/or to accept each other's assessed security posture to share information. (CNSSI 4009)

TERM	DEFINITION
Repeatable CDS	An instantiation of a CDS that has the same specific mission; the same hardware, software, and configuration; identical data types, filters, and flows; the same classification levels and information networks, which may include different enclaves; a matching risk environment; a proliferation control plan; and a tracking methodology for instantiations. (DoDI 8540.01)
Risk Management Framework (RMF)	A structured approach used to oversee and manage risk for an enterprise. (CNSSI 4009)
Security Assessment Plan	Provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. (DoDI 8510.01)
Security Assessment Report (SAR)	Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls. (DoDI 8510.01)
Security Domain	A domain that implements a security policy and is administered by a single authority. (CNSSI 4009)
Select and Native Programming Data Input System for Information Technology (SNaP-IT)	The electronic system used by the DoD CIO to collect IT Budget and Cyberspace Operations Budget data and generate reports mandated by the Office of Management and Budget and Congress. (DoDI 5000.76) The DoD CIO operates the SNaP-IT system. Additional SNaP-IT guidance can be located within the (DoD 7000.14-R, DoD Financial Management Regulation Volume 2B, Chapter 18) or within annual budget guidance issued by OUSD(C), OSD CAPE, and DoD CIO.

TERM	DEFINITION
Significant Change	A change that is likely to substantively affect the security or privacy posture of a system. Significant changes to a system that may trigger an event-driven authorization action may include, but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) changes in information types processed, stored, or transmitted by the system; or, (vi) modifications to cryptographic modules or services; or (vii) modifications to security controls. Significant changes to the environment of operation may include but not limited to: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations. The examples of changes listed above are only significant when they represent a change that is likely to affect the security and privacy posture of the system. (NIST SP 800-37) From the DoD perspective significant changes may include: • Deployment of a Cross Domain Solution • Deployment of a UC product enhancing the capability of the enclave (i.e., Voice over IP (VoIP), Voice over Secure IP Classified Voice, Video over IP, even if the application is accredited by the enclave AO • Rehoming of an authorized enclave to a new DEMARC, such as moving to a new facility where a new CCSD(s) is issued by DITCO, unless the Telecommunications Service Order (TSO) states that the authorization will transfer • Deployment of an on-premises Cloud Service Offering within the enclave • New Contract Vendor.
SIPRNet GIAP System (SGS)	The system on SIPRNet used to register, track, and manage SIPRNet connections for classified data services, VPN services, and Cross Domain Solutions.
SNAP	The system on NIPRNet used to register, track, and manage DISN connections used for unclassified voice, video, data, cloud services, and non-DISN solutions.

TERM	DEFINITION
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (NIST SP 800-145)
Sponsor	DoD Component that advocates a mission requirement to connect a Mission Partner (non-DoD organization) information system to the DISN.
System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See Information System (IS). (CNSSI 4009)
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. (NIST-SP 800-18)
Tactical CDS	A CDS deployment that operates in austere environment conditions or operates in environments where terrestrial communications are not possible, reliable, or survivable. Austere environment conditions include combat and related land, sea, or air vehicles. (P2P CDS Supporting Documentation (see ECDS P2P Tactical Criteria))
Telecommunications Service Request (TSR)	Telecommunications requirement prepared IAW chapter 3, DISAC 310-130-1 and submitted to DISA or DISA activities for fulfillment. A TSR will not be issued except by a specifically authorized Telecommunications Certification Office (TCO).
TIBI	This DISA application provides DISN customers the ability to see up-to-date Telecom and IT inventory and billing information. TIBI is a web-based tool that provides current and historical information for Telecom and IT services. This capability allows DISA's Mission Partners to monitor closely their services, inventory, and charges incurred.
Transfer CDS	A type of cross domain solution (CDS) that facilitates the movement of data between information systems operating in different security domains. (CNSSI 4009)
Trunk	A high-speed, high-capacity digital line that carries numerous signals or circuits between major switching centers or nodes using various multiplexing techniques in a communications system such as a long haul or wide area network.

TERM	DEFINITION
Unified Capabilities (UC)	The integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities. (DoDI 8100.04)
Unique Investment Identifier (UII)	1. Previously called a "BIN", the UII is a database index field automatically generated with the DITPR/SNaP-IT interface when registering or creating a new investment. (DoD 7000.14-R DoD Financial Management Regulation) 2. Unique Investment Identifier (UII) refers to a persistent numeric code applied to an investment that allows the identification and tracking of an investment across multiple FYs of an agency's investment portfolio. The UII is composed of a three-digit agency code concatenated with a nine-digit unique investment number generated by the agency. (OMB FY14 Guidance on Exhibits 53 and 300- Information Technology and E-Government
Universal System Identifier (USI)	A unique identifier assigned by SNAP when registering a DNS voice switch in SNAP.
Virtual Private Network (VPN)	Protected information system link utilizing tunneling, security controls (see information assurance (IA)), and endpoint address translation giving the impression of a dedicated line. (CNSSI 4009)
virtually on-premises:	IT infrastructure located in a physically off-premises location such as a Federal Government or commercial data center (i.e., facilities under the direct control of non-DoD personnel using non-DoD security policies) may be considered virtually on-premises under specific conditions. These conditions apply certain physical security controls and extend the DISN accreditation boundary. In essence this construct virtually extends the DoD protected perimeter or "fence line" around the infrastructure. (CC SRG)

Notes

DISN CONNECTION PROCESS GUIDE

Defense Information Systems Agency
Risk Adjudication and Connection (RE 4)
Post Office Box 549
Fort Meade, Maryland 20755-0549
https://cyber.mil/connect/connection-approval/

DCPG Version 6.1 ***2023***