A Combat Support Agency

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

Version 5.1
September 2016

Defense Information Systems Agency
Risk Management Executive (RME)
Risk Adjudication and Connection Division (RE4)
Post Office Box 549
Fort Meade, Maryland 20755-0549
http://disa.mil/connect

This page intentionally left blank.

EXECUTIVE SUMMARY

This Defense Information Systems Network (DISN) Connection Process Guide (CPG) (ref am) uses the information contained in references (a) through (an) to implement the requirement identified in Department of Defense Instruction (DoDI) 8500.01 *Cybersecurity* (ref a) for the Director, Defense Information Systems Agency (DISA), to oversee and maintain the connection approval process. CJCSI 6211.02D *Defense Information System Network (DISN): Responsibilities* (ref b) states that all connections to the DISN shall be in accordance with this DISN CPG. The goal of the DISN CPG is to provide a transparent, user-friendly, and agile process that will help the warfighter and DoD Components, as defined in directive DoDD 8000.01, *Management of the Department of Defense Information Enterprise* (ref c) efficiently obtain their necessary DISN connection approvals while ensuring DISA effectively tracks and manages DISN connections.

There are numerous key DoD policies either recently released or currently under revision that affect or will affect the DISN CPG. The recently released DoDI 8510.01 *Risk Management Framework (RMF) for DoD Information Technology (IT), Change 1* (ref d) requires the transition from the DoD Information Assurance Certification and Accreditation Process (DIACAP) to the DoD RMF. Another key policy is the extensively revised DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)* (ref e) and DoDI 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD* (ref f), DoDI 8540.01, *Cross Domain (CD) Policy* (ref ad), DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* (ref k). Another new DoD policy on the horizon impacting the DISN CPG is the draft: DoDI 8010.dd, *DoD Information Network Transport;* As new policies become official, the Risk Adjudication and Connection Division will continue to update the DISN CPG accordingly. However, until then, the DISN CPG will only reference current signed policy.

This Release of the DISN CPG:

- Incorporates comments received from the Joint Staff J6 and the Unified Cross Domain Services Management Office (UCDSMO)
- Reflects DISA's reorganization
- Adds detailed NIPRNet Federated Gateway connection approval flow diagram
- Updates references
- Removed the content of Appendix G, DODIN Waiver Process, pending DoD CIO announcement of an updated process.

Please send DISN CPG Version 5.1 improvement comments directly to the Connection Approval Office at disa.meade.ns.mbx.ucao@mail.mil or disa.meade.ns.mbx.ccao@mail.mil.

This guide is approved for public release and is available on the Internet from the DISA website at http://disa.mil/connect. The instructions in this guide are effective immediately.

SIGNATURE PAGE FOR KEY OFFICIALS

Approved by:

HEIN.MATTHEW.A.1101454327

Digitally signed by HEIN.MATTHEW.A.1101454327
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DISA, cn=HEIN.MATTHEW.A.1101454327
Date: 2016.09.09 14:08:25 -04'00'

Matthew A. Hein
Chief, Risk Adjudication and Connection Division

Date

REVISION HISTORY

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

Version	Date	Comments
3.0	May 2010	Baseline document released based on stakeholder input and extensive reformatting.
3.1	April 2011	Administrative changes to incorporate current policy and correct errors.
3.2	May 2011	Updated telephone numbers due to DISA BRAC relocation to Ft. Meade, MD.
4.0	June 2012	Major document layout changes. Document divided into Customer Type/Connection Type sections for ease of use. Several process updates. E-mail address updates due to Defense Enterprise E-mail (DEE) migration. Private IP (Layer 2/3 VPN) registration in System Network Approval Process (SNAP) was added. Included several Frequently Asked Questions (FAQs) into appendices.
4.1	September 2012	Incorporated Defense Security/Cybersecurity Authorization Working Group (DSAWG} clarifications in several areas. Includes updated Cross Domain Solutions (CDS) process flow chart. Updated NIPR e-mail addresses due to Enterprise e-mail changes.
4.1.1	October 2012	Added DAA/AO Appointment letter statement in Sections 3-6. Updated SIPR e-mail addresses due to Enterprise e-mail changes.
4.2	January 2013	Changed document title to DISN CPG. Added footer and header section titles. Updated NSC NIPR mailboxes. Added content to Executive Summary. Added new content and updated current processes resulting on SIPRNet Global Information Grid (GIG) Interconnection Approval Process (GIAP) System (SGS) 5.3 release on 3 Jan 13.
4.3	May 2013	Updated Section 3.5 to reflect CAP Policy. Added VPN Registration (Private IP) Process Guide. Added Section “CDS Repeatable Accreditation”. Updated Customer Connection Process Charts.
4.3.1	November 2013	Added preliminary questions to answer regarding respective enclave/system before submitting a DoD CIO temporary exception to policy request. Defined “Type Accredited Systems.” Changed “1st Validation Official” title to “DISN Classified IP Lead.” Includes the process for Notification of Discontinued or Cancelled Circuits. Finally updated Appendix D Remote Compliance Monitoring. Revised Appendix D (Scan Section). Updated the Vulnerability Scanning Section, scan types, and the

		FAQs. Changed Figure 1 title to "DISN Connection Overview." Changed the "Review and Issue/ATC" block in Figure 1 to "Connection Approval Process." Changed "GIG" to "DODIN" throughout the entire document. Changed Telecommunications Service Order (TSO) to In-Effect Report (IER)
5.0	November 2014	Provided connection approval requirement information related to the DIACAP to RMF transition. 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 NIPRNet Federated Gateway (NFG), SIPRNet Releasable De-Militarized Zone (REL DMZ), and SIPRNet Federal DMZ (FED DMZ). Removed previous language regarding the Connection Approval Office performing risk assessments. Added guidance on the requirements to update SNAP/SGS POCs. Updated NSC Remote Compliance Monitoring (RCM) scanning procedures. Added DoDI 8551.01, Ports, Protocols, and Services Management (PPSM) declaration requirement (ref e). 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 ▪ ATC renewal with continuous monitoring ▪ SIPRNet FED DMZ update ▪ NIPRNet Federated Gateway connection process ▪ JRSS Accreditation ▪ References the Cloud Computing Connection Guide ▪ Cyber Hygiene Analysis (CHA) ▪ Virtual Private Network (VPN) registration ▪ Initial Connection scans ▪ CDS Approval Process update ▪ References are updated ▪ Transition from TDM to IP-based solutions ▪ Revised timeline for transition to RMF (DoDI 8510.01, change 1) ▪ Incorporates DSAWG member recommendations

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page intentionally left blank.

SECTION 1: INTRODUCTION

1.1 Purpose

Cybersecurity is one of our Nation's most serious economic and security challenges that requires all elements of the Federal government to work together. Securing the Department of Defense Information Networks (DODIN) plays a vital role toward achieving these National objectives, providing secure connections to the DISN (DISA's provided portion of the DODIN), and is an important element of DoD's Risk Management Framework (RMF). This DISA DISN Connection Process Guide (CPG) (ref am) provides DoD and DoD Components the structured procedures and points of contact necessary to connect to the DISN. Stated simply, our combined connection approval actions significantly influence the cybersecurity of the DODIN. Together we must take this responsibility seriously and perform the necessary due diligence to ensure all the appropriate policies, procedures, and guidelines are followed.

1.2 Authority

The DISN Connection Process Guide (CPG) (ref am) derives its authority from DoDI 8500.01, *Cybersecurity* (ref a), DoDI 8510.01, *Risk Management Framework for DoD Information Technology (IT)* C, CJCSI 6211.02D, *Defense Information System Network (DISN): Responsibilities* (ref b), DoDI 8100.04, *DoD Unified Capabilities (UC)* (ref g), and DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)* (ref e), DoDD 5105.19, *Defense Information Systems Agency* (ref v), DoDD 5144.02, *DoD Chief Information Officer* (ref w), and DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* (ref k).

1.3 General Guidance

The CPG is a living document that continues to evolve as connection processes for new and existing networks/services are refined and as additional networks/services become available. This version of the CPG focuses on connections to the DISN as detailed below. Future versions of the CPG will cover DISA's ever-evolving capabilities such as the Cloud Computing connection process.

Use the DISN CPG often to help get through the connection process. However, before employing this guide, always check for the current version on our website at: http://disa.mil/connect.

DISN networks/services and controlled processes addressed in this guide are included in Table 1. Additional information about DoD enterprise services is at: http://www.disa.mil/.

Current DISN Network Services	Examples
Content Delivery	Global Content Delivery Service (GCDS)
Data Services	Sensitive but Unclassified IP Data Service (aka, NIPRNet), Secret IP Data Service (aka SIPRNet), Top Secret/Sensitive Compartmented Information (TS/SCI) IP Data Service (aka JWICS), Multicast
Dedicated Transport Services	N/A
Virtual Private Network (VPN) Services	Common Mission Network Transport (CMNT), DISN Test and Evaluation Service, Joint Information Environment (JIE) – Joint Regional Security Stack (JRSS) Community of Interest (COI) VPN service, Label Transport Service, Medical Community of Interest (MEDCOI) VPN, Private Data Internet Service Provider, Private IP Service
Voice Services	Sensitive but Unclassified Voice Service, Voice over secure IP (VOSIP), TS SCI voice service, Multilevel secure voice, Voice Internet Service Provider (ISP) - Public Switched Telephone Network (PSTN) Access.
Satellite Communications Services	Commercial Satellite Services, Distributed Tactical Communications System (DTCS), Enhanced Mobile Satellite Service (EMSS), Inmarsat.
Cross Domain Enterprise Services	Provides boundary applications to enhance security

Table 1: DISA Enterprise Services addressed in this Guide

1.4 Applicability

This guide applies to all DoD Component and Mission Partner enclave owners seeking to connect to the DISN. The *"DISN"* is defined in various documents and most recently in Joint Publication 1-02 *Department of Defense Dictionary of Military and Associated Terms* defines the DISN (ref h) as the *"Integrated network, centrally managed and configured to provide long-haul information transfer services for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services."* For the purposes of this document, the *DISN CPG* is only referring to DISA's provided portion of DODIN transport. The "*DODIN*" is defined by Joint Publication 3-12, *Joint Cyberspace Operation* (ref i) as *"the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security."* For a discussion of "*enclaves*," refer to DoDI 8500.01, *Cybersecurity* (ref a). For definition of "*enclave*," refer to Committee on National Security Systems Instruction Number 4009, *National Information Assurance (IA) Glossary* as amended (ref j). For a definition of *"Mission Partner,"* refer to DoDD 8000.01, *Management of the Department of Defense Information Enterprise* (ref c).

SECTION 2: DISN CONNECTION PROCESS OVERVIEW

2.1 Process Overview

The DISN CPG is a step-by-step guide that outlines procedures DISN customers (DoD Components and Mission Partners) must follow to obtain and retain enclave connections to the DISN. The guide consolidates the connection processes for DISN networks and services into one document, helps customers understand connection requirements and timelines, and provides contacts for assistance throughout the process. The Risk Adjudication and Connection Division is not the process owner for all the elements that comprise DoD's and DISA's requirements for establishing a DISN connection. Functions such as: Request Fulfillment (RF), Acquisition, Provisioning, Design and Testing, Assessment and Authorization (A&A) under the new RMF or Certification and Accreditation (C&A)[1] under DIACAP are performed by other offices. The DISN CPG focus is on the DISN Connection Approval Process (CAP) and where appropriate point customers to appropriate information services, websites, or offices wherever possible to help guide customers through other related processes. For example, request fulfillment (see paragraph 2.1.3) is provided by DISA Global Operations Command; Assessment and authorization of enclaves (2.2.3) is accomplished by the customer; DISA Infrastructure Engineering (IE) in collaboration with the customer determines the appropriate DISN service (3.1); Department of Defense Chief Information Officer (DoD CIO) validates the mission requirement for Mission Partner connections to DISN (3.5.2-3.5.4), and the customer accomplished the A&A for the customer network enclave being connected to DISN (2.1.4).

2.1.1 DISN Customers

There are two general types of customers/partners that connect to the DISN to utilize its networks/services: DoD and non-DoD. DoD customers are DoD Combatant Commands, Military Services and Organizations, and Agencies (DoD CC/S/A/), collectively referred to as "DoD Components." DoD customer enclaves include ISs or Platform Information Technology (PIT) systems that are developed jointly by DoD Components and Mission Partners, comprise DoD and non-DoD ISs, or contain a mix of DoD and non-DoD information consumers and producers (e.g., jointly developed systems, multi-national or coalition environments, or first responder environments) in accordance with DoDI 8500.01 (ref a). Non-DoD customers include: 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) and are collectively referred to as "Mission Partners."

[1] The transition to RMF introduces new terms. Under RMF systems undergo "Assessment and Authorization (A&A)" whereas under DIACAP terminology they undergo "Certification and Accreditation (C&A)" both RMF and DIACAP terms are used in this document reflecting the transition in terminology in accordance with DoDI 8510.01 (ref d).

In order to connect to the DISN, Mission Partners must have a validated requirement approved by a sponsoring CC/S/A or field activity headquarters and validation of the mission requirement from the DoD CIO in accordance with CJCIS 6211.02D (ref b). In addition, all DISN customer information systems will be aligned to DoD network operations and security centers (NOSCs). The NOSC and supporting cybersecurity service provider(s) will provide any required cybersecurity services to aligned systems in accordance with CJCSI 6211.02D,(ref b), DoDI 8530.01 (ref k), DoDI O-8530.01M (ref l), and the DoD CIO Memo on DoD Sponsor Responsibilities (ref m)[2]. Applicable issuances, Defense Finance and Accounting Regulations (DFAR), and requirements must be codified in an appropriate agreement (e.g., MOA or contract. Responsibilities of DoD sponsors are defined in several OSD and Joint Staff issuances.

2.1.2 DISN Networks/Services and Connections

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

2.1.3 Request Fulfillment

Customers requiring a new connection to the DISN and its services must use the DISA Direct Order Entry (DDOE) request fulfillment process to initiate the provisioning requirement and circuit activation (go to: https://www.disadirect.disa.mil/products/asp/welcome.asp for further information and guidance). The Telecommunications Service Request (TSR) and In-Effect Report (IER) processes involve the ordering, engineering, acquisition, and installation of the circuit and equipment necessary to connect to the DISN. Request fulfillment may only be initiated by a DoD entity. A DoD CC/S/A entity may elect to sponsor a Mission Partner, but the DoD sponsor remains responsible for all request fulfillment actions to include but not limited to completing and/or assisting the Mission Partner with A&A requirements. See the DoD CIO Sponsor Memorandum (ref m).

2.1.4 Assessment and Authorization

All enclaves connecting to the DISN require Assessment and Authorization (A&A) in accordance with an appropriate and acceptable process. For new and additional connections, the A&A process should be initiated in parallel to or soon after beginning the request fulfillment process. For reauthorizations, the customer should initiate enclave reauthorization actions with sufficient time prior to expiration of the current authorization and connection approval to prevent a potential circuit disconnect. Expiration notices are sent to the POCs for the subject enclave every 30 days starting 90 days prior to the expiration. For Out Of Band (OOB) point to point connections the Command Communications Service Designator (CCSD) and IER information will be uploaded in System Network Approval Process (SNAP) and SIPRNet Global Information Grid (GIG) Interconnection Approval Process (GIAP) System (SGS) as applicable.

---

[2]In 2012, DoD CIO issued a memo summarizing DoD sponsor responsibilities. Several of the issuances cited in this memo have been reissued but still are applicable. DoD sponsors are strongly encouraged to consult the current version of the issuances cited in the memo for additional details.

Additionally, the OOB connection will not have an expiration date. DoD Components and Mission Partners must ensure that all SNAP and SGS POC fields are maintained in an up-to-date and accurate status of the enclave at all times.

DoD Combatant Commands/Service/Agency/Field Activities (CC/S/A/FAs) must execute the RMF or DIACAP process in accordance with DoDI 8510.01 (ref d). For Mission Partners and defense contractors, the appropriate A&A process (i.e., RMF, DIACAP, NISPOM, NIST, DCID, etc.) depends on the type of customers and the network/service to be accessed. At the completion of the A&A process, the AO or Chief Information Officer (CIO) issues an authorization decision in the form of an Authorization to Operate (ATO), Authorization to Operation with conditions, or Interim Authorization to Test (IATT). Please note that under the RMF process there are no IATOs. Before a DISA DISN Approval to Connect (ATC) or Interim ATC (IATC) can be issued a number of documents are required depending on whether a connection request is a DoD RMF or DIACAP package[3]. For a RMF package these documents include the RMF Security Assessment Report (SAR), the System Security Plan (SP), Systems Enterprise and Information Security Architecture (system security design document or topology), plus the CTM and POA&M. For a DIACAP package these documents include the signed DIACAP Scorecard, System Identification Profile (SIP), Consent to Monitor (CTM), detailed topology, and Plan of Actions and Milestone (POA&M). Mission Partners require additional documentation addressed later in the CPG.

2.1.5 Connection Approval Office

The Connection Approval Office (CAO) is responsible for maintaining the information repository for exceptions to DISN policy on behalf of DoD CIO. The CAO also receives requests for DISN services that may involve a higher level of risk to the DISN than the CAO is authorized to accept. These requests are referred to the Defense Security/Cybersecurity Authorization Working Group (DSAWG). Additionally, the CAO works in concert with the DoD CIO to review and concur / non-concur with requests for exception to DISN policy.

2.1.6 Connection Approval Process Package

Connection requests are sent to the CAO in the form of a Connection Approval Process (CAP) package. These packages provide the CAO the information necessary to make the connection approval decision. The baseline requirements for what must be included in the CAP package depend on whether the customer is DoD or non-DoD and whether the connection is new or due for reauthorization. There may also be additional requirements, depending on the specific DISN network/service the customer needs to access. The DISA CAO will follow DoD CIO provided guidance regarding the DIACAP to RMF transition timeline and instructions for all DISN CAP packages.

[3]An IATC is normally granted for no more than 180 days. IATCs may be granted for up to one year for units deployed in the CENTCOM AOR

2.1.7 Compliance Assessment

As an integral part of the connection approval process, the CAO conducts an initial compliance assessment of a new or reauthorization connection to the DISN. Compliance assessments are based on the level of customer adherence with DoD CIO governance (e.g., DoDI 8510.01 (ref d)), DISA Security Technical Information Guides (STIGs), Security Requirements Guides (SRGs) and on-site and remote compliance monitoring and vulnerability assessment scans, DSAWG/DoD Information Security Risk Management Committee (ISRMC) decisions, etc.

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

2.1.8 Connection Decision

After the CAP package is reviewed and a compliance assessment conducted, the CAO makes a connection decision and notifies the DoD Component or Mission Partner. DoD Components or Mission Partners approved for connection to the DISN are granted either an ATC or an IATC, which are normally assigned an expiration date to coincide with the Authorization Termination Date (ATD) of the ATO. In the event of a non-compliant assessment for a new connection, the CAO will work with customers to address the matter until the concern is downgraded or mitigated allowing the issuance of an ATC or IATC.

2.2 Initiating the DISN Connection Approval Process

The process for network/service request fulfillment and approval of a connection to the DISN or service varies depending on:

- Whether the customer is a DoD Component or a Mission Partner
- Whether the request is for a new connection or a reauthorization
- What network/service is being accessed. When requesting network/service the request fulfillment and approval of a connection to the DISN or service, the process varies depending on customer type and customer requirements

Based on these determinations, the customer initiates the connection request using the appropriate process as described in section 3 and the appendices of this guide. The appendices also include the DoD CIO temporary exception to policy process, templates, POC tables, references, and glossary.

SECTION 3: CUSTOMER CONNECTION PROCESS

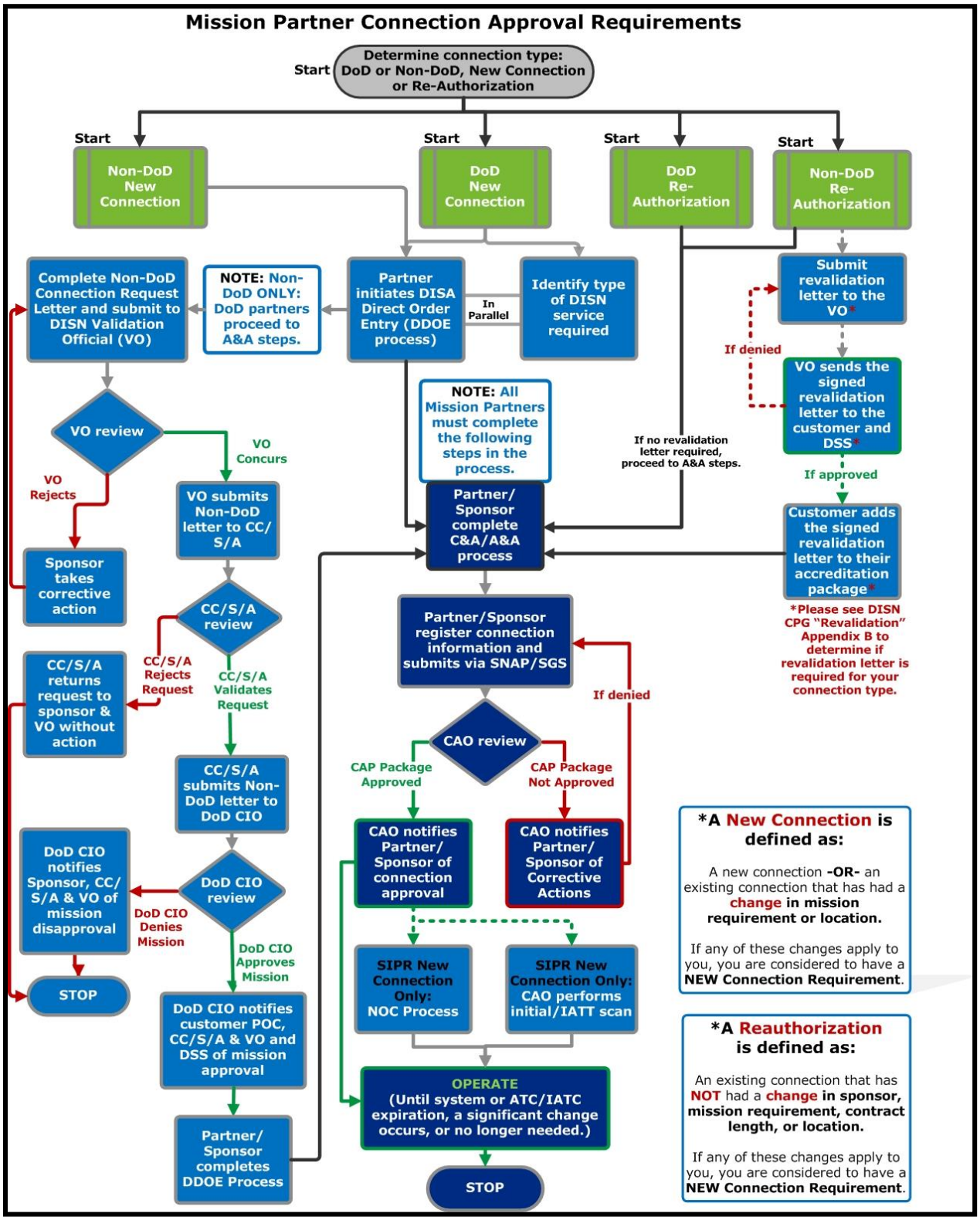

Figure 1: Customer Connection Requirements

3.1 Identify the Type of DISN Network/Service Required

Once the customer determines whether this is a new connection requirement or reauthorization of an existing connection, the next step is to identify the DISN network/service that is required. This involves matching customer needs to the most appropriate DISN network/service. All customers desiring connections to the DISN must first confirm with the DISN Validation Official that the desired network/service is appropriate for the mission. Customers who are not sure which network/service best meets their needs should review the description of DISN voice, video, and data services available at https://www.disadirect.disa.mil/products/asp/welcome.asp and/or contact the DISN Customer Contact Center (DCCC). The DCCC will facilitate contact with the appropriate DISN Validation Official.

DISN Customer Contact Center (DCCC)	
Unclassified E-mail	disa.dccc@mail.mil
Classified E-mail	disa.scott.conus.mbx.dccc@mail.smil.mil
Phone (Commercial)	844-347-2457, Option 2 or 614-692-0032, Option 2
Phone (DSN)	312-850-0032, Option 2

Table 2: DISN Customer Contact Center (DCCC)

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

3.2 Customer Initiates DISA Direct Order Entry (DDOE) Process

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

After the appropriate network/service is identified and applicable approvals are received, the customer initiates a request for service fulfillment through the DDOE process on the DISA direct website listed above. This is the ordering tool for DISN Telecommunications Business Services guide. If a circuit is ordered, DISA has a specified time to provide circuit delivery. Customers should utilize the below timelines for planning purposes when ordering circuits to minimize the time between delivery of circuit and activation of the circuit. Once a circuit is delivered, whether the customer is ready for use or not, the billing of the circuit will commence within 72 hours of delivery. The circuit should only be ordered when the customer is within the below appropriate specified time-line of completing all required actions otherwise, the circuit should not be ordered.[4]

[4]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) objectives by optimizing use of IP based network infrastructure. Legacy circuits should transition to existing IP bandwidth at DISN Subscriber Service (DSS) locations, or to a readily available commercial IP network at non-DSS locations. Continued use of TDM and other legacy circuits should only be used as a last resort. (ref ah)

DAYS:	
T1	45 days
DS3	60 days
OC3	90 days
OC12	120 days
OC48	120 days
OC192	120 days

*Networx PLS:		
	Standard	**Expedite**
T1	45	23
DS3	85	43
OC3	ICB	
OC12	ICB	
OC48	ICB	
OC192	ICB	

Table 3: Timeline of Required Actions

*Contact the DCCC for delivery timeline (844) 347-2457, Option 2)

In the event the service request qualifies as an Emergency or Essential National Security/Emergency Preparedness (NS/EP) telecommunications service, there is an expedited process available, both for service fulfillment and for connection approval.

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

(For additional information on the RMF, see NIST SP 800-37 (ref n) and the RMF Knowledge Service (ref o) at https://rmfks.osd.mil/)

3.3 Customer Registers Connection Information

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

Once the DDOE process has been completed with the receipt of a CCSD, customers are required to register and maintain their IS information (IP address ranges, hosts, POCs, etc.) in the appropriate databases based on classification of the connection:
Contact the Network Information Center (NIC) through the DCCC at (844) 347-2457, Option 2; CML: (614) 692-0032, Option 2; DSN: (312) 850-0032, Option 2; disa.dccc@mail.mil for all unclassified connection

- **SNAP** (https://snap.dod.mil) for:
  - Voice, video, data circuit registrations and connections to unclassified networks/ services DoD CIO temporary exception to policy registrations (Appendix G)
- **DCCC** at (844) 347-2457, Option 2; CML: (614) 692-0032, Option 2; DSN: (312) 850-0032, Option 2 ; disa.dccc@mail.mil for all classified connections
- **SGS** (https://giap.disa.smil.mil/gcap/home.cfm) for:
  - Voice, video, and data circuit registrations/connections to classified networks/services
- **Ports, Protocols, and Services Management (PPSM)** (https://pnp.cert.smil.mil) (http://iase.disa.mil/ppsm) for:
  - All networks/systems ports, protocols, and services for all IP solutions or applications, in accordance with DoDI 8551.01 (ref e)

Note: DoDI 8510.01, Change 1, (ref d) Enclosure 8 authorizes and encourages DoD Components to start using RMF immediately when authorizing DoD IS and PIT systems and provides a timeline and instructions for transition from DIACAP to RMF. DIACAP packages can be submitted to Component Authorizing Officials (AOs) up until 1 Oct 2016. Any DoD IS or PIT system with a DIACAP package submitted through 1 Oct 16 will only be authorized an ATO for at most 1.5 years from the date of the AO's signature. On 2 Oct 2016, only RMF packages can be submitted to AOs. In the case of significant financial or operational impacts of transitioning to RMF, an AO may submit a request for deviation from this guidance for specific systems to the respective DoD Component CIO for approval. All requests for deviation forwarded to the Component CIO must be accompanied by an IS transition plan and a plan of action and milestones. During the transition, DISA will accept a request for a DISN connection that is supported by an ATO with RMF or DIACAP artifacts but will not accept a package with a combination of RMF and DIACAP artifacts.

3.3.1 Account Registration for the SNAP and SGS Databases

CAP packages for connections will be uploaded by the customer in the SNAP (unclassified) or SGS (classified) database. The customer must first register and get a SNAP or SGS account in order to submit a CAP package, Note: a legacy version of SGS is provided as a reference. Legacy SGS is not updated and does not contain current information. At some point in the near future, the Legacy SGS system will be removed.

DISN ATCs will not be issued until the enclave's systems are properly registered in the PPSM registry and have a valid PPSM registration identification number. For questions regarding PPSM registration call the PPSM Office at 301-225-2904.

3.3.2 SNAP and SGS Account Request Procedures

- Go to https://snap.dod.mil for SNAP and https://giap.disa.smil.mil for SGS
- Click on "Request a SNAP account" or "Request a SGS account"
  - Upload a completed signed DD Form 2875 System Authorization System Request (SAAR); The DD Form 2875 can be downloaded from SNAP and/or SGS on the Reference Documents page
- Complete section 13 of the DD Form 2875, "Justification for Access" by specifying the SNAP and/or SGS module and user role for the CC/S/A/FA
- Complete the profile data, asterisked item are required fields
- Click "Submit Request" for approval

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

3.4 Registration and Submission Process for CAP Packages

The below steps detail the registration and submission process for both unclassified and classified CAP packages:

3.4.1 SNAP (Unclassified) and SGS (Classified) Submittal Process

- Log on to SNAP (https://snap.dod.mil) for Unclassified Connections and SGS (https://giap.disa.smil.mil) for Classified Connections
- Hover the mouse over "NIPR" for SNAP or "GIAP" for SGS and select "New Registration"
- Complete all required fields of the NIPR or GIAP Checklist (Sections with a locked icon are reserved for use by CAO Analyst)
- Upload Attachments for the RMF/DIACAP executive package artifacts in the Attachments/Documents Section as applicable
- Once all sections are completed, a submit button at the bottom of the screen will be available in order to submit the entire registration
- For NIPR packages that have classified artifacts, upload a placeholder document in the applicable section in SNAP stating that the artifact was submitted on SIPR. The date of the email and sender's name should be in the note. Send the email to the SIPR UCAO mailbox: disa.meade.ns.mbx.ucao@mail.smil.mil.

3.5 DISN Connection Approval Package Submission

The customer connection requests are submitted to the CAO in the form of a SNAP or SGS registration and uploading of the CAP package. This package provides the CAO the information necessary to make a connection approval decision. CAP packages should be submitted at least 30 days prior to the desired connection date, for new connections, or 30 days prior to the existing ATC or IATC expiration date, to ensure service continuity. The following documentation is required for the CAO to analyze a CAP package:

3.5.1 DoD Component Connections to the DISN:

Connection Approval Packages for DoD Component connections to DISN will include the following documentation:

CAP Package Required Documentation: DoD Component Connections	
DoD RMF	**DIACAP**
Authorization Decision Document (ADD) signed by the AO	ATO or ATO with conditions signed by the DAA
Security Assessment Report (SAR)	DIACAP Scorecard
Security Plan (SP)	System Identification Profile (SIP)
POA&M	IT Security POA&M

Detailed Topology Diagram	Detailed Topology Diagram
Consent to Monitor	Consent to Monitor
AO Appointment Letter	DAA Appointment Letter

Table 4: DoD Component Connection Documentation Requirements

For additional RMF guidance, please go to the RMF/DIACAP Knowledge Management website at: https://rmfks.osd.mil/login.htm.

3.5.2 Mission Partner Connections to the DISN

Connection Approval Packages for Mission Partner connections to DISN will include the following documentation: DoD Sponsors and Mission Partners will ensure information in SNAP/.SGS are kept up to date.

CAP Package Required Documentation: Mission Partner Connections
ATO or ATO with conditions signed by the AO/DAA
As appropriate: RMF Documentation or DIACAP Executive Package (DIACAP Scorecard) in accordance with DoDI 8510.01 (ref d), DoD 5220.22-M, NISPOM (ref s), NIST 800-37, ICD 503 documentation, or equivalent documentation
Statement of Residual Risk
Detailed Topology Diagram
DoD Sponsor Validation Letter (Appendix B) /Revalidation Letter (Appendix C)
DoD CIO Memo validating the mission requirement for a new Mission Partner connection to DISN
Consent to Monitor (the DoD Sponsor is responsible for signing the CTM)
AO/DAA Appointment Letter
The DoD Sponsor must validate the Mission Partner's need for access to the DISN. The DoD Sponsor and Mission Partner must understand and agree (e.g., MOA/MOU, contract) to their responsibilities as stated in the DoD CIO Sponsor Memorandum *–Responsibilities of DoD Components Sponsoring Mission Partner Connections to DISN-Provided Transport Infrastructure* (ref_m).

Table 5: Mission Partner Connection Documentation Requirements

3.5.3 DoD Classified Contractor Connections to DISN:

In addition to the requirements in paragraph 3.5.2, a Connection Approval Package for a Classified Defense Contractor connection to DISN will include:

CAP Package Required Documentation: DoD Contractor Connections
Master System Security Plan and Information Security Plan (ref s)
DoD 5220.22-M, NISPOM (ref s) executive package artifacts
The Defense Security Service (DSS) has responsibility for all AO actions related to Classified Contractor connections to DISN in accordance with NISPOM C&A; see the DSS-DISA MOA (ref an) for further specifics regarding classified DoD contractor connections.

Table 6: DoD Contractor Connection Documentation Requirements

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

3.5.4 Federal Departments, IC, and Other Mission Partners:

In addition to the requirements in paragraph 3.5.2, a Connection Approval Package for a Federal Department or Agency, IC or other Mission Partner (e.g., coalition partner) connection to DISN will include:

CAP Package Required Documentation: Federal Departments and Agencies, IC and Other Mission Partner Connections
The documentation used for authorization of a Federal Mission Partner IS not categorized as a National Security System (NSS) will use National Institute of Standards and Technology (NIST) SP 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. (ref n)
The documentation used for authorization of a Federal Mission Partner IS categorized as an NSS will use CNSS Instruction (CNSSI) No. 1253 Security Categorization and Control Selection for National Security Systems, 27 March 2014 (ref p), refer to CNSSI 4009 *National Information Assurance Glossary* (ref j) for the definition of an NSS.
The documentation used for authorization of an IC IS or other Mission Partner IS will be in accordance with ICD 503, RMF Documentation, DIACAP Executive Package (DIACAP Scorecard), or equivalent documentation. IC documentation and submitted artifacts will be commensurate with the IC reciprocity memorandum.
DoD CIO Memorandum of Agreement with Federal Departments and Agencies for connection to DISN in lieu of a DoD Sponsor validation memo.
Joint Staff approval memo for 5 Eyes/coalition partner connections to DISN
Connection requests for all Mission Partners require a validation/revalidation memo signed by the DoD sponsor and validated by the DoD CIO

Table 7: Federal Departments, IC, and Other Mission Partners Documentation Requirements

3.6 Reauthorization/Reaccreditation Connection Evaluation

If an enclave approaching its Authorization Termination Date (ATD), the system owner/program manager must reinitiate the A&A/C&A process and obtain a new authorization decision from the AO. Ideally, the new ATO will be issued and an updated CAP package uploaded to SNAP or SGS a minimum of 30-days prior to the expiration of the current ATC/IATC. In accordance with DoDI 8510.01 (ref d), "systems that have been evaluated as having a sufficiently robust system-level continuous monitoring program (as defined by emerging DoD continuous monitoring policy) may operate under a continuous reauthorization." AOs who determine that their DISN connected enclave has met DoD's continuous monitoring policy requirements are still required to update their respective ATO at a minimum of every three (3) years before a new ATC/IATC will be issued. For UC connection requirements please see Appendix E... If a system does not have a sufficiently robust system-level continuous monitoring program, the "Systems must be reassessed and reauthorized/reaccredited once every 3 years. The results of an annual review or a major change in the cybersecurity posture at any time may also indicate the need for reassessment and reauthorization of the system in accordance with Appendix III to OMB Circular A-130 (ref q).

The expiration date of an ATC/IATC is usually the same as (and will never go beyond) the ATD expiration date of the associated scorecard. In some instances, the results of the DSAWG risk assessment may warrant the issuance of an ATC/IATC with an authorization period shorter than that of the associated scorecard or RMF documentation. An expired ATC/IATC will prompt a review by Joint Force Headquarters DODIN (JFHQ DODIN), and may result in an order to disconnect the enclave from the DISN network/service. In accordance with DoDI 8510.01 (ref d), "An ADD/ATO authorization decision must specify an ATD that is within 3 years of the authorization date unless the IS or PIT has a system-level continuous monitoring program compliant with DoD continuous monitoring policy as issued."

The AO could decide that planned changes to an enclave are significant enough to warrant reinitiating the full A&A process, with subsequent issuance of a new reauthorization decision inside the normal 3-year authorization cycle. If no physical reconfiguration of the DISN circuit is needed to effect the planned changes, such modifications to an enclave (even if significant enough to warrant a new authorization decision) do not need to be coordinated with the corresponding DISN Validation Official. However, the planned events may have a significant impact on the IA[5]/cybersecurity posture of the enclave, and consequently on the risk the enclave poses to the DISN community at large. Pre-coordination with the CAO is necessary to ensure the updated topologies, CAP package artifacts, and risk decision artifacts are updated and available for the connection approval decision.

Examples of significant impact events:

- Deployment of a cross domain solution (CDS)

[5] Note Information Assurance (IA) is used interchangeably with the term cybersecurity in accordance with DoDI 8500.01

- Deployment of a UC product enhancing the capability of the enclave (i.e., softswitch VoIP, VoSIP, CVVoIP), even if the application is already 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 Defense Information Technology Contracting Office (DITCO), unless the TSO clearly states that the authorization will transfer.

An Automated Information System (AIS) that has already been authorized by the DISA AO for deployment on DISN/DODIN does not trigger a requirement for pre-coordination with the CAO if deployed to another enclave on DISN.

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

Examples:

- Deployment of new VoIP phones requiring a new VLAN segment within the enclave
- Deployment of new VTC products (on DoD UC APL)
- Changes in the IP address range assigned to the IS/enclave
- DISA transport re-homing actions that change the connection points to DISN but the enclave remains at the same facility
- Upgrade of bandwidth service

To update the registration for existing connections, use the following processes:

- Logon to SNAP (https://snap.dod.mil) for Unclassified Connections and SGS (https://giap.disa.smil.mil) for Classified Connections
- Hover the mouse over the respective tab (e.g., "Waiver," "Defense Switched Network," "VPN," or "NIPRNet") for Unclassified Connection in SNAP and the respective tab (GIAP or CDS) for Classified Connection in SGS and select "View/Update"
- Use the Search Field to locate the registration
- Complete all required fields of the Checklist (Sections with a locked icon are reserved for use by CAO Analyst)
- Upload Attachments for the RMF, DIACAP, or other applicable executive package artifacts in the "Attachments/Documents" section as applicable
- Once all sections are completed, a submit button at the bottom of the screen will be available in order to submit the entire registration

3.7 Connection Process Checklist

This checklist provides the key activities that must be performed by the Mission Partner or DoD Component sponsor during the connection approval process:

Item	DoD Component		Mission Partner	
	New	Existing	New	Existing
Obtain DoD CIO approval for Non-DoD connection			√	*
Provision the connection	√		√	*
Perform the A&A process	√	√	√	√
Obtain an authorization decision (ATO/IATT)	√	√	√	√
Register the connection	√	**	√	*
Register in the GIAP/SGS and/or SNAP database	√	**	√	*
Register in the PPSM database	√	**	√	*
Register in the DITPR database (NIPR Only)	√	**	√	*
Register in the SIPRNet IT Registry database (SIPR Only)	√	**	√	√
Register with the SIPRNet Support Center (SSC) (SIPR Only)	√		√	
Complete the CAP package	√	√	√	√
DIACAP Executive Package (or equivalent for non-DoD entities)/RMF Security Assessment Report	√	√	√	√
DIACAP Scorecard/Systems Authorization Package	√	√	√	√
System Identification Profile/System's Security Plan	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√
AO Appointment Letter	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
Proof of Contract/SLA/MOU/MOA			√	√
DoD CIO Approval Letter			√	√
Submit the CAP package to the CAO	√	√	√	√
Receive remote compliance scan (SIPR Only)	√		√	
Receive ATC/IATC	√	√	√	√
Proof of a funded agreement with a DoD accredited Computer Network Defense Service Provider (CNDSP)	√	√	√	√

Table 8: Connection Process Checklist

* - This step is not required for existing mission partner connections unless there has been a change in Sponsor, mission requirement, contract, location, or the connection has not been registered.
** - This step is not required for existing connections that are already registered and where all information is current.

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

3.8 Customer Network Enclave Topology Diagram Requirements

Network Topology Diagram/Systems Design Document – the diagram below depicts the network topology and security posture of the Customer network enclave that will be connecting to the DISN. The Network Topology Diagram document should:

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

It is important to note that in accordance with DoD and DISA guidance, firewalls, Intrusion Detection Systems (IDSs)\ and Wireless-IDSs (where applicable) are required on all partner enclaves. Private IP addresses (non-routable) are not permitted on SIPRNet enclaves without an acceptable RFC 1918 community risk assessment from the DSAWG. For more information go to the following link: (https://intelshare.intelink.gov/sites/dsawg/default.aspx). Indicate and label all of the devices, features, or information; minimum diagram size: 8.5" x 11."

All Cybersecurity and cybersecurity-enabled products that require use of the product's cybersecurity capabilities must comply with the evaluation and validation requirements of (ref p) in accordance with DoDI 8500.01 (ref a).

DoD Components are required to acquire or operate only UC products listed on the UC APL, unless, and until, a DoD CIO temporary exception to policy is approved in accordance with DoDI 8100.04, *Unified Capabilities* (ref g). The DoD UC Approved Products List and can be found at the DISA APLITS web page: https://aplits.disa.mil.

All Topologies MUST include IP address ranges, equipment make/model, and software version.

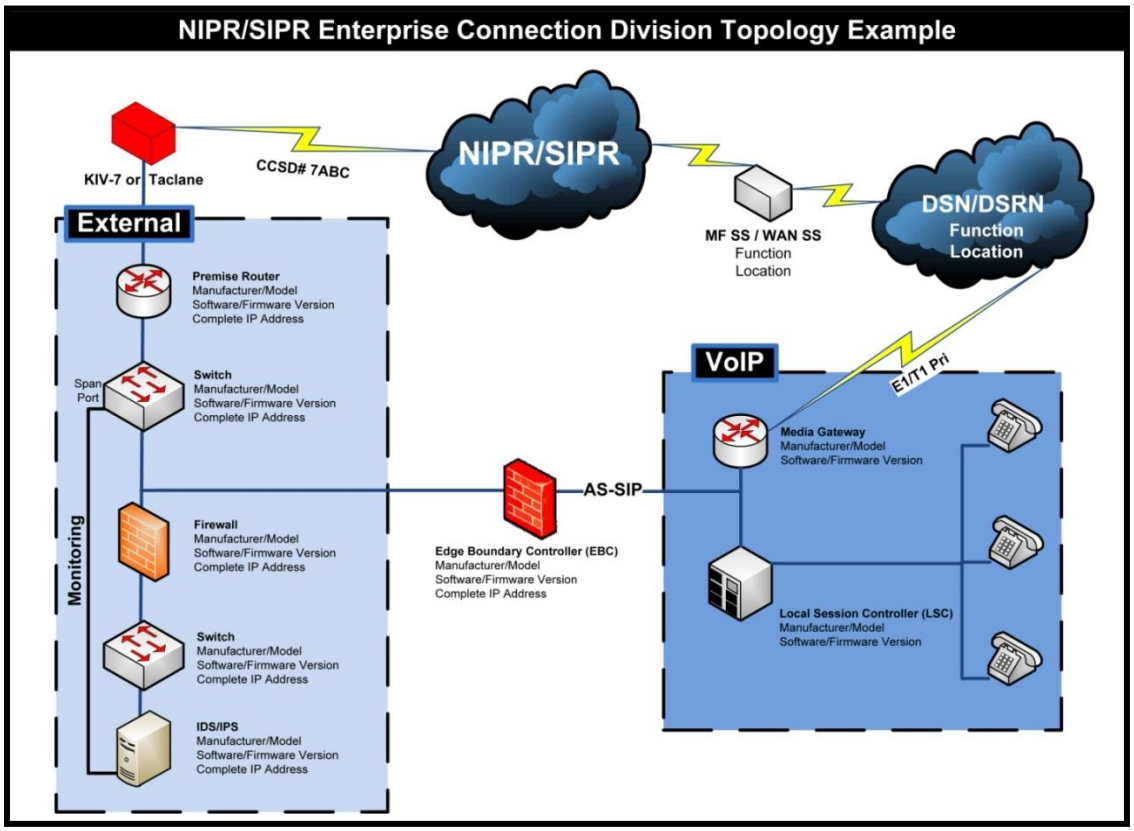

Figure 2: NIPR/SIPR Customer Network Enclave Topology Sample

3.9 Customer Network Enclaves Connecting via JRSS

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

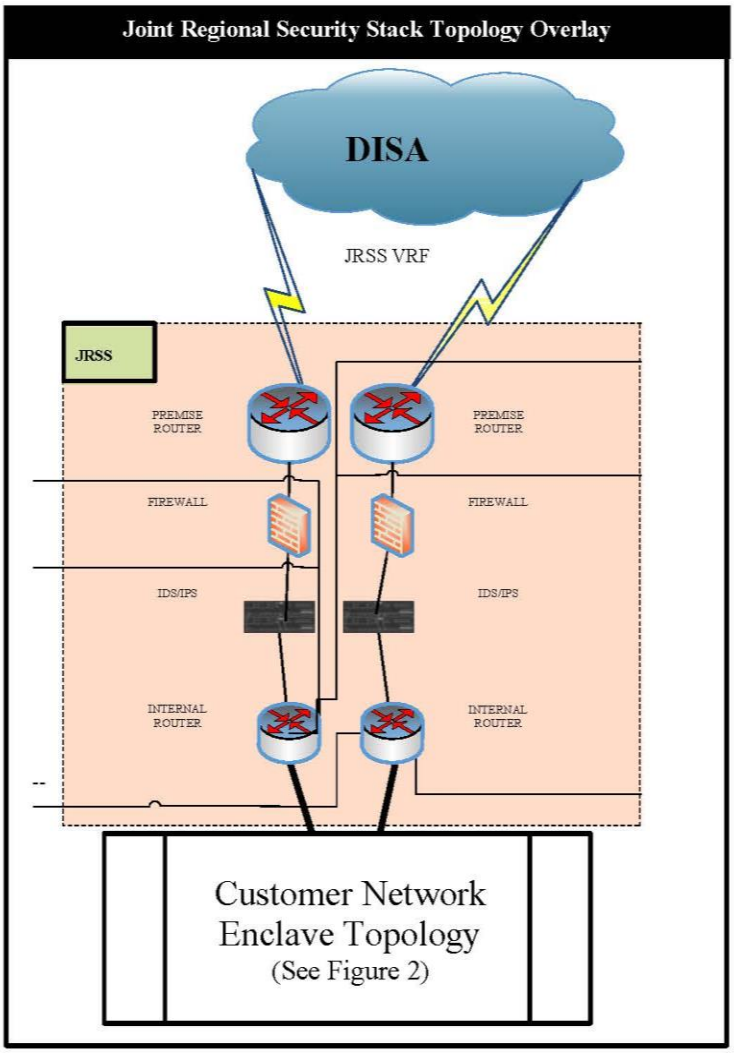

Figure 3 JRSS Security Stack Topology Overlay

3.10 Tactical Exercise/Mission CAP Packages

Tactical exercise/mission CAP packages must be submitted a minimum of eight (8) days prior to the start of the exercise/mission. Upon successful registration of the initial tactical mission/exercise, the registration will become valid for the duration of the ATO. The Registration ID number, that is auto-generated from SGS upon registration, will be used as a reference to access DoD Gateway SIPRNet services for the duration of the ATO. This Registration ID number will be used on all future missions, and provided to the CONEX in the

remarks section 1 of the Gateway Authorization Request (GAR). Remarks will be: "SGS Registration ID number xxxxx for SIPRNet IATC, expiration DD-MMM-YYYY."

Customers are not required to register for each mission after initial registration. The authorization is valid thru the ATO revocation and or expiration. If the current ATO will expire prior to the next time the Tactical user will enter a DoD Gateway, the user will start a new request so that a new Registration ID number can be issued. Any changes to equipment configuration affecting enclave security posture of the system resulting in a new ATO will require registration in the SGS database. A complete authorization package is not submitted with a CAP package for a tactical exercise/mission, however, the CAP package must include at a minimum, an ATO letter, Gateway Access Authorization (GAA), and topology/System Design Document (SDD).

The CAO will review the registration information and will issue an IATC/ATC for the duration of the ATO upon successful and complete registration. The IATC/ATC will be made available under section 10.1 of the SGS database (Scorecard). The DISA GSD/Tier II will verify the validity of the Registration ID number provided in the GAA against the SGS database prior to allowing access to SIPRNet.

For additional information, please review the Policy and Procedures for DoD Gateways (STEP/Teleport) SIPRNet DODIN Interconnection Approval Process System (SGS).

3.11 Mission Partner De-Militarized Zone (DMZ) or Gateway Connections

In accordance with CJCSI 6211.02D (ref b) non-Mission Partners, including defense contractor enclave connections to DISN-provided transport, information services must be through an established DISN DMZ and will follow DISN DMZ security requirements. DISA operates three (3) DMZs or Mission Partner Gateways; NIPRNet Federal Gateway (NFG), SIPRNet Federal DMZ (FED-DMZ), and the SIPRNet Releasable (SIPR REL) DMZ. In certain limited special use cases, the DoD CIO has approved some non-DoD Federal Agencies Mission Partner connections to the NIPRNet and SIPRNet, however, this is not the norm. Connections to the DISN DMZs/NFG can be made either physically or logically (see Figure 3). Mission Partners will work with the NIPRNet or SIPRNet DMZ offices listed in Table 2 to initiate their respective DMZ/NFG connections.

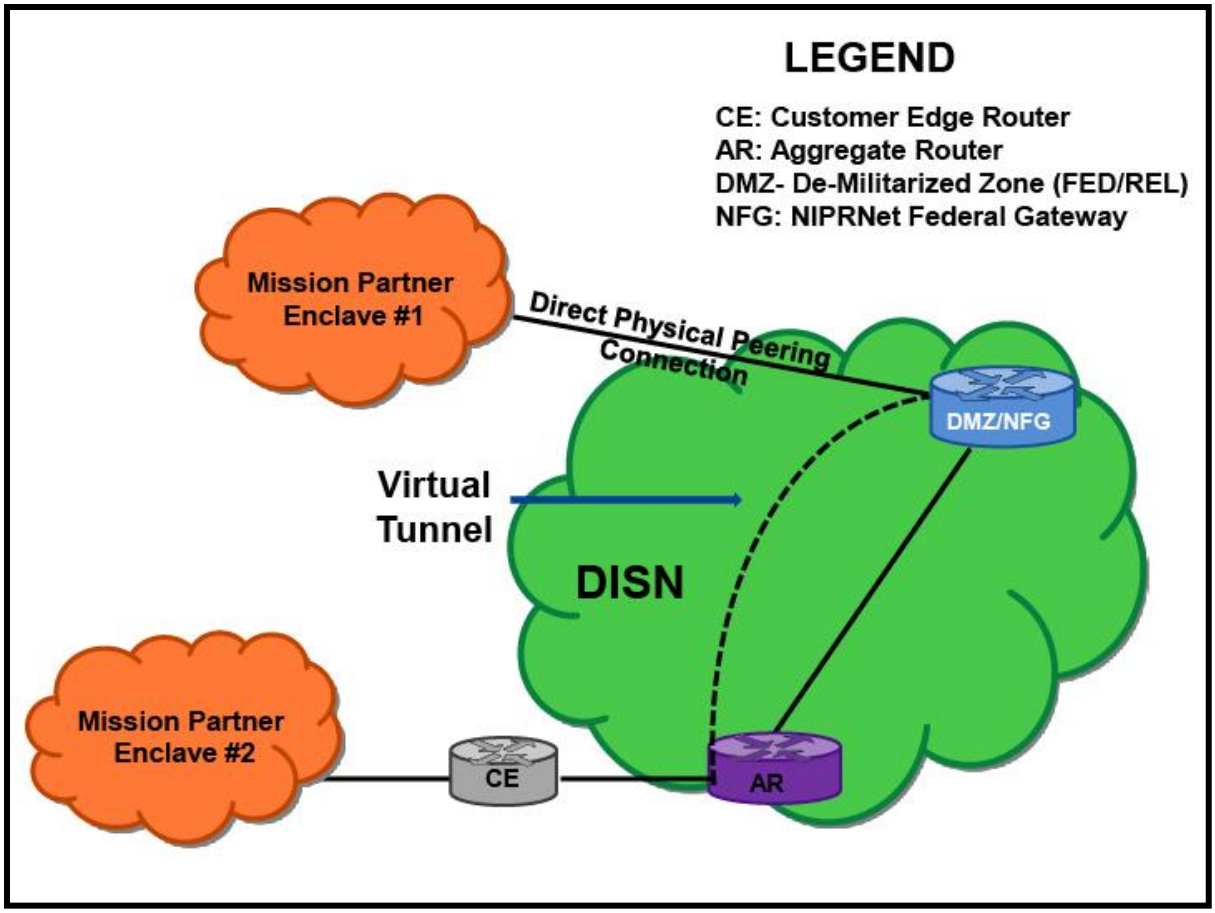

Figure 4: Generic DISN DMZ and Gateway Connections

DISA DMZ Offices	
NIPRNet NFG	301-225-8684 DSN 375
SIPRNet REL-DMZ/FED DMZs	301-225-9607 DSN 375

Table 9: DISN DMZ Contact Information

All Non-DoD NIPRNet/SIPRNet connections require DoD CIO Approval, a Contract/MOA/ MOU and DoD Sponsor to validate DoD mission need for Mission Partner access to the DISN. DoD Sponsors must understand and agree to their responsibilities as stated in the DoD CIO Sponsor Memorandum (ref m), applicable issuances, the Defense Finance and Accounting Regulations (DFAR), and the DoD Sponsor and Mission Partner responsibilities must be codified in an appropriate agreement (e.g., MOA, MOU, or contract). The DoD CIO will establish MOA with Federal Departments and Agencies that have a mission requirement to connect to DISN.

In addition to the requirements listed in this section, to connect to the NIPRNet Federated Gateway mission partners must complete a NIPRNet Federated Gateway, (NFG) Questionnaire, as well as the NIPRNet Federated Gateway Policy spreadsheet (https://www.disa.mil/Network-Services/VPN/MPG). The questionnaire provides baseline data for engineering teams to work with mission partners while the NFG Policy Spreadsheet identifies the firewall posture of the

NFG which will support mission partners. The customer must notify the NIPRNet NFG or SPIRNet DMZ offices of the PPSM registration ID, in addition to the above referenced documentation. The DMZ/NFG team works with the Web Content Filtering team to ensure that the applicable firewall rulesets are vetted and provided to the DISA Command Center (DCC) which issues a DISA Task Order (DTO) for DISA Global Operations Center (DGOC) to implement (See Figure 4 and 5). Should applicable PPSM not be identified, the corresponding services will not be available. This may result in subsequent submissions of firewall rule requests to support mission partner/sponsor requirements.

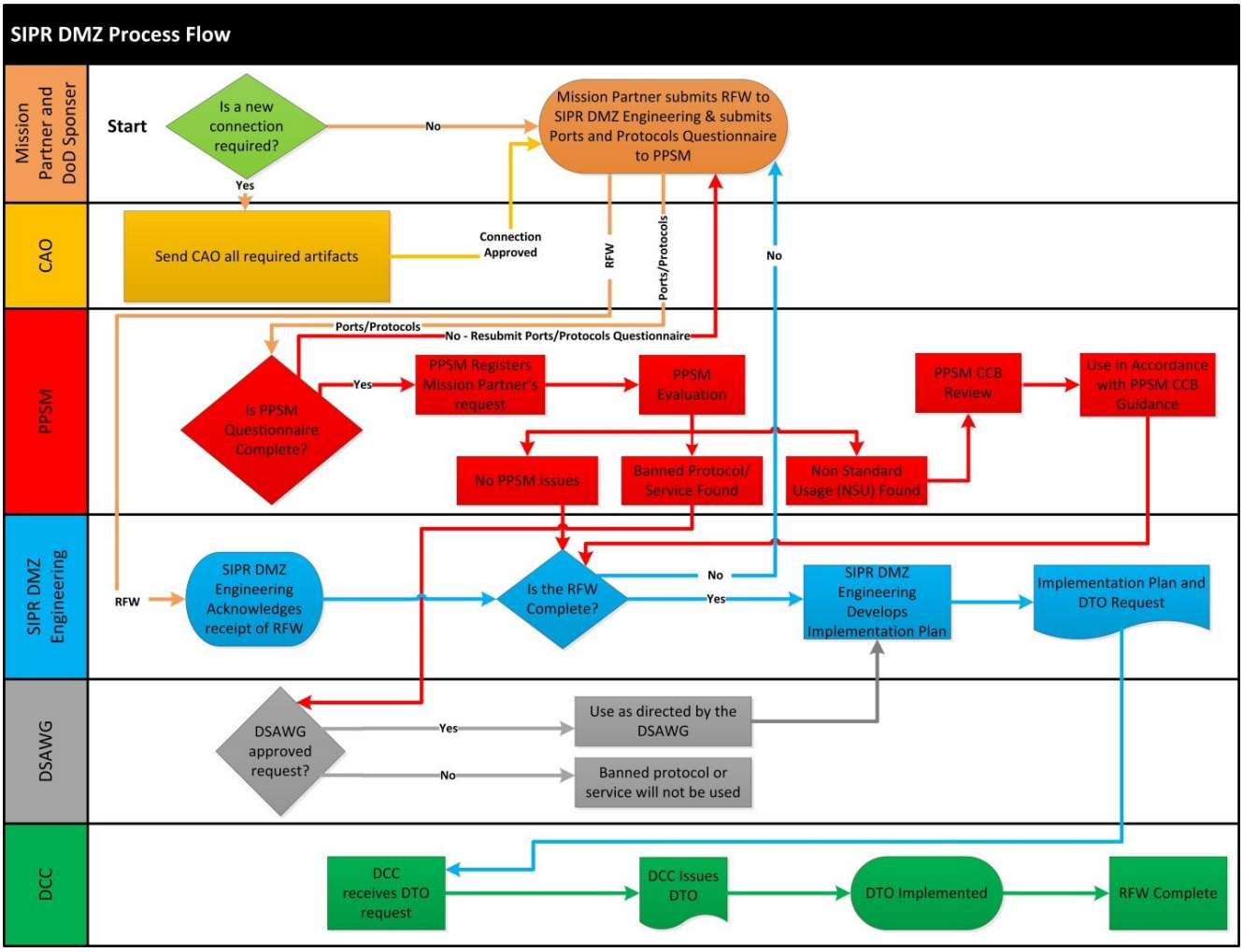

Figure 5: Over View of the DISN DMZ or NFG Process Approval Flow

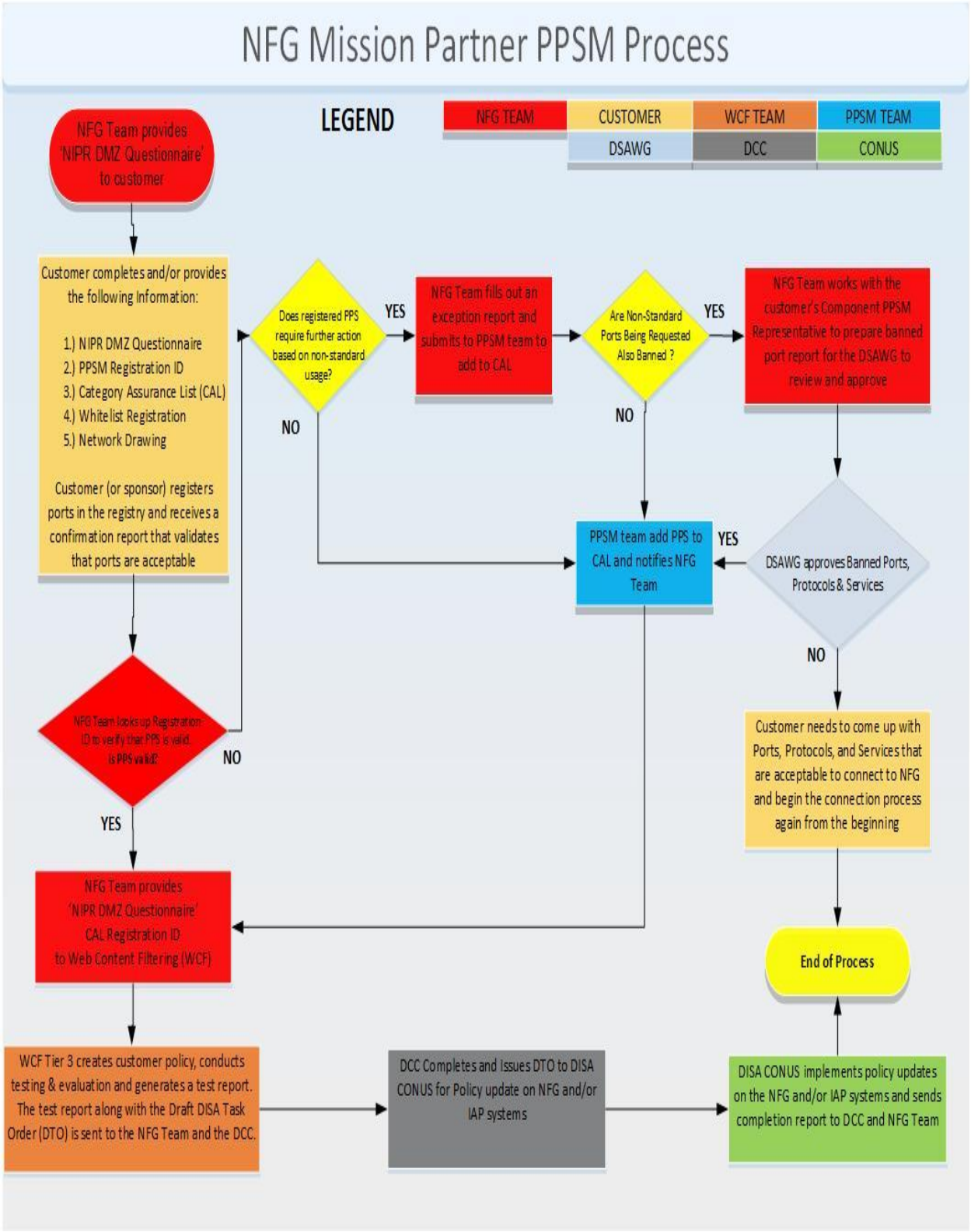

Figure 6: Detailed View of the DISN NFG Process Approval Flow

3.12 Mission Partner NIPRNet Federated Gateway (NFG) Connections

The NIPRNET Federated Gateway (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 Internet Protocol (IP) Router Network (NIPRNet). The NFG supports both logical and physical connections.

It is strongly recommended that mission partners communicate with current service providers to ensure the smooth circuit hand off to NFG site/DISN Transport nodes. Logical circuits are an interim solution for migration to NFG and not meant to be an end state/long term solution

3.12.1 NFG Logical Connections

Existing Mission Partner connections to NIPRNet may be extended to NFG without installing new physical circuits. This can be accomplished by provisioning logical tunnels using Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) or Internet Protocol Security (IPsec) VPN over the DISN. These tunnels extend existing Mission Partner connection(s) to the NFG and the traffic will flow to the NFG on a slightly different path than originating from physical connections. 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. Logical connections through sponsors or other DoD agencies are not supported. 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 connects to the NFG COI (MPLS VPN) for logical transport to the NFG site.
2. Mission Partners currently connected to the DISN router for NIPRNet access will connect to the NFG COI (MPLS VPN), eliminating NIPRNet access without passing through the NFG first.

3.12.2 NFG Physical Connections

Physical connections are terminated on the NFG using up to OC-12 SONET 1Gb and 10Gb 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 Premise Equipment (CPE) 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.

3.12.3 NFG Connection Approval Requirements

Connections to the NFG are either physical or logical.

Physical connections that are directly homed to the NFG use point-to-point circuits between the NFG and a Mission Partner's network. Logical connections are physically homed to a NIPRNet router but are connected to the NFG via an encapsulated tunnel. NFG connections 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/IATC and be reviewed in accordance with the established agreement (e.g., MOA/MOU/SLA).

CAP Package Required Documentation: NFG Connections
Signed DoD CIO validation memo (e.g., MOU/MOA/SLA)...
Network topology diagram/SDD
Valid PPSM registration identification number,
Required current POC information
Authorization to Operate (ATO) letter

Table 10 NFG Connection Documentation Requirements

3.12.4 Ordering NFG Connections

Orders for NFG circuits are submitted to the DISA Direct Order Entry (DDOE):

1. After obtaining access, Mission Partners use DDOE to generate Telecommunications Service Requests (TSR) to have circuits provisioned to the NFG. Refer to the DDOE website (https://www.disadirect.disa.mil/products/asp/welcome.asp) for information on the circuit-ordering process.
   a. For logical connections, the VPN Identification (ID) number for the NFG Community of Interest (COI) service is provided by DISA and is always the same for every Mission Partner
   b. The VPN ID for NFG COI Service is DKL300249
   c. DDOE assigns the VPN ID to all Mission Partners requesting NFG COI Service

The mission partner must first register for access to the DDOE site using the following link: https://www.disadirect.disa.mil/products/asp/welcome.asp.

2. The TSR initiates the process of identifying Mission Partner requirements and provisioning the new NFG circuit paths based on the approved engineering design and connection approval package.

3. To revise approved connections, Mission Partners must update the approved CAP or submit a new CAP based on the approved engineering solutions.

4. Mission Partners must ensure they have obtained and completed the NIPRNet Federated Gateway Questionnaire as well as the NIPRNet Federated Gateway Policy spreadsheet https://www.disa.mil/Network-Services/VPN/MPG). Should applicable PPSM not be identified, the corresponding services will not be available. This may result in subsequent submissions of firewall rule requests to support mission partner/sponsor requirements.

DoD policy also requires that DoD Components register their IS information in the DoD Information Technology Portfolio Repository (DITPR) at https://ditpr.dod.mil.

DoD policy also requires that DoD Components register their IS information in the DoD Information Technology Portfolio Repository (DITPR) at https://ditpr.dod.mil.

Use of the unclassified DITPR is preferred for registration of all information systems including classified systems. There are numerous classified systems registered in the unclassified DITPR, without inclusion of classified information about the system. However, an information system may be registered using the SIPRNet IT Registry (SITR) if the description of the information system must contain classified material, or, if the organization (such as a CCMD) routinely uses the SIPRNet. The link to the SITR on SIPRNet is: https://dodcio.osd.smil.mil/itregistry - for additional assistance using SITR, send email to: osd.mc-alex.dod-cio.mbx.ditpr-support-team@mail.mil and include 'SIPR IT Registry' in the subject line.

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

3.13 Mission Partner SIPRNet DMZ Connections

Mission Partners connecting to SIPRNet must complete a 'Non-DoD Connection Request Letter' and submit it to the DISN Validation Official. This will begin the process by which subsequent approval/disapproval by DoD CIO is granted. Mission Partner SIPRNet DMZ connections are either through the SIPRNet FED-DMZ or the SIPR REL DMZ. In rare cases, the DoD CIO may approve Mission Partner direct SIPRNet connections. Applicable Mission Partner connections must also adhere to DoDI 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD* (ref f) and CJCSI 6285.01C, *Multinational Information Sharing (MNIS) Operational Systems Requirements Management Process* (ref r) as part of the Mission Partner Environment (MPE) and Joining, Membership, and Exiting Instructions (JMEI) policy requirements.

Like Mission Partner NFG connections, Mission Partner SIPRNet FED DMZ connections can either be physical or logical. Physical connections are directly homed to the SIPRNet FED DMZ

(e.g., point-to-point circuits 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 via an encapsulated tunnel. SIPRNet FED DMZ connections require a modified Connection Approval Process package as illustrated below. Qualified SIPRNet FED DMZ connections will receive an ATC/IATC and be reviewed in accordance with the established agreement (e.g., MOA/MOU/SLA).

CAP Package Required Documentation: SIPRNet FED DMZ Connections
Signed DoD CIO validation memo (e.g., MOU/MOA/SLA).
Network topology diagram/SDD
Valid PPSM registration identification number,
Required current POC information
Authorization to Operate (ATO) letter

Table 11 SIPRNet FED DMZ Logical Connection Documentation

SIPRNet REL DMZ require a full Mission Partner Connection Approval Package (CAP) as explained in section 3.5.

3.14 JRSS Accreditation

Currently customers that have a current ATC for a traditional NIPR circuit are being reauthorized/reaccredited for moving to the JRSS Stack. This only applies to NIPR circuits. SIPR circuits are not yet being moved to JRSS.

The following procedures will allow the customer to create a SNAP registration:

1. To register a JRSS connection in SNAP, in the NIPR module select ‘New Registration’.

2. In Section 0.1, for Connection 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 in the block below. NOTE: Currently the VRF will not show if the customer goes to My Entries report. Until that is fixed the customer will have to search by Registration ID for that registration.

4. Internal boundary defense equipment (firewall, IDS/IPS) is no longer required on the topology and will not be evaluated by the analysts. The JRSS stack must be shown on the topology.

5. Other than the Virtual Routing and Forwarding (VRF) identifier instead of a CCSD, JRSS packages are submitted like any other Connection Approval package. Please remember to show the VRF on the documentation where the CCSD would previously have been identified.

The CAO analysts will review the package and an Approval to Connect (ATC) will be issued.

3.15 CAP Package Review and the Authorization to Connect Decision

Upon submittal of the registration, the CAO will review all sections of the registration or completeness and compliance. In the event a section is incomplete or a non-compliant artifact is uploaded to the database, that individual section will be rejected. The POCs listed in the database will receive notification of a rejected registration to include what documentation is missing or non-compliant from the package. The customer must log back into the database and complete or upload the updated artifact for the rejected section. Typically, when all the connection approval requirements are met an ATC or IATC will be issued within eight (8) business days.

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

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

If the CAO assesses that an enclave's connection to the DISN poses a potentially "high" impact community risk, it will forward the connection request to the DSAWG as part of the executive risk function in accordance with DoDI 8500.01 (ref a) and DoDI 8510.01 (ref d). The CAO will provide the AO the justification for the assessment and inform the AO that current guidance (i.e., policy, DSAWG decision, STIGs, etc.) from DISN/DODIN DAAs/AOs precludes the issuance of an ATC without additional review of the enclave cybersecurity status by the community authorization bodies.

3.16 Type Authorized/Accredited Systems

Type authorized/accredited systems refer to a generally standardized configuration for two or more circuits. Although they have similar configurations, they are still individual circuits, and are registered individually in SNAP or SGS. Each circuit under a type authorization must have an individual topology that shows, among other things, the unique IP addresses assigned to that circuit. They may all use the same Scorecard/SAR/ADD/ATO or ATO-with-conditions, SIP, and POA&M.

3.17 Notification of Connection Approval or Denial

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

Connection Approval

If the connection request is approved, the partner is issued an ATC or ATC with conditions. The validity period is specified in the ATC letter. After the connection is approved, the partner must

work with DISN Implementation to complete the installation of the circuit. The connection approval is valid until the expiration date. The AO must notify the CAO of significant changes, such as architecture changes requiring re-authorization /re-accreditation movement of the enclave to a new location, changes in risk posture, etc., that may cause a modification in the cybersecurity status of the enclave or if the connection is no longer needed.

Denial of Approval to Connect

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

3.18 Notification of Discontinued or Cancelled Circuits

If for any reason it becomes necessary to discontinue the use of an enclave, the customer must submit via e-mail the discontinuance or cancellation TSO/IER) to the CAO (e.g. SIPRNet: mailto:disa.meade.ns.mbx.ccao@mail.mil or NIPRNet: mailto:disa.meade.ns.mbx.ucao@mail.mil). CAO will upload the TSO or IER in the respective database and close the registration for that CCSD.

3.19 Primary Points of Contact:

Connection Approval Office (CAO)	
CAO for Unclassified Connections	disa.meade.ns.mbx.ucao@mail.mil disa.meade.ns.mbx.ucao@mail.smil.mil
CAO for Classified Connections	disa.meade.ns.mbx.ccao@mail.mil disa.meade.ns.mbx.ccao@mail.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901

Table 12: Connection Approval Office (CAO) Contact Information

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

Table 13: CONUS Provisioning Center Contact Information

3.20 Cloud Computing Connections

Procedures for connecting to Cloud computing services are currently documented in the Cloud Connection Process Guide (ref aL). Cloud connection procedures will be addressed in future editions of the DISN CPG.

This page intentionally left blank.

APPENDIX A - NON-DOD CONNECTION VARIATIONS

This appendix provides the necessary steps and information to process a Non-DoD Connection. It is intended to supplement the detailed information provided in Section 3.4 of this guide with Non-DoD Connection specific information. Any Variations from those steps or additional requirements are identified in this appendix.

A.1 Circuit Order Questionnaire

Prior to a sponsor ordering a circuit, the below circuit order questionnaire/checklist should be used:[6]

CIRCUIT ORDER QUESTIONAIRE
Cleared Contractor/Non-DoD SIPRNet Circuit Sponsors:

1. DoD Sponsor Unit:
   _____

   DoD Sponsor POC (Name, NIPR e-mail, SIPR e-mail, Phone #)
   _____
   _____

   Alternate DoD Sponsor POC (Name, NIPR e-mail, SIPR e-mail, Phone #)
   _____
   _____

2. Cleared Contractor/Non-DoD Location:
   _____

   a. Facility CAGE Code:
      _____
   b. Facility Clearance Level (must be at least Secret):
      _____
   c. COMSEC Custodian:
      _____
   d. SITE POC (Name, NIPR e-mail, SIPR e-mail, Phone #):
      _____

[6] 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) objectives by optimizing use of IP based network infrastructure. Legacy circuits should transition to existing IP bandwidth at DISN Subscriber Service (DSS) locations, or to a readily available commercial IP network at non-DSS locations. Continued use of TDM and other legacy circuits should only be used as a last resort. (ref ah)

3. Please Answer the following:
    a. Cybersecurity Service Provider (MOU/Service Agreement & Funds secured: YES or NO
    b. State how Host Based Security System (HBSS) will be implemented (e.g. provided by sponsor or Cybersecurity Service Provider):

    _____

4. Please provide order dates for the following required equipment:
    a. Crypto (e.g. KIV-7, HAIPE): _____
    b. Perimeter Router (list make/model):_____
    c. Firewall (list make/model):_____
    d. Internal IDS/IPS (list make model): _____

5. Circuit Order Questionnaire are to be turned into the DISN Validation Official at: disa.meade.ns.mbx.siprnet-management-office@mail.mil

References and Helpful Links:

1. DISN Connection Process Guide (ref am)
2. Non-DoD Connection Process: http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Approval
3. DISN customer training; http://iase.disa.mil/connect
4. DISA Approved Products Listing (APL): https://aplits.disa.mil/processAPList.do
5. National Information Assurance Partner (NIAP) Evaluated Products (ref ak): https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm?tech_name=ALL&CFID=17562266&CFTOKEN=d6d9fec5f6ead8d6-91AE90D6-FD36-EBE6-47E2D9D4D8217EB9

A.2 Complete and Submit Non-DoD Connection Request Letter

The sponsor may download the Non-DoD Connection Validation Letter from the DISA Connection Library at: http://disa.mil/connect/library. An example is located in paragraph A.1 above. The sponsor sends the completed letter, with an attached conceptual network topology diagram, to the appropriate DISN Validation Officials. The purpose of the conceptual network topology diagram is to provide the DISN Validation Official enough information to determine if their network/service is appropriate for the customer's mission. A detailed topology diagram is required in the CAP package.

A.3 DISN Validation Official Review

The DISN Validation Official reviews the Non-DoD Connection Validation Letter and network topology to determine the appropriate DISN solution.

A.3.1 Concurs with Solution

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

A.3.2 Non-Concurs with Solution

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

A.4 CC/S/A/ Review

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

A.4.1 CC/S/A Validated Request

If the CC/S/A/ validates the request, the representative will sign the letter and submit it to the Cybersecurity Architecture and Engineering Office in the DoD CIO, Cybersecurity Directorate for DISN access approval (with a copy to the sponsor).

A.4.2 CC/S/A Rejected Request

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

A.5 DoD CIO Review

Cybersecurity Architecture and Engineering Office in the DoD CIO, Cybersecurity Directorate will evaluate the connection request and either approve or deny access to the DISN in support of the sponsor's mission.

A.5.1 Approved Request

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

A.5.2 Denied Request

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

This page intentionally left blank.

APPENDIX B - NON-DOD DISN CONNECTION VALIDATION TEMPLATE

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

A full validation is required for all new circuit requests and significant events to existing DoD CIO Validated requirements. Validation letters are staffed, approved and validated through the CC/S/A HQ Element and sent to the DoD CIO for final approval. Validation/Revalidation letters remain in-effect indefinitely unless any of the following events occur, which will require a full validation through the DoD CIO:

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

Template begins below:

Package #_____
[Provided by DISA]

CCMD/Service/Agency/Field Activity Letterhead

From: DoD organization sponsor Date: DoD Sponsor Letter signed

Memorandum For: DISA/RE
Appointed Validation Official (2nd Endorser)
DoD CIO

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

1. OPERATIONAL REQUIREMENT: (Must answer all sections/questionnaires)
   a. Operational need for connection:
   b. State the DoD mission, program, or project to be supported by this connection
   c. Describe specifically how the connection will support the DoD sponsor organization and contractor or other non-DoD entity mission tasks
   d. Classification/Type of work to be conducted by the contractor or other non-DoD entity:
   e. Specify Classified or Unclassified and/or level, e.g. (Unclassified//for official use only (U//FOUO) – Secret and Top Secret.
   f. Specify type whether command and control, research and development, modeling and simulation, etc. (Specific to Statement of Work (SOW)/Contract)

g. Frequency of use: Describe how frequently the contractor or other non-DoD entity will be required to use this connection in support of the 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. DoD Security Individual: (name/title/unclass e-mail/classified e-mail/phone number from the sponsoring organization that will be assuming responsibility for this circuit)
   d. Cybersecurity Service Provider:
   e. DoD Sponsor Cybersecurity/IA Representative for Combatant Command/Service/Agency/Field Activity (CC/S/A):
   f. Non-DoD Entity/Contractor/Corporate (no acronyms) including the complete connection location address (street, city, state):
   g. Cage Code
   h. CCSD (if revalidating an existing connection)
   i. Funding Source: Responsible funding Source (may or may not be a DoD Sponsor):
   j. If Contractor Info: Contract Number, expiration date, contracting officer name, and phone number
   k. Non-DoD Security DODIN Readiness and Security Inspections (DRSI):

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, cybersecurity 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 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)* (ref d)
- DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)* (ref s) for connections between DoD and contractor information systems
- DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)* (ref e)
- DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* (ref k)
- CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities* (ref b)
- DISN Connection Process Guide (ref am)
- *DoD CIO Office Sponsor Memorandum* (ref m)

Signature _____

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

Sample of an IT Topology Diagram

ILAP Domain Configuration @ ABCDEF Systems

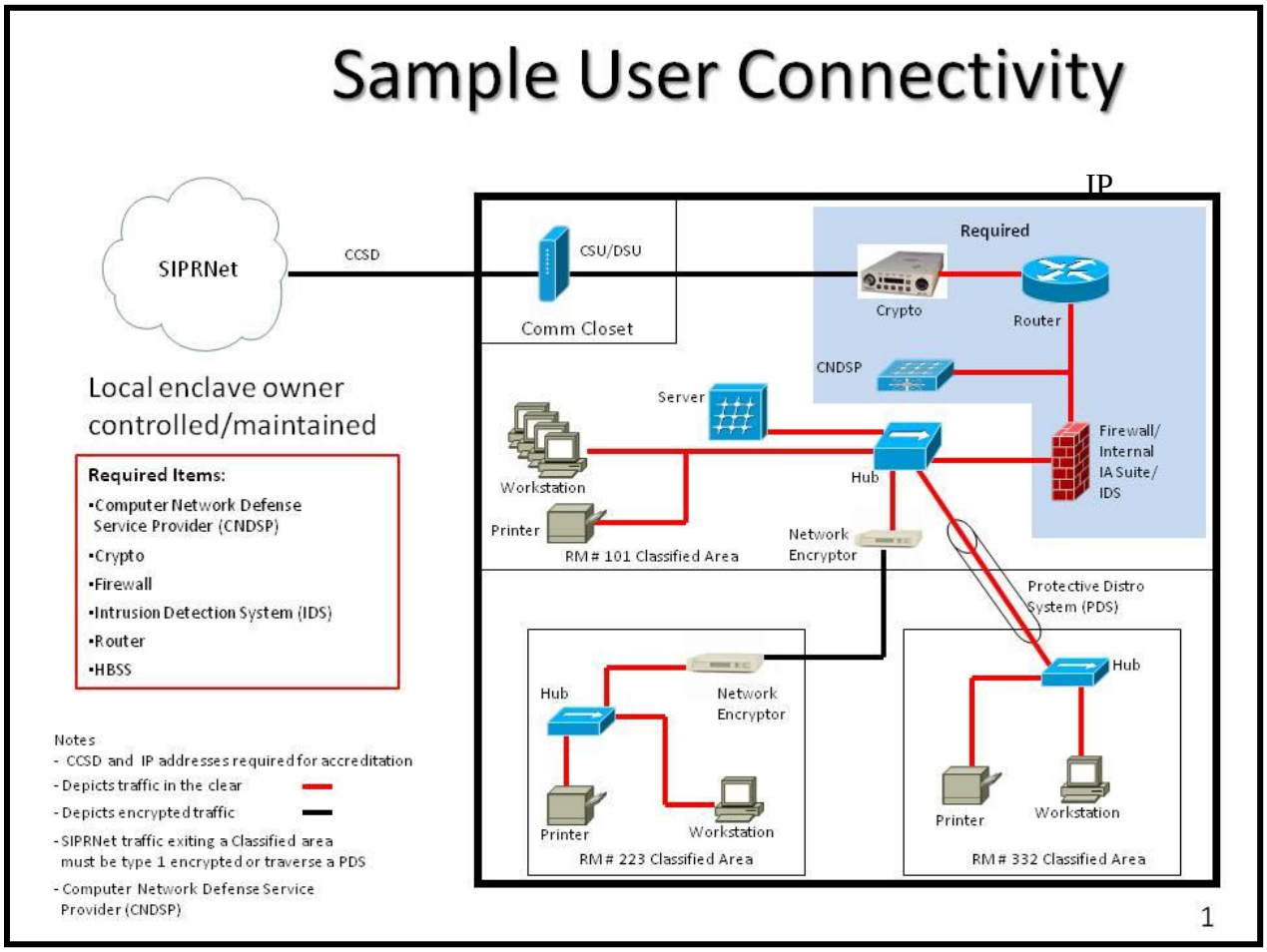

Figure 7: Sample User Connectivity

Identify equipment (e.g., XXX DSU/CSU; CISCO WC-1DSU-T1-V2-RF; Cisco 3600 Router; Cisco IDS 4210 Sensor, Cisco 4900 Catalyst Switch) and include all IP address ranges, equipment make/model and software versions. Tunneling SIPRNet traffic through NIPRNet/Corporate network requires DSAWG review approval in accordance with CJCSI 6211.02D, Defense *Information Systems Network (DISN) Responsibilities* (ref b).

The letter must include signature pages below. All sections in red **must** be filled out by the Sponsor. Signatures will be obtained within the respective offices.

Template begins below:

1st Endorser Date

We have reviewed/discussed this connection request with the DoD Component/
Mission Partner's sponsor - Concur or non-concur.
DISN Validation Official

2nd Endorser (Appointed Validation Official) Date

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

SIGNATURE
CC/S/A Validation Official

Template ends

APPENDIX C - NON-DOD DISN CONNECTION REVALIDATION TEMPLATE

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

A revalidation review is only required if there is a new contract with the same contract vendor/mission. Revalidations are not required for contractor option years or contract extensions.

Template begins below:

Package #_____
[provided by DISA]

Combatant Commands/Services/Agency's Letterhead

From: DoD organization sponsor Date: DoD Sponsor Letter sign

Memorandum For DISA/RE

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

1. OPERATIONAL REQUIREMENT (Must answer all sections/questionnaires):
   a. State the DoD mission, program, or project to be supported by this connection
   b. Describe specifically how the connection will support the DoD sponsor organization and contractor or agency mission tasks
   c. State whether there has been any change to the mission, contract, location, or sponsor. Any one single change will require a full evaluation through DISA to the CC/S/A CIO to DoD CIO

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

   d. Classification/Type of work to be conducted by the contractor or agency:
   e. Specify Classified or Unclassified
   f. Specify whether operations, sustainment, command and control, research and development, modeling and simulation, etc. (Specific to Statement of Work (SOW)/Contract)
   g. Frequency of use: Describe how frequently the contractor or agency will be required to use this connection in support of the DoD mission, program or project

2. Mission Partners/INFORMATION:
   a. DoD Sponsor Unit:
   b. DoD Sponsor: (name/unclass e-mail/classified e-mail/phone number)
   c. DoD Security Individual: (name/unclassified e-mail/classified e-mail/phone number from the sponsoring organization that will be assuming responsibility for this circuit)

d. Cybersecurity Service Provider
e. Non-DoD Agency/Contractor/Corporate (*no acronyms*) including the complete connection location address (*street, city, state*):
f. DoD Contract Name/Number/Expiration Date:
g. Cage Code:
h. CCSD #:

3. CONNECTION DETAILS:
a. Complete Connection location 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, cybersecurity 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 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)* (ref d)
- DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)* (ref s) for connections between DoD and contractor information systems
- DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)* (ref e)
- DoDI 8530.01, *Cybersecurity Activities Support to DoD Information Network Operations* (ref k)
- CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities* (ref b)
- DISN Connection Process Guide; http://www.disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/DISN_CPG.pdf
- *DoD CIO Office Sponsor Memorandum* (ref m)

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

Endorsement:

Page break to remain between the main body and Endorsement template below. All information in red below is to be completed. The completed document is to be e-mailed back to: disa.meade.ns.mbx.siprnet-management-office@mail.mil.

1. The DISA IE 11 Division has reviewed the supporting documentation for this request and acknowledges SIPRNet is still the appropriate DISN solution for CCSD XXX in support of Non-DoD agency located at *City, State* to the classified DoD enclave SIPRNet through the end of the contract or end of the ATO, whichever comes first.

2. A revalidation review is required on a reauthorization connection when the DoD CIO approval has expired. In the event any one item changes, a full DoD CIO revalidation will be required.

The DoD sponsor must also ensure connectivity requirements are properly coordinated, periodic inspections are conducted, and adequate controls are in place IAW:

- DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)* (ref d)
- DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM* (ref s) for connections between DoD and contractor information systems
- DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)* (ref e)
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information network Operations (ref k)
- CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities* (ref b)
- DISN Connection Process Guide (ref am)

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

A customer with an account can access the SIPR IT Registry at: http://osdext.osd.smil.mil/sites/dodcio/itregistry/default.aspx.

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

For additional information contact the DCCC at: (844) 347-2457, Option 2; CML: (614) 692-0032, Option 2; DSN: (312) 850-0032, Option 2; disa.dccc@mail.mil; disa.scott.conus.mbx.dccc@mail.smil.mil.

DISN Validation Official

This page intentionally left blank.

APPENDIX D - REMOTE COMPLIANCE MONITORING

D.1 Vulnerability Scanning

The Defense Information Systems Agency Risk Adjudication and Connection Division performs remote compliance scanning for all new DISN connections, for reauthorized connections, and on a on a case-by-case basis when requested for DISN connected enclave owners. RE 4 provides vulnerability scan result letters to the SGS POCs on the details of all scan results, and therefore it is crucial for AOs' and enclave owners to keep their information in SGS current. All RE 4 scans are currently uncredentialed.

D.1.1 Scan Types

- Unannounced scans, test the CCSD's circuit perimeter with penetration tools in order to assess its ability to deny intrusion from an unknown source
- Announced scans are coordinated with the CCSD owner to allow a known or "trusted" IP address to scan for vulnerabilities
- Interim Authority To Test (IATT) scans complete the Connection Approval Process for all new connection requests by conducting a vulnerability assessment (similar to an Announced scan)
- Ad Hoc scans are requested by customer organizations and can be either a perimeter defense scan and/or vulnerability assessment

D.1.2 Unannounced Scan

- Performed from a server which uses an unknown IP, to ascertain the defense in depth stance by simulating a probe from an unknown attacker
- A pass rating is attained when none of the devices on the inside of the network can be identified. Should any devices be identifiable within the internal network, it will be considered a failure of the perimeter's defense
- Only in the event of a failed penetration test will the results be forwarded to the POCs listed in SGS. Otherwise, a vulnerability scan (Announced) will commence

D.1.3 Announced Scan

- After a site passes the Unannounced scan, the Announced Scan portion is conducted
- The POC(s) listed in SGS will coordinate with the Scan Team for the IP Address to permit access to the CCSD. A passed rating is attained when no RMF critical/very high/high vulnerabilities, or DIACAP Category (CAT) I vulnerabilities are found IAW current STIGs
- A failed rating is assigned when RMF critical/very high/high vulnerabilities, or DIACAP Category (CAT) I vulnerabilities are found, or the announced scan was unable to access the circuit. Results will be uploaded into SGS and sent to the POCs listed in SGS for review and mitigation

D.1.4 IATT Scan

- IATT Scans are performed on all new SIPR circuit requests as a requirement for an Authority to Connect/Interim Authority to Connect (ATC/IATC)
- IATT scans are conducted the same as an Announced Scan
- Please reference the IATT Process Checklist below

D.1.5 Ad Hoc Scan

- Ad Hoc scans are conducted on request, usually as a rescan to confirm remediation of initial failed scans. Sites that fail any type of scan may request a rescan
- (A rescan for a failed Announced Scan would not be subject to an Unannounced scan)
- The requirements for pass/fail remain the same as the original scan
- An Ad Hoc Scan typically takes up to 8 business days to complete, but may require more time depending on network size

D.1.6 Cyber Hygiene Analysis (CHA)

The overall objective of the Cyber Hygiene Analysis (CHA) is to aid enclave owners in their ability to improve their respective cybersecurity posture. The Risk Adjudication and Connection Division's CHA efforts are focused in three areas: assisting enclave owners and DISA DODIN Readiness and Security Inspections (DRSI/RS) in preparing for or conducting Command Cyber Readiness Inspections (CCRIs), fulfilling individual AO (formerly DAA) CHA requests, and performing CHAs in support of requesting enclaves on the DODIN.

The CHA capability combines results of passive DISN backbone sensors and active tools,[7] which when employed effectively, can present a more holistic and accurate picture of the health of a perspective enclave. In particular, CHA analysts look for evidence of compliance with DoDI 8551.01, *Ports, Protocols, and Services Management* (ref e) requirements, proper boundary configurations, Operational System (OS) fingerprinting, vulnerability analysis, and evidence of proper CDS configuration. Effectively using this expanded CHA information will potentially allow the Compliance Monitoring Team (CMT) to provide perspective enclave owners a more in depth and accurate input to better prepare for upcoming CCRIs, cross validate Continuous Monitoring and Risk Scoring (CMRS) results, and assist enclave owners in improving their own effective cybersecurity decisions. In addition to CHAs providing useful vulnerability information in preparation for CCRIs, CHAs may also provide valuable CCRI follow-on analysis information. Ultimately, the CHA effort is designed to help, not penalize, DoD and its mission partners to improve the overall cybersecurity of the DODIN. If interested in participating in the CHA, please contact the CMT POC found in paragraph E3 below.

[7] DISA RE 4 active scanning will only be conducted on DISA enclaves with the enclave owner's permission, or as approved by USSTRATCOM and USCYBERCOM jointly in accordance with CJCSI 6510.01F (ref t).

D.2 Frequently Asked Questions (FAQs)

Q: I received results from a scan, but some of the recipients no longer work for/with my site. What do I need to do to get this changed?
A: When the POCs or site information for the CCSD change, please log on the SGS database at https://giap.disa.smil.mil/gcap/home.cfm and update the POCs for the perspective CCSD.
Q: I received a failed Unannounced/Announced IATT scan. What steps do I need to take now?
A: For Unannounced scans, review the boundary protection systems to ensure they are locked down as much as possible. For Announced scans, review the RMF critical/very high/high findings or DIACAP Category (CAT) I findings and fix/mitigate them. Once these items have been addressed, contact the CAO CMT to schedule an Ad Hoc scan.

D.3 IATT Process Checklist

Steps To be Completed PRIOR to an Initial Scan for ATC/IATC Issuance:	
1	Equipment installed, configured, and turned on.
2	72 hour burn-in completed by IT&A.
3	At least one (1) server, workstation, or laptop with at least one (1) port, protocol or service enabled. (Please refer to PPSM for allowed ports and protocols – disa.meade.ns.mbx.ppsm@mail.mil)
4	HBSS disabled for initial scan or Compliance Monitoring Team (CMT) "Announced" IP Address added to the HBSS allowed IP's.
5	Windows firewall disabled for the target system(s) initial scan.

Table 14: Steps to Complete Before an Initial Scan

Compliance Monitoring Team (CMT) Contact Information	
NIPR Scan E-mail	disa.meade.ns.mbx.caoscans@mail.mil
SIPR Scan E-mail	disa.meade.ns.mbx.caoscans@mail.smil.mil
Phone (Commercial)	301-225-2902
Phone (DSN)	312-375-2902

Table 15: CMT Contact Information

Implementation Test and Activation (IT&A) Contact Information	
Phone (Commercial)	618-220-8627

Table 16: IT&A Contact Information

DISN Customer Contact Center (DCCC)	
Unclassified E-mail	disa.dccc@mail.mil
Classified E-mail	disa.scott.conus.mbx.dccc@mail.smil.mil
Phone (Commercial)	844-347-2457, Option 2 or 614-692-0032, Option 2
Phone (DSN)	312-850-0032, Option 2

Table 17: DCCC Contact Information

This page intentionally left blank.

.

APPENDIX E - DSN/UC PRODUCTS - UNCLASSIFIED

This appendix provides the necessary steps and information to process a Defense Switched Network (DSN) telecommunication switch and Unified Capabilities (UC) product connection to the DISN provided transport (including data, voice and video). This appendix is intended to supplement the detailed information provided in Section 3.6 of this guide with DSN unclassified voice switch specific information. Any variations from those steps or additional requirements are identified in this appendix.

E.1 DSN Connection Process

Follow steps in the Customer Connection Process (Section 3) of this guide.

E.2 Process Variations and/or Additional Requirements

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

Connection of a DSN telecommunication switch or UC product to the DISN requires procurement of interfacing hardware and/or software components that are identified on the DoD UC Approved Products List (APL). All items on the UC APL are required to be certified for interoperability and cybersecurity in accordance with DoDI 8100.04, *Unified Capabilities* (ref g). If the intended product is not on the UC APL, it will either need to be JITC Interoperability IO and cybersecurity/IA tested and certified and placed on the UC APL, or authorized for purchase via DoD CIO temporary exception to policy before the product can be purchased and connected to the DISN in accordance with DoDI 8100.04, *Unified Capabilities* (ref g).

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

- DSN/DoD UC APL pages: https://aplits.disa.mil/processAPList.do
- UC APL Testing and Certification: https://www.disa.mil/Network-Services/UCCO
- DSN Services and Capabilities: http://www.disa.mil/Network-Services/Voice

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

- Voice softswitches connected to the DISN shall be registered in SNAP DSN and obtain connection approval. (i.e., Local Session Controller (LSC), SoftSwitch (SS), Enterprise Session Controller (ESC))

IAW DoD Unified Capabilities Master Plan (UC MP); Section 5.d. (1) (h) and (i); Pg. 28, 29 **(**ref u).

Circuit switched based services shall begin migrating to IP-based non-assured/assured services over DoD Component Assured Services Local Area Networks (ASLANs)/Intranets and UC transport using products from the DoD UC APL. During this implementation timeframe, both converged and non-converged UC shall be provided by Time Division Multiplexing (TDM)/Internet Protocol (IP) hybrid technologies.[8] The Voice over Secure Internet Protocol (VoSIP), Digital Video Services (DVS), Standard Tactical Entry Point (STEP)/Teleport, and deployable programs shall upgrade respective infrastructures using products from the DoD UC APL. The phase out of circuit-switched technologies shall be based on the following individual conditions:

- New TDM Circuit Switched Products. New TDM circuit switched products shall no longer be tested and certified for placement on the UC APL as of January 2011.
- Existing UC APL Circuit Switched Products. Existing circuit switched products on the UC APL may be purchased until certification/assessment expires and removed from the APL.
- Installed UC Circuit Switched Products. Existing circuit switched products already installed, UC APL products procured before the UC APL expiration date, or on the Retired UC APL List may remain until business case or mission need dictates replacement, or vendor is no longer willing to support. Continued testing and certification for software patches is allowed for these components while in use, however this testing and certification/assessment shall not result in renewed UC APL status.

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) objectives by optimizing use of IP based network infrastructure. Legacy circuits should transition to existing IP bandwidth at DISN Subscriber Service (DSS) locations, or to a readily available commercial IP network at non-DSS locations. Continued use of TDM and other legacy circuits should only be used as a last resort. (ref ah)

DISA shall deploy SoftSwitch (SS), allowing DoD Components to implement UC employing IP while maintaining backward interoperability with the remaining circuit-switch/TDM technologies. DISA's enterprise voice and video services, with collaboration capabilities (Instant

Messaging (IM), presence, and chat), shall be evaluated during UC Pilot Spiral 2 and shall begin operations in select geographic regions during this timeframe.

- VoIP capable softswitches that are configured to function as a Private Branch Exchange (PBX1) and connected behind the local user's installation DSN End Office (EO)/Small End Office (SMEO) do not require a SNAP registration or connection approval; unless, directed as a MAJCOM, CCMD or Theater Command requirement. The PBX1 voice switch shall be identified on the customer's host installation enclave topology for the associated DSN EO/SMEO voice switch RMF/DIACAP package
- All TDM/DSN voice switches connected to the DSN as a servicing voice switch in accordance with CJCI 6211.02D (ref b) will be registered in SNAP DSN and obtain connection approval
- ALL TDM/DSN voice switches connected behind the local user's installation DSN EO/SMEO do not require a SNAP registration or connection approval; unless; directed as a MAJCOM, CCMD or Theater Command requirement (e.g., PBX1, PBX2, Network Element (NE) SHOUTS, Remote Switching Unit (RSU)). These type of switches will be identified and depict the interconnection to the host installation DSN EO/SMEO in the enclave topology diagram
- ALL TDM/DSN voice switches that connect via a tandem/nodal connection to the Multifunction Switch (MFS) will be registered in SNAP and obtain a DoD CIO temporary exception to policy in accordance with DoDI 8100.04 (ref g) or have a completed Tailored Internet Service Provider (ISP) for connection approval (e.g., PBX1, NE-SHOUTS, Switch Multiplex Unit (SMU), Inverse Multiplexer (IMUX))
- 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 and obtain connection approval, if they have not previously obtained formal connection approval
- Customers requesting connection approval for a legacy switch that has fallen off the UC End of Sale list must register the voice switch in SNAP DSN and obtain a DoD CIO temporary exception to policy
- Customers that procure a legacy voice switch that is on the UC APL End of Sale list are required to register the voice switch in SNAP DSN and obtain a DoD CIO temporary exception to policy
- PBX2 switches can only be procured or implemented after obtaining a DoD CIO temporary exception to policy waiver for Military Unique Feature (MUF) requirements by the DoD CIO's office in accordance with DoDI 8100.04, *Unified Capabilities* (ref g).

E.3 DSN CONNECTION PROCESS CHECKLIST

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

Item	DoD Component		Mission Partner	
	New	Existing	New	Existing
Obtain DoD CIO approval for Non-DoD connection			√	*
Obtain APL approval for voice equipment not currently on the APL list in accordance with (ref g)	√		√	
Provision the connection	√		√	*
Perform the A&A process	√	√	√	√
Obtain an Authorization to Operate (ATO)	√	√	√	√
Register the connection	√	**	√	*
Register in the SNAP database	√	**	√	*
Register in the PPSM database	√	**	√	*
Register in the DITPR database	√	**	√	*
Complete the CAP Package	√	√	√	√
DIACAP Executive Package/RMF Security Authorization Package (or equivalent)	√	√	√	√
DIACAP Scorecard/RMF Security Assessment Report	√	√	√	√
System Identification Profile (include switching equipment—i.e., vendor model and software)/System's Security Plan	√	√	√	√
Plan of Actions and Milestones, if applicable	√	√	√	√
AO Appointment current in database	√	√	√	√
Network/Enclave Topology Diagram	√	√	√	√
Consent to Monitor	√	√	√	√
Proof of Contract			√	√
DoD CIO Approval Letter			√	√
Complete ATC Submittal form (see 1.4)	√	√	√	√
Submit the CAP Package to the CAO	√	√	√	√
Receive DSN ATC/IATC	√	√	√	√

Table 18: DSN Connection Process Checklist

* - This step is not required for existing mission partner connections unless there has been a change in Sponsor, mission requirement, contract, location, or the connection has not been registered.
** - This step is not required for existing connections that are already registered and where all information is current.

E.4 Points of Contact:

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

Table 19: Unified Capabilities Certification Office (UCCO) E-mail Address

Connection Approval Office (CAO)	
Connection Approval Office for DSN Connections	disa.meade.ns.mbx.cao-dsn@mail.mil disa.meade.ns.mbx.cao-dsn@mail.smil.mil
Phone (Commercial)	301-225-2900, 301-225-2901
Phone (DSN)	312-375-2900, 312-375-2901
Address	Defense Information Systems Agency ATTN: RE 41 PO Box 549 Fort Meade, MD20755-0549

Table 20: Connection Approval Office (CAO) Contact Information

E.5 Topology Diagram Requirements

Network Topology Diagram/SDD – this diagram depicts the network topology and security posture of the customer enclave that will be connecting to the DISN.

The Network Topology Diagram should:

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

- Identify Internetworking Operating System (IOS) version
- Include the model number(s) and IP's of the devices on the diagram; diagram must show actual and planned interfaces to internal and external LANs or WANs (including backside connections)

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

All TDM/IP DSN topologies must include:

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

Addendum for voice switches connecting to ASLAN or Assured Services Virtual Local Area Network (ASVLAN):

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

Addendum for voice softswitch and Enterprise Session Controller connections to the DISN:

- Depict the function and location of the source softswitch 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 SBC)
- Depict NIPRNet CCSD(s) providing the Ethernet/IP connection within the enclave (preferably near the CER)
- Select connection type "backbone" if the softswitch or Enterprise Session Controller is managed by DISA and provides UC services for multiple DoD and mission partners.

E.6 SNAP DSN Switch Registration and RMF/DIACAP Submittal Process:

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

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

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

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

- Once all sections are completed, with the exception of Section 10 and Section 11.12; A Submit button at the bottom of the screen will be available in order to submit the entire registration for "Validator Approval"
- SNAP DSN Validator Role
- The SNAP DSN validator reviews the contents of all submitted connection requests within his or her agency or sub-agency and either approves or rejects the registration based on conformity, completeness, and correctness
- If the validator rejects a request, the reason is captured in the comment and the POCs identified in the registration are notified via an automated e-mail. The requestor or one of the POCs in the registration must update and complete the rejected sections and resubmit the registration

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

For 24/7 SNAP assistance; contact the DCCC at (844) 347-2457.

E.7 Sample Topology Diagrams

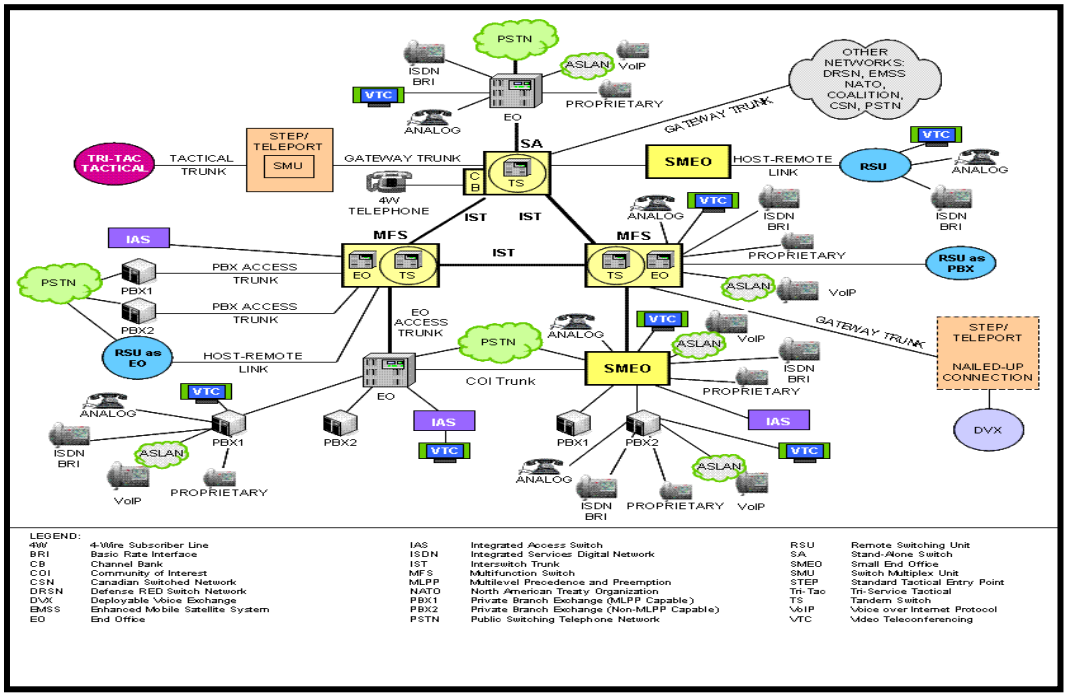

Figure 8: Sample DSN Topology

E.8 Example Installation Configurations

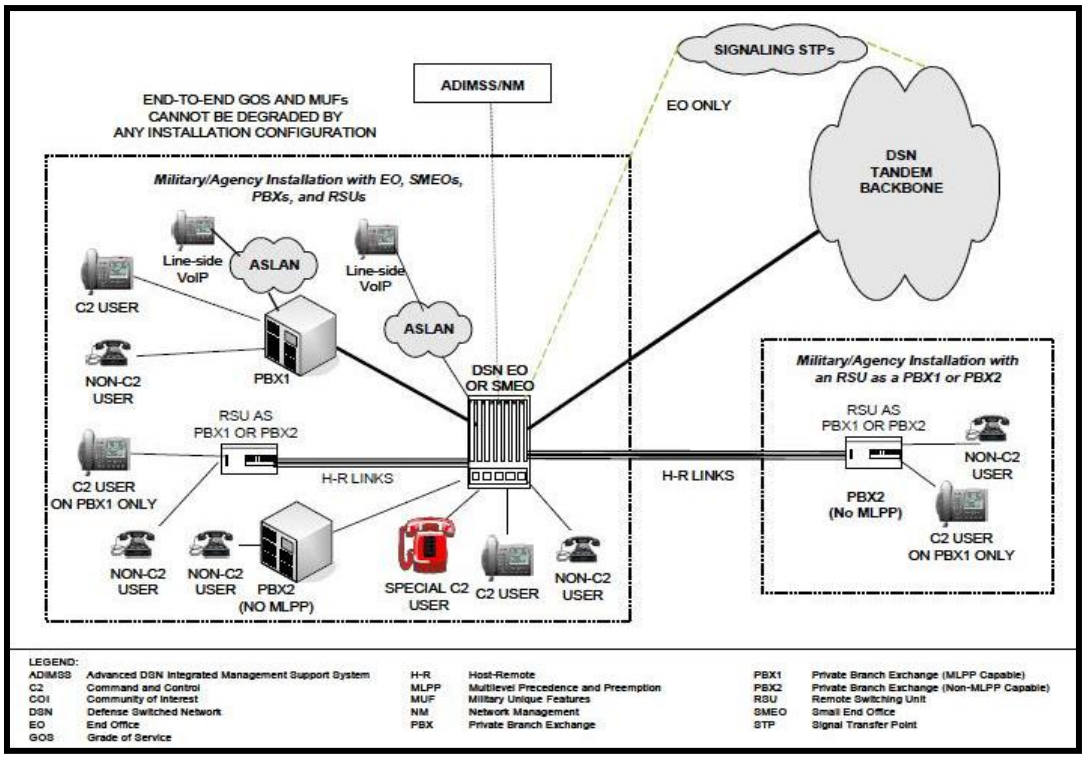

Figure 9: Example Installation Configurations

APPENDIX F - VPN REGISTRATION (PRIVATE IP)

DISN VPN services provide an enterprise-wide solution to all DISN customers who need to segment their IP traffic from that of other customers using MPLS to create VPNs. These services are offered as capabilities provided on the Sensitive but Unclassified (SBU) data network and are transport services only. As such, the connection process differs slightly from that usually required for connection to NIPRNet/SIPRNet. For VPN services, the customer is required to register each VPN and connections to the VPN are tracked in the SNAP/SGS database. The customer is responsible for ensuring that the appropriate Cybersecurity services, capabilities and measures are in place on the system/network associated with the VPN.

The DISN Test and Evaluation Service (DTES) is hosted as a Layer 3 VPN (L3VPN) across the DISN Internet Protocol (IP) core, providing IP transport-only service for test and evaluation (T&E) and test and development (T&D) Communities of Interest (COIs). VPN solutions isolate COIs as separate enclaves and segregate test traffic from the operational network using Multi-Protocol Label Switching (MPLS), VPN tunnels, network encryption, approved Type I encryption devices, and/or other approved solutions as needed.

USCYBERCOM) distributed TASKORD 12-0371 instructing all CCSAs to transition all Unrestricted and Restricted public facing applications into a DMZ Extension. The NIPRNet Internet Access Point (IAP) Demilitarized Zone (DMZ) Virtual Private Network (VPN) Community of Interest Network (COIN) (IAP DMZ VPN) is designed to improve security posture to protect DoD assets by isolating public facing Internet applications traffic flows from the NIPRNet flows. CCSAs network administrators who are responsible for providing the routing policy on the customer premise routers will use the "*Internet Access Point Demilitarized Zone Virtual Private Network Community of Interest Customer User's Guide*" which supplements the *VPN Customer Ordering Guide* and provides additional information to assist customers in ordering the IAP DMZ VPN service via DDOE/Storefront and ensuring the DMZ extensions are compliant with the *NIPRNet DoD DMZ Security Technical Implementation Guidance (STIG)* requirements.

The VPN customer guides are located in the 'Policy→User Guide' modules of the SNAP and SGS databases.
(https://snap.dod.mil/gcap/user-guide.do)
(https://giap.disa.smil.mil/gcap/user-guide.do)

For assistance contact the DISN Customer Contact Center (DCCC).

DISN Customer Contact Center (DCCC)	
Unclassified E-mail	disa.dccc@mail.mil
Classified E-mail	disa.scott.conus.mbx.dccc@mail.smil.mil
Phone (Commercial)	844-347-2457, Option 2 or 614-692-0032, Option 2
Phone (DSN)	312-850-0032, Option 2

Table 21: DCCC Contact Information

This page intentionally left blank.

APPENDIX G – DOD CIO DODIN WAIVER PROCESS - UNCLASSIFIED

The DoD CIO is revising the DODIN Waiver Process. Please contact osd.pentagon.dod-cio.mbx.dcio-cs-ae@mail.mil for further information.

G.1 Point of Contact

POC For the DoD CIO Temporary Exception To Policy Process	
DoD CIO, Security Architect/Engineer	osd.pentagon.dod-cio.mbx.dcio-cs-ae@mail.mil

Table 22: Point of Contact for the DoD CIO Temporary Exception to Policy Process

This page intentionally left blank.

APPENDIX H - DOD CROSS DOMAIN SOLUTION (CDS) APPROVAL PROCESS

H.1 Cross Domain Solution: Definition

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. (ref ad)

H.2 DoD CDS Approval Process Scope, Applicability and Exclusions

The DoD CDS process covers CDSs connecting to networks classified Top Secret (TS) and below, including standalone, isolated, and test networks. This includes Intelligence Community (IC)-owned CDSs which connect to DoD networks (but not to TS-SCI). CDS devices connecting to networks classified TS – Sensitive Compartmented Information (SCI) and above follow different approval processes as determined by DNI policy and guidance.
This process is separate from the review and approval of the ATC for the Command Communications Service Designators (CCSD). However, a Cross Domain Solution Authorization (CDSA) will not be issued beyond the connection approval date granted for the enclave in which it resides. This appendix provides the steps necessary to obtain a CDSA which is the official document authorizing operational use of a Cross Domain (CD) device per DoDI 8540.01 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) in accordance with this instruction."*

H.3 Categories of Cross Domain Solutions

The two main categories of CDSs are Point to Point CDSs and Enterprise Cross Domain Solutions (ECDS). A Point to Point Solution is purchased, implemented and managed by a component within the authorization boundary of the components own network. An Enterprise Solution is centrally managed and provides CD Services to multiple components.

Per DoDI 8540.01 3.e "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."

1. Point to Point CDSs:
   a. Standard Point to Point
      i. Includes access, transfer and multi-level solutions
   b. For Tracking Purposes Only (FTPO) CDS: Four Cases of Transfer CDSs:
      i. Completely Isolated: The networks connected to the CDS are completely isolated.

ii. Controlled Interfaces of Interest: The CDS is connected to two networks of the same security classification which 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 (VLoR assertions) (ref aa) and VLoR Implementation Guide (ref z) is a transfer CDS architecture/system which implies that the low side system(s) provide very minimal threat to the high side network and the solution and its connected enclaves present minimal risk to the High side enclave(s). VLoR 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 which forward network traffic into a closed collection enclave for analysis. In such cases the CDSE and CDTAB 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.

2. Enterprise Cross Domain Solutions

   a. ECDS Candidate:

      i. This term refers to a component with CDS requirements in negotiation with a CDS Enterprise Service Provider which will be brought through the CDS Phase 1 just as any other point-to-point CDS. Once ECDS implementation is approved at the DSAWG in Phase 1 the DSAWG Secretariat will close the original CDS Request in SGS. The requirement will be implemented on an ECDS System under an ECDS Ticket number

   b. ECDS CDS System Ticket or Request

      i. An ECDS System Ticket or Request is a CDS which represents a centrally managed service which supports multiple components

3. IC Owned Cross Domain Solutions

   a. This is a cross domain solution which is owned, approved, and managed by an intelligence agency. Only IC devices connecting 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

The CDS Authorization process for all categories except the IC CDS Registration process is included in section H.4. The IC CDS Registration Process is described in Section H.10.

H.4 CDS Authorization Process

The CDS Authorization Process consists of four distinct phases, however depending on the classification of CDS as described in Section H.3 some of the phases may be compressed. The figures below cross reference the different RMF steps to the various CDS phases and provide greater detail for each of the phases. The four phases are:

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

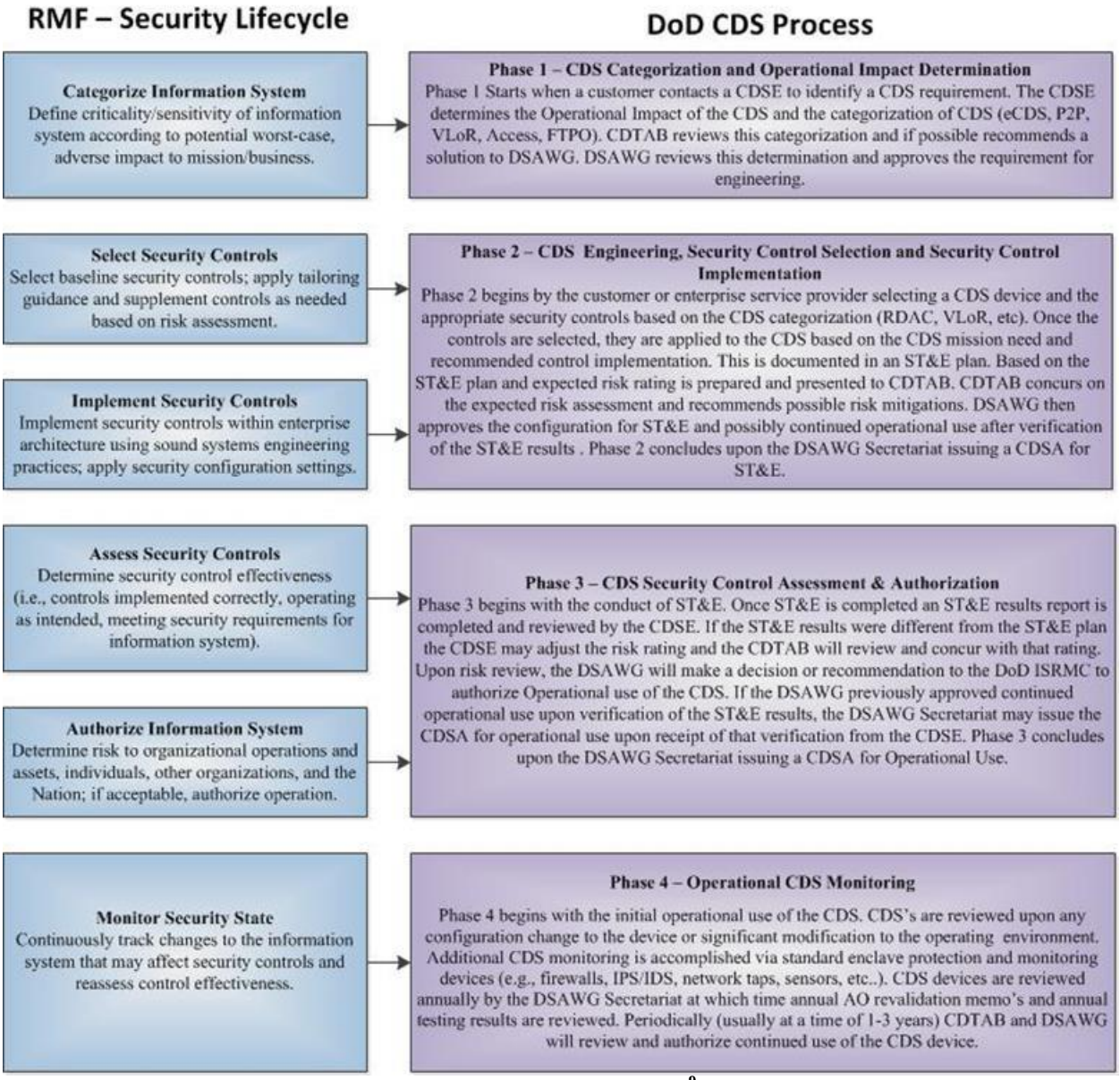

Figure 10: RMF Lifecycle[9]

[9] Note the transition to RMF brings changes in terminology. For example the term "Site Test and Evaluation (ST&E)" is being superseded by the term "Site-Based Security Assessment (SBSA)"

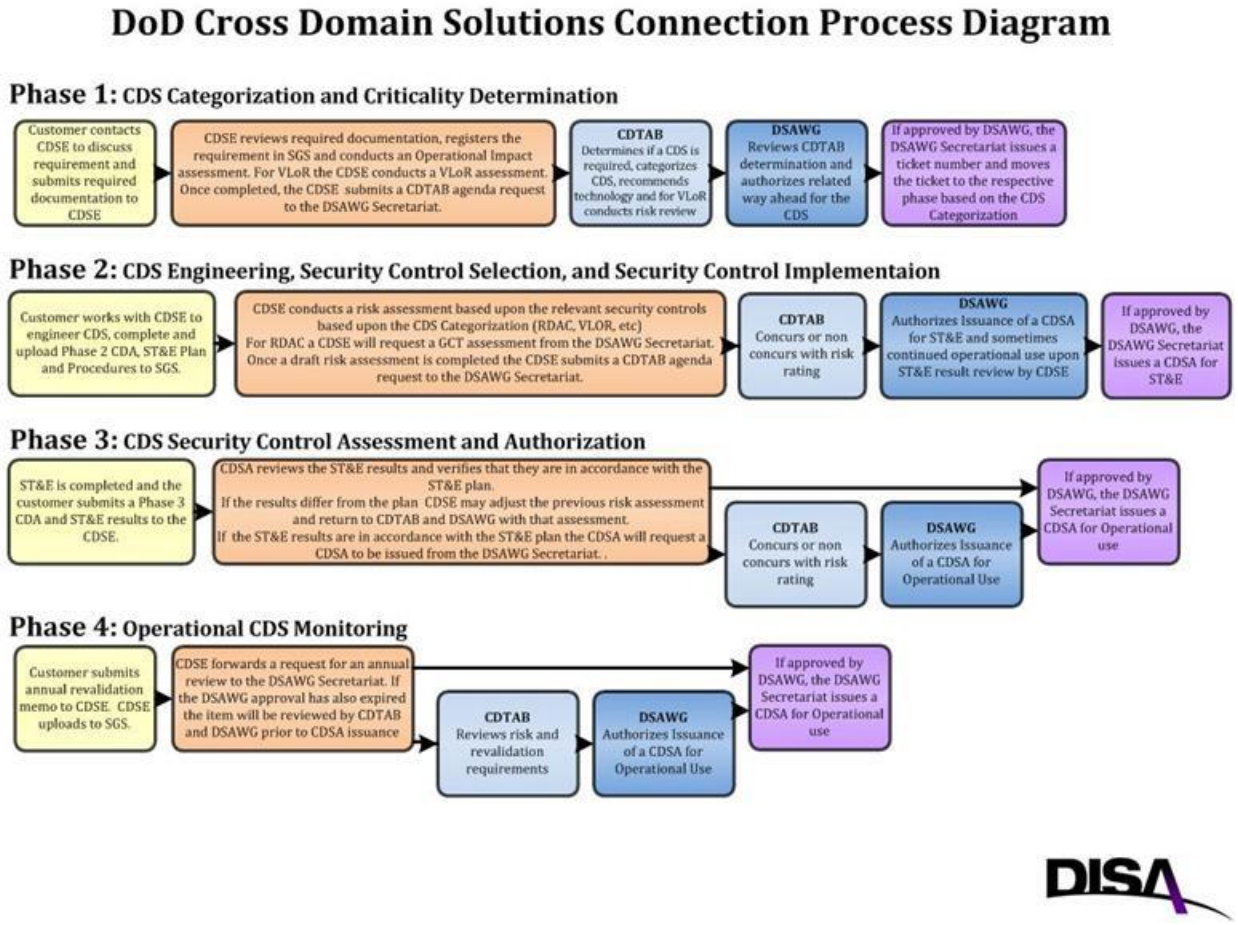

Figure 11: CDS Connection Process

H.5 Phase 1: CDS Categorization and Criticality Determination

Phase 1 of the CDS process consists of five specific actions. Any exceptions to the CDS process must be coordinated with the Cross Domain Support Element (CDSE) and Cross Domain Technical Advisory Board (CDTAB) Charter (ref ac) Chair.

1. The CDS component must coordinate with their respective CDSE representatives to determine and document the information transfer and mission requirements. If uncertain about whom the respective CDSE is, would like information on standing up a CDSE, or would like to utilize the services of another CDSE, please review 8540.01 Enclosure 5 CD and RMF Roles paragraph 4. CDSE (ref ad).

Per DoDI 8540.01 Enclosure 5.4.g. "Support to Combatant Commands will be in accordance with DoDD 5100.03." *Support of the Headquarters of Combatant and Subordinate Joint Commands"* (ref ad)

a. DoD component's respective CDSE obtains access to SGS, opens a new CDS request filling out all required database fields, and uploads all required documents as stated in item c below.

b. Access to the SGS database: To obtain access to the SGS database CDSEs go to https://giap.disa.smil.mil and select "request an account." The CDSE will be required to upload a completed DD2875. A template is provided on the entry page of the website.

c. Phase 1 Documentation Requirements: (must be uploaded in SGS)

i. Validation Memorandum, Authorization Official O-6 or civilian equivalent signature required

ii. Cross Domain Appendix with Section 1.0 Completed, Designated Command Representative signature required in phase 1

iii. DISA Cross Domain Enterprise Service Response Memorandum
- This will be provided by DISA Cross Domain Enterprise Services (CDES) once the component submits a CDES Questionnaire to DISA CDES.
- A CDES Memorandum is not required if the CDS Configuration meets a requirement specifically called out in the CDES Non-Consideration Memorandum or if the DSAWG or DoD ISRMC have designated the requestor as a mission specific enterprise service.

iv. VLoR Additional Phase 1 Requirements:
- CD Appendix (CDA) Section 2.0 Completed (Section 2.1 not required)
- Site Based Security Assessment (SBSA) Plan (detailed procedures not required)
- VLoR Assertions Response Completed

d. Repeatable Accreditation/Authorization Additional Phase 1 Requirements:

i. Repeatable CDS Entrance Criteria Checklist (ref af) (Copy and paste the following link into the web browser.)
https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fdsawg%2FShared%20Documents%2FCDS%2FRepeatable%5FAccreditation%5FCriteria&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence

ii. Planned Repeatable Inventory Template

iii. The requirement for Repeatable Accreditation/Authorization should also be documented within section 1.0 of the CDA

Per 8540.01 (ref ad), Enclosure 4.b.4 "The DoD Component CDS owner must establish a tracking process approved by the CDSE and must track 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."

2. The DoD mission partner's respective CDSE validates and prioritizes the request by completing the SGS Validation Section including the Validation and Operational Impact Determination sections 6.3 and 6.5 for the respective request and submits an agenda request form (ref aj) to the DSAWG Secretariat. All agenda requests must be submitted by the respective CDSE to the DSAWG Secretariat 14 calendar days prior to the next CDTAB meeting. Agenda requests will not be accepted by the DSAWG Secretariat directly from the Component. The DSAWG Secretariat will verify that all required items have been submitted and notify the CDSE of the CDTAB date or if additional items are needed.
3. CDTAB Phase 1 Review. During the CDTAB review, the CDTAB will review the requirement and determine if a CDS is required to meet the mission requirement. CDTAB will also :
   a. For a Standard Point to Point: Recommend a baseline solution to meet the transfer or access requirement and review the CDES response or grounds for CDES exclusion as to why CDES is not being used.
   b. For a FTPO (non-VLOR) request: Determine if the criteria for a "tracking purposes only" CDS have been met.
   c. ECDS Candidate where the Enterprise CD Service Provider (ECDSP) has responded they can meet the requirement and the Component intends to utilize CDES services: ensure there is a valid mission requirement for the proposed solution.
   d. ECDS CDS Request: review the proposed system architecture and the DSAWG approved component requirements (specific component requests approved by DSAWG for ECDS implementation) and make any comments/suggestions regarding the technology selection.
   e. For FTPO VLoR: Conduct a Risk Review of the VLoR assertions and make a determination if the CDTAB determines the requirement meets the intent of VLoR.
   f. For Repeatable Accreditation Candidate CDS: Review the architecture, CDS and data flows and provide comments to DSAWG For Repeatable Accreditation/Authorization Candidate: Determine if Repeatable Accreditation/Authorization Requirements are met.

4. DSAWG Phase 1 Review: The DSAWG will review the CDTAB's recommendation and comments and make a decision 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 Standard Point to Point: Approval for ticketing and phase 2 analysis OR direction that ECDS must be utilized.
   b. For a "FTPO" (non-VLOR) request: Approval for 3 years of operational use. SBSA approval is within AO purview and does not require separate DSAWG approval)

c. For an ECDS Candidate where the ECDSP has responded that they could meet the requirement and the Component intends to utilize CDES services: approval for ECDS implementation.

d. For FTPO 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.

5. Based on the DSAWG decision, the DSAWG Secretariat will update SGS milestones and also take the following actions based on the approval which was given: (see Section H.9)

H.6 Phase 2: CDS Security Control Assessment & Authorization

This phase applies only to Standard Point to Point solutions and ECDS Systems which are required to receive a Risk Decision Authority Criteria (RDAC) (ref ag) analysis. FTPO Tickets usually skip this phase.

1. The component or ECDSP works with their respective CDSE to engineer the CDS, and to complete and upload the following into SGS:

   a. Documentation Requirements

      i. Phase 2 CDA, Section 2.0 completed

      ii. SBSA Plan and Procedures

      iii. Draft Risk Assessments

- Draft risk analysis results are completed by designated entities. Usually the Data Risk and all portions of the Attack Risk are provided by the CDSE, except the Partner Type, which is provided by Defense Intelligence Agency (DIA) and the Grid Connectivity Threat (GCT) which is provided by the DISA Risk Adjudication Branch. The CDSE ensures the results are uploaded into SGS. The respective CDSE reviews the data and contacts the necessary entities which will assist in conducting portions of the RDAC risk analysis

2. The respective CDSE submits a CDTAB agenda request (ref ai) to the DSAWG Secretariat. Agenda requests will not be accepted by the DSAWG Secretariat directly from the component and all agenda requests must be submitted by the respective CDSE to the DSAWG Secretariat 14 calendar days prior to the next CDTAB meeting. Any late submissions beyond the 14 days will not be accepted.

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

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 make a decision whether or not to approve a CDSA for SBSA based on the following scenarios:

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. If the component 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: SBSA approval for 2 weeks within a 90 day window will be granted. Note: Components may request additional time for SBSA if needed. After SBSA, the component will proceed to Phase 3.

b. 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.

The duration of the operational use is dependent upon many factors. Based on the risk analysis results, the DSAWG is authorized by the DoD ISRMC to authorize a CDS to operate for up to 3 years if the risk rating is 2 steps within the RDAC "shot group," 2 years if 1 step within the shot group/on the edge, or 1 year if 1 step out of the shot group.

c. 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 which 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 a 1 year CDSA upon successful review of the SBSA results by the CDSE."

5. Based on the DSAWG decision, the DISA Risk Adjudication Branch will update SGS milestones and also take the following actions based on the approval which was given: (see CDSA Issuance Section H.9)

H.7 Phase 3: CDS Security Control Assessment & Authorization

This phase applies only to Standard Point to Point solutions and ECDS Systems which are required to receive a Risk Decision Authority Criteria (RDAC) (ref ag) analysis. FTPO Tickets usually skip this phase.

1. The Component or ECDSP works with their respective CDSE to conduct SBSA, to review the SBSA results, and to complete and upload the following into SGS:

   a. Required Documentation

   i. Upon completion of SBSA, the component must submit the SBSA results and updated Phase 3 CDA to their CDSE for upload to SGS.

   ii. The respective CDSE will review the SBSA results to verify no changes exist between the Draft Risk Analysis and the actual test results.

   iii. If there are no changes and the DSAWG already approved operational use upon CDSE review of the SBSA results, then the CDSE must notify the DISA CDS team and request issuance of the CDSA. (Proceed to step 4)

   b. If the CDSE discovers that the SBSA results differ from the SBSA plan, if recommended mitigations were applied between phase 2 and phase 3, or if DSAWG otherwise requires the ticket to return to DSAWG for operational use, continue the steps below.

   c. 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.

2. Once the revised ratings are provided, the CDSE will submit an agenda request to the DSAWG Secretariat. Agenda requests will not be accepted by the DSAWG Secretariat directly from the Component. All agenda requests must be submitted by the respective CDSE to the DSAWG Secretariat 14 calendar days prior to the next CDTAB meeting and any late submissions after the 14 days will not be accepted.

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.

4. DSAWG Phase 3 Review: The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to approve a CDSA for Operational Use.

5. Based on the DSAWG decision, the DISA Risk Adjudication Branch will update SGS milestones and also take the following actions based on the approval which was given: (see CDSA Issuance Section H.9)

H.8 Phase 4: Operational CDS Monitoring

CDSs can receive up to 3 years operational approval from DSAWG. This means that they do not need to return to DSAWG for 3 years. However, the CDS (unless a FTPO CDS) still requires an annual review by the CDSE and the DISA Risk Adjudication Branch. The process described below describes actions necessary for an annual review when CDTAB/DSAWG review is required as well as an annual review where CDTAB/DSAWG review is not required.

DISA CDES will conduct annual reviews IAW the Annual Review Schedule for CDES Systems.

1. Component contacts CDSE and submits required paperwork and updates SGS as required
   a. Required Documentation
   b. Revalidation Memorandum: A revalidation memo from the AO stating that the CDS is still required, the CDS configuration has not changed, and that it has been tested. CDES: For DISA CDES, the revalidation memorandum is split into multiple revalidation memorandums. A revalidation memorandum which revalidates the mission requirement for the CDS is required for each component AO supported by CDES. This revalidation memorandum which verifies the unchanged configuration and testing of the system is required from the DISA AO.
   c. CDS Annual Self-Assessment Report

DoDI 8540.01 (ref ad), Enclosure 2 (CD and RMF Roles) Section 8 (IS Owner)
k. Directs a periodic self-assessment be conducted to assess the protection mechanisms and security controls implemented to protect CD activities. The assessment will:
(1) Review the security relevant configuration, operation, and administration of the CDS in its operational environment.
(2) Verify that the CDS is utilized per the approved security relevant configuration and documentation requirements.
(3) Identify possible security vulnerabilities.
(4) Document findings in an assessment report and updated IS POA&M to support annual CDSA revalidation.

   d. DISA CDES Enterprise Response Memorandum (uploaded to SGS): If the CDS is not an Enterprise system and does not meet the exclusions listed in the CDES Non-Consideration Memorandum, a CDES response memorandum is required.
   e. Repeatable Accreditation/Authorization: An updated CDS tracking spreadsheet of the repeatable CDS inventory is also required to be submitted to the CDSE and uploaded into SGS.
   f. POA&M (if required) uploaded to SGS: If the Information System Owner is using a non-baseline CDS device or an ECDSP has stated they can meet the requirement or if the current system being deployed has been directed by DSAWG or DoD ISRMC to be improved, the Information System Owner must submit a POA&M detailing their schedule to migrate to a new solution, to CDES or to apply other mitigations within the architecture.

DoDI 8540.01 (ref ad), Enclosure 2 (CD and RMF Roles) Section 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 Reference (u).

2. CDSE must notify the DISA Risk Adjudication Branch the DISA Risk Adjudication Branch of these completed actions. If the DSAWG operational period has not expired, the DISA Risk Adjudication Branch the DISA Risk Adjudication Branch will proceed to step 5. If the ticket needs an extended operational approval, the DSAWG Secretariat will schedule the CDS for CDTAB review. Agenda requests will not be accepted by the DSAWG Secretariat directly from the Component. All agenda requests must be submitted by the respective CDSE to the CDTAB Secretariat 14 calendar days prior to the next CDTAB meeting. Any late submissions will not be accepted.
3. CDTAB Phase 4 Review: The CDTAB voting members will review the CDS Annual Review required documents, any additional information provided/extracted from the Component's CDA, and the previous risk rating prior to providing a concur or non-concur vote with the risk rating and any associated comments.
4. DSAWG Phase 4 Review: The ticket will then be presented to the DSAWG with the CDTAB's risk rating and comments. The DSAWG will make a decision whether or not to extend the operational approval for the ticket.
5. Based on the DSAWG decision, the DISA Risk Adjudication Branch will update SGS milestones and also take the following actions based on the approval which was given: (see CDSA Issuance Section H.9)

H.9 Post DSAWG/DoD ISRMC Actions and Cross Domain Solution

Authorization Issuance

1. Based on the DSAWG decision, the DSAWG Secretariat will update SGS milestones and also take the following actions based on the approval which was given:
   a. If ticketing was approved for a standard point to point 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 and the requirement will be given an ECDSP ticket number. The ECDSP will notify the mission partner of the ticket number for the system they intend to use to meet their requirement. The original request number will always be used to reference the component requirement and DSAWG approval of the requirement for ECDS implementation.
   c. If SBSA was approved, the DISA Risk Adjudication Branch 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 which 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 CCSDs connecting 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 SGS Section 10.2 and show the CDS and CDS ticket number. 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 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)

d. If Operational Use was approved, the DISA Risk Adjudication Branch 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 CCSDs connecting 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 SGS Section 10.2 and show the CDS and CDS ticket number. 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 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)

v. SBSA Results (If SBSA was required)

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

If the documentation requirements are not sufficient for a CDSA to be issued at the time of the DSAWG/ DoD ISRMC decision the DISA Risk Adjudication Branch will notify the CDSE of the missing requirements. In order to obtain a CDSA once the documentation requirements are completed, a CDSA request form must be submitted to the DISA Risk Adjudication Branch

CDSA's 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

If more than 1 year of operational use was approved by DSAWG or the DoD ISRMC, 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 H.8) If the CDS was approved FTPO then a 3 year CDSA can be issued not to exceed three years from the date of the DSAWG or DoD ISRMC review. CDSA's will not be issued past AO authorization for the CDS.

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

The CDS device is marked operational in SGS upon the initial issuance of a CDSA by the DISA Risk Adjudication Branch following a DSAWG or DoD ISRMC approval. It remains operational until the DISA Risk Adjudication Branch receives evidence from the Component's respective CDSE that the device is non-operational.

H.9.1 Configuration Changes to Operational CDSs

Planned changes to the configuration of the CDS including patches and upgrades must be coordinated with the Component's respective CDSE and entered into the SGS as Phase I requests. If the change is a patch, software upgrade or other configuration change such as adding a channel or network, the DISA Risk Adjudication Branch will administratively move the request to Phase 2 and issue a new CDS ticket number provided the normal phase 1 documentation requirements and SGS updates have been completed. The CDS ticket will return to DSAWG once the Phase 2 risk rating has been concurred upon by CDTAB.

If the request is for a change in technology, the CDS ticket will not be administratively moved to Phase 2 and should follow the normal Phase 1 process.

H.9.2 Closure of a CDS Requirement

If for any reason it becomes necessary to discontinue use of a CDS or a component is no longer continuing their mission, the respective CDSE must submit a closure request in order to stop tracking of the CDS ticket in SGS. The CDS analyst who performs the closure will upload the closure request to SGS under the ticket in question, and close the ticket with the comment "Closed per CDSE request." If the CDS device connects to SIPRNet, the related CCSD sections 4 (Classified Network Information) and 10.2 (Topology) should be updated as well to remove the CDS.

H.10 IC CDS Registration Process

The DoD ISRMC requested that all IC owned, UCDSMO baseline CDSs which 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 and maintaining an accurate depiction of DoD network environments and interconnections and facilitate rapid incident response.

H.10.1 Step 1: Obtain and Complete an IC CDS Registration Form

To obtain an IC CDS Registration form template, contact the DISA Risk Adjudication Branch at 301-225-2903 or via e-mail at: disa.meade.ns.mbx.cdtab@mail.smil.mil. The form is also posted on both the CDTAB and DSAWG SIPR Intelink Sites. The IC registration form contains all of the data necessary to complete an SGS database registration. .

H.10.2 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: To obtain access to the SGS database components, go to: https://giap.disa.smil.mil and select "request an account." The CDSE will be required to upload a completed DD2875. A template is provided on the entry page of the website. Once the registration is complete, the IC component or CDSE will notify the CDTAB Secretariat of a completed registration. the DISA Risk Adjudication Branch will review the registration, generate a CDS Ticket Number, and notify the submitting IC Component and/or CDSE of the CDS Ticket Number.

H.10.3 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 DISA Risk Adjudication Branch that all documents have been submitted. the DISA Risk Adjudication Branch will send notification of a completed IC CDS registration to the DSAWG Chair.

H.10.4 Step 4: CDSA Issuance

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

H.10.5 Step 4: Operational CDS Monitoring

Annually, the DISA Risk Adjudication Branch will request the IC POC to verify if the CDS is still operational. Any time that the devices are modified in a manner which requires the IC registration to be updated, the IC agency should provide that update to the DISA Risk Adjudication Branch. If the device is decommissioned, the IC agency is requested to provide notification via a signed memo or digitally signed e-mail to the DISA Risk Adjudication Branch and they will close the registration in SGS.

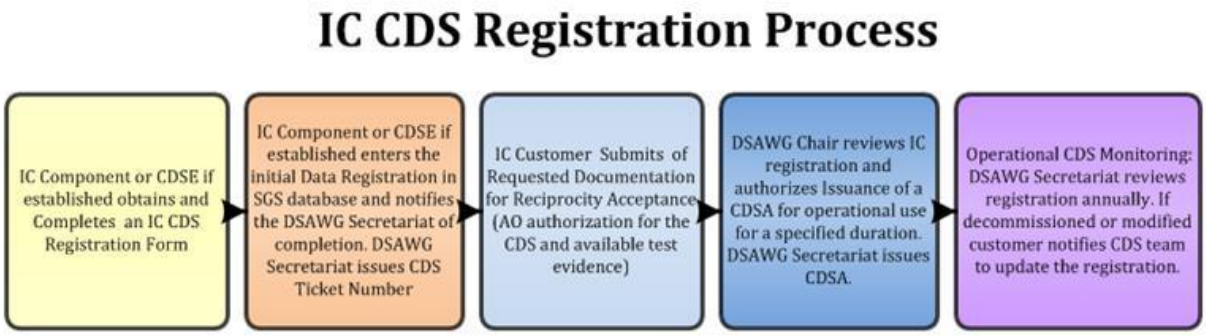

Figure 12: IC CDS Registration Process

H.11 Frequently Asked Questions (FAQs)

Q: Do I need to create a request for every CDS device/distribution console I intend to meet a specific requirement? What if it is a hot or cold spare or being used for load balancing?
A: A separate request/ticket is required for each CDS device/distribution console if the device is used as a hot spare or load balancing. A separate request is not needed for a cold spare but the cold spare must go through 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 DISA Risk Adjudication Branch must be notified and a new request must be opened.

- The exception to this is if the ticket is a DISA CDES ticket or a Repeatable Accreditation/Authorization ticket. In this case, the "Instantiations" field of SGS will be updated to reflect the number of instantiations a single CDS ticket represents. All documentation will be maintained under that single CDS ticket number in SGS.

Q: What is the significance of the three partitions of a CDS ticket number?
A: Once a 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 listed below:

- **First partition (*1234*-0001-001):** The first partition represents the component requirement. If this is a new component requirement, the Request will receive a ticket number with a unique first partition. The second and third partitions will be 1.

- **Second partition (1234-*0001*-001):** The second partition represents the instantiation of the CDS device. For example, if three CDS devices were needed for load balancing, the ticket numbers would be 1234-0001-001, 1234-0002-001, and 1234-0003-001. The configuration and Component requirement is the same, but there are three devices meeting this requirement. These devices could be the same configuration at the same location or they could be the same configuration at three different locations.

    - The exception to this is if the ticket is a DISA CDES ticket or a Repeatable Accreditation ticket. In this case the "Instantiations" field of SGS will be updated to reflect the number of instantiations a single CDS ticket represents. All documentation will be maintained under that single CDS ticket number in SGS.

- **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 components. 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.

Q: What is the difference between a CDSA and an ATC?
A: Once a Security Authorization Package (SAP) is submitted, reviewed, and accepted by the CAO, an ATC for the CCSD is issued. The ATC contains the statement, "This ATC does not authorize any Cross Domain Solutions. A separate Cross Domain Solution Authorization Letter will be issued authorizing Cross Domains." A CDSA is issued after DSAWG approval of a CDS contingent upon a current ATC for the CCSD and the ATO, and Topology properly referencing the CDS ticket number. Also, the CDSA expiration date will not exceed the ATC expiration date if the ATC expires prior to the DSAWG approval expiration. Once a new ATC is issued, another CDSA will be issued for the remainder of the DSAWG approval window.

H.12 Points of Contact

Cross Domain Solutions (CDS)	
DSAWG Secretariat – CDTAB Support	301-225-2903 (commercial), 312-375-2903 (DSN) disa.meade.ns.mbx.cdtab@mail.mil (NIPR) disa.meade.ns.mbx.cdtab@mail.smil.mil (SIPR) http://intelshare.intelink.sgov.gov/sites/cdtab (SIPR)
DSAWG Secretariat – DSAWG Support	301-225-2905 (commercial), 312-375-2905 (DSN) disa.meade.ns.mbx.dsawg@mail.mil (NIPR) disa.meade.ns.mbx.dsawg@mail.smil.mil (SIPR) (Copy and paste the following links into the web browser.) https://intelshare.intelink.gov/sites/dsawg (NIPR) http://intelshare.intelink.sgov.gov/sites/dsawg
DISA Cross Domain Enterprise Services	disa.meade.peo-ma.list.peo-ma-IA32-cdescna@mail.mil
UCDSMO	Unified Cross Domain Services Management Office (UCDSMO): http//:intelshare.intelink.sgov.gov/sites/ucdsmo/default1.aspx

Table 23: Cross Domain Solutions (CDS) Contact Information

H.13 Additional Policy and Guidance Documents

Policy	Title
CJCSI.6211.02D	*Defense Information Systems Network (DISN): Policy and Responsibilities* (ref b)
CDTAB Charter	*Cross Domain Technical Advisory Board* (ref ac)
DSAWG Charter	*DSAWG Charter* (ref x)
RDAC 2.3, NSA	*Risk Decision Authority Criteria* (ref ag)
DoDD 5100.3	*Support of the Headquarters of Combatant and Subordinate Joint Commands* (ref ae)
VLoR IG	*Very Low Risk Implementation Guide* (ref z) http://intelshare.intelink.sgov.gov/sites/dsawg/shared/CDS/risk_rating_methodologies/VLOR
VLoR Assertions	*Very Low Risk Assertions* (ref aa)
DoD CDSE Memorandum	*Cross Domain Support Element Responsibilities* (ref ab)
DISA CDES	*DISA CDES Non Consideration Memorandum* (ref ad)
DoD CIO and IC CIO Memorandum	*Establishment of the Unified Cross Domain Services Management Office as the Cross Domain Requirements and Engineering Services Manager* (ref y)
Repeatable CDA Authorization	*Repeatable CDS Entrance Criteria* (ref ad) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fdsawg%2FShared%20Documents%2FCDS%2FRepeatable%5FAccreditation%5FCriteria&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence
DoDI 8510.01	*Risk Management Framework for DoD Information Technology (IT)* (ref d)

Table 24: Additional Policy and Guidance Documents

This page intentionally left blank

.

APPENDIX I - REFERENCES

Reference Number	Title
(a) DoDI 8500.01	*Cybersecurity*, March 14, 2014 http://www.dtic.mil/whs/directives/corres/ins1.html
(b) CJCSI 6211.02D	*Defense Information Systems Network (DISN) Responsibilities*, 4 August 2015 http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm
(c) DoDD 8000.01	*Management of the Department of Defense Information Enterprise*, March 17, 2016 http://www.dtic.mil/whs/directives/corres/dir.html
(d) DoDI 8510.01	*Risk Management Framework (RMF) for DoD Information Technology (IT), Change 1*, May 24, 2016 http://www.dtic.mil/whs/directives/corres/ins1.html
(e) DoDI 8551. 01	*Ports, Protocols, and Services Management*, May 28, 2014 http://www.dtic.mil/whs/directives/corres/ins1.html
(f) DoDI 8110.01	*Mission Partner Environment (MPE) Information Sharing Capability*, November 25, 2014 http://www.dtic.mil/whs/directives/corres/ins1.html
(g) DoDI 8100.04	*DoD Unified Capabilities (UC)*, December 9, 2010 http://www.dtic.mil/whs/directives/corres/ins1.html
(h) JP 1-02	*Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 February 2016) http://www.dtic.mil/doctrine/new_pubs/jointpub_reference.htm
(i) JP 3-12(R)	*Joint Publication 3-12 Cyberspace Operations*, 5 February 2013 http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm
(j) CNSSI 4009	*National Information Assurance Glossary*, April 6, 2015 (Copy and paste the following link into the web browser –may require TLS2 for access https://www.cnss.gov/CNSS/issuances/Instructions.cfm
(k) DoDI 8530.01	*Cybersecurity Activities Support to DoD Information Network Operations, March 7, 2016* http://www.dtic.mil/whs/directives/corres/ins1.html
(l) DoD O-8530.01M	*Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program*, December 17, 2003 http://www.dtic.mil/whs/directives/

(m) DoD CIO Office Sponsor Memorandum	*Responsibilities of DoD Components Sponsoring Mission Partner Connections to DISN-Provided Transport Infrastructure*, 14 August 2012[10] http://disa.mil/Services/Network-Services/DISN-Connection-Process/~/media/Files/DISA/Services/DISN-Connect/Policy/Memo_Summary_of_DoD_Sponsor_Responsibilities.pdf
(n) NIST SP-800-37, Rev 1	*Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010 (updates as of 06-05-2014) http://csrc.nist.gov/publications/PubsSPs.html
(o) DoD RMF KS	*DoD Risk Management Framework Knowledge Service* https://rmfks.osd.mil
(p) CNSSI 1253	*Security Categorization and Control Selection for National Security Systems*, 27 March 2014 (Copy and paste the following link into the web browser –may require TLS2 for access) https://www.cnss.gov/CNSS/issuances/Instructions.cfm
(q) OMB A-130	*Management of Federal Information Resources* https://www.whitehouse.gov/omb/circulars_default
(r) CJCSI 6285.01C	*Multinational Information Sharing (MNIS) Operational Systems Requirements Management Process*, 15 May 2013 http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm
(s) DoD 5220.22-M	*National Industrial Security Program Operating Manual*, 28 February 2006 (Incorporating Change 2 May 18, 2016) http://www.dtic.mil/whs/directives/corres/pdf/522022M.pdf
(t) CJCSI 6510.01F	*Information Assurance (IA) and Support to Computer Network Defense (CND)*, 9 February 2011 (Current as of 9 Jun 2015) http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm
(u) UC MP	*Unified Capabilities Master Plan*, October 2011 http://www.disa.mil/Network-Services/UCCO/~/media/Files/DISA/Services/UCCO/APL-Process/Unified_Capabilities_Master_Plan.pdf
(v) DoDD 5105.19	*Defense Information Systems Agency*, July 25, 2006 http://www.dtic.mil/whs/directives/corres/dir.html
(w) DoDD 5144.02	*DoD Chief Information Officer*, November 21, 2014 http://www.dtic.mil/whs/directives/corres/dir.html

[10] In2012, DoD CIO issued this memo on DoD sponsor responsibilities. Although several of the issuances cited in this memo have been reissued, DoD sponsors are strongly encouraged to consult the current version of issuances cited in the memo for additional details.

(x) DSAWG Charter	*Defense Security/Cybersecurity Authorization Working Group (DSAWG} Charter,* 8 April 2016 (Copy and paste the following link into the web browser.) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/DSAWG%20Charter/DSAWG%20Charter%20-%20(8%20Apr%202016).pdf
(y) DoD CIO and IC CIO Memorandum	*Establishment of the Unified Cross Domain Services Management Office as the Cross Domain Requirements and Engineering Services Manager,* March 26, 2014 (Copy and paste the following link into the web browser.) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/DSAWG%20References/UCDSMO%20Establishment%20Letter.pdf
(z) VLoR IG	*Very Low Risk Process Implementation Guide,* version 2.4 13 July 2013 (Copy and paste the following link into the web browser.) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/CDS/risk_assessment_methodolgies/VLOR/VLoR_Process_Guidance_v2.4.docx
(aa) VLoR Assertions	*Very Low Risk Assertions,* version 2.4, 13 July 2013 https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/CDS/risk_assessment_methodolgies/VLOR/VLoR_Process_Guidance_v2.4.docx
(ab) DISA CDES Memorandum	*DISA CDES Non-Consideration Memorandum* - (Copy and paste the following link into the web browser.) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fdsawg%2FShared%20Documents%2FCDS%2FCDES%20material&FolderCTID=0x012000CC2A7A98C1295C45AFD9DAC8E15A4267&View=%7BEC1D88D1%2DBA36%2D4AA1%2D98FD%2D1D47AEB1CEF1%7D
(ac) CDTAB Charter	*Cross Domain Technical Advisory Board Charter,* 18 April 2007 – (Copy and paste the following link into the web browser.) https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/DSAWG%20References/CDTAB_Charter_%20REVISION%2031%20March%202008.pdf
(ad) DoDI 8540.01	*Department of Defense Instruction Cross Domain Policy,* 8 May 2015 http://www.dtic.mil/whs/directives/corres/pdf/854001p.pdf
(ae) DoDD 5100.3	*Support of the Headquarters of Combatant and Subordinate Joint Commands,* February 9, 2011 http://www.dtic.mil/whs/directives/corres/dir.html
(af) CDS Repeatable Process	*Repeatable CDS Entrance Criteria – (Copy and paste the following link into the web browser.)* 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%2D1D47AE

	B1CEF1%7D
(ag) RDAC 2.3, NSA	*Risk Decision Authority Criteria (Copy and paste the following link into the web browser.)* 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
(ah) DoD CIO Memo, Circuit Optimization	*DoD CIO Memo, Circuit Optimization,* May 5, 2016
(ai) CDTAB Agenda Request Form	*CDTAB Agenda Request Form (Copy and paste the following link into the web browser.)* https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/DSAWG%20References/CDTAB_Charter_%20REVISION%2031%20March%202008.pdf
(aj) CDSA Request Form	*CDSA Request Form (Copy and paste the following link into the web browser.)* https://intelshare.intelink.gov/sites/dsawg/Shared%20Documents/DSAWG%20References/CDTAB_Charter_%20REVISION%2031%20March%202008.pdf
(ak) National Information Assurance Partner (NIAP) Evaluated Products	*National Information Assurance Partner (NIAP) Evaluated Products* https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm?tech_name=ALL&CFID=17562266&CFTOKEN=d6d9fec5f6ead8d6-91AE90D6-FD36-EBE6-47E2D9D4D8217EB9
(aL) DISA Cloud Connection Process Guide	*Defense Information Systems Agency (DISA) DISA Cloud Connection Process Guide (CCPG),* Version 1.01, September 2015 http://iasecontent.disa.mil/stigs/pdf/CCPG_v1.01.pdf
(am) DISN Connection Process Guide (CPG)	*DISN Connection Process Guide,* Current published Version) http://disa.mil/connect
(an) DISA Agreement # GO-11-019	*Memorandum of Agreement Between The Defense Information Systems Agency and the Defense Security Services, National Industrial Security Programs Contractors Connection to the Defense Information Systems Network,* 9 September 2011

Please go to the following website to obtain connection information for DISN services:
http://www.disa.mil/Services/Network-Services

1 **APPENDIX J - ACRONYMS**

Acronym	Definition
AA	Accrediting Authority
A&A	Assessment and Authorization
AAD	Access Approval Document
ADD	Authorization Decision Document
AIS	Automated Information System
AO	Authorizing Official
APAN	All Partners Access Network
APL	Approved Products List
APLITS	Approved Products List Tracking System
ASLAN	Assured Services Local Area Network
ASVLAN	Assured Services Virtual Local Area Network
ASN	Autonomous System Number
ATC	Approval to Connect
ATD	Authorization Termination Date
ATO	Authorization to Operate
BD	Business Development
B/P/C/S	Base/Post/Camp/Station
C2	Command and Control
C&A	Certification & Accreditation
CA	Certifying Authority
CAO	Connection Approval Office
CAP	Connection Approval Process
CC/S/A	Combatant Command, Service, or Agency
CCAO	Classified Connection Approval Office (now referred to as CAO)
CCMD	Combatant Command
CCSD	Command Communications Service Designator
CDA	Cross Domain Appendix
CDES	Cross Domain Enterprise Services (also see “DISA CDES”)
CDMA	Code Division Multiple Access
CDRB	Cross Domain Resolution Board
CDS	Cross Domain Solution
CDSAP	Cross Domain Solutions Assessment Panel
CDSE	Cross Domain Solutions Element
CDTAB	Cross Domain Technical Advisory Board
CER	Customer Edge Router
CIO	Chief Information Officer
C-ISP	Commercial-Internet Service Provider
CMT	Compliance Monitoring Team
CND	Computer Network Defense
CODEC	Coder-Decoder
COMSEC	Communications Security

COTS	Commercial Off-The-Shelf
CPE	Customer Provider Edge
CPG	Connection Process Guide
CTM	Consent to Monitor
CTO	Communications Tasking Order
DAA	Designated Accrediting Authority
DADS	DMS Asset Distribution System
DATC	Denial of Approval to Connect
DCCC	DISA Partner Contact Center
DDOE	DISA Direct Order Entry
DECC	DISA Defense Enterprise Computing Center
DIACAP	Defense Information Assurance Certification and Accreditation Process (DIACAP is superseded by DoDI 8510.01 (ref d))
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISN CPG	Defense Information Systems Network Connection Process Guide
DISN-LES	Defense Information Systems Network - Leading Edge Services
DITCO	Defense Information Technology Contracting Office
DITPR	DoD Information Technology Portfolio Repository
DKO	Defense Knowledge Online
DKO-S	Defense Knowledge Online-Secret
DMS	Defense Messaging System
DMZ	Demilitarized Zone
DNI-U	Director National Intelligence-Unclassified
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DODIN	Department of Defense Information Networks
DREN	Defense Research and Engineering Network
DRSI	DODIN Readiness and Security Inspections
DRSN	Defense Red Switch Network
DSAWG	Defense Security/Cybersecurity Authorization Working Group
DSN	Defense Switched Network
DSS	Defense Security Service
DTEN	DISN Test and Evaluation Network
DTES	DISN Test and Evaluation Service
DVS	DISN Video Services
DVS-G	DISN Vide Services – Global
DVS-WS	DISN Video Services – Website
EKMS	Electronic Key Management System
EMSS	Enhanced Mobile Satellite Services
EoIP	Everything over Internet Protocol
ESC	Enterprise Session Controller
EUCOM	European Command
FAQ	Frequently Asked Questions

FOM	Fiber Optic Modem
FOUO	For Official Use Only
FRAGO	Fragmentary Order
FSO	Field Security Operations
FTPO	For Tracking Purposes Only
GCA	Government Contracting Authority
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
GSM	Global System for Mobile Communications
IA	Information Assurance
IATC	Interim Approval to Connect
IATO	Interim Authorization to Operate (No longer a valid authorization category under RMF in accordance with DoDI 8510.01 (ref d)).
IATT	Interim Authorization to Test
IC	Intelligence Community
ICD	Intelligence Community Directive
ICTO	Interim Certificate to Operate
IDS	Intrusion Detection System
IER	In Effect Report
IM	Instant Messaging
IMUX	Inverse Multiplexer
INFOSEC	Information Security
IO	Interoperability
IOS	Internetworking Operating System
IP	Internet Protocol
IS	Information Systems
ISDN	Integrated Services Digital Network
ISE	Information Sharing Environment
ISP	Internet Service Provider
ISRMC	Information Security Risk Management Committee
ISSE	Information System Security Engineering
IT	Information Technology
JIE	Joint Information Environment
JITC	Joint Interoperability Test Command
JMEI	Joining, Membership, and Exiting Instructions
JWICS	Joint Worldwide Intelligence Communications System
KS	Knowledge Service
LAN	Local Area Network
MCU	Multipoint Control Unit
MDA	Missile Defense Agency
MG	Media Gateway
MHS	Military Health System
MPE	Mission Partner Environment
MPLS	Multi-Protocol Label Switching

MSAB	Multi-national Security and Accreditation Board
MSL	Multiple Security Level
MUF	Military Unique Function
NA	Not Applicable
NC	Non-Compliant
NIAP	National Information Assurance Partnership
NIC	Network Information Center
NIPRNet	Non-classified Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NS/EP	National Security/Emergency Preparedness
OPR	Office Primary Responsibility
OSD	Office of the Secretary of Defense
OTAR	Over The Air Rekey
OWA	Outlook Web Access
PDA	Personal Digital Assistant
PDC	Program Designator Code
PIN	Personal Identification Number
PIT	Platform Information Technology (system)
PLADS	Plain Language Address Distribution System (PLADS)
PO	Program Office
POA&M	Plan of Action & Milestones
POC	Point of Contact
PPSM	Ports, Protocols, and Services Management
PTC	Permission to Connect
RDAC	Risk Decision Authority Criteria
RF	Request Fulfillment
RFS	Request for Service
RMF	Risk Management Framework
RSU	Remote Switching Unit
RTS	Real Time Services
SAP	Security Authorization Package
SAR	Security Assessment Report
SAAR	System Authorization Access Request
SBC	Session Boundary Controller
SBD	Short Burst Data
SBU	Sensitive But Unclassified
SDD	Systems Design Document
SDP	Service Delivery Point
SGS	SIPRNet GIAP System
SIP	System Identification Profile
SIPRNet	Secret Internet Protocol Router Network
SME	Subject Matter Expert

SME-PED	Secure Mobile Environment-Portable Electronic Device
SMO	Service Management Office
SMU	Switch Multiplex Unit
SNAP	System/Network Approval Process
SP	Security Plan
SRG	Security Requirements Guide
SRO	Service Representative Officer
SS	softswitch
SSAA	System Security Authorization Agreement
SSC	SIPRNet Support Center
SSE	System Security Engineer
SBSA	Site Based Security Assessment
STIG	Security Technical Implementation Guide
TCO	Telecommunications Certification Office
TR	Telecommunications Request
TS	Top Secret
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
UC	Unified Capabilities
UCAO	Unclassified Connection Approval Office (now referred to as CAO)
UCDSMO	Unified Cross Domain Services Management Office
USCC	USCYBERCOM
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
VM	Validation Manager
VOC	Video Operations Center
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VPL	Validated Product List
VPL	Virtual Private LAN
VPN	Virtual Private Network
VTC	Video Tele-Conference
VTF	Video Teleconferencing Facility
WAN	Wide Area Network
WAN-SS	Wide Area Network softswitches

2

This page intentionally left blank.

APPENDIX K - GLOSSARY

Term	Definition
Authorization decision	A formal statement by an Authorizing Official regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim authorization to test (IATT), or denial of ATO (DATO). The Authorization decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD public key infrastructure (PKI)-certified digital signature. (ref j)
Approval to Connect (ATC)	A formal statement by the Connection Approval Office granting approval for an IS to connect to the DISN. The ATC cannot be granted for longer than the period of validity of the associated ATO. An ATO may be issued for up to 3 years.
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 Assessment and Authorization (A&A) documentation (for RMF packages) or Certification & Accreditation (C&A) information (for DIACAP package), and provide evidence of compliance with the assigned cybersecurity controls. (ref d)
Authorization to Operate (ATO)	Authorization granted by a DAA/AO for a DoD IS to process, store, or transmit information; an ATO indicates a DoD IS has adequately implemented all assigned cybersecurity controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to three (3) years. (ref j)
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. (ref j) ("Authorizing Official is the RMF term that supersedes the term "Designated Accrediting Authority" used under DIACAP)
Authorization Termination Date (ATD)	The date assigned by the DAA/AO that indicates when an ATO or IATT expires.
Connection Approval Process (CAP)	Packages provide the CAO the information necessary to make the connection approval decision.
Certification	A comprehensive evaluation and validation of a DoD IS to establish the degree to which it complies with assigned cybersecurity controls based on standardized procedures. (ref j) (Note: this term is superseded by "Assessment.")
Certification Determination	A CA's determination of the degree to which a system complies with assigned cybersecurity controls based on validation results. It identifies and assesses the residual risk with operating a system and the costs to correct or mitigate cybersecurity security weaknesses as

	documented in the Information Technology (IT) Security Plan of Action and Milestones (POA&M)
Certifying Authority (CA)	The senior official having the authority and responsibility for the certification of Information Systems governed by a DoD Component cybersecurity program.
Consent to Monitor (CTM)	This is the agreement signed by the DAA/AO granting DISA permission to periodically monitor the connection and assess the level of compliance with cybersecurity policy and guidelines.
Connection Approval Process	Formal process for adjudication requests to interconnect information systems.
Connection Approval Office (CAO)	Single point of contact within DISA for all DISN connection approval requests.
Command Communications Service Designator (CCSD)	A unique identifier for each single service including use circuits, package system circuits, and interswitch trunk circuits.
Computer Network Defense (CND)	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.
Cybersecurity Service Provider	DoDI 8530.01 (ref k) requires DoD IT to be aligned to a DoD network operations and security centers (NOSCs). The NOSC and supporting cybersecurity service provider(s) will provide any required cybersecurity services to aligned systems. Cybersecurity Service Providers will: (1) Offer and provide cybersecurity services in accordance with DoD O-8530.01-M (ref L). (2) Execute cybersecurity responsibilities and authorities in accordance with DoD Component policy, MOAs, contracts, or support agreements. (3) Comply with directives and orders of USSTRATCOM and supported DoD Component NOSC and organizations. (4) Document all supported entities and associated systems in accordance with DoD Component policy, MOAs, contracts, or support agreements.
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 capability to manually and/or automatically access and/or transfer information between different security domains and enforce their security policies. (ref ad)
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 CC/S/A/), 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."
Defense Information Systems Connection Process Guide (DISN CPG)	Step-by-step guide to the detailed procedures that Customers must follow in order to obtain and retain connections to the DISN (ref am).
Defense Information Systems Network (DISN)	DoD integrated network, centrally managed and configured to provide long-haul information transfer for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery and video teleconferencing services.
Defense Information Systems Network-Leading Edge Services (DISN-LES)	Defense Information Systems Network-Leading Edge Services (DISN-LES) is a Mission Assurance Category III program designed to pass encrypted unclassified and classified traffic over the Classified Provider Edge (CPE) routers of the DISN, and provide capability for subscriber sites requiring "next generation" network, encryption, software, NETOPS, and advanced services not offered by other DISN Subscription Services (DSS). The network provides a non-command-and-control, risk aware infrastructure identical to the core DISN data services (NIPRNet and SIPRNet).
Denial of Approval to Connect (DATC)	A formal statement by the Connection Approval Office withholding (in the case of a new connection request) or rescinding (in the case of an existing connection) approval for an IS to connect (or remain connected) to the DISN.
Denial of Authorization to Operate (DATO)	A DAA/AO decision that a DoD IS cannot operate because of an inadequate cybersecurity design, failure to adequately implement assigned cybersecurity controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.
Department of Defense Information Network	The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security."
Designated Accrediting Authority (DAA)	The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approving authority and delegated accrediting authority. (Superseded by the RMF term "Authorizing Official)
DISA Defense Enterprise Computing Center (DECC)	Services provided within a backdrop of world-class computing facilities located in both the continental United States (CONUS) and outside of the continental United States (OCONUS).
Defense Information Assurance Certification and	The DoD processes for identifying, implementing, validating, certifying, and managing cybersecurity capabilities and services, expressed as cybersecurity Controls, and authorizing the operation of

Accreditation Process (DIACAP)	DoD information systems in accordance with statutory, Federal and DoD requirements. (The Risk Management Framework (RMF) supersedes DIACAP as stipulated in DoDI 8510,01 (ref d))
Defense Security/Cybersecurity Authorization Working Group (DSAWG)	Provides, interprets, and approves DISN security policy, guides architecture development, and recommends Authorization decisions to the DISN Flag panel. Also reviews and approves Cross Domain information transfers (as delegated from the DISN/DODIN Flag Panel) or forwards such recommendation(s) to the Flag Panel.
DIACAP Scorecard	A summary report that succinctly conveys information on the cybersecurity posture of a DoD IS in a format that can be exchanged electronically; it shows the implementation status of a DoD Information System's assigned cybersecurity controls (i.e., compliant (C), non-compliant (NC), or not applicable (NA)) as well as the C&A status. (DIACAP is superseded by DoDI 8510.01 (ref d))
Demilitarized Zone (DMZ)	Physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
Defense Information Systems Agency (DISA) Direct Order Entry (DDOE)	This is the ordering tool for DISN telecommunications services.
DoD Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. It includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections. (ref c)
DoD Component	DoD Combatant Commands, Military Services and Organizations, Agencies, and Field Activities (CC/S/A), which are collectively referred to as DoD Components.
DoD Unified Capabilities (UC) Approved Products List (APL)	Is established in response to DoDI 8100.04 DoD Unified Capabilities (UC) and the Unified Capabilities Requirements (UCR Change III September 2011). Its purpose is to provide Interoperability (IO) and cybersecurity authorized products for DoD Components to acquire and to assist them in gaining approval to connect to DoD networks in accordance with policy.
DODIN Readiness and Security Inspections (DRSI)	Produces and deploys cybersecurity products, services, and capabilities to combatant commands, services, and agencies to protect and defend the Global Information Grid (GIG).
DODIN Interconnection Approval Process (GIAP)	Electronic process to submit connection information and register a DODIN connection.
Information Assurance (IA)	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection,

	detection, and reaction capabilities. (ref o)
IA Certification and Accreditation	The legacy DoD approach (under DIACAP) for identifying information security requirements, providing security solutions and managing the security of DoD information systems. (ref o) (Superseded by Assessment/Authorization)
Information Systems (IS)	Computer-based information systems are complementary networks of hardware/software that people and organizations use to collect, filter, process, create, and distribute data.
Interim Approval to Connect (IATC)	Temporary approval granted by the Connection Approval Office for the connection of an IS to the DISN under the conditions or constraints enumerated in the connection approval. An IATC is normally granted for no more than 180 days. IATCs may be granted for up to one year for units deployed in the CENTCOM AOR.
Interim Authorization to Test (IATT)	A temporary authorization to test a DoD IS in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the Authorization decision.
Interim Certificate to Operate (ICTO)	Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use. The decision to grant an ICTO will be made by the MCEB Interoperability Test Panel based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.
Internet Protocol (IP)	Protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.
Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (ref o)
Mission Partner	Those with whom Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments, allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. (DoDD 8000.01)
Plan of Action & Milestones (POA&M)	A permanent record that identifies tasks to be accomplished in order to resolve security weaknesses; required for any Authorization decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks; also used to document DAA-accepted non-compliant cybersecurity controls and baseline cybersecurity controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.
Platform Information Technology (PIT)	Defined in ref a

Program or System Manager (PM or SM)	The individual with responsibility for and authority to accomplish program or system objectives for development, production, and sustainment to meet the user's operational needs.
Request For Service (RFS)	The document, used to initially request telecommunications service, which is submitted by the requester of the service to his designated TCO.
Risk Management Framework	A structured approach used to oversee and manage risk for an enterprise. (ref j))
Service Delivery Point (SDP)	The point at which a user connects to the DISN. The DISN provides cybersecurity controls up to the SDP. The Partner/user is responsible for cybersecurity controls outside of the SDP.
System Identification Profile (SIP)	A compiled list of system characteristics or qualities required to register an IS with the governing DoD Component cybersecurity program.
Telecommunications Certification Office (TCO)	The activity designated by a Federal department or agency to certify to DISA (as an operating agency of the National Communications System) that a specified telecommunications service or facility is a validated, coordinated, and approved requirement of the department or agency, and that the department or agency is prepared to pay mutually acceptable costs involved in the fulfillment of the requirement.
Telecommunications Service Order (TSO)	The authorization from Headquarters, DISA, a DISA area, or DISA-DSC to start, change, or discontinue circuits or trunks and to effect administrative changes.
Telecommunications Service Request (TSR)	Telecommunications requirement prepared in accordance with chapter 3, DISAC 310-130-1 and submitted to DISA or DISA activities for fulfillment. A TSR may not be issued except by a specifically authorized TCO.
Unified Capabilities (UC)	The seamless integration of voice, video, and data applications services delivered ubiquitously across a secure and highly available Internet Protocol (IP) infrastructure to provide increased mission effectiveness to the warfighter and business communities. UC integrate standards-based communication and collaboration services including, but not limited to, the following: messaging; voice, video and Web conferencing; Presence; and UC clients. (ref g)
Unified Cross Domain Services Management Office (UCDSMO)	The UCDSMO provides centralized coordination and oversight of all cross-domain initiatives across the Department of Defense and the Intelligence Community.
Virtual Private LAN (VPL)	Means to provide Ethernet-based multipoint-to-multipoint communication over IP/MPLS networks.
Wide Area Network (WAN)	A computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries).

This page intentionally left blank.

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