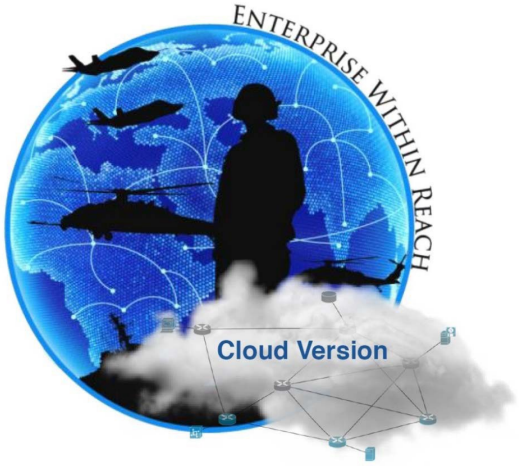
# DEPARTMENT OF DEFENSE (DoD)

# CLOUD CONNECTION PROCESS GUIDE




**Version 3**
**December 2025**

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

This page intentionally left blank

# EXECUTIVE SUMMARY

The Cloud Connection Process Guide (Cloud CPG) expands the Defense Information Systems Network Connection Process Guide (DISN CPG) to include guidance for Department of Defense (DoD) connection and use of cloud computing services. The goal of the Cloud CPG is to help a Cloud Service Provider (CSP) navigate the DoD's process for connecting a Cloud Service Provider-Cloud Service Offering (CSO) to the DISN and make it available for use by DoD Mission Owners. The Cloud CPG also helps a DoD Component[1] Mission Owner to connect to an authorized CSO and "on-board" (or implement) a DoD Cloud Information Technology Project (C-ITP) in accordance with DoD cloud policy.

Section 1 of this guide provides an introduction and general guidance. Section 2 provides guidance to CSPs and their DoD Sponsors for registering and connecting Impact Levels 2, 4, and 5 CSOs to the DISN. Section 3 provides guidance to DoD Mission Owners for registering and opening a connection to an authorized CSO. Appendix F provides guidance for Classified (Impact Level 6) cloud connections.

Nothing in this Cloud CPG is intended or designed to usurp or impede: a DoD Component's authorities to develop and implement its own compliant cloud strategies under Title 10; or an Authorizing Official's (AO) authorities under DoD Instruction (DoDI) 8500.01 (ref a) and DoDI 8510.01 (ref b). In addition, nothing in this Cloud CPG alters or supersedes the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of sensitive compartmented information (SCI), as directed by Executive Order 12333 and other laws and regulations.

This release of the Cloud CPG reflects the evolution of the DoD cloud strategy. This document incorporates the lessons learned and process insights from "cloud pilots" and various other efforts. DISA will maintain this guide to comply with DoD CIO Memo, *Department of Defense Joint Warfighting Cloud Capability and Next Steps to Rationalize Cloud Use Across the Department of Defense* (ref c), and the DoD Cloud Computing Security Requirements Guide (Cloud SRG) (ref d). [2]

The instructions in this guide are effective immediately. Major updates shall be approved by DoD CIO. Interim updates to this guide (e.g., Version 3.1) shall be issued as required by the DISA Risk Management Executive/Authorizing Official.

Please send your improvement comments directly to the DISA Connection Approval Office (CAO) at disa.meade.re.mbx.ucao@mail.mil.

The instructions in this guide are effective immediately and publicly available from the DISA website at https://public.cyber.mil/dccs/dccs-documents/.

[1] The term "Component(s)" collectively refers to OSD; the Military Departments; the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff; the Combatant Commands (CCMDS); the Office of the Inspector General of the DoD; the Defense Agencies, the DoD Field Activities; and all other organizational entities within the DoD.

[2] The DoD Cloud Computing Security Requirements Guide (Cloud SRG (ref d)) and related documents are at: https://public.cyber.mil/dccs/dccs-documents/

# SIGNATURE PAGE

SNOUFFER.JACQUELINE.P.1229435538 Digitally signed by SNOUFFER.JACQUELINE.P.1229435538 Date: 2025.12.19 14:07:53 -05'00'

JACQUELINE P. SNOUFFER Date

Director, Risk Management
DISA Co-Authorizing Official

# REVISION HISTORY

DISA will review and update this document as needed. The revision history table documents significant changes to this guide.

| Version | Date | Revisions |
|---|---|---|
| 1.0 | 21 Aug 2015 | • Initial Release<br>• The emphasis was registration of CSPs and DoD C- ITPs in the DISA SNAP Database (ref e) |
| 1.01 | 22 Sep 2015 | • Incorporated guidance from the DISA Document Release Group (DRG) to authorize public release |
| 2.0 | March 2017 | • Approved draft for formal review and comment<br>• Expands the scope from a DISA to a DoD Cloud Process Guide<br>• Reorganizes the material by major cloud processes: CSP-CSO Registration and Connection, Sustaining, Services Discontinuation; and, C-ITP Registration and Connection, Sustainment, and Service Discontinuation<br>• Presents processes in a step-by-step fashion<br>• Adds appendices for DoD Component Cloud Connection, Cloud Points of Contact, Classified C-ITP Registration, and documentation requirements |
| 3.0 | May 2025 | • Updated DISA Logo on cover page to include version number and date.<br>• Updated the Executive Summary to correct the reference to the DISN Cloud Connection Process Guide<br>• Updated signature page<br>• Updated reference links and POC lists<br>• Removed Figure 1 and 2 for BCAP and ICAP references<br>• Updated Section 2 reflecting improved processes<br>• Removed incorrect references of Component BCAP or Access Points to DOD CIO Approved Cloud Access Points (CAP)<br>• Removed obsolete tables for Checklists<br>• Removed Table 2 of DoD Mandated Cloud Computing Standards as the SRG is the consolidated requirements source<br>• Updated Section 3 reflecting improved processes |

Please send comments on the DoD Cloud CPG to the DISA Cloud Support Team at disa.meade.re.mbx.cloud-team@mail.mil

# TABLE OF CONTENTS

This page intentionally left blank

# SECTION 1: INTRODUCTION

## 1.1 Purpose

The Cloud Connection Process Guide (CPG) provides guidance, points of contact, and processes for a Cloud Service Provider (CSP) to connect a Cloud Service Offering (CSO) to the DISN and to make the CSO available for use by DoD Mission Owners. The guide also provides guidance for a Mission Owner to register and open a connection to an authorized CSO and "on-board" (or implement) a Cloud Information Technology Project (C-ITP) within an authorized CSO.

## 1.2 Authority

The Cloud CPG derives its authority from the same sources as the *DISN Connection Process Guide* (DISN CPG) (ref f). Further, the DoD CIO Memo, Department of Defense Joint Warfighting Cloud Capability and Next Steps to Rationalize Cloud Use Across the Department of Defense (ref c) establishes authorities and guidance for Commercial Cloud Computing Services. Finally, the DoD Cloud SRG (ref d) outlines the security controls and requirements necessary for using cloud-based solutions within the DoD and states that the DoD Cloud CPG defines responsibilities needed to establish and maintain connections between CSOs and DoD C-ITPs.

## 1.3 General Guidance

The DoD Cloud CPG is a living document that will continue to evolve as connection processes are refined and as additional cloud computing services become available. This version of the Cloud CPG focuses on processes for connecting CSOs and DoD C-ITPs via the DISN. This Cloud CPG will remain separate from the DISN CPG (ref f) to allow this guide to remain agile and flexible in response to the changes driven by new technical advancements and process changes. References to this DoD Cloud CPG and the key or primary processes will be included in the DISN CPG (ref f). Additional information about DISA enterprise cloud computing services is at https://public.cyber.mil/dccs/.

Use the DoD Cloud CPG to help get through the cloud connection process. However, before employing this guide, always check for the current version at website: https://public.cyber.mil/dccs/dccs-documents/.

## 1.4 Applicability

This guide applies to all Mission Owners and Cloud Service Providers involved in using or offering cloud computing services.

## 1.5 Background

In the current political, economic, and technological landscape, information technology (IT) will continue to provide extensive and ever-increasing capabilities while consuming fewer resources. With the increase of both state-sponsored and independent cyber threats, the DoD recognizes the growing importance of leading a strong and secure presence in cyberspace while responding to the need for continued budgetary constraints and stricter financial oversight. As a result, the Department must transform the way in which it acquires, operates, and manages its IT in order to realize increased efficiency, effectiveness, and security as outlined in the DoD CIO Cloud Strategy (ref g).

The Department has specific cloud computing challenges that require careful adoption considerations, especially in areas of cybersecurity, continuity of operations, information assurance (IA), and resilience. To help meet these challenges, the Department has established a Cloud Service Provider (CSP) Security Requirements Guide (SRG) (ref d) that provides the security controls and requirements necessary for hosting Department data in a Cloud Service Offerings (CSOs).

## SECTION 2: CLOUD SERVICE PROVIDER-CLOUD SERVICE OFFERING (CSP- CSO) REGISTRATION AND CONNECTION LIFE CYCLE

### 2.1 Introduction

This section describes the Cloud registration and onboarding procedures involved with connecting a CSO to the DISN as illustrated in Figure 1. The DoD Mission Owner/Sponsor must initiate the process. Once successfully completed, the CSO is available for use by Mission Owners following the procedures outlined in Section 3 of the guide. While some cloud connection processes are standard for all CSOs, there are variations based on the authorized Information Impact Level of the CSO.

The process for connecting a CSO to a DoD BCAP involves collaboration among the CSP, DISA, the DoD Security/Cybersecurity Authorization Working Group (DSAWG), the DoD CIO (ref c), and may include a DoD Mission Owner, a DoD Sponsor, and the sponsoring DoD Component's cloud migration office. The requirements for registering and connecting a CSO to the DISN include obtaining a DoD PA, registering the CSO in the DISA SNAP (ref e) database with the assistance of DISA Cloud Assessments Division, connecting the CSO to the DISN through an appropriate access point, maintaining the CSO connection and DoD PA, and discontinuing the CSO connection at the end of its life cycle.

### 2.2 Obtain a DoD PA for a CSO

To host a DoD C-ITP, a CSO must have a DoD PA and be connected to the NIPRNet via a DoD CIO-approved BCAP (Off-Premises Impact Level 4 or 5 CSO), or an IAP (Impact Level 2 CSO). Section 3 of the DoD Cloud SRG (ref d) provides guidance for determining the appropriate impact level. DoD must assess a CSO for compliance with DoD Cloud SRG (ref d) requirements for the impact level authorization requested by the CSP.

Steps 1-10 of Figure 1 illustrate the process for obtaining and maintaining a DoD PA for the CSO. Steps 11 and 12 illustrate the process for a Mission Owner (the Cloud Consumer) to register and connect a C-ITP to an authorized IL4 or IL5 CSO via the DISA Enterprise BCAP.

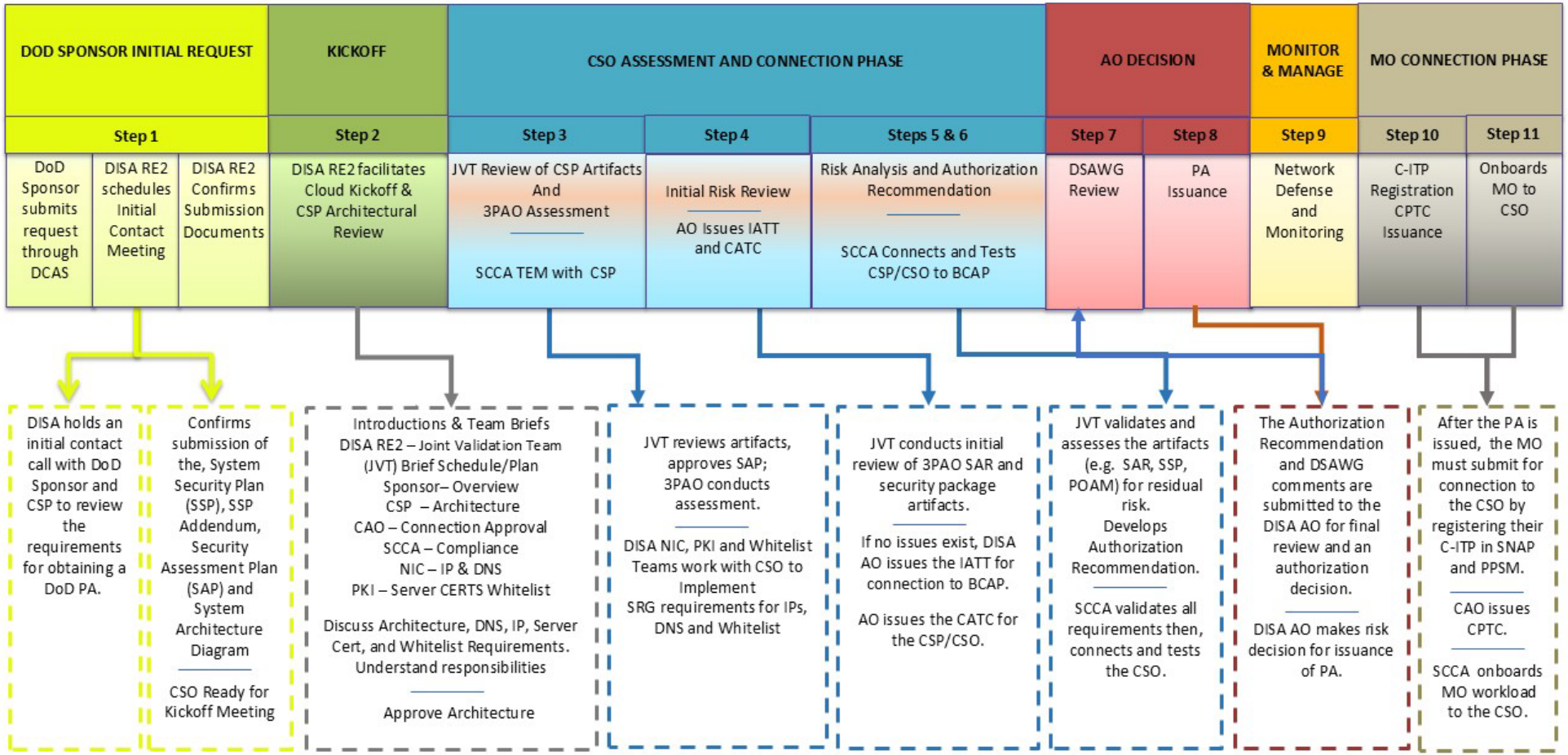



**Figure 1: Cloud Registration and Connection Process**

**Step 1**

### 2.2.1 Complete DoD Cloud Support Offering Initial Contact Form

**Input:**

a) The CSP and its DoD Sponsor contact the DISA Cloud Assessments Division to obtain and complete a *DoD Cloud Service Offering Initial Contact Form* accessible at the DoD Cloud Authorization Services (DCAS) web site (ref m).

b) DoD Sponsor submits request Onboarding Questionnaire through DCAS online.

c) https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/

d) DISA Cloud Assessments Division contacts the Mission Sponsor to schedule the Initial Contact Meeting.

**Action:**

a) The DoD Sponsor completes the second part of the Onboarding Questionnaire in DCAS.

b) DISA Cloud Assessments Division holds an Initial Contact Meeting with the Mission Sponsor and Cloud Service Provider to outline prerequisite artifacts and review the roles and responsibilities of the authorization process.

c) The Cloud Service Provider request eMASS access and uploads the prerequisite artifacts into eMASS.

d) https://cloud.emass.apps.mil/App/Home/Inbox/

**Output:**

a) DoD Sponsor and CSP completed the requested artifacts and submitted required artifacts and information in DCAS and eMASS.

b) Upon successful review of all required information, DISA Cloud Assessments Division will schedule the Kickoff Meeting.

Additional artifacts may be required dependent on the project type. The DISA Cloud Assessments Division will help the CSP, and any DoD Mission Sponsor navigate the DoD PA, registration and connection process and schedule administrative and technical information interchange meetings as required.

Documentation that will be due from the CSP and Mission Sponsor during the approval process:

a) Documentation checklist for readiness (Cloud CSP Onboarding Questionnaire)

b) Systems Architecture Diagram

c) System Security Plan (SSP) and SSP Addendum(s)

d) Security Assessment Plan (SAP)

e) Mission Sponsor must provide two sponsor analysts

CSPs must work with DISA Cloud Assessments Division to register their Impact Level 4 & 5 CSP-CSOs in SNAP. Impact Level 6 (secret) CSP-CSOs must be registered in SGS (Appendix F).

## Step 2

### 2.2.2 Conduct DoD Cloud Kickoff Meeting

This is the first of several Cloud connection meetings among the stakeholders, which includes DISA Cloud Assessments Division, Connection Approval Office, DISA J9, DoD Network Information Center (NIC), DoD Mission Sponsor, Mission Owners, and the CSP. The DISA Cloud Assessments Division hosts this Technical Exchange Meeting (TEM). Additional TEM meetings will be scheduled as required with the CSP, DISA Cloud Assessments Division, DISA Connection Approval Office (CAO), SCCA, NIC, and the sponsor to review the architecture, connection requirements, System Security Plan, Security Assessment Plan, etc.

**Input:**

a) The CSP and Sponsor complete and submit checklists and all artifacts requested to be uploaded into eMASS as described at least 10 days in advance of the scheduled meeting.

**Action:**

a) DISA Cloud Assessments Division facilitates the Kickoff Meeting by providing stakeholders an overview of the DoD cloud registration and connection process, DoD requirements to obtain a DoD PA, the CSP's CSO capabilities, and the responsibilities of the CSP, the DoD Sponsor, Mission Owners, and DISA.

b) The DISA Cloud Assessments Division identifies the DoD assessor (e.g., the DISA JVT Cloud Assessments Division or DoD Component in collaboration with the DISA Cloud Assessments Division).

c) DISA Stakeholders, to include the Cloud Assessment Division and SCCA, conducts an architectural review to ensure the CSO compliance with the Cloud SRG (ref d).

d) The CSP brokers the request for the NIC to issue IP space and DNS for the CSO.

**Output:**

a) DISA Cloud Assessments Division establishes the Joint Validation Team (JVT).

b) DISA Cloud Assessments Division and the SCCA approved the architectural diagram or established a follow up meeting to address any corrections identified during the review.

## Step 3

### 2.2.3 JVT Review of CSP Artifacts and 3PAO Assessment

DISA will host recurring meetings as required to assess and validate all artifacts

provided ensuring validation of CSO SRG (ref d) compliance.

**Input:**

a) Architecture Diagrams approved by all stakeholders of the DoD Cloud Kickoff Meeting.

**Action**:

a) The participants review the assessment package for readiness.

b) DISA presents an overview of the assessment process and establishes the timeline for the assessment.

c) The JVT begins a thorough review all CSP artifacts. This is a cooperative and collaborative process between the JVT, CSP, and the 3PAO for review to ensure technical completeness. This ongoing action continues concurrently through Step 7.

d) The CSP will remediate all issues discovered and update the artifacts. The CSP will retest as required and respond to DISA comments.

e) SCCA conducts the Technical Exchange Meeting (TEM) with the CSP.

**Output:**

a) The JVT approves the SAP to permit 3PAO assessment to begin.

b) The 3PAO will conduct/begin the official assessment upon approval of the SAP by the JVT.

## Step 4

### 2.2.4 Initial Risk Review and Issuance of IATT and CATC

**Input:**

a) Architecture Diagrams approved by all stakeholders of the DoD Cloud Kickoff Meeting.

b) 3PAO completed SAR.

**Action:**

a) The JVT conducts the initial review of 3PAO SAR for any significant findings.

b) DISA Cloud Assessments Division prepares, and submits for AO approval, an Interim Authorization To Test form imposing standard restrictions to permit connection to a DISA BCAP, prohibiting operational use until a Provisional Authorization is issued.

c) The DISA AO reviews issues the IATT and the CATC for the CSO.

d) DISA Cloud Assessments Division posts the IATT and CATC into SNAP.

**Output:**

a) Upon review and approval, the DISA AO will issue an IATT and CATC for the CSO for the purpose of connecting to the BCAP.

b) The DISA Cloud Assessments Division will provide the IATT Memo to the CSP and the DISA SCCA.

c) The DISA Cloud Assessments Division will post the IATT as the Authorization Decision Document (ADD) into SNAP.

d) DISA Cloud Assessments Division will establish and complete the PPSM and SNAP/SGS entries on behalf of the CSP to ensure all registration requirements and artifacts are accurately documented for the approval process.

e) DISA SCCA and the CSP will begin the connectivity process to connect the CSO to the BCAP upon receipt of the CATC.

## Step 5

### 2.2.5 JVT Validation of Artifacts

Note: Steps 5 and 6 can be done concurrently.

**Input:**

a) Prerequisite package artifacts from Step 1

b) Approved Diagrams from Step 2

c) Final SAR from Step 4

**Action:**

a) The JVT completes the validation of artifacts and assessment of the Security Package to include current POA&Ms, the 3PAO SAR, and any CSP responses or corrections to JVT findings.

b) The JVT drafts an Authorization Recommendation and Provisional Authorization for the consideration of the DSAWG and a DISA Authorizing Official.

**Output:**

a) The DISA JVT submits the Authorization Recommendation to the DSAWG for review and comment.

## Step 6

### 2.2.6 SCCA Connects CSP/CSO to the BCAP

**Input:**

a) CSO architecture briefing

b) IATT

c) CATC

**Action:**

a) DISA SCCA facilitates the CSP (Collective Stakeholder) TEM

b) DISA SCCA will confirm receipt of the IATT and CATC artifacts, then begin the connection phase of the CSO to the BCAP

c) DISA SCCA will engineer and provision the CSO connection to the DISA Enterprise BCAP.

**Output:**

a) DISA SCCA and the CSP will begin the connectivity and testing process to connect the CSO to the BCAP upon receipt of the CATC.

## Step 7

### 2.2.7 DSAWG Review and Recommendation

If there are no non-standard boundary connections or non-approved Ports Protocols and Services (PPS), the DISA Cloud Assessments Division may only provide the DSAWG a summary of the Security Package and their assessment of the CSO. The DSAWG will provide a risk assessment recommendation to the DISA Authorizing Official (AO) when requested. The Cloud Assessment Division Authorization and DSAWG recommendation are factors considered by the DISA AO when determining whether to issue a DoD PA. CSPs can bring technical subject matter experts to the DSAWG meetings to assist in responding to the DSAWG member's inquiries.

The members of the DSAWG represent the Principal Authorizing Officials of the DoD Mission Areas (Warfighting, Intelligences, Business, and Enterprise Information Environment) and DoD Components. The DSAWG assesses the risk to the DODIN community related to the CSO connection to the DISN.

**Input:**

a) The DISA Cloud Assessments Division Authorization Recommendation.

**Action:**

a) The DSAWG will review the Cloud Assessment Divisions Authorization Recommendation. The Cloud Assessment Division will coordinate responses to any questions raised by the DSAWG with the CSP and/or 3PAO.

b) The DSAWG will return any comments and recommendations for a DISA AO's consideration in making an authorization decision

**Output:**

a) DSAWG comments and recommendation.

## Step 8

### 2.2.8 DISA AO Issues the DoD PA

The DISA AO issues a DoD PA for the CSO following a positive recommendation by the DoD Assessor and the DSAWG. The DoD PA signifies that a CSO has met minimum-security requirements to host DoD data at the assessed information impact level.

**Input:**

a) The DISA Cloud Assessments Division Authorization Recommendation.

b) The DISA Cloud Assessments Division drafted Provisional Authorization.

c) The Cloud Service Offering Security Package.

d) The DSAWG comments and recommendations (if applicable).

**Action:**

a) DISA Cloud Assessments Division will work with the CSP to update pertinent repositories with CSO information.

b) The DISA AO will review the body of evidence and render a risk decision, issuing a PA if the CSO has met an acceptable risk threshold for supporting DoD data.

c) The DISA Cloud Assessments Division will post the issued PA to the DoD Approved Cloud Service Offerings Catalog for access to all MOs.

**Output:**

a) The signed DoD PA and the associated security documentation package is complete.

b) The CAO updates SNAP.

In addition to obtaining a DoD PA and being registered in DISA SNAP, an On-Premises CSP-CSO must also obtain an Authorization to Operate in accordance with DoDI 8510.01 (ref b) and the DoD Cloud SRG (ref d) along with an Approval to Connect to the NIPRNet in accordance with the DISN CPG (ref f).

## Step 9

### 2.3 CSO Sustainment and Maintenance

**Input:**

a) The signed DoD PA and the associated security documentation package.

b) CSO SNAP and PPSM registration updated.

c) Deployed and operational CSO has been entered into the catalog.

**Action:**

a) CSP must comply with all CSO Connection Sustainment and Maintenance requirements as listed below.

**Output:**

a) CSP maintains the operational and secure CSO.

### 2.3.1 Meet all Contract Requirements

The CSP and DoD Mission Owners using a CSO must meet all obligations within their contract including those specified in the Defense Federal Acquisition Regulation Supplement (DFARS): Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013–D018) (ref r).

### 2.3.2 Maintain the DoD PA

The CSPs must conduct Continuous Monitoring activities for the CSO in compliance with conditions specified in the DoD Cloud SRG (ref d) and the DoD PA for the CSO. The CSPs must also submit timely renewal requests prior to the expiration date when specified in the CSP-CSO's DoD PA.

### 2.3.3 Comply with USCYBERCOM and JFHQ DODIN OPORDS

In the case that a USCYBERCOM or JFHQ DODIN Operational Order (OPORD) affects a CSO, the Cybersecurity Services Provider and Contract Officer are responsible for providing the unclassified portion of the OPORD to the CSP and ensuring compliance. CSPs must ensure CSOs comply with applicable USCYBERCOM and JFHQ DODIN OPORDS.

### 2.3.4 Fulfill Cybersecurity Service Requirements

All DoD Mission Owners are required to ensure their use of CSOs comply with Cyber Security Service Provider (CSSP) (ref ii) requirements in accordance with the DoDI 8530.01 and DoD Cloud SRG (ref d).

Personnel should not discuss ongoing cybersecurity events or incidents using unclassified means. Use the unclassified DIBNET format to report cyber incidents at the unclassified level. Any follow-on discussions must be via appropriately secured communications channels.

### 2.3.5 Comply with USCYBERCOM Disconnect Orders

Non-compliance or cyber incidents may result in USCYBERCOM ordering DISA to temporarily disconnect the CSO service from the DISN until the CSO complies with the USCYBERCOM Task Order (TASKORD). The USCYBERCOM TASKORD provides the conditions and procedures for reactivating a CSO connection. USCYBERCOM, DISA, DoD Mission Owners, CSP, and AO jointly assess the mission impact before USCYBERCOM orders DISA to disconnect temporarily or discontinue permanently a CSO connection to the DISN.

### 2.3.6 Maintain Accurate Information within SNAP

The CSP must collaborate with the DISA Cloud Assessments Division to ensure the information about the CSO in DISA SNAP (ref e) is updated to reflect the accurate status of the CSO including personnel contact information. The Cloud Assessments Division will upload the current authorization document in Section 0.4 of the SNAP registration for the DISA CAO to review. The DISA CAO

will review the artifacts in SNAP and update the CSO's Authorization Termination Date (ATD) accordingly. The CAO will then send the updated CATC to SCCA and the Cloud Provider.

## 2.4 Discontinue CSO Service

USCYBERCOM or a CSP may permanently discontinue a CSO connection. Permanent discontinuation of a connection could be for several reasons:

a) A CSP wishes to discontinue offering a CSO and its connection to the DISN.

b) The DISA AO may revoke the DoD PA for a particular CSO.

c) The PA may expire.

d) USCYBERCOM may issue a TASKORD to discontinue the CSO connection if the CSO does not comply with DoD cybersecurity requirements.

Discontinuing a CSO connection involves the following actions:

### 2.4.1 Notify Stakeholders about CSO Service Discontinuation

The POCs listed within the CSO and C-ITP registrations will be notified of discontinuation via an automated email when the CSO and C-ITP registrations are closed.

### 2.4.2 Discontinue the CSO Connection

The DISA Joint Operations Center (DJOC) issues the DISA Task Order to Discontinue the CSO connection and update the NIPRNet DMZ Whitelist as needed. DISA CONUS executes the DTO and discontinues the connection to the DISN.

### 2.4.3 Update Status in SNAP

The CSP in coordination with the DISA Cloud Assessments Division ensures DISA SNAP (ref e) entry for the CSO contains accurate information about the discontinued status of the CSO including contact information for key Points of Contact.

### 2.4.4 Release Assigned CSO Technical Resources

SCCA PMO will work with CSP and if appropriate Mission Owner Cloud Projects to decommission associated circuits, configured networks and/or BCAP technical resources.

**Step 10**

# SECTION 3: C-ITP REGISTRATION AND CONNECTION PROCESS

## 3.1 Introduction

This section addresses the process for a Mission Owner (the Cloud Consumer) to register and connect a C-ITP to an authorized IL4 or IL5 CSO via the DISA Enterprise BCAP. The process includes Registration and Connection, C-ITP on-boarding to the CSO, C-ITP sustainment and maintenance, and C-ITP discontinuation. Each Mission Owner must determine whether a C-ITP will migrate to a CSO. A DoD Component's Cloud migration office will assist its Mission Owners in the CSO selection process. The Mission Owner of a

candidate C-ITP takes the following steps:

**Input:**

a) Mission Owner identifies the CSO being used for the C-ITP.

b) Component AO issued the ADD or ATO.

c) Component AO identified the CSSP.

d) Component AO approved the topology diagram.

**Action:**

a) Mission Owner obtains IP Addresses.

b) Mission Owner enters required artifacts into SNAP/SGS and submits the C-ITP registration.

c) DISA CAO works with the MO to resolve any issues with the C-ITP registration.

d) DISA CAO reviews the C-ITP artifacts for completeness.

**Output:**

a) DISA CAO issues the CPTC for the C-ITP.

b) If necessary, DISA SCCA PMO may schedule a Mission Owner focused Technical Exchange Meeting to determine C-ITP requirements when CPTC is available.

MO and CSP obtain IP Addresses and Whitelisting, DNS, PKI Certs, PPS reg in parallel with registration process.

### 3.2 Obtain IP Addresses

The Mission Owner is responsible for obtaining the required IP addresses. The Mission Owner reaches out to the NIC, DISA Cloud Assessments Division, or DoD Component Cloud migration office (Appendix B) for assistance in acquiring the necessary IP addresses. The NIC has designated IP address space for various Cloud Service Offerings for DoD Component offices. The DoD Component points of contact who are allocated IP address space for CSOs can be located on the NIC website**.**

The DoD Component points of contact that are allocated IP address space for CSOs can be located on the NIC website, https://www.nic.mil, or by contacting the NIC at disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil. (ref Appendix B).

### 3.3 Register C-ITP in SNAP/SGS and Update Pertinent Repositories

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

Government supervisor and security manager signatures are required on the uploaded DD2875. See the DISN CPG for more information.

The Mission Owner must register the C-ITP in SNAP or SGS for classified connections, selecting the appropriate CSO. Once the Mission Owner has a DISA SNAP (ref e) account and their CPTC, the Mission Owners will log into the DISA SNAP database and follow the instructions in the DISA SNAP C-ITP module to provide the information and documentation indicated in Appendix F (C-ITP Registration) of this guide. Mission Owners should also update other pertinent repositories (e.g., DITPR, eMASS) as needed. If the selected CSO is undergoing the DoD PA assessment process, the Mission Owner is encouraged to update the C-ITP entry in DISA SNAP accordingly.

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

a) Authorization Decision Document (ADD) or ATO as outlined in Section 2.2.6 of this guide and signed by the Agency Authorizing Official (AO)

b) CSSP agreement IAW DoDI 8530.01 or as stipulated in agreements with Mission Partners.

c) Topology prepared in accordance with guidance in Appendix G.

d) Consent to Monitor (may be included in the ADD or ATO - see the sample with instructions in Appendix H.

e) Mission Sponsor's request for a Mission Partner connection to DISN:

   a. For a DoD Contractor, Federal Department/Agency mission partner connection request, the Mission Sponsor is required to upload the DoD CIO approval memorandum or Memorandum of Agreement (MOA).

   b. For a FVEY, allied, or coalition mission partner connection request, the Mission Sponsor must also upload the Chairman of the Joint Chiefs of Staff approval memorandum IAW DoDI 5530.3 and CJCSI 6740.01C[3].

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

The Mission Owner ensures the C-ITP name used in the DISA SNAP (ref e) entry corresponds to the official name of the project used in the SNaP-IT and DITPR databases.

The SNAP video user guide link listed below has additional instructions for entering information into SNAP modules. See the DISN CPG for more information. https://public.cyber.mil/?s=SNAP

#### 3.3.1 Submit C-ITP SNAP Package

Once the Mission Owner submits all the required information, DISA SNAP will allow the Mission Owner to select the "SUBMIT" button at the bottom of the DISA SNAP screen.

#### 3.3.2 DISA SNAP Package Review

If the CAO cannot validate information in the connection request package, the CAO will work with the Mission Owner to resolve issues, and the Mission Owner can make required changes and resubmit the package when ready. If issues are not resolved, DISA will mark the request as "Pending" and will retain the documentation submitted in DISA SNAP pending further action by the Mission Owner.

#### 3.3.3 DISA Issues a Cloud Permission to Connect (CPTC)

Once the DISA CAO validates the information and artifacts within the C-ITP registration, the DISA CAO will issue a CPTC for a C-ITP connecting via a DISA BCAP.

## Step 11

### 3.4 Connect the C-ITP to an Authorized CSO

**Input:**

a) DISA CAO Issued CPTC.

**Action:**

a) DISA SCCA will collaborate with the CSP and MO to provision the connection between the C-ITP and the authorized CSO. The subsequent steps for provisioning the connection will vary based on the Impact Level of the C-ITP and the Cloud access point that the Mission Owner will utilize to connect to the CSO, as depicted in figure 2.

b) The DISA SCCA PMO will design the connection for IL4 or IL5 Off-Premises connection to the DISA BCAP.

c) The MO will work with the CSP to complete all activities necessary to on-board a C-ITP onto the authorized CSO following the SRG.

**Output:**

a) DISA SCCA completes the BCAP configuration and testing. The CSO is accessible to the component.

b) The Mission Owner must follow and maintain all Connection Sustainment and Maintenance requirements.

IL2 CSO does not involve a DoD CIO-approved CAP, the Mission Owner is not required to obtain a CPTC. The Mission Owner may contact the CSP to commence implementation of the C-ITP using the selected CSO in coordination with its DoD Component Cloud migration office.

### 3.4.1 IL4 or IL5 C-ITP Connection to DISA BCAP

In this case, the Mission Owner must obtain a Cloud Permission to Connect (CPTC) to an authorized CSO via the DISA BCAP as follows**.**

a) Order a Circuit or VPN to the DISA BCAP (if required). The Mission Owner may find that a C-ITP requires a dedicated circuit or logical connection (e.g., VPN) to the DISA BCAP. If that is the case, the Mission Owner may utilize the DISA Direct Store Front (DDSF) (ref z) to acquire the connection. This process entails the ordering, engineering, acquiring, and installing the circuit and equipment essential for connecting to the DISN. The DISN Connection Process Guide (ref f) documents the step-by-step DISN connection process.

b) Connect the C-ITP to a DISA BCAP. The DISA SCCA PMO designs the connection of an IL4 or IL5 to a DISA BCAP. The connection will be activated once DISA issues the CPTC for the C-ITP.

### 3.4.2 IL2 C-ITP Connection to a CSO Via an IAP

Since the connection to an IL2 CSO does not involve a DoD CIO-approved CAP, the Mission Owner is not required to obtain a CPTC. The Mission Owner may contact the CSP to commence implementation of the C-ITP using the selected CSO in coordination with its DoD Component Cloud migration office (Appendix B). Since an Information IL2 CSO is typically connected to the Internet, Mission Owners need to work with their PPSM Technical Advisory Group (TAG) representative (ref k) to determine if the user connections must be registered in the NIPRNet DMZ Whitelist to enable connections through the IAP (ref l).

### 3.4.3 C-ITP Connection to an On-Premises IL4 or IL5 CSO

An On-Premises CSO that connects directly to the DISN (e.g., STRATUS) does not connect via a DoD CIO-approved BCAP (see Figure 1). The Mission Owner is not required to obtain a CPTC.

## 3.5 On-Board the C-ITP to an Authorized CSO

After DISA configures the BCAP to make the CSO accessible to users, a Mission Owner must submit a SCCA onboarding request form to officially submit a CSO

connection request. The MO will work with DISA and the CSP to complete all onboarding requirements. The MO may then work with the CSP to complete activities necessary to on-board a C-ITP onto the authorized CSO following the SRG (ref d).

## 3.6 C-ITP Connection and Maintenance Process

### 3.6.1 Comply with, Maintain, and Update the C-ITP ATO

Mission Owners must continuously monitor compliance with the conditions specified in the DoD Cloud SRG (ref d), ATO, and CPTC for the C-ITP. The Mission Owner must also submit timely renewal request before the expiration date as specified in the C-ITP ATO and/or CPTC.

### 3.6.2 Meet all contract requirements

The CSP and DoD Mission Owners utilizing a CSO must meet all obligations within their contract including those specified in the DFARS (ref r).

### 3.6.3 Comply with USCYBERCOM Operational Orders (OPORDS)

Mission Owners must maintain awareness of USCYBERCOM OPORDS and directives issued via SIPRNet, have personnel cleared for access to OPORDS that may be classified, and ensure the C-ITP complies with the applicable USCYBERCOM OPORDS.

### 3.6.4 Fulfill Cybersecurity Service Requirements

DoD Sponsors are required to ensure their CSO, and C-ITPs comply with DoD Cyber Security Service Provider requirements in accordance with the DoD Cloud SRG (ref d) and annual re-assessment requirements described in DoD Cybersecurity Policy and STIGS. If the Mission Owner intends to make changes to an approved C-ITP configuration that will alter the security posture of the C-ITP, then the Mission Owner must follow these steps:

a) Document and submit the change request to DISA Cloud Assessments Division using a Security Impact Analysis Form described in the DoD Cloud SRG (ref d).

b) Obtain approval from the appropriate configuration change authority prior to the alteration.

c) Update applicable entries in the DISA SNAP database for the C-ITP.

d) Obtain new CPTC from the DISA CAO.

Cybersecurity events or incidents should not be discussed using unclassified means but use appropriately secured communications channels.

#### 3.6.5 Conduct Continuous Monitoring and Incident Response

DoD policy (ref b) requires a Mission Owner to align a C-ITP with a CSSP (ref ii). Mission Owners must report cyber incidents in accordance with the DoD Cloud SRG (ref d). DoD accredited CSSPs are required, per DoDI 8530.01, to perform Information Security Continuous Monitoring (ISCM).

#### 3.6.6 Comply with USCYBERCOM Disconnect Orders

Non-compliance or cyber incidents may lead to USCYBERCOM instructing DISA to temporarily disconnect the C-ITP from the DISN until the C-ITP or the hosting CSO meets cloud connection requirements. The USCYBERCOM TASKORD will outline the conditions and procedures for reinstating the C-ITP. USCYBERCOM, DISA, DoD Mission Owners, CSP, and AO will collaborate to evaluate the impact of any proposed disconnection to assess potential mission impacts before instructing DISA to temporarily disconnect or permanently discontinue a C-ITP connection to a CSO.

#### 3.6.7 Maintain DISA SNAP or SGS Account

DISA SNAP users must annually submit their certificate of completion for the DoD Annual Cybersecurity Awareness Training to the DISA Connection Approval Office (See Appendix B) for their DISA SNAP or SGS accounts to remain active.

#### 3.6.8 Maintain Accurate Information within DISA SNAP

The Mission Owner must ensure the information about the C-ITP in DISA SNAP or SGS is updated to reflect the current, accurate, and complete status of the C-ITP including personnel contact information.

### 3.7 Discontinue C-ITP Service

Discontinuing a C-ITP involves several actions, as described below:

a) A CSP wishes to discontinue offering a CSO and its connection to the DISN. In this case, the CSP decides to discontinue the CSO and its connectivity to the DISN. This could prompt the end of life for the associated C-ITP.

b) A Mission Owner decides to discontinue use of a CSO to host a C-ITP. If the Mission Owner determines to cease using the CSO hosting the C-ITP, it necessitates the discontinuation of the C-ITP.

c) The DoD PA for a particular CSO is expired or revoked. The DISA AO may revoke the DoD PA for a C-ITP based on the recommendations of a DoD assessor or the DSAWG based on non-compliance with DoD Cloud policy. If the DoD PA for a specific CSO is expired or revoked, it may lead to the discontinuation of the C-ITP hosted by that CSO.

#### 3.7.1 Notify Stakeholder about C-ITP Service Termination

USCYBERCOM will issue an order to DISA to either temporarily disconnect or permanently discontinue the connection to the C-ITP. The DISA Cloud Assessments Division will communicate with stakeholders about any proposed actions or steps

that may impact the C-ITP connection to a CSO.

### 3.7.2 Off-Board the C-ITP from the CSO

a) C-ITP discontinuation and off-boarding specifications and requirements must be incorporated into contracts or service level agreements with CSPs as per the DFARS (ref r). Mission owners need to plan for the eventual CSO off-boarding, and CSPs must assist in this process promptly. The off-boarding process involves two stages: data retrieval/migration and data sanitization or destruction. Additionally, plans for the reuse and disposal of storage media, software, and hardware should be established. It is advisable to release resources promptly and test the off-boarding processes for efficiency.

b) A Mission Owner may request a C-ITP discontinuation by submitting a SCCA decom request. SCCA will work with MO to release all C-ITP related technical resources.

### 3.7.3 Update Status in SNAP

The Mission Owner is responsible for ensuring that the DISA SNAP or SGS entry for the C-ITP reflects accurate information regarding the discontinued status of the C-ITP's connection, including updated contact information for key points of contact.

# APPENDIX A: REFERENCES


a. Department of Defense, DoDI 8500.01 Cybersecurity, 14 March 2014, CH1 07 Oct 2019 [Online] https://www.esd.whs.mil/

b. Department of Defense, DoDI 8510.01 Risk Management Framework for DoD Systems, 19 July 2022 [Online] https://www.esd.whs.mil/

c. DoD CIO Memorandum, Department of Defense Joint Warfighting Cloud Capability and Next Steps to Rationalize Cloud Use Across the Department of Defense, 31 July 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/NextStepRationalizeCloudUse.pdf

d. DoD Cloud Computing Security Requirements Guide (SRG), September 2025. [Online] https://public.cyber.mil/dccs/dccs-documents/ and https://www.cyber.mil/stigs/downloads

e. System Network Approval Process (SNAP) [Online] https://snap.dod.mil/index.do

f. Defense Information Systems Agency, Defense Information Systems Network (DISN) Connection Process Guide [Online] http://cyber.mil/connect/

g. DoD CIO, Cloud Strategy, December 2018. https://media.defense.gov/2019/feb/04/2002085866/-1/-1/1/dod-cloud-strategy.pdf

h. U.S. CIO, Federal Risk Authorization and Management Program, [Online] https://www.fedramp.gov/

i. NIST Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*, May 2012 [Online] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

j. DoD CIO Memorandum to DISA CAO, Summary of DoD Sponsor Responsibilities for Mission Partner Connections to the Defense Information Systems Network (DISN) 14 August 2012

k. PPSM Technical Advisory Group Representatives. [Online] https://cyber.mil/connect/ppsm/

l. NIPRNet DMZ Whitelist. The NIPRNet DMZ Whitelist is **on SIPRNet at**: https://niprdmzwhitelist.csd.disa.smil.mil/whitelist.aspx

m. DoD Cloud Authorization Services (DCAS) Portal [Online] https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/

n. CSP Security Package Documentation Checklist [Online] https://dod365.sharepoint-mil.us/sites/DISA-SCCA/Shared%20Documents/SCCA%20CSP%20%26%20MO%20Onboarding%20Checklists%20vd1.pdf/

o. DoD Approved Cloud Service Offerings Catalog [Online] https://storefront.disa.mil/kinetic/disa/service-catalog#/category/cloud-computing/

p. Enterprise Mission Assurance Support Service (eMASS) [Online] https://www.dcsa.mil/Systems-Applications/Enterprise-Mission-Assurance-Support-Service-eMASS/

q. DoDI 8410.01, Internet Domain Name and Internet Protocol Address Space Use and Approval, 4 December 2015, CH1 4 July 2021 https://www.esd.whs.mil/

r. 80 FR 51739 - Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), August 26.2015 [Online] https://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf

s. NIST Special Publication 800-37 Rev 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

t. 20 FedRAMP Continuous Monitoring Strategy Guide: [Online] https://www.fedramp.gov/

u. 21 NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011 [Online] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

v. FedRAMP Incident Response Requirements and Process Verification [Online] https://www.fedramp.gov/

w. DoD CIO Memo, Use of Enterprise Information Technology Standard Business Case Analysis, October 23, 2014. https://dodcio.defense.gov/Portals/0/Documents/Use%20ofEnterprise%20Information%20Technology%20Standard%20Business%20Case.pdf

x. DISA Cloud Assessments Division DoD Cloud IT Project Initial Contact Form, [Online] https://disa.deps.mil/ext/CloudServicesSupport/Cloud%20Form%20Repository/Forms/AllItems.aspx

y. PPSM Category Assurance List (CAL). [Online] https://cyber.mil/connect/ppsm/

z. DISA Direct Store Front (DDSF) [Online] https://storefront.disa.mil/kinetic/disa/service-catalog#/category/cloud-computing/

aa. Best Practices Guide for Department of Defense Cloud Mission Owners Version 1.0 [Online] https://nsarchive.gwu.edu/sites/default/files/documents/4176844/United-States-Department-of-Defense-Best.pdf

bb. Open Grid Forum, Open Cloud Computing Interface – Core, April 7, 2011, [Online] https://www.ogf.org/documents/GFD.183.pdf

cc. Open Grid Forum, Open Cloud Computing Interface – RESTful HTTP Rendering, June 21, 2011, [Online] https://www.ogf.org/documents/GFD.185.pdf

dd. Committee on National Security Systems Instruction (CNSSI) No. 4009, National Information Assurance (IA) Glossary, 26 April 2010. [Online] https://www.cnss.gov

ee. NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011 [Online] http://dx.doi.org/10.6028/NIST.SP.800-145

ff. DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), May 28, 2014 [Online] http://www.dtic.mil/whs/directives/corres/ins1.html

gg. DoD Information Technology Program Repository (DITPR). [Online] https://ditpr.dod.mil

hh. Department of Defense, DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations, March 7, 2016, Incorporating change 1 date 7/25/17 [Online] https://www.esd.whs.mil/Directives/issuances/dodi/

ii. Certified and Authorized Cybersecurity Service Providers (CSSP) https://intelshare.intelink.gov/sites/jfhq-dodin/JD/CSSP/Pages/Authorized-CSSP-Listing.aspx

This page intentionally left blank

# APPENDIX B: CLOUD POINTS OF CONTACT

| DISA CLOUD COMPUTING TEAM | CONTACT INFORMATION |
|---|---|
| **Cloud Assessments Division** | Email:<br>disa.meade.re.mbx.cloud-team@mail.mil<br><br>DoD Cloud Authorization Services<br>https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas/SitePages/CASHome.aspx |
| **Cybersecurity Service Provider (CSSP) Office (formerly Computer Network Defense Service Provider)** | DISA CSSP Office<br>(For DISA and DoD Component C-ITPs)<br>Email:<br>NIPR: disa.letterkenny.j3-5-7.list.cssp@mail.mil<br>SIPR: disa.letterkenny.j3-5-7.list.cssp@mail.smil.mil<br><br>Website:<br>https://dod365.sharepoint-mil.us/sites/DISA-CSSP |
| **Mission Partner Support Contact Information** | DISA Global Service Desk (24x7)<br>1-844-347-2457<br><br>HaCC Customer Success Team<br><br>Email: Disa.CST@mail.mil<br><br>Mission Partner Portal<br>https://storefront.disa.mil/kinetic/disa/service-catalog#/category/cloud-computing/ |
| **DISA Joint Operations Center** | Email: disa.meade.J-3.mbx.djoc-bc@mail.mil |
| **DISA CONUS Provisioning Center** | Email: PROVTMS@Scott.DISA.mil |
| **DISN Connection Approval Office** | Email: disa.meade.ns.mbx.ucao@mail.mil<br>Phone: 301-225-2900/2901 or DSN 312-375-2900/2901 |
| **DSAWG Secretariat** | Email: disa.meade.re.mbx.dsawg@mail.mil<br><br>Website:<br>https://intelshare.intelink.gov/sites/dsawg/default.aspx<br>Phone: 301-225-2905 |

| DISA CLOUD COMPUTING TEAM (continued) | CONTACT INFORMATION |
|---|---|
| **Department of Defense Network Information Center (NIC)** | For all unclassified connections contact the NIC through the DISA Customer Contact Center (DCCC)<br>Email: disa.dccc@mail.mil<br>Website: https://www.nic.mil<br>Phone:<br>(844) 347-2457, Option 2;<br>(614) 692-0032, Option 2;<br>DSN: (312) 850-0032, Option 2 |
| **PPSM Configuration Control Board (CCB)/Technical Advisory Group** | Phone: 301-225-2904 |
| **Web Content Filtering Office** | Email: disa.meade.ma.list.wcftieriii@mail.mil |
| **Secure Cloud Computing Architecture (SCCA) Program Management Office (PMO)** | Email: disa.meade.se.mbx.disa-scca-pmo@mail.mil |
| **Navy / Marine Corps PEO Digital Neptune Cloud Management Portal** | https://digital.navy.mil/<br><br>ServiceNow-as-a-Service Enterprise (SNaaS-E) Team<br>email: SNAASINFO@us.navy.mil<br><br>Neptune Cloud Management Office<br>Email: infoneptuneus.navy.mil@us.navy.mil |
| **U.S. Army Enterprise Cloud Management Agency** | https://www.army.mil/ecma<br>Email: armycloud@army.mil |
| **Air Force Digital Transformation Activity** | https://dafdto.com/ |
| **Unites States Space Force Nebula Controlled Service Environment** | https://nebula.spaceforce.mil/ |

# APPENDIX C: ACRONYMS

| ACRONYM | DEFINITION |
|---|---|
| **ADD** | Authorization Decision Document |
| **AT&L** | Acquisition, Technology, and Logistics |
| **ATC** | NIPRNet Approval to Connect |
| **ATO** | Authorization to Operate |
| **BCA** | Business Case Analysis |
| **BCAP** | Boundary Cloud Access Point |
| **CAD** | Cloud Assessments Division |
| **CAO** | Connection Approval Office |
| **CAP** | Cloud Access Point |
| **CATC** | Cloud Authorization to Connect |
| **CCPG** | Cloud Connection Process Guide |
| **CCSD** | Command Communications Service Designator |
| **CIO** | Chief Information Officer |
| **C-ITP** | Cloud Information Technology Project |
| **CPTC** | Cloud Permission to Connect |
| **CSO** | Cloud Service Offering |
| **CSP** | Cloud Service Provider |
| **CSSP** | Cyber Security Service Provider |
| **CTM** | Consent to Monitor |
| **DCAS** | DoD Cloud Authorization Services |
| **DISA** | Defense Information Systems Agency |
| **DISN** | Defense Information Systems Network |
| **DJOC** | DISA Joint Operations Center |
| **DMZ** | De-Militarized Zone |
| **CNSS** | Committee on National Security Systems |
| **DODIN** | Department of Defense Information Network |
| **DSAWG** | Defense Security/Cybersecurity Authorization Working Group |

| ACRONYM | DEFINITION |
|---|---|
| **FedRAMP** | Federal Risk and Authorization Management Program |
| **GIAP** | GIG Interconnection Approval Process |
| **GIG** | Global Information Grid |
| **IAP** | Internet Access Point |
| **IIL** | Information Impact Level |
| **ISRMC** | Information Security Risk Management Committee |
| **IT** | Information Technology |
| **JSP** | Joint Services Provider (Pentagon) |
| **JVT** | Joint Validation Team |
| **MCD** | Mission Cyber Defense |
| **MO** | Mission Owner |
| **NFG** | NIPRNet Federated Gateway |
| **NIC** | Department of Defense Network Information Center |
| **PA** | Provisional Authorization |
| **PM** | Program Manager |
| **POA&M** | Plan of Actions and Milestones |
| **POC** | Points of Contact |
| **PPSM** | Ports, Protocols, and Services Management |
| **RMF** | Risk Management Framework |
| **SAP** | Security Assessment Plan |
| **SAR** | Security Assessment Report |
| **SGS** | SIPRNet GIAP System |
| **SLA** | Service Level of Agreement |
| **SNAP** | System Network Approval Process (Registers DISN connections) |
| **SNaP-IT** | Select & Native Programming Data Input System for Information Technology (SNaP-IT) (Registers DoD Department IT investments) |
| **SSP** | System Security Plan |
| **3PAO** | Third Party Assessment Organization |

# APPENDIX D: DEFINITIONS

| | |
|---|---|
| **Assessor (aka Auditor)** | An Assessor is an individual party authorized to conduct independent assessment of cloud computing services, information system operations, performance, and security of the CSO. |
| **Approval to Connect (ATC)** | An ATC is a formal statement by the DISA Connection Approval Office (CAO) granting approval of a circuit used by an enclave to connect to the NIPRNet. The CAO will grant a NIPRNet ATC for no more than three years. (Not to be confused with a Cloud Approval to Connect (CATC).) |
| **Artifacts** | System policies, documentation, plans, test procedures, test results, and other evidence that express or enforce the information assurance (IA)/cybersecurity posture of the DOD IS, make up the certification and accreditation (C&A)/assessment and authorization (A&A) information, and provide evidence of compliance with the assigned cybersecurity controls. |
| **Authorization Decision** | A formal statement by an Authorizing Official (AO) 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 AO may issue the authorization decision in hard copy with a traditional signature or sign it electronically with a DoD Public Key Infrastructure (PKI)-certified digital signature. |
| **Authorization Termination Date (ATD)** | The date assigned by the AO that indicates when an ATO or IATT expires. |
| **Authorizing Official (AO)** | Senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (CNSSI No. 4009 (ref dd)).<br><br>This term is synonymous with Designated Approving Authority (DAA) and Delegated Accrediting Authority (DAA). |

| TERM | DEFINITION |
|---|---|
| **Authorizing Official (AO)** | Senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (CNSSI No. 4009 (ref dd)).<br>This term is synonymous with Designated Approving Authority (DAA) and Delegated Accrediting Authority (DAA). |
| **Authorization to Operate (ATO)** | The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (CNSSI No. 4009 (ref dd)) |
| **Boundary Cloud Access Point (BCAP)** | The BCAP establishes a protected boundary between the DISN and a CSO. BCAPs provide the capability to detect and prevent cyber-attacks from reaching the DODIN. DoD users are required by the SRG to use the DISA BCAPs or DoD CIO Approved Cloud Access Points to access their Cloud workloads hosted in CSOs. |
| **Carrier** | A Carrier provides connectivity and transport of cloud computing services from providers to Mission Owners (e.g., DISN). |
| **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. Note: DoDI 8510.01 Risk Management Framework transitions DoD from “certification and accreditation” to “assess and authorize”. |
| **Cloud Access Point** | A system of network boundary protection and monitoring devices, otherwise known as a cybersecurity stack, through which CSP infrastructure will connect to a DoD Information Network (DODIN) service, the NIPRNet, or the Secret Internet Protocol Router Network (SIPRNet). |

| TERM | DEFINITION |
|---|---|
| **Cloud Approval to Connect (CATC)** | A CATC is a formal statement by the DISA CAO granting approval for a Cloud Service Provider (CSP) to be connected to the DISN via a DISA BCAP. The CAO will not issue a CATC for longer than the period of validity of the associated DoD PA. The CAO will grant CATC for no more than three years duration. See Section 2 of this guide. |
| **Cloud Broker** | A proxy on behalf of cloud customers |
| **Cloud Computing** | Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-145 (ref ee)) |
| **Cloud IT Project (C-ITP)** | A C-ITP is a Mission Owner's project that implements a machine, software application, or information service within one or more authorized CSOs and is registered in DISA SNAP (ref e) using the same project name the Mission Owner gave the C-ITP in the SNaP-IT and DITPR databases. |
| **Cloud Denial To Connect (CDTC)** | A CDTC is a formal statement by the Connection Approval Office withholding or rescinding approval for a CSO to connect (or remain connected) to the DISN. |
| **Cloud Permission To Connect (CPTC)** | A formal statement by the DISA Connection Approval Office granting approval for a Mission Owner to connect a C-ITP to a CSO via a DISA BCAP. DISA CAO will grant a CPTC for no more than three years duration. |
| **Cloud Service Provider-Cloud Service Offering (CSO)** | A CSO is the IaaS/PaaS/SaaS solution available from a CSP. A CSP may provide several different CSP-CSOs. |

| TERM | DEFINITION |
|---|---|
| **Cloud Service Provider (CSP)** | A CSP is a DoD or non-DoD entity that offers one or more cloud computing services in one or more deployment models. A CSP might leverage or outsource services of other organizations and other CSPs (e.g., placing certain servers or equipment in third party facilities such as data centers, carrier hotels / collocation facilities, and Internet Network Access Points (NAPs)). CSPs offering SaaS may leverage one or more third party CSP's (i.e., for IaaS or PaaS) to build out a capability or offering.<br>• Commercial vendor or Federal organization offering or providing cloud computing services (Includes DoD CSPs)<br>• Provides CSOs for mission use<br>• Provides Cyber Defense services (all tiers) for its infrastructure and service offerings (DoD Cloud SRG (ref d)) |
| **Command Communications Service Designator (CCSD)** | A CCSD is a unique identifier for each single service including use circuits, package system circuits, and inter-switch trunk circuits. |
| **Community Cloud** | A Community Cloud is an infrastructure provided by a CSP for exclusive use by a specific community of Mission Owners from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist On-Premises or Off-Premises. (NIST SP 800-145 (ref ee)) |
| **Continuous Monitoring** | Maintaining ongoing awareness to support organizational risk decisions. CNSSI No. 4009 (ref dd) |
| **Provisional Authorization to Connect (PA-C)** | A Conditional DoD PA includes conditions for using a CSO, for example:<br>• A requirement to use a CSO in conjunction with another CSO(s).<br>• A requirement to use the CSO only in a specific environment or configuration. |
| **Connection Approval Office (CAO)** | Single point of contact within DISA for DISN connection approval requests. |

| TERM | DEFINITION |
|---|---|
| **Consent to Monitor (CTM)** | This is the agreement signed by the AO granting DISA permission to periodically monitor the connection and assess the level of compliance with cybersecurity policy and guidelines. |
| **Cybersecurity** | Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. |
| **Cyber Security Service Provider (CSSP)** | An organization that provides one or more cybersecurity services to implement and protect the DODIN. The DoD Component-owned or -operated portion of the DODIN will be aligned to a JFHQ-DODIN certified and authorized CSSP supported by a Network Operations Security Center (NOSC) and an integrated capability to conduct cybersecurity activities. This cybersecurity capability may be obtained from within a DoD Component or from an authorized external DoD Component service provider. All service providers must be authorized in accordance with DoD O-8530.1-M, "Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program," December 17, 2003, per DoDI 8530.01 of 07 March 2016) (ref hh). |
| **Defense Security/Cybersecurity Authorization Working Group (DSAWG)** | Provides, interprets, and approves the DISN security policy, guides architecture development, and recommends accreditation decisions to the DoD ISRMC. Also reviews and approves Cross Domain information transfers (when delegated by the ISRMC) or forwards such recommendation(s) to the ISRMC. |
| **Defense Information Systems Agency (DISA) Store Front** | This is the ordering tool for DISN telecommunications services. (Formerly DISA Direct Order Entry (DDOE)) |
| **Defense Information Systems Network Connection Process Guide** | The DISN CPG is a step-by-step guide to the detailed procedures that Partners must follow in order to obtain and retain connections to the DISN. (ref f) |
| **Defense Information Systems Network (DISN)** | DOD integrated network, centrally managed and configured to provide long-haul information transfer for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery and video teleconferencing services. |

| TERM | DEFINITION |
|---|---|
| **Demilitarized Zone (DMZ)** | 1. Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.<br>2. A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet.<br>3. An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. (CNSSI No. 4009 (ref dd)) |
| **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 a reaccreditation connection) approval for an IS to connect (or remain connected) to the DISN. |
| **Denial of Authorization to Operate (DATO)** | A DATO is an 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 (DODIN)** | 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." (DoDI 8110.01) |
| **Department of Defense Information Security Risk Management Committee (ISRMC)** | The DoD ISRMC, comprised of the four-mission area Principal Authorizing Officials (PAOs) and other major DoD and Intelligence Community (IC) stakeholders, provides the Tier 1 [Organizational] risk management governance for DoD. (DoDI 8500.01) |

| TERM | DEFINITION |
|---|---|
| **Designated Accrediting Authority (DAA)** | "Authorizing Official" supersedes this term. |
| **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. |
| **DoD Assessor** | An Assessor is a DoD organization that leverages any existing, Federal Agency, or DoD Self-Assessed Provisional Authorization (PA) and assesses CSOs for compliance with FedRAMP+ requirements as stipulated in the DoD Cloud SRG (ref d) (e.g., DISA Cloud Assessments Division, DoD Component Cloud Assessor). |
| **DoD Mission Sponsor** | A Mission Sponsor (MS) is the DoD Component responsible for ensuring the connection or CSO has a valid DoD mission essential requirement, is properly maintained, resourced and secure throughout the cloud connection's lifecycle. The DoD Sponsor and DoD Mission Owner can be one in the same. The responsibilities of DoD sponsors are defined in several OSD and Joint Staff issuances and are summarized in the DoD CIO ***Summary of DoD Sponsor Responsibilities for Mission Partner Connections to the Defense Information Systems Network (DISN)***, Memorandum, 14 August 2012 (ref j) |
| **DODIN Readiness and Security Inspections (DRSI)** | Produces and deploys information assurance (IA) products, services, and capabilities to combatant commands, services, and agencies to protect and defend the DODIN. |
| **Enclave** | A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (CNSSI No. 4009 (ref dd)) |

| TERM | DEFINITION |
|---|---|
| **Hybrid Cloud** | The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). (NIST SP 800-145 (ref ee)) |
| **Information Impact Level (IIL)** | Cloud security information impact levels (e.g., High, Moderate, or Low) are defined by the combination of: 1) the sensitivity or confidentiality level of information (e.g., public, private, classified, etc.) to be stored and processed in the CSP environment; and 2) the potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information. (DoD Cloud SRG (ref d)) |
| **Information Systems (IS)** | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C. Sec 3502) Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (CNSSI No. 4009 (ref dd) |
| **Infrastructure as a Service (IaaS)** | The capability provided to the Mission Owner is to provision processing, storage, networks, and other fundamental computing resources where the Mission Owner is able to deploy and run arbitrary software, which can include operating systems and applications. The Mission Owner does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (NIST SP 800-145 (ref ee)) |
| **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. |

| TERM | DEFINITION |
|---|---|
| **Interim Authorization to Test (IATT)** | Temporary authorization to test an information system in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization. (CNSSI No. 4009 (ref dd)) |
| **Internet Access Point (IAP).** | An IAP establishes a protected boundary between the NIPRNet and the public Internet. An IAP has capabilities to detect and prevent a cyber-attack on the NIPRNet from the Internet. |
| **Internet Protocol (IP)** | Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (CNSSI No. 4009 (ref dd)) |
| **Joint Services Provider (JSP) - Pentagon** | JSP provides Cloud Cyberspace Defense services for designated DoD Components in the National Capital Region that use the JSP private AWS GovCloud service. For additional information, contact your Organization's JSP Customer Account Manager (CAM) or the JSP Service Desk. |
| **Joint Validation Team (JVT)** | JVT (Joint Validation Team) is comprised of a DISA Cloud SCA, a.k.a. JVT Lead, and resources provided by the CSO sponsoring organization. |

| TERM | DEFINITION |
|---|---|
| **Mission Owner (MO)** | The MO is a person or DoD component that maintains a business relationship and uses (or intends to use) authorized CSOs. Entities such as IT system/application owner/operators or program managers within the DoD Components/Agencies responsible for instantiating and operating one or more information systems and applications who may leverage a CSP's CSO in fulfilment of IT missions. (DoD Cloud SRG (ref d)) |
| **Mission Partners** | Those with whom Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments, allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. |
| **Approval to Connect (ATC)** | A NIPRNet ATC is a formal statement by the DISA Connection Approval Office (CAO) granting approval of a circuit used by an n enclave to connect to the NIPRNet. The CAO will grant a NIPRNet ATC for no more than three years. |
| **Off-Boarding** | Off-boarding is the set of activities that take place when a Mission Owner discontinues use of a CSO. An off-boarding process is required when a Mission Owner migrates to a new cloud service, a mission reaches end of life, a contract ends, or a CSO ceases operations. (DoD Cloud SRG (ref d)) |
| **On-Boarding** | On-boarding is the set of activities that take place when a Mission Owner migrates a C-ITP to an authorized CSP-CSO. |
| **Plan of Action & Milestones (POA&M)** | A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (CNSSI No. 4009 (ref dd)) |

| TERM | DEFINITION |
|---|---|
| **Platform as a Service (PaaS)** | The capability provided to the Mission Owner is to deploy onto the cloud infrastructure Mission Owner - created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The Mission Owner does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (NIST SP 800-145 (ref ee)) |
| **Private Cloud** | The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple Mission Owner s (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist On-Premises or Off-Premises. (NIST SP 800-145 (ref ee)) |
| **Program or System Manager (PM or SM)** | A PM or SM is 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. |
| **Provisional Authorization (PA)** | A DoD Provisional Authorization (PA) is an acceptance of risk based on an evaluation of the CSPs offering and the potential for risk introduced to DoD networks. It provides a foundation that Authorizing Officials (AOs) responsible for mission applications can leverage in determining the overall risk to the missions/applications that are executed as part of a CSO. (DoD Cloud SRG (ref d)) |
| **Public Cloud** | The cloud infrastructure is provisioned for open use by the public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the Premises of the cloud provider. (NIST SP 800-145 (ref ee)) |
| **Request For Service (RFS)** | The document submitted to the TCO to request telecommunications service. |

| TERM | DEFINITION |
|---|---|
| **Security Assessment Plan (SAP)** | The SAP provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. (DoDI-8510.01) |
| **Security Assessment Report (SAR)** | The SAR provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls. [DoDI 8510.01] |
| **Select & Native Programming Data Input System for Information Technology (SNaP-IT)** | SNaP-IT is the authoritative Department of Defense (DoD) database used for publishing the DoD Information Technology (IT) Budget Estimates to Congress, the Circular A-11 Section 53 and Section 300 exhibits to the Office of Management and Budget (OMB), and for monthly IT performance reporting to the OMB IT Dashboard. The DoD CIO operates the SNaP-IT system. Additional SNaP-IT guidance can be located within the DoD Financial Management Regulation (7000.14-R, Volume 2B, Chapter 18) or within annual budget guidance issued by OUSD(C), D, CAPE, and DoD CIO. |
| **Significant Change** | NIST SP 800-37 defines a *significant change* as a change that is likely to affect the security state of an information system. Significant changes to an information system may include for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations. The examples of changes listed above are only *significant* when a change is likely to affect the security state of the information system. |

| TERM | DEFINITION |
|---|---|
| **Software as a Service (SaaS)** | The capability provided to the Mission Owner is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The Mission Owner does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (NIST SP 800-145 (ref ee)) |
| **DoD Mission Sponsor (MS)** | DoD component responsible for ensuring the connection or CSO has a valid DoD mission essential requirement to be connected to the DISN. The DoD Sponsor and DoD Mission Owner can be one in the same. The responsibilities of DoD Sponsor for a CSO will be stipulated in future versions of this guide.) |
| **Systems Security Plan (SSP)** | Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [NIST-SP 800-18] |
| **Third Party Assessment Organization (3PAO)** | A 3PAO is an independent organization accredited to help CSPs and government agencies meet FedRAMP compliance regulations. A 3PAO has demonstrated independence and technical competency required to test security implementations and collect representative evidence. The American Association for Laboratory Accreditation (A2LA) accredits FedRAMP 3PAOs with the FedRAMP PMO providing final approval. |
| **Virtual Private Network (VPN)** | Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.<br>(CNSSI No. 4009 (ref dd))<br>DoD enterprise VPN services are described at:<br>https://storefront.disa.mil/kinetic/disa/service-catalog?#/category/virtual-private-network-vpn |

| TERM | DEFINITION |
| --- | --- |
| **Virtual Routing and Forwarding (VRF)** | A technology that allows multiple routing tables to exist within the same router/switch. Provides the ability to support communities of interest, separate applications, and coalitions on a single physical network. |

# APPENDIX E: RESPONSIBILITIES

## 1. DISA Enterprise BCAP Connection Responsibilities

This section only addresses roles and responsibilities after the CSP receives a Cloud Approval to Connect (CATC) to the DISA Enterprise BCAP from the DISA Connection Approval Office (CAO). The key stakeholders are DISA Enterprise BCAP Program Manager/Service Manager, DISA IP Tier 3 Engineers, DISA Global NetOps Support Center (GNSC), transport, and CSPs.

## 2. DISA Enterprise BCAP Program Manager/Service Manager

The Program Manager or Service Manager is responsible for planning, budgeting, and providing overall network policy and guidance. Specific duties include:

a. Analyze/concur/approve new CSP connection

b. Approve operating system and hardware life-cycle support and upgrades

c. Analyze/concur/approve funding for new equipment, new DISA Enterprise BCAP site(s) and backbone bandwidth requirements

d. Provide annual funding for the operations, hardware life-cycle support and upgrade of the DISA Enterprise BCAP including circuits

## 3. DISA IP Tier 3 Engineers

The DISA IP Tier 3 Engineers are responsible for overall network architectural design and network evolution of the DISA Enterprise BCAP. The DISN IP Tier 3 Engineers also assist in troubleshooting analysis of DISA Enterprise BCAP outages. Specific duties in the CSO Connection Process include:

a. Responsible for network architecture and long-range network planning

b. Perform requirement analysis of the CSP connection to the DISA Enterprise CAP

c. Evaluate/Analyze/Recommend new equipment, new DISA Enterprise BCAP site(s) and backbone bandwidth requirements

d. Recommend operating system and hardware life-cycle support and upgrades

e. Provide assistance to DISA GNSC and the DoD contracted transport provider during troubleshooting of complex problems/outages

## 4. DISA GNSC

The DISA GNSC is responsible for the management and operations of the DISA Enterprise Infrastructure to ensure delivery of services and capabilities in support of the Combatant Commands, Service Branches, and DoD Agencies. Specific duties in the CSO Connection Process include:

a. Coordinate the requirement analysis of the CSP connection to the DISA Enterprise CAP

b. Participate in the Initial Testing and Acceptance (IT&A) of new CSP connections/circuits

c. Manage and maintain NFG configurations, access and permission levels for all users

d. Coordinate new equipment, DISA Enterprise BCAP site(s), and backbone bandwidth requirements

e. Assist the DoD contracted transport provider during troubleshooting of complex problems/outages

f. Coordinate operational assessment/testing with stakeholders

g. Perform day-to-day capacity planning (modeling). If a need for DISA Enterprise BCAP bandwidth or hardware is determined, it is engineered and forwarded to the Program Manager/Service Manager for concurrence/funding approval

h. Perform Initial Testing and Acceptance (IT&A) of new network elements and circuits

i. Escalate issues to the DISA IP Tier 3 Engineers to troubleshoot configuration issues and resolve problems

j. Coordinate network architecture and long-range network planning

k. Coordinate operating system and hardware life-cycle support and upgrades

**5. CSPs**

A CSP is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to businesses, agencies and services. Specific duties in the CSO Connection Process include:

a. Coordinate the requirement analysis of the CSP connection to the DISA Enterprise CAP

b. Coordinate the Meet-Me Router provisioning actions

c. Coordinate engineering support with DISA, the DoD contracted transport and Meet-Me-Point providers

d. Participate in IT&A with DISA, the contracted transport and Meet-Me-Point providers

Coordinate operational assessment/testing with stakeholders

# - APPENDIX F: CLASSIFIED (IL6) C-ITP REGISTRATION AND CONNECTION PROCESS

1. DoD authorizes a Level 6 CSO to accommodate information that has been determined to be classified national security information. The classification determination is pursuant to (i) Executive Order 13526, *Classified National Security Information* (December 29, 2009), or (ii) pursuant to the Atomic Energy Act of 1954, as amended, (P.L. 83-703)16 to be Restricted Data (RD).
2. At this time, only information classified as SECRET, in accordance with the applicable Executive Orders, is applicable to Impact Level 6. DISA's STRATUS offers a SECRET IaaS/PaaS CSO connected to SIPRNet.
3. The DISA STRATUS web site has instructions for registering, connecting, and on-boarding to a STRATUS CSO on SIPRNet.
4. CSOs and C-ITPs running at classification levels above SECRET are outside the scope of this guide.

Mission Owners must register their Impact Level 6 (secret) DoD Cloud IT Projects in the SIPRNet GIAP System (SGS) when the SGS cloud module becomes available.

This page intentionally left blank

# APPENDIX G: SAMPLE OF AN IT TOPOLOGY DIAGRAM

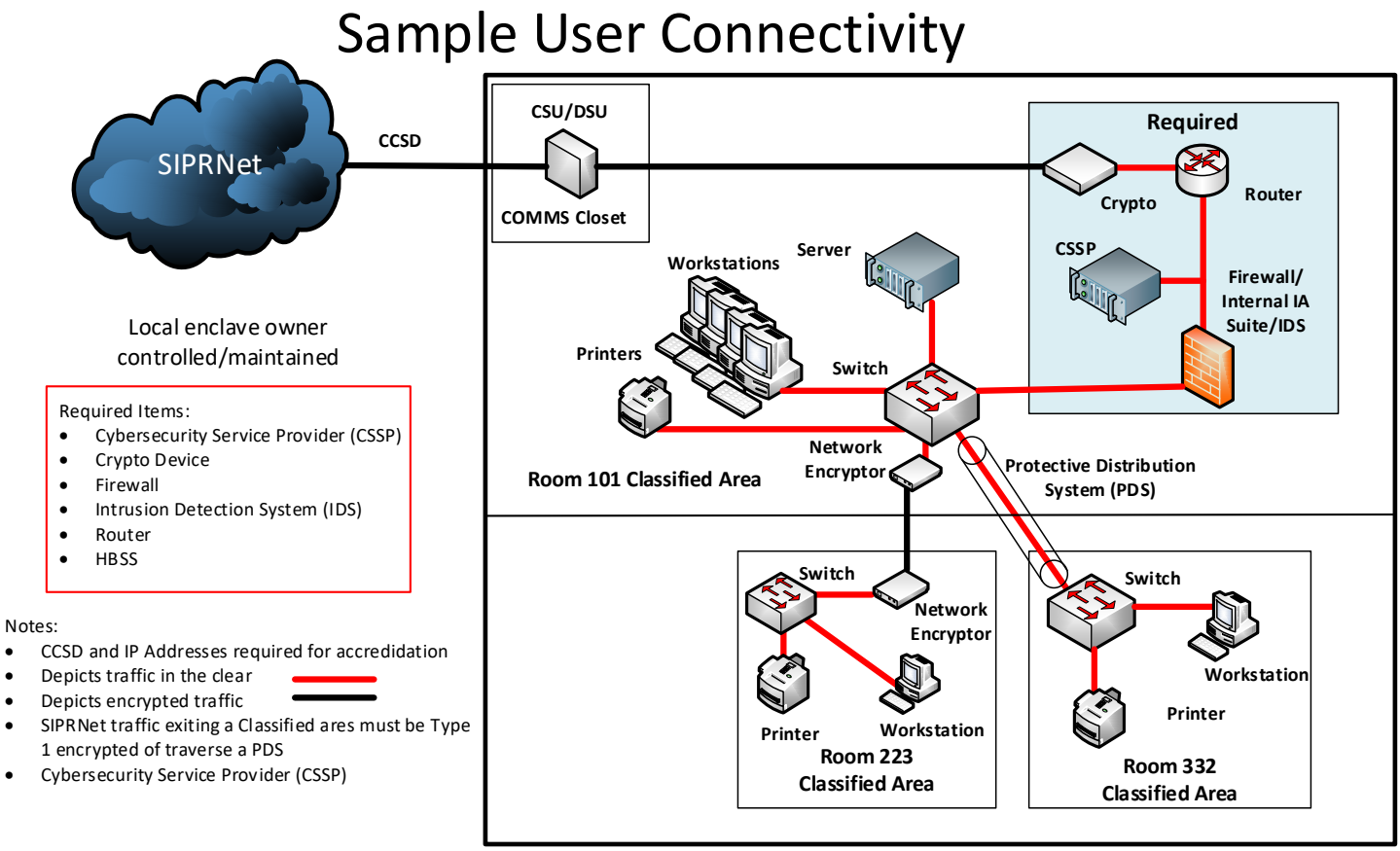



**Figure 2: Sample Connectivity Topology Diagram**

An IT Topology identifies equipment (e.g., XXX DSU/CSU; CISCO WC-1DSU-T1-V2-RF; Cisco 3600 Router; Cisco IDS 4210 Sensor, Cisco 4900 Catalyst Switch) and includes all IP addresses, etc. Figure 6 is an illustration from the DISN Connection Process Guide. Although Figure 6 illustrates a sample IT topology for a SIPRNet connection, it provides an example that can be used for illustrating an enclave connected to the NIPRNet.

This page intentionally left blank

# APPENDIX H: CONSENT TO MONITOR AGREEMENT (SAMPLE)

**DEPARTMENT OF THE <*Service*>**

*<Address>*

**REPLY TO**
**ATTENTION OF:**

*The Consent To Monitor (CTM) is a mandatory document. The Mission Owner must submit a signed CTM to DISA (Defense Information Systems Agency) to complete the Cloud Connection Approval Package.*

*Cut and paste the text below, format as appropriate, and print on Organization Letterhead. Be sure to provide the Cloud Service Offering and Cloud IT Project names as appropriate...*

*When complete, Mission Owner will upload the CTM statement into the SNAP registration package.*

*Questions about the CTM may be directed to the Connection Approval Office at:*

*301-225-2900 or 301-225-2901 (DSN prefix is 312-)*

*Email: disa.meade.re.mbx.ucao@mail.mil*

---

<Date>

SUBJECT: Consent to Monitor for <*CSO or C-ITP Name*>, CCSD <*Circuit, VPN or VRF Identifier (if any)*>

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

Authorizing Official

This page intentionally left blank


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