DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

CLOUD CONNECTION PROCESS GUIDE (CCPG)

Version 1.01

September 2015

EXECUTIVE SUMMARY

The Cloud Connection Process Guide (CCPG) is designed to help DoD Components[1] and cloud service providers navigate DOD's Assessment and Connection Processes to obtain a DoD Provisional Authorization (PA) and Cloud Approval to Connect (CATC) and provide guidance for Mission Owners to onboard[2] to DOD approved Cloud Service Offerings (CSOs). This document describes the process of connecting Mission Owners to CSOs through the DISA provided Cloud Access Point (CAP). It ensures the cloud security requirements have been implemented before a CATC is granted, and describes the process of registering DOD cloud usage in SNAP, the centralized repository for DOD cloud connections.

Nothing in the CCPG is intended or designed to usurp a DOD Component's individual authorities or impede a Component's ability to develop and implement their own compliant cloud strategies and cloud service offerings. Nothing in the CCPG restricts an individual Component's acquisition authorities under Title 10 or a Component's authorities as an Authorizing Official (AO) under DoD Instruction (DoDI) 8500.01 and DoDI 8510.01 references ((e) and (f)). Nothing in this CCPG alters or supersedes the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information (SCI), as directed by Executive Order 12333 (ref g) and other laws and regulations.

This document incorporates the lessons learned and process insights from cloud pilots and various other DISA led efforts. The CCPG is a living document and will be updated to remain compliant with policies, including the Cloud SRG and as DISA and DoD move forward in this dynamic environment with the intention of evolving the DISA CCPG into an approved *DoD* CCPG.

The CCPG is divided into three sections. Section 1 provides a general introduction and overview. Section 2 addresses the connection of Cloud Service Offerings. Section 3 addresses the onboarding of Mission Owners to Cloud Service Offerings.

[1] The term Components 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, 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] Onboard: The process of adding a mission owner to an approved DoD CSO.

Please send your DISA CCPG comments directly to DISA's Cloud Services Support Office at disa.meade.re.mbx.disa-commercial-cloud@mail.mil. This guide is approved for public release and is available on the Internet from the DISA website at http://disa.mil/computing/cloud-services. 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: 2015.09.22 14:51:41 -04'00'

Matthew A. Hein

Chief, Risk Adjudication and Connection Division

REVISION HISTORY

This document will be reviewed and updated as needed (minimum annually). Significant changes will be reflected in the revision history table.

Version	Date	Comments
1.0	21 Aug 2015	Initial Release
1.01	18 Sep 2015	Incorporates DRG input.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1: INTRODUCTION AND DOCUMENT OVERVIEW

1.1 Background

The DoD CIO Memorandum, *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services*, 15 December 2014 (ref a) rescinded two previous DoD CIO memorandums[3] and provided direction for use of commercial cloud services. DISA released the *DoD Cloud Computing Security Requirements Guide (SRG) Version 1, Release 1*, 12 January 2015 (ref b) providing an attenuated DoD cloud Impact Level framework, 2, 4, 5, and 6. Impact level 1 and 3 of the original cloud security model were combined with level 2 and 4 respectively. The Cloud SRG identifies and clarifies DoD specific security requirements that are not required as part of the FedRAMP certification (FedRAMP+). Following the SRG's release, DoD Acquisition, Technology, and Logistics (AT&L) memorandum, *Class Deviation-Contracting for Cloud Services*, 9 February 2015 (ref d) provided key guidance regarding contracting requirements for commercial cloud services.

1.2 Purpose

The CCPG provides guidance and the procedural processes for DoD Components and DoD Mission Partners[4] with a requirement to:

- Provide Commercial Cloud Service Offerings at Level 2 (Non-DISN Connected) to their mission owners.
- Provide the Connection and Assessment Processes for Cloud Service Offerings at Levels 4-5[5] (DISN-Connected).

The CCPG provides links to DOD Cloud Service Offerings Catalogue and the processes and procedures required to add a cloud service offering to the Catalogue.

[3] DoD Memorandum, "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker," June 26, 2012 (Canceled) and DoD Memorandum, "Supplemental Guidance for the Department of Defense's Acquisition and Secure Use of Commercial Cloud Services," December 16, 2013 (Canceled)

[4] DoD Mission Partners: Those with whom the 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.

[5] Level 6 commercial cloud offerings will be addressed at a later date. For level 6 cloud services please see DISA's milCloud offerings at https://milcloud.mil

DISA cloud points of contact (POCs) in table 2.3.3: Cloud Points of Contact. Guidance on registering the use of cloud service offerings in the System/Network Approval Process[6] (SNAP) database, are also outlined. SNAP is DoD's cloud usage tracking mechanism. The SNAP database is the data repository for connection approval artifacts. DISA's SIPRNet GIAP (GIG Interconnection Approval Process) System (SGS) will serve a similar function for cloud service offerings at Level 6 cloud.[7] Currently, classified CSOs are registered and connected via milCloud, which is not covered by this version of the CCPG. Please see https://milcloud.mil for more information on milCloud.

1.3 Authorities

The CCPG is an authoritative document based primarily on references ((a)-(c)), and is provided under the authorities and responsibilities of the DISA AO in relation to connections to the DISN as described in DoDI 8500.01 (ref e) and DoDI 8510.01 (ref f). References ((e) and (f)) also provide DoD's Risk Management Framework (RMF) and Executive Risk Functions used for CSPs hosting DoD Information. FedRAMP, the Federal Risk Assessment and Management Program (ref c) provides policies regarding all federal cloud computing. Other references germane to the CCPG include, the DoD CIO Memorandum, *Use of Enterprise Information Technology Standard Business Case Analysis*, 23 October 2014, (ref h) requiring Business Case Analysis (BCA). The CJCSI 6211.02D, Defense Information Systems Network (DISN) Responsibilities (ref i) requires a DoD sponsor for non-DoD mission partner's connections to the DISN. Therefore, commercial cloud service providers must be sponsored by a DoD Component before an approval to connect will be issued. The DISN Connection Process Guide (ref j) provides additional DISN connection process information that supports CJCSI 6211.02D.

Reference (a) requires all commercial cloud service offerings hosting data categorized as Level 4 or higher, to be connected to the DISN and that DoD cloud consumers access those service offerings through a DoD CIO approved Cloud Access Point (CAP) (ref a). A CAP can be provided by DISA or a DoD Component. Mission Owners connecting to the DISA provided

[6] DISA's SNAP is not to be confused with Select and Native Programming Data Input System- Information Technology (SNaP-IT)

[7] See DoD's Cloud Computing Security Requirements Guide (SRG), Version 1, Release 1

CAP must adhere to DoDI 8551.01 Ports, Protocols, and Services Management (PPSM) (ref k) declaring the use of all Ports, Protocols, and Services (PPS) using DoD IT, [8] and adhere to requirements in (ref b). Reference (b) also requires CSOs to have appropriate security controls that shall be addressed in Service Level Agreements (SLAs). Reference (a) requires DoD cloud consumers to register the use of CSOs in the Defense Information Portfolio Registry (DITPR) as part of the Component's[9] Federal Information Security Management Act (FISMA) responsibilities. Reference (ref a) also requires Components to report the required information in the Select and Native Programming Data Input System-Information Technology (SNaP IT) as directed in the DoD CIO annual IT budget guidance for each cloud computing service utilized.

DoD O-8530.1-M DoD, *Computer Network Defense (CND) Service Provider Certification and Accreditation Process* (ref l) requires all DoD information systems to be supported by a certified CND Provider[10].

All CSOs utilized by DoD Components must maintain a DoD Provisional Authorization (PA) in accordance with (ref b), current DoD CIO policies and DISA practices.

DoD components may request exceptions to DoD Cloud policies through the DoD Information Networks (DoDIN) Waiver Panel (DWP) process[11] in accordance with the DoD CIO memorandum ref (a). The DISN Connection Process Guide (CPG) ref (j) provides guidance on the DWP process. In the unlikely event that a cloud service offering requires a DoDIN waiver, it will be reviewed by the DSAWG. The results of the DSAWG recommendation will be provided to the Deputy DoD CIO for waiver issuance/approval via the DoDIN waiver panel Secretariat.[12]

[8] DoDI 8500.01 defines DoD IT as DoD-owned IT and DoD-controlled IT. DoD IT includes IS, PIT, IT services, and IT products. IT: CNSS 4009 defines IT as: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

[9] DoD Components: OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD

[10] DoD O-8530.1-M, paragraph C1.1.3.1 page 9

[11] The DoD CIO is drafting specific cloud waiver policies that will be published in a new DoD instruction DoDI 8220.bb

[12] Current DoD CIO policy does not remove the formal DWP vote from this procedure.

All Components or DoD Sponsors of CSOs must register their Level 4-5 CSPs in SNAP, so that DISA, on behalf of the DoD CIO, can track all CSPs hosting DoD information in accordance with (refs (i) and (j)). All DoD Level 2 CSO usage should be registered in the SNAP Cloud module for DoDIN documentation and tracking purposes.

1.4 CSO Connection Overview

This section of the guide discusses the high level views of CSO DoDIN connections and CAPs, provides the Connection and Assessment processes, and the specific DISA Connection Approval Office (CAO) cloud process for issuing a Cloud Authority to Connect (CATC).

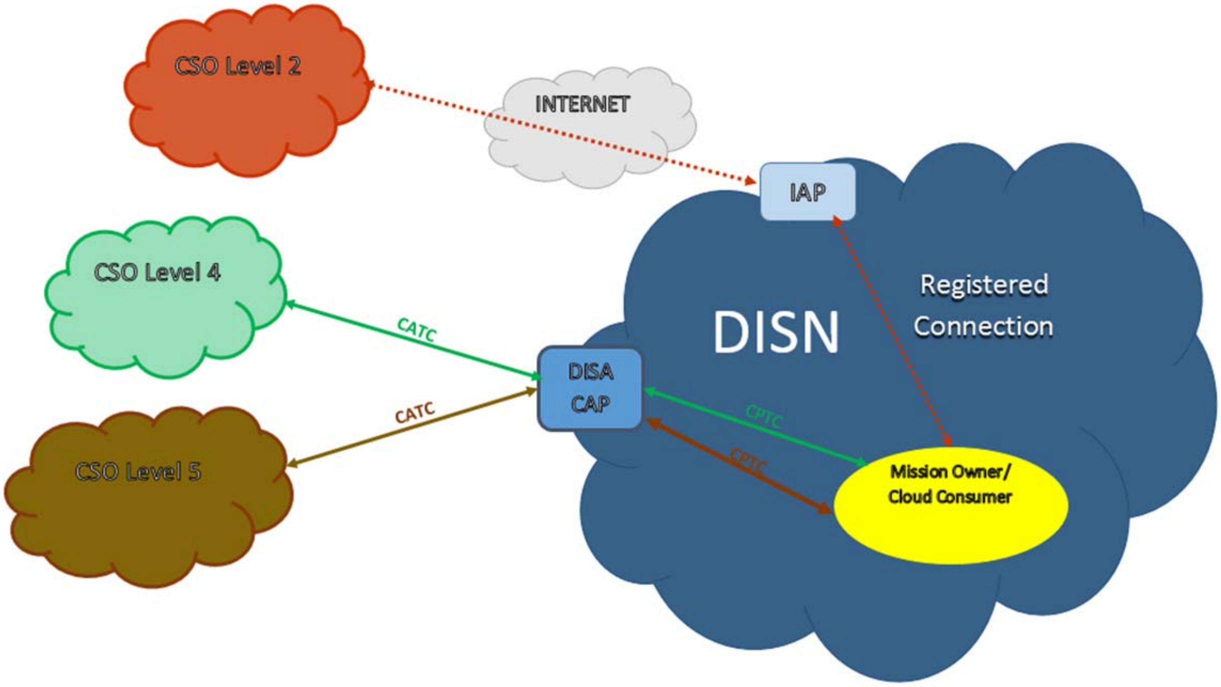


Figure 1: High Level Cloud Connection View

Figure 1 above, provides a high level DISN connection view of CSO with Impact Levels[13] 4-5. CSOs connected to the DISA CAP which receives a CATC. CSOs at Level 2, with no DISN connection, are not issued a CATC, Mission Owner’s utilizing these Level 2 CSOs, are not

[13] “Impact Levels”, “impact levels”, “Levels”, “levels”, and “levels (followed by a number level 2, level 4 or Level 5) are synonymous.

issued a Cloud Permission to Connect (CPTC). DoD Component CAPs are issued an ATC for the DISN connection and will not be addressed in this version of the CCPG with the exception of the following statements. CSOs connecting to DoD Component CAPs are not issued CATCs by DISA but the connection is registered in SNAP. Mission Owners onboarding CSOs connecting to Component CAPs are not issued CPTC but the connections are registered in SNAP.

Cloud service providers may offer more than one, cloud service offering and may offer CSOs at differing impact levels. Each CSO and the approved impact level are registered in SNAP. The DISA CAP is connected to the DISN at the Unclassified but Sensitive Internet Protocol Router Network, *NIPRNet* Federated Gateway (NFG) security architecture. DISA's CAP architecture will continue to evolve and mature as specific CAP requirements and capabilities are developed and expanded to meet mission needs. Each CSO will be authorized for use by a DoD PA. A significant change in the configuration which is an alteration of the security posture of a CSO will necessitate the review of the associated DoD Cloud PA and may require the issuance of a new PA and reevaluation of the CATC to the DoD CAP. Finally, note that one CSP may provide services to several mission owners. Each mission owner will have a separate ATO granted by their respective AOs that is associated with a CPTC.

1.5 Cloud Access Points (CAP)

A CAP is an approved connection between a cloud service provider and a DoD consumer. For example, off premise cloud service providers with CSOs authorized to host data at impact levels 4 and 5 are connected to the DISN by the DISA CAP as depicted in Figure 1. The CAP provides cybersecurity, performance monitoring and a location for the sharing of common services and functions (ref b). CAPs must meet the requirements in the CAP Functional Requirements Document (FRD) reference (m). DISA's CAP will integrate with pre-existing and emerging DoDIN capabilities such as the NIPRNet De-Militarized Zone (DMZ) and the Joint Regional Security Stack (JRSS) to provide an additional layer of security functionality necessary to defend against threats from using the CSP. DoD CAPs will provide the following generalized functions:

- Intrusion Detection

- Intrusion Protection
- Data Loss Prevention
- Full Packet Capture
- Network Routing/Switching
- Network Access Control to Cloud Service Providers
- Next Generation Firewall
- Application Firewall

Some cloud service offering will have connections that are internal to the DoDIN, with the DoD Component’s network infrastructure and located on/at DoD or Federal Government facilities. These cloud service offerings are referred to as “On Premises[14]”and have internal CAPs (ICAPs). Cloud Service Offerings located externally to a Components network infrastructure are “Off Premises[15]” and have external boundary CAPs (BCAPs) (Figure 2).

[14] DoD Cloud Computing SRG: CSP Infrastructure (dedicated to DoD) located inside the B/C/P/S “fence-line” (i.e., on-premises) connects via an Internal CAP (ICAP). The architecture of ICAPs may vary and may leverage existing capabilities such as the IA Stack protecting a DoD Data center today or may be a Joint Regional Security Stack (JRSS). On the other hand, an ICAP may have special capabilities to support specific missions, CSP types (commercial or DoD), or cloud services.

[15] DoD Cloud Computing SRG: CSP Infrastructure (shared w/ non-DoD or dedicated to DoD) located outside the B/C/P/S fence-line which connects to the DoDIN/NIPRNet does so via one or more Boundary CAP (BCAPs). The BCAP terminates dedicated circuits and VPN connections originating within the CSP’s network infrastructure and/or Mission Owner’s virtual networks. All connections between a CSP’s network infrastructure or Mission Owner’s virtual networks that is accessed via or from the NIPRNet/SIPRNet must connect to the DoDIN via a BCAP.

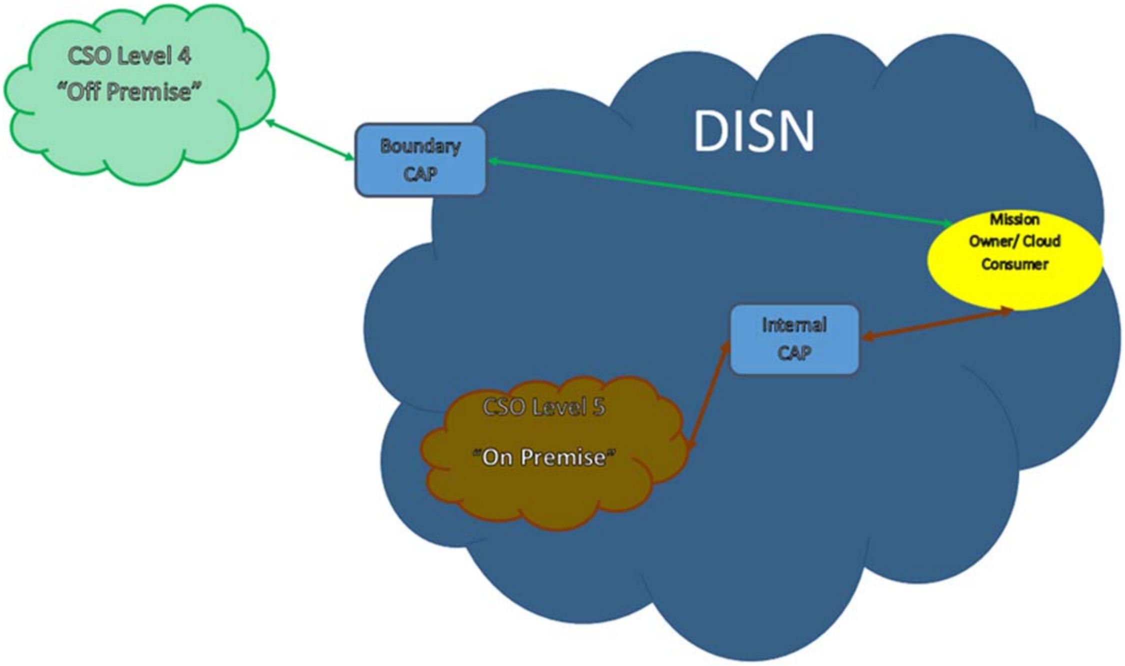
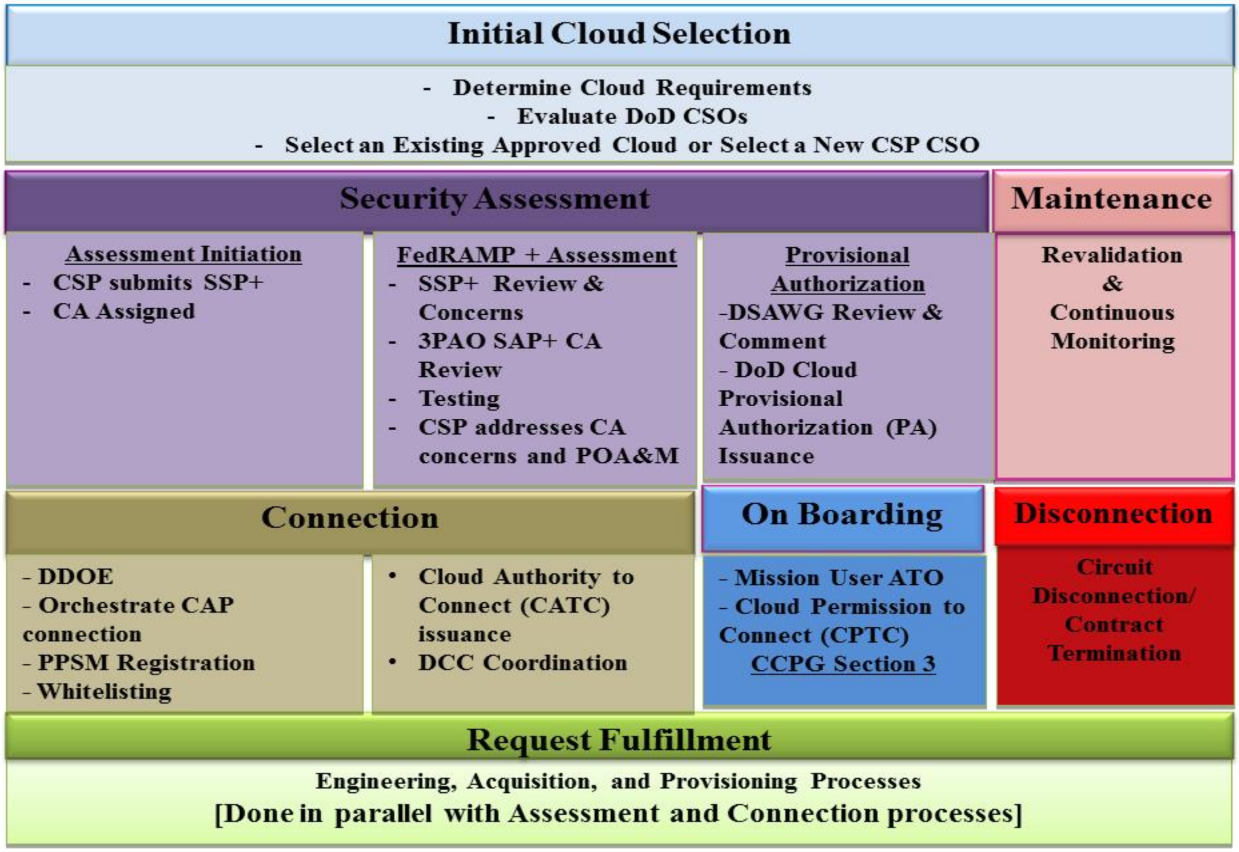


Figure 2: On Premise & Off Premise Cloud Service Offerings with Internal and External CAPS

1.6 Cloud Connection Processes

This section of the guide describes the key steps and process from "Initiation" of first contact with DISA through the assessment, review and evaluation phases to the issuance of the PA, connection approval, request fulfillment process, cybersecurity maintenance of the authorization, and finally termination. Figure 3 provides the overview in a process flow format with little attention to the detail involved in all the various steps in each of the processes required to either produce the documentation or approval to move forward. It is an overview of key cloud steps beginning with the determination of cloud requirements and ending with monitoring or decommission. Additional clarification information can be found in section 1.6. The output of this process is a DoD PA that DoD Mission owners can leverage to issue an Authorization to Operate (ATO) within those cloud environments.

The path in the diagram for a new CSO (Purple) does not include a Mission owner ATO.	If a Mission Owner brings on a CSP/CSO they end up bypassing the need to get an ATO for their hosting.



Initial Cloud Selection

- Determine Cloud Requirements
- Evaluate DoD CSOs
- Select an Existing Approved Cloud or Select a New CSP CSO

Security Assessment

Assessment Initiation
- CSP submits SSP+
- CA Assigned

FedRAMP + Assessment
- SSP+ Review & Concerns
- 3PAO SAP+ CA Review
- Testing
- CSP addresses CA concerns and POA&M

Provisional Authorization
-DSAWG Review & Comment
- DoD Cloud Provisional Authorization (PA) Issuance

Maintenance

Revalidation & Continuous Monitoring

Connection

- DDOE
- Orchestrate CAP connection
- PPSM Registration
- Whitelisting

- Cloud Authority to Connect (CATC) issuance
- DCC Coordination

On Boarding

- Mission User ATO
- Cloud Permission to Connect (CPTC)
CCPG Section 3

Disconnection

Circuit Disconnection/ Contract Termination

Request Fulfillment

Engineering, Acquisition, and Provisioning Processes
[Done in parallel with Assessment and Connection processes]

Figure 3: Overview of Key Cloud Steps

1.6.1 Cloud Selection

The cloud connection process starts during the Initiation Phase (see Figures 3 and 4) with the DoD Mission Owner, DoD Sponsor, or potentially a Commercial CSP identifying that there is an unfulfilled mission need that may be met by a CSP offering. If the mission need cannot be met through cloud technology, then the mission owner/sponsor will have to seek a non-cloud solution elsewhere that may be available through various non-cloud procurement processes. If the mission can be met through cloud technology, the next step is to consult the DoD Cloud Catalogue maintained by DISA. The DoD Approved Cloud Service Provider Catalogue can be found by following the link from the DISA.mil cloud computing webpage here: http://www.disa.mil/Computing/Cloud-Services/Cloud-Support to determine if an existing milCloud or commercial CSO can be used. The mission owner/sponsor selects the CSO of their choice based on their needs and entirely at their own discretion. Entries in the Catalogue are a reflection of approved DoD Cloud Service Offerings. DoD Component CIOs need to approve

BCAs in accordance reference (h). If the mission owner does decide to use a DISA CSO then they should contact the DISA Cloud Service Support Office.

1.6.2 Assessment Initiation

During the initiation phase of the connection and assessment processes and after the determination of the requirement for a DoD Cloud, the DoD mission owner or mission owner's representative contacts the DISA Cloud Support Office at disa.meade.re.mbx.disa-commercial-cloud@mail.mil to sponsor a cloud service offering for a DoD PA.

The next step is for the Commercial CSP to download the Self-Assessment and Readiness Checklist and the DoD Assessment Request form found by following the link from the disa.mil Cloud Computing Webpage at: https://disa.mil/Computing/Cloud-Services

Once the forms are completed they should be emailed to disa.meade.re.mbx.disa-commercial-cloud@mail.mil. The report generated from this questionnaire is used by the Cloud Service Support Office to assist in identifying the technical and mission requirements and are part of the next step; the Security Assessment.

1.6.3 FedRAMP+ Assessment

The Security Assessment includes the evaluation of the IS, the data impact level, the CSO type, deployment model, service model, architecture, transport model, physical location of the CSO (on premises or off premises), and identifying all the roles (consumer, provider, broker) are assessed. FedRAMP+ requirements will be assessed by a FedRAMP certified Third Party Assessment Organization (3PAO) or an approved DoD assessor. The DoD Cloud Computing SRG (ref b) states there are three avenues for assessing a CSP for a DoD PA:

(1.) CSP's with a FedRAMP Joint Acquisition Board (JAB) PA or in the process of obtaining a JAB PA,
(2.) FedRAMP Agency ATO or
(3.) DoD Self-Assessed PA. For all assessments, the DISA Cloud Security Assessment Team reviews the DoD FedRAMP+ security artifacts as part of the DoD PA process.

1.6.4 Provisional Authorization

The assessment of security controls and other DoD requirements for commercial and non-DoD CSPs is based the use of FedRAMP, supplemented with DoD considerations as outlined in the Cloud Computing SRG. DoD enterprise service programs providing cloud capabilities or service offerings (e.g. milCloud, Defense Enterprise Email) use DoD's assessment and authorization process under the DoD RMF. Both processes utilize the NIST SP 800-53 Revision 4 ref (n) security controls as the basis of the assessment; providing a common framework under which DoD can determine the level of risk.

DoD FedRAMP+ is the concept of leveraging the work done as part of the FedRAMP assessment, and adding specific security controls and requirements necessary to meet and assure DoD's critical mission requirements. A CSO is assessed in accordance with the criteria outlined in the Cloud Computing SRG, with the results used as the basis for awarding a DoD provisional authorization.

As stated in section 1.6.3 FedRAMP+ Assessment, the DISA Cloud Security Assessment Team is responsible for DoD FedRAMP+ security assessments. The team assesses the security risk of the CSO and makes a recommendation to the DSAWG; the DSAWG adds its cybersecurity recommendations for input to the DISA Authorizing Official (AO). The DISA AO may accept the risk based on an evaluation of the CSP's offering and the potential for risk introduced to DoD networks. The output of this process is the DoD PA, signed by the DISA AO, and its associated security documentation package, which is based on DoDI 8500.01 and 8510.01 references (e) and (f).

1.6.5 Provisional Authorization Maintenance

All CSPs and sponsoring DoD Components are required to ensure their CSOs are in compliance with DoD CNDSP requirements in accordance with the SRG ref (b) including the annual re-assessment requirements described in the SRG ref (b). Any changes to the security posture of a cloud service offering should be submitted on the Security Impact Analysis Form, as identified in the Cloud SRG reference (b) section 5.3.2.1.g. Substantial architecture changes include initial CSP connections that were not through a DISN CAP that later included the CAP. In addition, the

SNAP cloud database must be updated to reflect the current, accurate, and complete status of the CSO. Any alteration to the approved CSO's configuration or substantial architecture changes that alter the security posture of the network must be approved by the appropriate configuration change authority prior to the alteration, issued a new PA and updated in the SNAP database. The SNAP database should also be updated to accurately reflect when points of contacts change for the CSO. Additionally, all SNAP entries must be updated to reflect cloud and mission owner final termination and disconnection of registered cloud connections.

Important Note: All CSPs hosting DoD information at impact levels 2, 4 and 5, regardless of whether the CSP is a commercial CSP provider, DoD Component CSP provider, or a DoD mission partner CSP will be registered in SNAP. All CSPs hosting classified (Secret and Below) Level 6 DoD information in a CSP will be registered in SGS once the SGS cloud module becomes available.

1.6.5.1 Cloud Monitoring

Both FedRAMP and DoD require an ongoing assessment and authorization capability for CSPs providing services to the DoD. This capability is built upon the DoD RMF and the foundation of the FedRAMP continuous monitoring strategy, as described in the FedRAMP CONOPS and Continuous Monitoring Strategy Guide. These ongoing assessment processes include continuous monitoring and change control. Continuous monitoring includes monitoring security controls and monitoring associated with Computer Network Defense. The DoD will review all significant changes planned by a CSP in their respective CSOs and a mission owner's applications or programs. The Cloud Computing SRG provides additional details. Processes and information flows differ depending on the origin of the cloud service offering's authority.

DoD policy ref (f) requires information systems be configured in accordance with SRGs which requires a CNDSP for CSOs. CSPs must report cyber incidents in accordance with ref (b) and FedRAMP incident report requirements found in ref (o). DoD CSP's CNDSPs will report all incidents in accordance with normal DoD processes using the Joint Incident Management System (JIMS).

Commercial CSPs will report all incidents via the on-line Defense Industrial Base (DIB) Cyber Incident Collection Form (ICF) 27 found at http://dibnet.dod.mil/ Use of this on-line form is preferred. Access to this form requires a DoD-approved medium assurance External Certificate Authority (ECA) certificate. If you are unable to access this form, please call (877) 838-2174 or email: DCISE@DC3.mil. The Defense Industrial Base Network (DIBNet) portal access and cybersecurity incident reporting can be found at http://dibnet.dod.mil/ .

1.6.6 Request Fulfillment Processes

Completed in parallel with the Connection and Assessment processes, new CSO connections may need to coordinate their specific connection requirements with the DISA CAP PM Office. Mission owners/sponsors requiring a new connection for a CSP offering connecting to the DISN and its services must use the DISA Direct Order Entry (DDOE) request fulfillment process to initiate the provisioning requirement and circuit activation (go to https://www.disadirect.disa.mil/products/asp/welcome.asp for further information and guidance). The Telecommunications Service Request (TSR) and Telecommunication Service Order (TSO) processes involve the ordering, engineering, acquisition, and installation of the circuit and equipment necessary to connect to the DISN. Request fulfillment may only be initiated by a DoD entity. A DoD Combatant Command/Service/Agency (CC/S/A) entity may sponsor a non-DoD Mission Partner, but the DoD sponsor remains responsible for all request fulfillment actions.

1.6.7 CSO Disconnection/Termination

The proper management of the end of life, i.e. (termination or decommissioning) of a commercial CSO is as important as the initial connection of a CSO and while there are no specific established processes there are several best or recommended practices. Cloud termination and decommissioning specifications and requirements should be built in up front and referenced as part of the Service Level Agreement (SLA). It should be a standard practice to release resources as quickly as possible, and to test the processes. There should be established data recovery and destruction plans as well as plans for the reuse and disposal of storage media, software, and hardware. Only the DoD CIO, USCYBERCOM, or the specific DoD Component mission owner can make the decision to disconnect a CSO.

SECTION 2: CLOUD SERVICE OFFERINGS CONNECTIONS TO THE DISN

2.1 CSP Level 2 CSOs Connections

Level 2 CSOs host publicly releasable data and are not directly connected to the DISN. The advantage of Level 2 CSOs is they can be accessed by anyone (with some minimal levels of access control)[16], anywhere in the world, at any time directly through the Internet. Level 2 CSOs must still be FedRAMP approved in accordance with references ((a) and (b)). In accordance with current DoD and DISA policy all Level 2 CSOs will also receive a PA. All mission owners utilizing a Level 2 CSO must also have a signed Component CIO BCA in accordance with (ref a). Level 2 CSOs may also be processed "off premises" using virtual separation in accordance with (ref b). In the case when a private DoD Level 2 CSO may have a connection to the DISN using DoD IT then the PPS must be declared in the DoD PPSM registry in accordance with ref (k).

Individual Components may add additional Level 2 CSO requirements as desired. Since Level 2 CSOs are not connected to the DISN, there are no DISN Cloud Connection Approval requirements other than the SNAP[17] registration requirement and the need for an ATO. Access to SNAP requires registration for a SNAP account. See Appendix F.

2.2 CSP Levels 4-5 CSOs Connections

The following steps outline the CSO Level 4-5 connection process.

a. A mission owner identifies a DoD approved CSO that meets their mission needs.
b. If the CSO is selected from the Catalogue of approved DOD cloud service offerings, the mission owner will begin the "Onboarding Process" outlined in Appendix G: Onboarding.

[16] Cloud Computing Requirements SRG: *Impact Level 2:* "Whenever a CSP is responsible for authentication of entities and/or identifying a hosted DoD information system, the CSP will use DoD PKI in compliance with DoDI 8520.03. CSPs will enforce the use of a physical token referred to as the "Common Access Card (CAC)" or "Alt Token" for the authentication of privileged users. CSPs must make use of DoD Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) resources for checking revocation of DoD certificates and DoD Certificate Authorities; and must follow DoD instructions and industry best practices for the management and protection of cryptographic keys".

[17] Registration in SNAP provides DoD an existing tracking and reporting mechanism for DoD cloud instantiations.

c. If the CSO selected is not available for selection from the Catalogue of approved DOD cloud service offerings, the mission owner may "sponsor" the cloud service offering to the DoD for a DoD FedRAMP+ assessment leading to a DoD PA. A DoD PA signifies that a cloud service offering meets the minimum security requirement necessary to provide service to DoD components. The DoD PA process is described in Appendix H: Obtaining and Maintaining a DoD Provisional Authorization.

d. If the Cloud Service Offering will host data at Level 4 and/or 5 a DISN connection via an approved DOD CIO approved CAP is required. The CAP connection process is described in Appendix I: CAP Connections.

e. Once the CSO is determined to be FedRAMP compliant the process in Figure 3 should be followed to achieve and receive a signed DoD PA. Issues of exceptions or waivers to DoD cloud policy requirements will be addressed by the DoDIN Waiver Panel (DWP) in accordance with (ref b).

f. In parallel with steps 1-3, the mission owner should be working towards gaining a CAP connection. The CAP may be provided by a DoD Component or DISA. If the cloud connection is through the DISN CAP the mission owner will need to coordinate the CSP requirements with the DISA CAP Program Management Office. Early contact with CAP PM Office will act to reduce actual connection implementation timelines. The NFG connection requirements are addressed in DISN Connection Process Guide reference (j) and the process is outlined.

Figure 4 below shows the DISA CAP/NFG process flow. The DISA CAP/NFG circuit connection requirements can be found in the DISN Connection Process Guide available at disa.mil/connect.

   a. As part of the connecting to the DISN CAP the mission owner must complete a CAP/NFG Questionnaire, which can be obtained by calling 301-225-8684 DSN 375 to ensure the required services are available.

b. The mission owner must ensure the PPS are registered in accordance with reference (k) and receive their PPSM Tracking identification number. For more information please see http://iase.disa.mil/ppsm/Pages/index.aspx.

c. The mission owner must also ensure whitelisting requirements are completed in accordance with USCYBERCOM TASKORD 15-0005, JFHQ-DODIN Application Access Control for DODIN, 132137ZFEB15 ref (p). The SIPRNet Whitelisting registry can be found at: https://niprdmzWhitelist.csd.disa.smil.mil

g. The NIPRNet CAP/NFG Program Management Office (PMO) will review and verify the PPSM registration, DoD Whitelisting registrations, and confirm the DSAWG's recommendations and Connection Approval Office CATC as applicable and the DISA Command Center (DCC) will be notified to allow the agreed PPS through the CAP/NFG.

h. In order for the mission owner to actually connect their respective CSP to the DISN they will need to be issued a signed IATC or CATC from the DISA's Connection Approval Office in accordance with references ((i) and (j)). This process is initiated, tracked, and managed through the SNAP database for cloud levels 2-5 and eventually SGS for level 6. Note: Level 2 clouds are not required to connect to the DISN. DoD level 2 CSPs will register cloud computing usage in the SNAP database for tracking and reporting purposes. All DISN CSO connections to the DISN CAP approval packages must include:

(1) FedRAMP PA (if CSP underwent FedRAMP assessment) OR Federal Agency ATO (non-DoD Federal CSP) OR exception statement

(2) DoD Provisional Authorization signed by the DISA DAA/AO

(3) DoD FedRAMP+ assessment results or a Systems Security Plan indicating that FedRAMP+ security controls defined in the DoD Cloud Computing Security Requirements Guide (SRG) have been implemented

(4) PPSM Tracking identification number #

(5) Whitelisting Registration number #

(6) Common Communication Service Designator (CCSD). This is a DISA issued designator to identify the circuit.

(7) All POA&Ms. These are POA&Ms for any cloud security related issues.

(8) A signed Consent To-Monitor (CTM) as applicable. Note: CTM allows DISA to perform remote scanning and monitoring of all DISN connections.

(9) CSP topology annotating 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 including IP addresses assigned to that circuit.

(10) A copy of the signed Component CIO BCA approval in accordance with reference (a)

(11) Hosted CSP applications associated with that specific CSO such as HBSS, etc.

(12) A copy of the Service Level Agreement (SLA). The SLA should assist others who may also wish to procure a similar CSP.

(13) CSP's Computer Network Defense shall be in accordance with DoD O-8530.1-M, reference (l), the DoD Cloud SRG reference (b), and all other DoD published cloud cybersecurity and cloud CND requirements.

(14) POC information. POC information includes several important cloud POCs such as Mission Sponsor/Owner, CNDSP, etc.

i. Ongoing with these steps, the DISA Commercial Cloud Office will continue to update DISA's enterprise CSOs and non-Enterprise CSO Catalogue in order to promote reciprocity and ability "to build once and use often, by many concept." The DISA Commercial Cloud Office will also routinely check FedRAMP for newly approved Level 2 CSOs and ensure this information is sent to DISA's Cloud assessment team to issue DoD PAs. DISA will also maintain a web assessable list of FedRAMP approved DoD PA eligible CSOs.

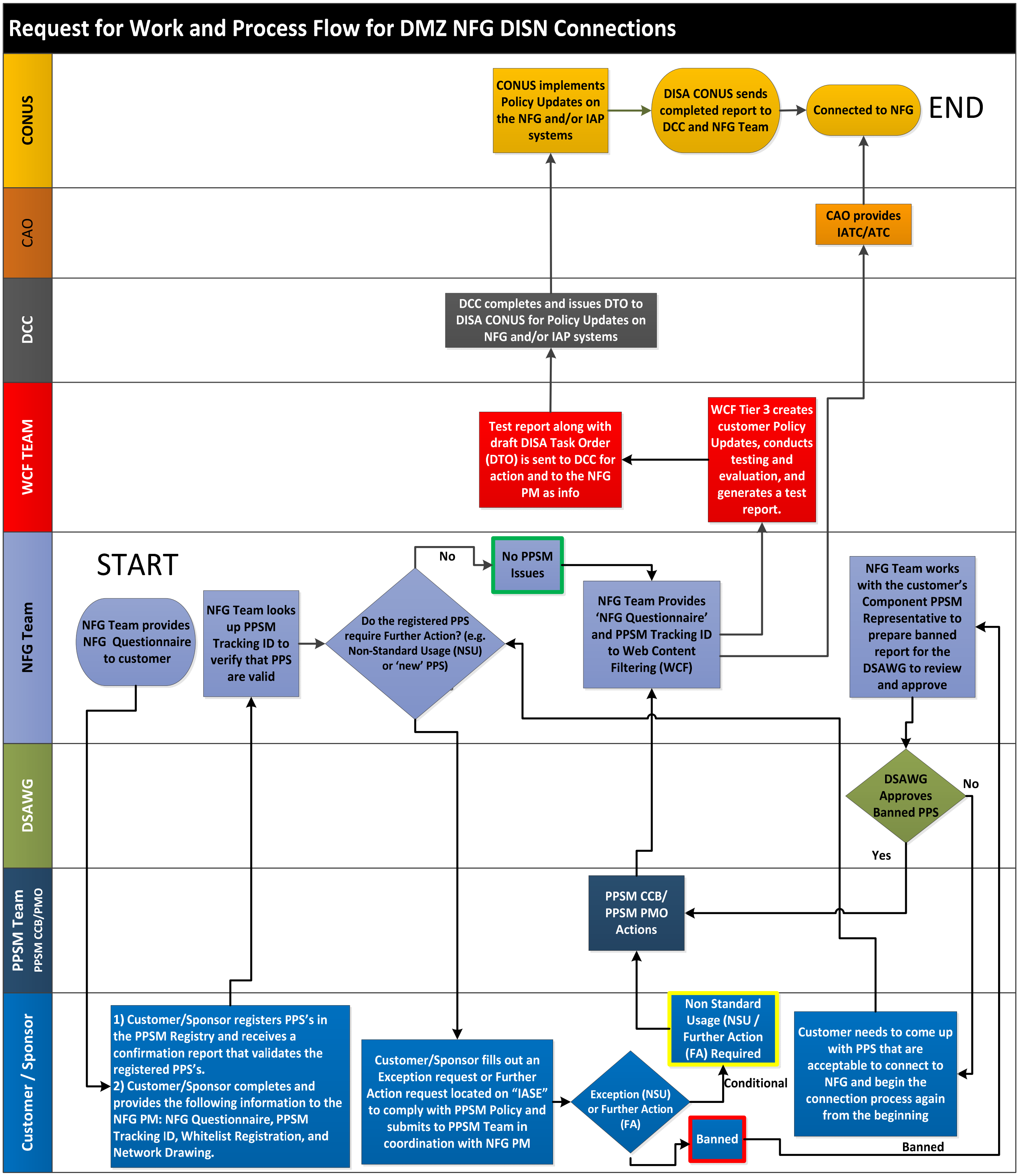

Request for Work and Process Flow for DMZ NFG DISN Connections
CONUS
CAO
DCC
WCF TEAM
NFG Team
DSAWG
PPSM Team
PPSM CCB/PMO
Customer / Sponsor
START
END
NFG Team provides NFG Questionnaire to customer
NFG Team looks up PPSM Tracking ID to verify that PPS are valid
Do the registered PPS require Further Action? (e.g. Non-Standard Usage (NSU) or 'new' PPS)
No
No PPSM Issues
NFG Team Provides 'NFG Questionnaire' and PPSM Tracking ID to Web Content Filtering (WCF)
WCF Tier 3 creates customer Policy Updates, conducts testing and evaluation, and generates a test report.
Test report along with draft DISA Task Order (DTO) is sent to DCC for action and to the NFG PM as info
DCC completes and issues DTO to DISA CONUS for Policy Updates on NFG and/or IAP systems
CONUS implements Policy Updates on the NFG and/or IAP systems
DISA CONUS sends completed report to DCC and NFG Team
Connected to NFG
CAO provides IATC/ATC
NFG Team works with the customer's Component PPSM Representative to prepare banned report for the DSAWG to review and approve
DSAWG Approves Banned PPS
No
Yes
PPSM CCB/ PPSM PMO Actions
1) Customer/Sponsor registers PPS's in the PPSM Registry and receives a confirmation report that validates the registered PPS's.
2) Customer/Sponsor completes and provides the following information to the NFG PM: NFG Questionnaire, PPSM Tracking ID, Whitelist Registration, and Network Drawing.
Customer/Sponsor fills out an Exception request or Further Action request located on "IASE" to comply with PPSM Policy and submits to PPSM Team in coordination with NFG PM
Exception (NSU) or Further Action (FA)
Non Standard Usage (NSU / Further Action (FA) Required
Conditional
Banned
Banned
Customer needs to come up with PPS that are acceptable to connect to NFG and begin the connection process again from the beginning

Figure 4: Process Flow

2.3 CSO Cloud Authorization to Connect (CATC)

Authorization to connect to the DISN/CAP is granted based on the issuance of a DoD PA and the verification of required artifacts in SNAP. At the time the initial CATC is granted, the CSO will not contain any operational data or DOD users consuming their services. Therefore, the CATC is directly associated with the CSP's security and ability to partition data based on the CSP's designated cloud security level, without any DoD customers' hosting data or applications within the CSO. A CATC is granted with the requirement that all DoD component will obtain an ATO for any mission hosted within the CSO prior to using its connection to the DISN. The CSP Sponsor will ensure the CSP's CATC is updated with mission partners'/customers' mission owners ATOs as new missions are added to the CSO. Mission owners will ensure that all CSP mission partners/customers hold a valid signed mission owner ATO prior to the on-boarding of their mission to the CSP, and prior to the customer using the CSP's DISN connection.

Once completed, the CSP's DISN connection approval will be subject to a maximum 3 year re-authorization to renew the CATC to ensure that the all the SNAP/SGS information is regularly reviewed for currency and accuracy. The additional work resulting from this requirement will be outweighed by the benefits of ensuring DoD maintains an accurate view of DoD's cloud implementation from both reporting and cybersecurity perspectives.

2.3.1 DISN Connection Process for CSP Level 6 CSOs

Level 6 CSO connection procedures will be addressed in future versions of the CCPG. DoD Components desiring a Level 6 CSO should see https://milcloud.mil.

2.3.2 Expediting the CSO Connection Process

Using the procedures outlined in the CCPG should help increase clarity and minimize the time required to complete the connection and assessment processes for a new cloud service offering. In order to assist in reducing timelines processes should be executed in parallel (Figure 5) whenever possible, in order to allow the engineering of solutions, procurement of the equipment, and other requisite steps, while coordinating the issuance of the DoD Provisional Authorization (PA) for the CSP or cloud service offering.

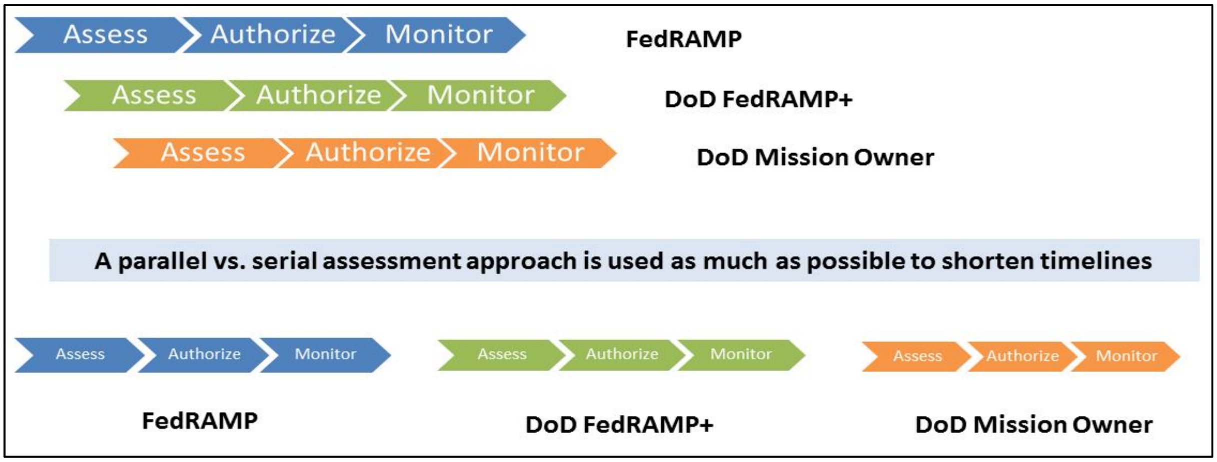


Figure 5: Parallel Process Flows

2.3.3 Cloud Points of Contact

The DISA Cloud Connection POC Table 1 below notes POC associated with areas of knowledge and organization, to answer specific cloud related questions.

Organization	Contact Information	Area of Knowledge
Connection Approval Office	301-225-2905	SNAP Database
Commercial Cloud Services Support	301-225-4530	Cloud Connection Processes
milCloud	https://disa.deps.mil/org/ID3/ID33/SitePages/Home.aspx	milCloud
PPSM	301-225-2904	Ports and Protocols
DDOE (Special Projects Team)	https://disa.deps.mil/ORG/IE1/default.aspx Phone : 301-225-2395	DISN Implementation https://disa.deps.mil/org/ID3/ID33/SitePages/Home.aspx

Table 1: DISA Cloud Connection Points of Contact

SECTION 3: ONBOARDING MISSION OWNERS

3.1 Onboarding Mission Owners to CSPs

A separate but related process is connecting mission owners to DoD approved CSOs. A mission owner will obtain their own respective ATOs while inheriting the security controls in place in existing CSO environment. DoD consumers of a DOD approved CSO must obtain an ATO from their respective AO prior to using a CSOs with operational data. Component ATOs will leverage the FedRAMP and DoD PAs of the CSP. The DoD onboarding process for new mission owners of a DoD approved CSO may be initiated after the DoD PA is issued. It is important to note, however, that initiating the SNAP registration process early on is recommended. In those cases when the CSO is connected to the DISN, DoD mission owners will share the DISN connection established for the CSP. See Appendix G.

3.1.1 Non-DoD CSP Mission Owners

Governance authority for connecting non-DoD cloud mission partners/customers to the DISN resides with the CSP mission owner, the DoD Sponsor for the CSP, the DISN AO, DSAWG, and the DoD CIO. The CSP will typically carry out the actual connection of a mission partner's/customer's hosted mission to the DISN through mechanisms such as access control to their services or their internal network configuration. The DISN Connection Process Guide (CPG) provides the DISN connection requirements for non-DoD mission partners/customers. For unclassified non-DoD mission partners/customers, DISN connections utilize the Non-secure Internet Protocol Router Network (NIPRNet) Federated Gateway (NFG). Note: The issue of Mission owner access to Releasable Mission Partners (REL) access Level 6 CSOs is outside of the scope of this document.

3.1.2 Mission Owner Tracking

The DoD cloud governance process requires maintaining visibility into which DoD mission partners are connected via CSP DISN connections. From the perspective of operating and defending the DISN, the DISN AO must maintain an accurate accounting of who, what and how entities and systems are connected to the DISN. From the perspective of the DoD CIO, it is necessary to also track and maintain a record of all DoD Cloud owners including Level 2 CSOs not connected to the DISN. For CSPs going through the DISN Connection Process, that information will be captured and maintained within the SNAP and in the future the SIPRNet Global Information Grid (GIG) Interconnection Approval Process System (SGS). SNAP and SGS will be used to track the DoD customers, hosted within CSOs, their specific connection details and all the various other required documentation. Commercial and DoD CSPs shall keep all information up-to-date. As a mission progresses through its lifecycle and mission partners/customers leave a CSP, their ATO will be revoked by the cloud mission owner.

3.1.3 SNAP Mission Owner Requirements

Sponsors will register new CSOs in SNAP (see paragraph 2.1) and upload the respective ATO information along with the other required artifacts. For DISN connected CSOs, the mission owner will receive a Cloud Permission to Connect (CPTC) that allows that mission owner to begin using the CSO with their own respective CSO’s applications and systems. For DISA Enterprise CSOs the DoD sponsor is responsible for ensuring CSO CATC is kept up to date. A CPTC will not extend past the CATC. Note: One CSP may have several CSOs connected to the DISN CAP and each CSO connected to the DISA CAP will receive a CATC. Each mission owner of each individual CSO connected to the DISA CAP will receive a CPTC (Figure 1). Note: CPTC will not be issued for Level 2 CSO. DISA Enterprise CSOs mission owners will be required to provide the following in their SNAP entry prior to receiving a DISA CPTC:

- ATO
- POA&Ms
- Specific applications of the CSO
- PPSM Tracking ID#
- Topology diagram with IP addresses
- CNDSP information
- BCA as applicable
- SLA as applicable
- Signed CTM as applicable

- POC information

For mission owners of non-DISA CSOs, the respective owning CSO must update SNAP; however, the DISA Connection Approval Office will not be providing a CPTC. The information in the SNAP update should be the same as above.

The technical onboarding of mission owners to an existing CAP will have to be coordinated with the respective CAP and CSO owners. In the case of the DISA CAP mission owners will need to coordinate with the CAP (NFG) PM Office at 301-225-8684 DSN 375.

3.1.3 Mission Owner Assistance

For issues with DISA CPTCs, please contact DISA's Connection Approval Office at 301-225-2900/2901 or DSN 312-375-2900/2901 or disa.meade.ns.mbx.ucao@mail.mil.

APPENDIX A: REFERENCES

a. DoD CIO Memorandum, *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services*, 15 December 2014

b. *DoD Cloud Computing Security Requirements Guide (SRG) Version 1, Release 1*, 12 January 2015

c. U.S. CIO, *Federal Risk Authorization and Management Program*, http://fedramp.gov

d. DoD Acquisition, Training, and Logistics (AT&L) Memorandum, *Class Deviation-Contracting for Cloud Services*, 9 February 2015

e. Department of Defense, DoDI 8500.01 *Cybersecurity*, 14 March 2014

f. Department of Defense, DoDI 8510.01 *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2014

g. Executive Order 12333, "*United States Intelligence Activities*," 4 December 1981, as amended

h. DoD CIO Memorandum, *Use of Enterprise Information Technology Standard Business Case Analysis*, 23 October 2014

i. Chairman of the Joint Chiefs of Staff, CJCSI 6211.02D *Defense Information Systems Network DISN Responsibilities*, 24 January 2012

j. Defense Information Systems Agency, *DISN Connection Process Guide*, http://www.disa.mil/network-services/enterprise-connections

k. Department of Defense, DoDI 8551.01, *Ports, Protocols, and Services Management (PPSM)*, 28 May 2014

l. Department of Defense, DoD O-8530.1-M DoD, *Computer Network Defense (CND) Service Provider Certification and Accreditation Process*, 17 December 2003

m. DISA Risk Management Office, *Cloud Access Point (CAP) Security Functional Requirements Document (FRD) V1.7*, 2April 2015 https://disa.deps.mil/disa/applications/ESPortal/EntResAna/RAO/Project%20Documents/Cloud%20Access%20Point%20(CAP)%20-%2033/CAP%20FRD%20draft%2004-10-2015%20v1.6.pdf

n. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev4, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 22 2015

o. FedRAMP Incident Response Requirements and Process Clarification Comment Disposition and FAQ, 27 Nov 2014 https://www.fedramp.gov/provide-public-comment/incident-response-requirements-and-process-verification/

p. United States Cyber Command Task Order 15-0005, *JFHQ-DODIN Application Access Control for DODIN*, 132137ZFEB15.

q. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *The NIST Definition of Cloud,* September 2011

r. Department of Defense, DoDD O-8530.1, *Computer Network Defense (CND),* 8 January 2001

s. Committee of National Security Systems Instruction (CNSSI) No. 4009, *National Information Assurance (IA) Glossary,* 26 April 2010.

t. DoD CIO, *Summary of DoD Sponsor Responsibilities for Mission Partner Connections to the Defense Information Systems Network (DISN),* Memorandum, 14 August 2012 http://disa.mil/network-services/DISN-Connection-Process/~/media/Files/DISA/Services/DISN-Connect/Policy/Memo_Summary_of_DOD_Sponsor_Responsibilities.pdf

u. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006

APPENDIX B: DISA CAP NFG CONNECTION PROCEDURES

Procedures under development

APPENDIX C: ACRONYMS

ACRONYMS	DEFINITION
AT&L	Acquisition, Technology, and Logistics
ATC	Authorization to Connect
ATO	Authorization to Operate
BCA	Business Case Analysis
BCAP	Boundary Cloud Access Point
CAO	Connection Approval Office
CAP	Cloud Access Point
CAP	Connection Approval Process
CATC	Cloud Authorization to Connect
CCPG	Cloud Connection Process Guide
CCSD	Command Communications Service Designator
CIO	Chief Information Officer
CNDSP	Computer Network Defense Service Provider
CPG	Connection Process Guide
CPTC	Cloud Permission to Connect
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CTM	Consent to Monitor
DCC	DISA Command Center
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMZ	De-Militarized Zone
DODIN	Department of Defense Information Network
DSAWG	Defense Information Assurance/Security Accreditation Working Group
DWP	DoDIN Waiver Panel
FedRAMP	Federal Risk and Authorization Management Program
GIAP	GIG Interconnection Approval Process
GIG	Global Information Grid
IAP	Internet Access Point
IATC	Interim Authorization to Connect

ICAP	Internal Cloud Access Point
ICATC	Interim Cloud Authorization to Connect
ISRMC	Information Security Risk Management Committee
IT	Information Technology
JRSS	Joint Regional Security Stack
MCND	Mission Computer Network Defense
NFG	NIPRNet Federated Gateway
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
SSP	System Security Plan

APPENDIX E: DEFINITIONS

TERMS	DEFINITION
Accreditation Decision	A formal statement by a designated accrediting authority (DAA) or 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 ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO). The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DOD public key infrastructure (PKI)-certified digital signature.
Approval to Connect (ATC)	A formal statement by the DISA Connection Approval Office granting approval for an enclave to connect to the DISN. The ATC cannot be granted for longer than the period of validity of the associated ATO. An ATC will be granted for a maximum of three years.
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 Termination Date (ATD)	The date assigned by the DAA/AO that indicates when an ATO, IATO, or IATT expires.
Authorization to Operate (ATO)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (CNSS 4009)
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. (CNSS 4009) This term is synonymous with designated approving authority and delegated accrediting authority.
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.
Certification	A certifying Authority's (CA's) determination of the degree to which

Determination	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.
Cloud Access Point	A DoD Cloud Access Point (CAP) is a system of network boundary protection and monitoring devices, otherwise known as an IA stack, through which CSP infrastructure will connect to a DoD Information Network (DoDIN) service; NIPRNet, or Secret Internet Protocol Router Network (SIPRNet).
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 (q))
Cloud Connection to Connect (CATC)	A formal statement by the DISA Connection Approval Office granting approval for a Cloud Service Provider (CSP) to connect to the DISN. The CATC cannot be granted for longer than the period of validity of the associated Provisional Authorization (PA). A CATC will be granted for a maximum of three years.
Cloud Denial To Connect (CDTC)	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 the DISA DISN Cloud Access Point (CAP) based on the Mission Owner's Authorization to Operate (ATO). A CPTC will be granted for a maximum of three years.
Cloud Service Offering (CSO)	A Cloud Service Offering (CSO) is the actual IaaS/PaaS/SaaS solution available from a CSP. A CSP may provide several different CSOs.
Cloud Service Provider (CSP)	Any or all DoD or non-DoD entities that offers one or more cloud services in one or more deployment models. A CSP might leverage or outsource services of other organizations and other CSPs (e.g., placing certain servers or equipment in third party facilities such as data centers, carrier hotels / 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. • Commercial vendor or Federal organization offering or providing cloud services (Includes DoD CSPs)

	• Provides CSOs for mission use • Provides CNDSP services (all tiers) for their infrastructure and service offerings [DoD Cloud Computing SRG]
Command Communications Service Designator (CCSD)	A unique identifier for each single service including use circuits, package system circuits, and inter-switch trunk circuits.
Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. (NIST SP 800-145 ref (q))
Computer Network Defense (CND)	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks.
Computer Network Defense Service Provider (CNDSP)	A DoD service required by policy provided or subscribed to by owners of DoD information systems or computer network in order to maintain and Provide CND situational awareness; implement CND protect measures; monitor and analyze in order to detect unauthorized activity; and implement CND operations. (DoDD O 8530.1 ref (r)) Provides Computer Network Defense (CND) and Command and Control (C2) direction addressing the protection of the network, detection of threats, and response to incidents. (DoD Cloud Computing SRG)
Connection Approval Office (CAO)	Single point of contact within DISA for DISN connection approval requests.
Connection Approval Process	Formal process for adjudication requests to interconnect information systems.
Connection Approval Process (CAP)	Packages provide the CAO the information necessary to make the connection approval decision.
Consent to Monitor (CTM)	This is the agreement signed by the DAA granting DISA permission to periodically monitor the connection and assess the level of compliance with 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.
Defense IA/Security Accreditation Working Group (DSAWG)	Provides, interprets, and approves DISN security policy, guides architecture development, and recommends accreditation decisions to the DoD ISRMC. 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.
Defense Information Systems Agency (DISA) Direct Order Entry (DDOE)	This is the ordering tool for DISN telecommunications services.
Defense Information System Network Connection Process Guide (DISN CPG)	Step-by-step guide to the detailed procedures that Partners must follow in order to obtain and retain connections to the DISN.
Defense Information Systems Network (DISN)	DOD integrated network, centrally managed and configured to provide long-haul information transfer for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery and video teleconferencing services.
Demilitarized Zone (DMZ)	Physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
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 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 (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)
Designated Accrediting Authority (DAA)/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. (CNSS 4009 ref (s)) This term is synonymous with designated approving authority and delegated accrediting authority.
DOD Information	Set of information resources organized for the collection, storage,

System (IS)	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.
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.
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 (q))
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.
Information System (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.
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.
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (NIST SP 800-145 ref (q))
Interim Approval to Connect (IATC)	Temporary approval granted by the Connection Approval Office for the connection of an IS to the DISN under the conditions or constraints enumerated in the connection approval.
Interim Authorization to Operate (IATO)	Temporary authorization granted by the DAA to operate a DOD information system under the conditions or constraints enumerated in the accreditation decision. (ref f)
Interim Authorization to Test (IATT)	A temporary authorization to test a DOD IS in a specified operational information environment or with live data for a specified time period within the timeframe and under the conditions or constraints enumerated in the accreditation decision. (ref f)
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.
Mission Owner	Mission Owners are entities such as program managers within the DoD Components responsible for instantiating information systems and applications leveraging a CSP's Cloud Service Offering. • DoD entity that acquires cloud services in support of its mission • Performs assessment to issue ATO for their mission systems/applications • Ensures Tier 2 Mission Computer Network Defense (MCND) Service Provider is identified and funded • Serves as CND Tier 3 for their mission systems/applications • Ensures CSP requirements for CND and other SRG requirements are included in any cloud contracts.
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.
Non-DOD Partner	All organizations and entities that are not components of the Department of Defense; this includes contractors and federally funded research and development centers; other USG federal departments and agencies; state, local, and tribal governments; foreign government organizations/ entities (e.g., allies or coalition partners); non-government organizations; commercial companies and industry; academia (e.g., universities, colleges, or research and development centers); etc.
Plan of Action & Milestones (POA&M)	A permanent record that identifies tasks to be accomplished in order to resolve security weaknesses; required for any accreditation decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks; also used to document DAA-accepted non-compliant 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 as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (NIST SP 800-145)

Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (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 or off premises. (NIST SP 800-145 ref (q))
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.
Provisional Authorization (DoD)	A DoD Provisional Authorization 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 Computing SRG]
Public Cloud	The cloud infrastructure is provisioned for open use by the general 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 (q))
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.
Security Assessment Plan (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)	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]
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (NIST SP 800-145 ref (q))
Sponsor (DoD)	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 t)

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 ref (u)]
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.
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).

Appendix F: SNAP Information

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

- The detailed instructions for requesting a SNAP account can be accessed by completing the following steps:
  - Go to https://snap.dod.mil for SNAP
  - Scroll to the bottom of the "Home Page"
  - Select the "User Guide" link
  - Select "Accounts Management Guide"
- Once the account is approved, proceed with the creation/registration of the CSO in the Cloud module. The SNAP module, which is still being refined,[18] requires the sponsor to ensure specific items are uploaded and completed. These items include:
  - Evidence of FedRAMP documentation
  - Signed DoD PA
  - Specific CSO applications
  - PPSM Tracking ID# (as applicable)
  - Topology diagram with Internet Protocol (IP) addresses

[18] SNAP Cloud Module Increment 1 was released in March and additional SNAP Cloud module incremental releases are planned and ongoing as SNAP module requirements continued to be developed, determined, and approved.

- Signed Component CIO approved BCA
- CNDSP information
- Consent To Monitor (CTM) as applicable
- POCs information

- The specific steps to complete a SNAP registration are available in the SNAP Cloud Module User Guide. Below are the instructions for accessing the SNAP Cloud Module User Guide:
  - Go to https://snap.dod.mil for SNAP
  - Log into SNAP
  - Scroll to the bottom of the “Home Page”
  - Select the “Reference Documents” link
  - Select “Cloud”
  - Select “SNAP Cloud User Reference”

Appendix G: Onboarding

Appendix H:

Appendix I: DISA CAP Connections

Appendix J: Component CAPS

Instructions for connecting to component CAPs will be described in a future version of this document.

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