DoD Cloud Authorization Process

DISA Cloud Assessment Division (RE2)
DISA Risk Management Directorate
June 2024

FedRAMP and DoD Authorization Processes

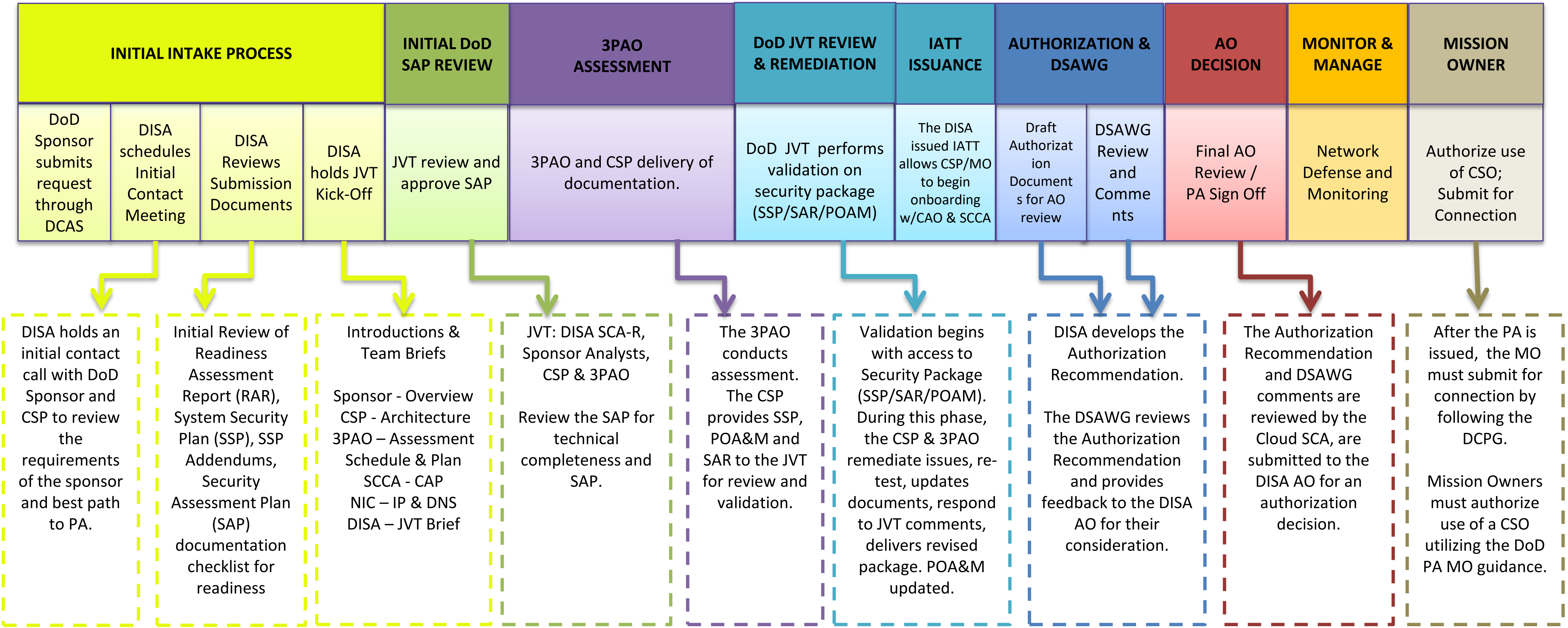
FedRAMP

- The Cloud Service Providers (CSPs) may obtain a FedRAMP Authorization for their Cloud Service Offering (CSO) through the FedRAMP Agency process.

DoD

- The authorization process for commercial and non-DoD CSPs is based on FISMA and NIST RMF processes leveraging FedRAMP, supplemented with DoD considerations.
- DISA validates CSOs and 3PAO results for consideration with issuing a DoD PA.
- There are two paths to obtaining a DoD PA:
  1. Uplift/Leverage FedRAMP Agency ATO
  2. 3PAO Assessed + DISA validation + 10 General Readiness Requirements outlined in the Cloud Computing SRG

DoD Provisional Authorization Process



INITIAL INTAKE PROCESS

DoD Sponsor submits request through DCAS

DISA schedules Initial Contact Meeting

DISA holds an initial contact call with DoD Sponsor and CSP to review the requirements of the sponsor and best path to PA.

DISA Reviews Submission Documents

Initial Review of Readiness Assessment Report (RAR), System Security Plan (SSP), SSP Addendums, Security Assessment Plan (SAP) documentation checklist for readiness

DISA holds JVT Kick-Off

Introductions & Team Briefs

Sponsor - Overview
CSP - Architecture
3PAO – Assessment Schedule & Plan
SCCA - CAP
NIC – IP & DNS
DISA – JVT Brief

INITIAL DoD SAP REVIEW

JVT review and approve SAP

JVT: DISA SCA-R, Sponsor Analysts, CSP & 3PAO

Review the SAP for technical completeness and SAP.

3PAO ASSESSMENT

3PAO and CSP delivery of documentation.

The 3PAO conducts assessment. The CSP provides SSP, POA&M and SAR to the JVT for review and validation.

DoD JVT REVIEW & REMEDIATION

DoD JVT performs validation on security package (SSP/SAR/POAM)

Validation begins with access to Security Package (SSP/SAR/POAM). During this phase, the CSP & 3PAO remediate issues, re-test, updates documents, respond to JVT comments, delivers revised package. POA&M updated.

IATT ISSUANCE

The DISA issued IATT allows CSP/MO to begin onboarding w/CAO & SCCA

AUTHORIZATION & DSAWG

Draft Authorization Documents for AO review

DSAWG Review and Comments

DISA develops the Authorization Recommendation.

The DSAWG reviews the Authorization Recommendation and provides feedback to the DISA AO for their consideration.

AO DECISION

Final AO Review / PA Sign Off

The Authorization Recommendation and DSAWG comments are reviewed by the Cloud SCA, are submitted to the DISA AO for an authorization decision.

MONITOR & MANAGE

Network Defense and Monitoring

MISSION OWNER

Authorize use of CSO; Submit for Connection

After the PA is issued, the MO must submit for connection by following the DCPG.

Mission Owners must authorize use of a CSO utilizing the DoD PA MO guidance.

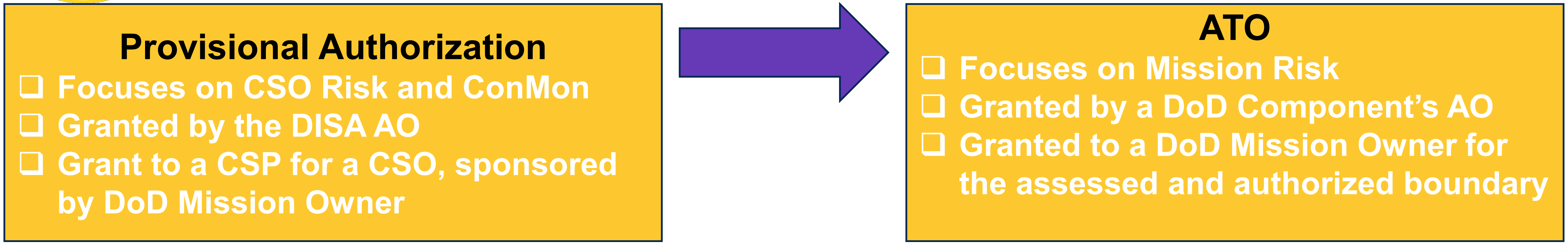
Provisional Authorization Memo

- **Initial DoD Provisional Authorization (PA)**
  - The DoD Provisional Authorization (PA) is issued by the DISA Authorizing Official (AO) for a CSO based on FedRAMP and additional DoD security requirements (Impact Levels 4/5/6).
  - A DoD PA is issued with an expiration date to be leveraged by DoD Mission Owners (MO) until it is revoked or expires.
  - The PA is issued with general and/or specific conditions for the CSO and usage considerations for the DoD MO.

- **Ongoing Provisional Authorization Process**
  - The CSPs must comply with all Continuous Monitoring (ConMon) requirements to maintain the DoD PA, i.e., 30-90-180-day vulnerability resolution/mitigation requirements and annual assessments.

- **Reauthorization**
  - Before the PA expires, if there is an ongoing need within the DoD community and the CSP has upheld a satisfactory security posture, a CSO can be reauthorized. An updated PA memo will be issued by the DISA AO.

The PA and the ATO



Provisional Authorization

- □ Focuses on CSO Risk and ConMon
- □ Granted by the DISA AO
- □ Grant to a CSP for a CSO, sponsored by DoD Mission Owner

ATO

- □ Focuses on Mission Risk
- □ Granted by a DoD Component's AO
- □ Granted to a DoD Mission Owner for the assessed and authorized boundary

- A DoD PA is primarily issued and or leveraged for enterprise/Mission Owner use
  - When possible, DoD typically leverages a CSO's FedRAMP JAB P-ATO or Federal Agency's ATO
  - The CSO's security authorization package is assessed by a 3PAO and is validated by Security Control Assessors from DISA and reviewers from the DoD Component sponsoring the CSO.
  - Monthly ConMon and Annual Assessments are performed on each CSO that is issued a DoD PA.
  - Security controls can be leveraged from eMASS.
- The DoD Component ATO
  - ATO is issued by a DoD Component AO to a MO for its system/data that makes use of the CSO
  - IAW the CC SRG, DoD MO must leverage a CSO's DoD PA

DoD Mission Owner Sponsorship Requirements

- All the required documentation listed below must be submitted to DISA Cloud Team (RE2) via the Cloud eMASS instance. Once the documentation is uploaded to eMASS and reviewed by the DISA RE2, the CSO will be scheduled for a Kick-Off meeting.

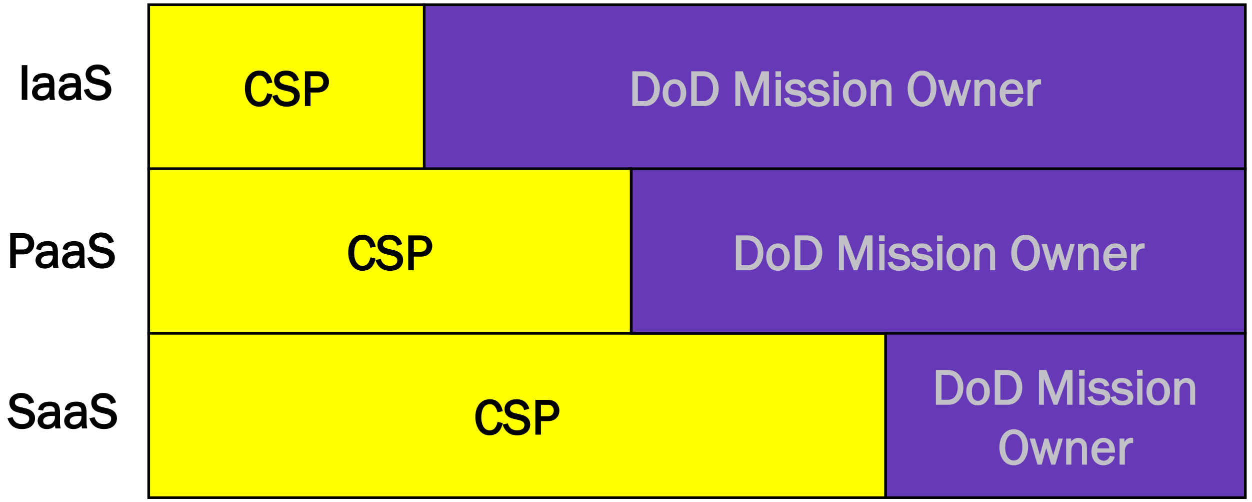
  - Readiness Assessment Report (RAR) or FedRAMP baseline documentation
  - System Security Plan (SSP)
  - Security Assessment Plan (SAP)
  - DoD SSP Addendum
  - CSO Architecture Brief

Mission Owner AO Responsibility

- **Maximize the reuse of existing body of evidence by leveraging existing security package**
  - Determine if scope of testing is adequate for the authorization boundary.
  - Review test results from 3PAO's Security Assessment Report (SAR).
  - Review residual risk by reviewing POA&Ms, continuous monitoring data, DISA's Authorization Recommendation and PA memos.
  - Identify and proceed with any additional testing required (with CSP and 3PAO).

- **If risk is acceptable to the Mission Owner AO, issue an IATT or ATO**
  - Accept risk and liabilities identified in the DoD PA for the Mission Owner's unique system and mission.
  - Impose any conditions/restrictions deemed necessary for the secure operation of the CSO in the context of the Mission Owner system requirements, interconnections, and processed data.

Mission Owner AO Risk Decision – Security Responsibility



IaaS: CSP | DoD Mission Owner

PaaS: CSP | DoD Mission Owner

SaaS: CSP | DoD Mission Owner

Reuse of Authorized CSO Packages

- The DoD authorization process promotes reuse of security authorization packages from FedRAMP and Federal agency authorizations.
- This allows the CSO to go through the authorization process once, and after achieving authorization, the security package can be reused.
- The FedRAMP Marketplace provides a list of cloud services authorized by both the JAB and Agencies under FedRAMP.
- The DoD Cloud Authorization Services (DCAS) and the DISA Storefront websites provide a list of authorized cloud services with DoD PAs.
- The DoD Cloud Computing (CC) Security Requirements Guide (SRG) provides DoD-specific guidance and requirements for using cloud-based solutions.

JVT Resources

- The CSP’s DoD sponsor must provide 2 or more additional resources to participate in the review of the CSP’s security authorization package.

- The DISA Cloud Assessment Team will provide a Joint Validation Team (JVT) Lead to function as overall manager of the DoD JVT process.

- The sponsor’s support analysts should be deeply familiar with RMF. If the resources have limited or no RMF experience, this will prolong the review process.

- The CSP and their 3PAO will be expected to collaborate and provide input to information exchange meetings and work with the JVT to establish the schedule and timeline to completion.

JVT Responsibilities

Lead Responsibilities (DISA)

- Performs initial review to verify readiness prior to kickoff.
- Develops a review schedule.
- Prepares a consolidated team review comment spreadsheet for each of the primary cloud security documents under review.
- Tasks individual team members, tracks items, and collects responses per document.
- Schedules weekly meetings with JVT and biweekly meetings for all stakeholders to share progress.
- Sends comments to CSP/3PAO for adjudication and resolution.
- Liaises with CSP/3PAO for all matters related to validation of requirements for DoD PA.
- Prepares authorization documents.

JVT Members (Sponsor Analysts)

- Review all documents included in the CSP's security authorization package.
- Review documents for completeness and structural thoroughness.
- Assess/validate compliance of implemented controls.
- Ensure compelling evidence maps to applicable security controls.
- Review system architecture for in-depth understanding of authorization boundary.
- Review architecture for data flows, trusted connections, remote access activities.
- Provide comments to JVT lead on provided comment sheet.
- Review response comments from CSP and 3PAO for adjudication.
- Meet weekly or as needed with JVT Lead and 3PAO/CSP to adjudicate comments.
- Provide input to stakeholders briefing slides.

Cloud eMASS

- Cloud eMASS site: https://cloud.emass.apps.mil/.
- It can be accessed by CSPs and their designated 3PAO POC.
  - Medium Token Assurance Certificate or a Medium Hardware Assurance Certificate is required. More information on certificates and the External Certification Authority (ECA) is located at https://public.cyber.mil/eca/.
- The CSP is responsible for updating their eMASS package for their CSO that provides inheritance to DoD MOs eMASS packages. The Cloud eMASS packages are managed and validated by the DISA Cloud Team.
- The use of the Cloud eMASS instance provides a consolidated location for the evidence and test results for CSOs that have a provisional authorization.
- All Cloud eMASS questions should be directed to the DISA Cloud eMASS Team at disa.meade.re.mbx.disa-cloud-emass-team@mail.mil

Cloud eMASS Artifacts

- Documentation submitted to DISA RE2 via the Cloud eMASS instance:
  - Readiness Assessment Report (RAR)
  - System Security Plan (SSP)
  - Security Assessment Plan (SAP)
  - Security Assessment Report (SAR)
  - DoD SSP Addendum
  - CSO Architecture/Data Flow Diagrams
  - Monthly Vulnerability Scans (ConMon Reporting)
  - Plan of Actions and Milestones (POA&M)
  - Authorization Recommendation
  - DoD PA
  - Other Artifacts
- Please note that uploading an artifact to eMASS does not make it available for inheriting, it must be attached to a control.
- **The MO can request any of the BOE (FedRAMP or DoD) from the DISA Cloud Team at disa.meade.re.mbx.cloud-team@mail.mil.**

Additional Considerations and/or Requirements for IL4/IL5

- Connection to a DoD approved Boundary Cloud Access Point (BCAP)
- DoD PKI authentication by DoD privileged and non-privileged users
- Connection to a DoD approved DNS and CSSP services
- DoD IP addressing
- CSO management plane (and/or specific devices/systems) and its integration with the CSP’s corporate network or the general commercial CSO management plane
- CSP personnel managing and/or monitoring the CSO infrastructure
- Reliance on Internet access to reach the CSO management/service-ordering portal or API endpoints from either NIPRNet or from within the CSO.
- The robustness of the CSP’s required boundary protection (defense-in-depth security / protective measures) implemented between the Internet and the CSO for its protection from Internet based threats.
- All other requirements as defined in the CC SRG and other considerations as realized while assessing the CSO or as a result of lessons learned.

Cloud Connection Process – SCCA Team

- The DoD Authorization (IATT or DoD PA) is issued by the DISA AO.
- Every Mission Owner must register their instantiation of the CSO in the SNAP database (https://snap.dod.mil/index.do).
- Cloud Approval to Connect (CATC) is issued by the DISA Connection Approval Office (CAO).
- The DISA SCCA PMO will only activate the CSO BCAP connection when a DoD Mission Owner receives a Cloud Permission to Connect (CPTC) to connect a Cloud IT Project (C-ITP) to the CSO from the CAO.
- IL4/5 CSOs must obtain, sustain, and fund a connection between CSP enclave hosting the CSO and the DISA BCAPs to be used.
  - DISA BCAPs: Equinix facilities in Ashburn, VA; San Jose, CA; Dallas, TX; and Chicago, IL.
- The DoD Mission Owner will contact the SCCA PMO (disa.meade.se.mbx.disa-scca-pmo@mail.mil) when the CATC and CPTC are achieved to initiate BCAP connections.

Cloud Resources

- DoD Cloud Authorization Process
  - https://dod365.sharepoint-mil.us/sites/DISA-RE-Apps/cas
  - CAC-enabled site
  - Sponsorship Request Form, Authorization Process, Services Catalog, etc.
- DoD Cyber Exchange
  - https://public.cyber.mil/
  - Public Content
  - Cloud Computing SRG, Templates, Other documents related to cloud
- DISA Website
  - https://storefront.disa.mil/kinetic/disa/service-catalog#/category/cloud-computing
- Contact Us
  - disa.meade.re.mbx.cloud-team@mail.mil
  - disa.meade.re.mbx.disa-cloud-emass-team@mail.mil

Terms and Abbreviations

Terminology	Acronym	Definition
Cloud Service Provider	CSP	An organization, commercial or private, that offers/provides Cloud Services.
Cloud Service Offering	CSO	Refers to a CSP's product or service offering. The actual IaaS/PaaS/SaaS solution that is available from a CSP.
Mission Owner	MO	A DoD cloud consumer.
Provisional Authorization	PA	A pre-acquisition type of Risk Management Framework Information System authorization used by DoD and FedRAMP to pre-qualify Commercial CSOs to host Federal Government and/or DoD information and information systems.

Questions?

DEFENSE INFORMATION SYSTEMS AGENCY

DISA: The premier IT and telecommunications provider for the US military

/DISA @USDISA /USDISA DISA.mil