DoD Cloud Authorization Process

DISA Cloud Assessment Division

DISA RME/RE2

August 2021
The DISA Cloud Assessment Division provides support to DoD Component Sponsors/Mission Owners through the pre-screening, assessment, validation, authorization, and continuous monitoring of Cloud Service Offerings (CSO).

They ensure the Cloud Service Provider (CSP) and CSO meet DoD cloud security requirements for a DoD Provisional Authorization (PA).

They serve as technical reviewers on the FedRAMP Joint Authorization Board (JAB).
What You Must Know

- FedRAMP authorization processes
- DoD cloud authorization process
- Shared responsibility model
- Cloud security requirements exist for CSPs and DoD mission owners.
- The DoD provisional authorization is not the Authorization to Operate (ATO).
- The connection approval process for the mission owner and the CSP occurs after the PA is issued.
- Continuous monitoring requirements must be performed before and after authorization based on FedRAMP and DoD requirements.
The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security authorizations for Cloud Service Offerings in accordance with FISMA and OMB Circular A-130.

Two authorization paths for the CSO:
- Joint Authorization Board (JAB)
- Individual agency

Visit the FedRAMP.gov detailed information and requirements.
The authorization process for commercial and non-DoD CSPs is based on FISMA and NIST RMF processes through the use of FedRAMP, supplemented with DoD considerations.

DISA assesses CSP’s service offerings and 3PAO results for consideration in issuing a DoD PA.

The DISA AO is responsible for approving and revoking DoD PAs.

There are three paths to obtaining a DoD PA:

1. Leverage FedRAMP JAB PATO
2. Leverage FedRAMP Agency ATO
3. DoD Component Assessed

Review the CC SRG for detailed information about the authorization process.
The Cloud Computing (CC) Security Requirements Guide (SRG) outlines the security model and requirements by which DoD will leverage cloud computing.

The minimum baseline for a DOD PA is the FedRAMP Moderate Baseline.

Download the CC SRG from the DoD Cyber Exchange at https://public.cyber.mil/dccs/dccs-documents/.
Leveraging FedRAMP Authorized Services

- FedRAMP Plus 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.
- For IL2, there are no additional security controls required for a DoD PA.
- For IL4/IL5, DISA leverages the FedRAMP authorization and assesses the additional controls and requirements.
- The DISA AO issued a reciprocity memo for IL2 CSOs.
  - Using the IL2 reciprocity memo a DoD component may leverage any CSO assessed, authorized, and listed in the FedRAMP marketplace at a minimum of the FedRAMP Moderate Baseline.
- Download the IL2 Reciprocity memo from https://disa.deps.mil/org/RMED/cas/SitePages/CSOCatalog.aspx
Reuse of Authorized CSP Packages

- Both the FedRAMP and DoD authorization processes promote reuse of security authorization packages.
- A CSP goes through the authorization process once, and after achieving authorization for a CSO, the security package can be reused.
- The FedRAMP Marketplace has a list of FedRAMP authorized cloud services – JAB and Agency.
- The DoD Cloud Authorization Services (DCAS) site has a list of cloud services with DoD PAs.
- Review the DoD CC SRG for DoD-specific guidance.
System/Data Categorization

• DoD Mission Owners must categorize mission information systems in accordance with DoDI 8510.01 and CNSSI 1253.
• Mission owners must identify the cloud information impact level that most closely aligns with the defined categorization and information sensitivity.
• Information types and requirements for each impact level are outlined in the CC SRG.
### Summary Requirements per Information Impact Level

<table>
<thead>
<tr>
<th>IMPACT LEVEL</th>
<th>INFORMATION SENSITIVITY</th>
<th>SECURITY CONTROLS</th>
<th>LOCATION</th>
<th>OFF-PREMISES CONNECTIVITY</th>
<th>SEPARATION</th>
<th>PERSONNEL REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>PUBLIC or Non-critical Mission Information</td>
<td>FedRAMP v2 Moderate</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>Internet</td>
<td>Virtual / Logical PUBLIC COMMUNITY</td>
<td>National Agency Check and Inquiries (NACI)</td>
</tr>
<tr>
<td>6</td>
<td>Classified SECRET National Security Systems</td>
<td>Level 5 + Classified Overlay</td>
<td>US / US outlying areas or DoD on-premises</td>
<td>SIPRNet DIRECT With DoD SIPRNet Enclave Connection Approval</td>
<td>Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems &amp; Information</td>
<td>US Citizens w/ Favorably Adjudicated SSBI &amp; SECRET Clearance NDA</td>
</tr>
</tbody>
</table>
FedRAMP/FedRAMP+ Security Control Requirements

FedRAMP Moderate Baseline 325

FedRAMP High Baseline 421

DoD Impact Level 4 Baseline 325+38

DoD Impact Level 5 Baseline 325+38+9

325 Controls/Control Enhancements (C/CE)

FedRAMP MBL + 96 additional C/CE = 421 HBL C/CE

FedRAMP MBL + 38 FedRAMP+ C/CE = 363 IL4 C/CE + DoD General Readiness & DoD Unique Requirements

IL4 + 9 FedRAMP+ C/CE = 372 IL5 C/CE / + DoD General Readiness & DoD Unique Requirements

Note: Controls are cumulative and may vary based on parameter values for moderate v. high baselines (approx. 137-143), mission requirements, and additional requirements. See section 5.1.7 of CC SRG V1R3.
DoD Component Sponsorship for DoD PA

• The DoD Component sponsoring the CSP must:
  • Be committed to use
  • Align with a CSSP
  • Provide a minimum of two qualified support analysts to complete review of the CSP's security authorization package.
  • Understand and be capable of responsibility for the customer’s portion of controls under the shared responsibility model for cloud use.
• One DISA SCA-R and the DoD Component-sponsored support analysts make up the Joint Validation Team (JVT).
• A mission owner leveraging the DoD PA is responsible for mission owner requirements and responsibilities, including continuous monitoring.
Prioritization for Security Assessment

- Top Priority: CSPs with a DoD sponsor that supports a high priority DoD mission as recognized by a DoD Chief Information Officer or J6 General Officer. In the event multiple CSPs fall into this category, resolution of priorities will be determined by a designated SecDef or JCS senior.
- CSP renewing an expiring Provisional Authorization that currently hosts DoD IT Projects.
- CSP with a DoD sponsor with these prerequisites:
  1) CSP has completed the FedRAMP authorization process;
  2) CSP has an existing contract;
  3) CSP rates high on readiness checklist;
  4) CSP Sponsor has reviewers to help with the analysis of the 3PAO's assessment products.
- CSP with DoD sponsor currently operating in a DoD private cloud scenario and has a second DoD sponsor seeking its services.
- CSP with a DoD sponsor not meeting the above conditions.
- Least Priority: CSPs without a DoD sponsor but have a capability aligned to a recognized DoD interest.
Uplift from a JAB P-ATO

- A FedRAMP JAB P-ATO is issued by the JAB to a CSP for a CSO.
- The CSP’s security authorization package is reviewed by JAB Reviewers from three agencies (DoD, DHS, GSA).
- This is the DoD preferred path to a DoD PA because the DoD CIO and the DISA Cloud Security Control Assessor (SCA) team are involved in FedRAMP JAB assessment and authorization activities.
- The CSP and 3PAO submit documentation (SSP/SAP/SAR/POAM, etc.) to DISA for review and validation by the JVT.
- For IL4/IL5, DoD leverages the documentation and artifacts produced for the JAB P-ATO in addition to documentation developed for any additional DoD requirements not addressed by FedRAMP.
Uplift from an Agency ATO

- An Agency Authorization to Operate (ATO) is issued by a Federal Agency Authorizing Official (AO) to a CSP for a CSO based on compliance with FedRAMP requirements.
- A Federal Agency ATO listed in the FedRAMP Marketplace can be leveraged for a DoD PA.
- For IL4/IL5, DoD will leverage the Federal Agency ATO authorized baseline, to include all relevant continuous monitoring documentation, in addition to documentation developed for any additional DoD requirements not addressed through the FedRAMP authorization process.
- A FedRAMP-approved 3PAO must perform any required additional assessment.
- The CSP and 3PAO submit documentation (SSP/SAP/SAR/POAM, etc.) to the DISA Cloud SCA for review and validation toward issuing a DoD PA.
- The DISA Cloud SCA will request all baseline documentation and applicable continuous monitoring artifacts.
DoD Assessed PA

- Without a FedRAMP JAB P-ATO or Agency ATO, a DoD Component assessment of a CSP’s CSO may only be performed under two circumstances:
  - If a DoD organization has a validated mission requirement that only the specific CSP’s CSO can fulfill requiring it to be authorized.
  - If a DoD organization acting as a CSP develops and instantiates a CSO.
- The CSP’s CSO is fully assessed by a FedRAMP-approved 3PAO against a FedRAMP Moderate or High Baseline and DoD’s FedRAMP+ requirements.
- The DoD sponsoring organization must provide personnel for the full assessment and validation in coordination with the DISA Cloud SCA organization.
- It may take five to eight to complete assessment and validation.
- The CSP/3PAO submits assessment documentation (RAR/SSP/SAP/SAR/POAM, etc.) to the DISA Cloud SCA.
- The CSP’s assessment package may be shared with FedRAMP and be available through the FedRAMP secure repository if needed to be leveraged by other Federal Agencies.
The PA and the ATO

- **DoD Provisional Authorization (PA)** is issued by the DISA Authorizing Official (AO) to a CSP for a CSO based on FedRAMP and additional DoD security requirements (Impact Levels 4/5/6)
  - A DoD PA is primarily issued for enterprise use
    - Typically leverages a CSP’s JAB P-ATO or Federal Agency ATO
    - A reciprocity memo was issued at Impact Level 2 for CSOs on the FedRAMP Marketplace
    - The CSP’s security authorization package is reviewed by reviewers from DISA and the DoD Component sponsoring the CSP
  - **DoD Component ATO**
    - Issued by a DoD Component AO to a Mission Owner for its system/data that makes use of the CSP’s CSO
    - Must leverage a CSP’s DoD PA
    - IL2 requests where IL2 reciprocity memo is not leveraged must apply FedRAMP Agency Authorization Process directly with FedRAMP PMO.

---

Provisional Authorization
- Focuses on CSO Risk
- Granted by the FedRAMP JAB and/or the DISA AO
- To a CSP for a CSO

ATO
- Focuses on Mission Risk
- Granted by a DoD Component’s AO
- To a DoD Mission Owner for a system
Mission Owner AO Responsibility

- Inherit/Leverage – Maximize use of existing body of evidence
  - Scope of testing adequate? If so, review the 3PAO’s Security Assessment Plan (SAP)
  - Review test results: 3PAO’s Security Assessment Report (SAR)
  - Residual risk: Review POA&Ms, continuous monitoring data, DISA’s Authorization Recommendation and Provisional Authorization memos
  - Identify and proceed with any additional testing required (with CSP and 3PAO)
- If risk is acceptable, 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 deemed necessary for the secure operation of the CSO in the context of the Mission Owner system requirements, interconnections, and data processed
  - Issue ATO to a Mission Owner for a system that makes use of the CSP’s CSO
Mission Owner AO Risk Decision

Security Responsibility

Authorized by:
- FedRAMP JAB
- DISA AO

JAB P-ATO

+ DoD PA

Reuse: Maximize use of existing bodies of evidence (e.g. scope, testing, results, residual risk)

Authorized by:
- Mission Owner AO

IaaS
- CSP
- DoD Mission Owner

PaaS
- CSP
- DoD Mission Owner

SaaS
- CSP
- DoD Mission Owner

DoD Mission Owner

Authorized by:
- FedRAMP JAB
- DISA AO

Authorized by:
- Mission Owner AO
DoD Provisional Authorization Process Timeline

**INITIAL CONTACT PHASE**
- DoD Sponsor submits ICF to DCAS
- DISA schedules initial planning conference call
- DISA holds process & requirements strategy meeting
- DISA SCA-R, JVT and CSP review and approve SAP

**KICKOFF**
- Introductions & Team Briefs
  - Sponsor - Overview
  - CSP - Architecture
  - 3PAO - Assessment
  - SCCA - CAP
  - NIC - IP & DNS
  - DISA - JVT Brief
  - Assigns priority and notional schedule.

**JVT**
- JVT: DISA SCA-R, Sponsor Analysts, CSP & 3PAO
- Access to CSP document repository initiated.
- Initial Review of RAR, SSP, SSP Addendums, & documentation checklist for Readiness.
- Review and approve SAP.

**3PAO ASSESSMENT**
- 3PAO conducts assessment.
- CSP provides SSP & POA&M; 3PAO provides SAR. Time varies depending on FedRAMP baseline.

**DoD JVT Review & Remediation**
- 8-10 weeks
  - DoD JVT performs validation on security package (SSP/SAR/POAM)

**AUTHORIZATION & DSAWG PREP**
- 1-3 weeks
  - Draft Authorization Recommendation and DSAWG Brief. Submit to DSAWG

**DSAWG REVIEW**
- 1-2 weeks
  - DSAWG Review and Comments

**AO DECISION**
- 1-2 weeks
  - Final AO Review / PA Sign Off
  - Network Defense and Monitoring

**MONITOR & MANAGE**
- 3PAO conducts assessment.
- CSP provides SSP & POA&M; 3PAO provides SAR. Time varies depending on FedRAMP baseline.

**MISSION OWNER**
- Authorization Recommendation submitted to DSAWG for comments then to DISA AO for authorization decision
- Mission Owners must authorize use of a CSO utilizing the DoD PA MO guidance. After authorization is issued, submit for connection.

**Estimated duration (per CSP) is 11 – 17 weeks (not including time for 3PAO Assessment)**

---

Trust in DISA: Mission First, People Always!
<table>
<thead>
<tr>
<th>Deliverable / Task</th>
<th>Submission Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed and signed sponsor request form</td>
<td>Within two weeks of initiating the form</td>
</tr>
<tr>
<td>Readiness Assessment Report (RAR) or FedRAMP baseline</td>
<td>Within two weeks of DoD Sponsor submitting request</td>
</tr>
<tr>
<td>baseline documentation, as applicable</td>
<td></td>
</tr>
<tr>
<td>Initial Planning Meeting</td>
<td>Within two weeks of sponsor submitting the request</td>
</tr>
<tr>
<td>CSO Architecture Briefing</td>
<td>Within two weeks of Initial Planning Meeting</td>
</tr>
<tr>
<td>DoD SSP Addendum, ILx</td>
<td>Within two weeks of Initial Planning Meeting</td>
</tr>
<tr>
<td>Security Assessment Plan (SAP)</td>
<td>Within two weeks of Kickoff Meeting</td>
</tr>
<tr>
<td>Complete Security Authorization Package –</td>
<td>As soon as final SAR is signed</td>
</tr>
<tr>
<td>• CSP submits SSP, DoD SSP Addendum &amp; POA&amp;M in eMASS</td>
<td></td>
</tr>
<tr>
<td>• 3PAO submits SAP &amp; SAR in eMASS</td>
<td></td>
</tr>
</tbody>
</table>
Provisional Authorization Memo

- **Initial DoD Provisional Authorization (PA)**
  - The DISA AO is the Authorizing Official (AO) for a DoD PA.
  - Typically, a DoD PA is issued with an expiration date to be leveraged by DoD Mission Owners until it expires or is revoked.
  - The PA is issued with general and/or specific conditions for the CSP and usage considerations for the DoD Mission Owner.

- **Ongoing Provisional Authorization**
  - CSPs must comply with all Continuous Monitoring (ConMon) Requirements to maintain the DoD PA.

- **Reauthorization**
  - Upon expiration, a CSP’s CSO may be reauthorized if there is continued need by the DoD community and the CSP has maintained a satisfactory security posture. The DISA AO will issue an updated PA memo.
• A separate instance of eMASS is available for cloud services.
• It can be accessed by CSPs and their designated 3PAO POC.
• CSPs will create eMASS packages for their CSOs that will provide inheritance across to DoD Mission Owners leveraging the CSO.
• The use of the Cloud eMASS instance will provide a consolidated location for the evidence and test results for CSOs that have a provisional authorization.
• eMASS site: https://cloud.emass.apps.mil/
Summary of Additional Requirements from CC SRG
Additional Considerations and/or Requirements for IL4/IL5

- DoD PKI authentication by DoD privileged and non-privileged users
- DoD IP addressing
- CSP Data center locations
- CSO management/monitoring 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.
- The availability of a private connection capability between the off-premises CSP’s/CSO’s network and DoD networks in support of connections through the BCAP and meet-me points.
Additional Considerations for IL4/IL5, contd.

- Reliance of the CSO or user experience on Internet based capabilities such as the public DNS or content delivery networks.
- Reliance on Internet access to reach the CSO management/service-ordering portal or API endpoints from either NIPRNet or from within the CSO.
- The protections in place in the CSP’s network and CSO to prevent any Internet connection to the CSP’s/CSO’s network and CSO from becoming a back door to the NIPRNet via the private connection through the BCAP.
- 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.
Joint Validation Team (JVT) Review Methodology
JVT Analysts

- The CSP’s DoD Sponsor must provide additional resources to participate in the review of the CSP’s security authorization package.
- The DISA Cloud Assessment team will provide a Cloud SCA-R to function as overall manager of the DoD JVT process. The DoD sponsor’s analysts accomplish most of the review and validation work.
- The sponsor’s support analysts should be deeply familiar with the RMF.
- The scope of effort is estimated to take 12-14 weeks for an uplift and five to eight months when a FedRAMP authorization is not leveraged.
- 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 Skill Requirements

- Specific skills needed:
  - In-depth familiarity with NIST Risk Management Framework (RMF)
  - Knowledge of DoD RMF
  - Familiarization with FIPS-199, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-37
  - Familiarization with FedRAMP documentation review processes (training on FedRAMP.gov)
  - Ability to review and analyze CSP artifacts for completeness, consistency, compliance, and due diligence
  - Knowledge of cryptographic protocols and standards such as FIPS 140, SSH, SSL/TLS, etc.
  - Knowledge of multifactor authentication methodology and types
  - Knowledge of network architecture
  - Ability to review and understand dataflow diagrams
  - Writing skills for clarity and conciseness in comments
  - Familiarity with and knowledge of DoD/85XX documents
JVT Review Methodology

• The JVT will perform a technical review and validation of the following CSP/3PAO completed and signed documentation, and any other relevant documents:
  • Readiness Assessment Report (RAR)
  • Architecture/Network Topology
  • SSP & IL4/5/6 SSP Addendum for FedRAMP+ controls
  • FedRAMP baseline continuous monitoring artifacts, if applicable
  • Security Assessment Plan (SAP)
  • Security Assessment Report (SAR)
    • SAR brief requested from 3PAO after SAR is submitted
  • Plan of Action & Milestones (POA&M)
    • CSP to provide review of risk remediation and mitigation plans from the Plan of Action & Milestones
  • All additional supporting documentation
JVT Lead Responsibilities

- 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 document 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 Responsibilities

- 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
- May attend the DSAWG security briefing for the CSO
CSP leverages FedRAMP JAB PATO or Agency ATO for DoD PA

• Without FedRAMP authorization, DISA & DoD Sponsor coordinate process with CSP/3PAO

DoD Component sponsors CSP for DoD Impact level 4/5/6

• DISA RME holds initial planning meeting
• DoD sponsor commits resources

DISA assigns JVT Lead

• JVT, CSP, and 3PAO teams coordinate, develop and plan work schedule milestones

CSP completes DoD FedRAMP/FedRAMP+ assessment

• FedRAMP baseline documents, DoD RAR, DoD SSP Addendum and any applicable security overlays

Initiation

Sponsor contacts DISA to initiate process

DISA schedules Initial Planning Meeting
CSP/3PAO submit documentation
• CSP/3PAO submit FedRAMP baseline documentation, SSP Addendum, RAR, and SAP
• DISA Cloud SCA-R/JVT conduct quality review of readiness
• Identify major findings or showstoppers
• Determine possible timelines for JVT detailed review to begin
• Schedule kickoff meeting

Kickoff meeting
• Discuss authorization boundary external connections, summary of control implementation
• SCCA team shares BCAP info
• DoD NIC shares info on .mil domain, DNS, and IP address space

DISA SCA-R/JVT approve SAP, with Cloud SCA approval
• Approval of the SAP and SSP Addendum

DoD PA Process – Kickoff
DISA SCA-R/JVT reviews RAR, SSP Addendum, SAP, and documentation checklist for readiness. If not ready SCA-R will push back for resubmission and restart.
DoD PA Process – JVT Detailed Review

- Prerequisites:
  - 3PAO Assessment

  **DISA SCA-R/JVT verifies quality and completeness of CSP/3PAO artifacts**
  - JVT validates DOD requirements through review of documentation and discussions
  - Schedule JVT weekly meetings
  - Schedule stakeholder biweekly updates
  - Schedule meetings with CSP/3PAO as needed

  **DISA SCA-R provides comment sheet to CSP/3PAO for adjudication of findings**
  - Analyze full package for flaws
  - Return package for rework if flawed then restart validation clock upon resubmission
  - CSP/3PAO provide written response to all comments as applicable

  **CSPremediates findings, and 3PAO attests to remediation performed**
  - Findings should be remediated prior to completion of validation
  - 3PAO attestation may be required for remediation performed after assessment
  - Findings that remain open must be mitigated and have a remediation plan subject to approval

Review and Remediation

JVT performs quality review, analysis on security package (SSP/SAP/SAR/POAM)
DoD PA Process – Authorization Recommendation

• Prerequisites:
  • DISA SCA-R/JVT review completed
  • All comments adjudicated

DISA Cloud SCA-R develops risk determination and authorization documents, including briefing for the DSAWG

Cloud SCA Review & Approval

• Updated artifacts/evidence submitted by CSP/3PAO as requested

### Authorization Recommendation & DSAWG Presentation

<table>
<thead>
<tr>
<th>Draft Auth Rec and DSAWG Brief for Submission</th>
<th>Final Auth Rec and DSAWG Brief Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Recommendation &amp; DSAWG Presentation</td>
<td>TRUST IN DISA: MISSION FIRST, PEOPLE ALWAYS!</td>
</tr>
</tbody>
</table>
DoD Provisional Authorization Process – DSAWG & AO

**Prerequisites:**
- Cloud SCA Approval for submission to DSAWG

**DSAWG Review**
- Updated artifacts/evidence may be requested from CSP/3PAO

**AO Decision**
- PA Memo signed and posted on DCAS site
Continuous Monitoring

- FedRAMP & DoD Continuous Monitoring requirements apply until the DoD Provisional Authorization is revoked or expires.
- DISA Cloud SCA-R schedules monthly meetings between CSP POCs and DISA.
- Visit FedRAMP.gov for training, documents, and templates.
- Visit DoD Cyber Exchange for DoD requirements and documents related to DoD cloud use.
- CSPs maintain test results and evidence in eMASS.
- Mission owners inherit security controls in eMASS.
DoD Cloud Authorization Services (DCAS) Site

• Find information about DoD Cloud Authorization Process, DoD templates, and useful links
• DoD component sponsors can initiate the onboarding process for a CSP/CSO
• Browse list of authorized and candidate cloud services
Cloud Resources

- DoD Cloud Authorization Process
  - https://disa.deps.mil/org/RMED/cas
  - CAC-enabled site
  - Sponsorship Request Form, Authorization Process, Services Catalog, etc.

- DoD Cyber Exchange
  - https://cyber.mil/
  - Public and CAC-enabled Content
  - Cloud Computing SRG, Templates, Other documents related to cloud

- DISA Website

- Contact Us
  - disa.meade.re.mbx.cloud-team@mail.mil