DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DoD Cloud Authorization Process

DISA Cloud Assessment Division

DISA RME/RE2

October 2022

DISA Cloud Assessment Division

- **The DISA Cloud Assessment Division (RE2) 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).**

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).
  - Typically, 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**
  - The CSPs must comply with all Continuous Monitoring (ConMon) requirements to maintain the DoD PA.
- **Reauthorization**
  - Upon expiration, a CSO may be reauthorized if there is a continued need by the DoD community and the CSP has maintained a satisfactory security posture. The DISA AO will issue an updated PA memo.

The PA and the ATO

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 the authorization boundary

- **A DoD PA is primarily issued for enterprise use**
  - Typically leverages a CSO's JAB P-ATO or Federal Agency ATO
  - A reciprocity memo was issued at Impact Level 2 for CSOs on the FedRAMP Marketplace
  - The CSO's security authorization package is reviewed by reviewers from DISA and the DoD Component sponsoring the CSO
- **The DoD Component ATO**
  - Issued by a DoD Component AO to a MO for its system/data that makes use of the CSO
  - Must leverage a CSO's DoD PA

FedRAMP and DoD Authorization Processes

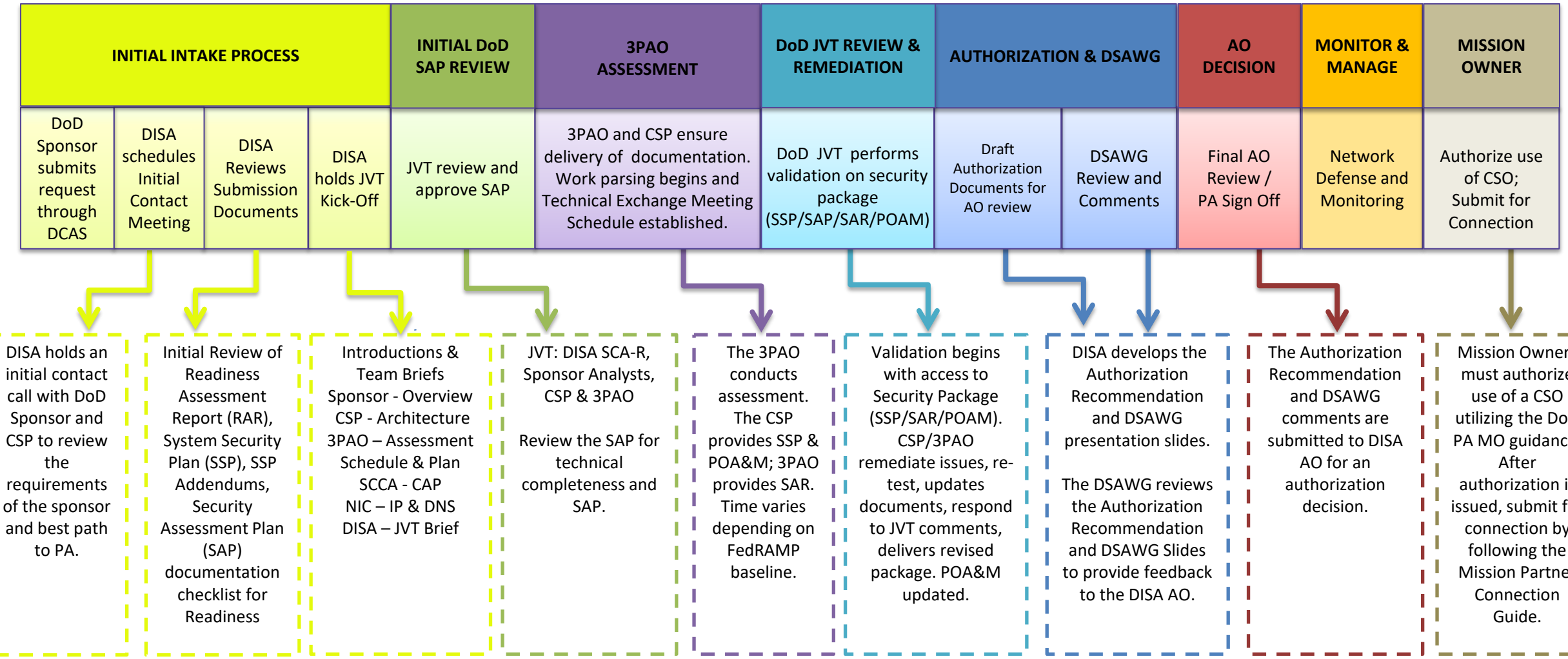
- **The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security authorizations for Cloud Service Offerings in accordance with FISMA and OMB Circular A-130.**
- **Two authorization paths for the CSO:**
  - Joint Authorization Board (JAB)
  - Individual 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 using FedRAMP, supplemented with DoD considerations.**
- **DISA assesses CSP's service offerings and 3PAO results for consideration in issuing a DoD PA.**
- **There are three paths to obtaining a DoD PA:**
  1. Uplift/Leverage FedRAMP JAB PATO
  2. Uplift/Leverage FedRAMP Agency ATO
  3. DoD Component Assessed
- **Review the Cloud Computing Security Readiness Guide (CC SRG) for detailed information regarding the authorization process.**

What You Must Know Prior to the PA Process

- ❑ Shared Responsibility Model
- ❑ Cloud security requirements exist for CSPs and DoD MOs
- ❑ The DoD PA is not the ATO
- ❑ The connection approval process for the MO and the CSP occurs after issuing the PA
- ❑ Continuous monitoring requirements must be performed before and after authorization based on FedRAMP and DoD requirements
- ❑ Cloud eMASS is required to be used for all CSOs with a DoD PA
- ❑ The Cloud Computing (CC) Security Requirements Guide (SRG) outlines the security model and requirements by which DoD will leverage cloud computing

DoD Provisional Authorization Process



Requirements for proceeding with the DoD PA Process

- **In order to proceed with the DoD PA process, the follow documentation must be submitted to DISA RE2 via the Cloud eMASS instance:**
  - Readiness Assessment Report (RAR) or FedRAMP baseline documentation, as applicable
  - System Security Plan (SSP)
  - DoD SSP Addendum, ILx
  - Security Assessment Plan (SAP)
  - CSO Architecture Briefing

- **Once all required documentation has been submitted to DISA RE2 via the Cloud eMASS instance, RE2 will review the documentation and schedule the Kick-Off meeting.**

Cloud eMASS

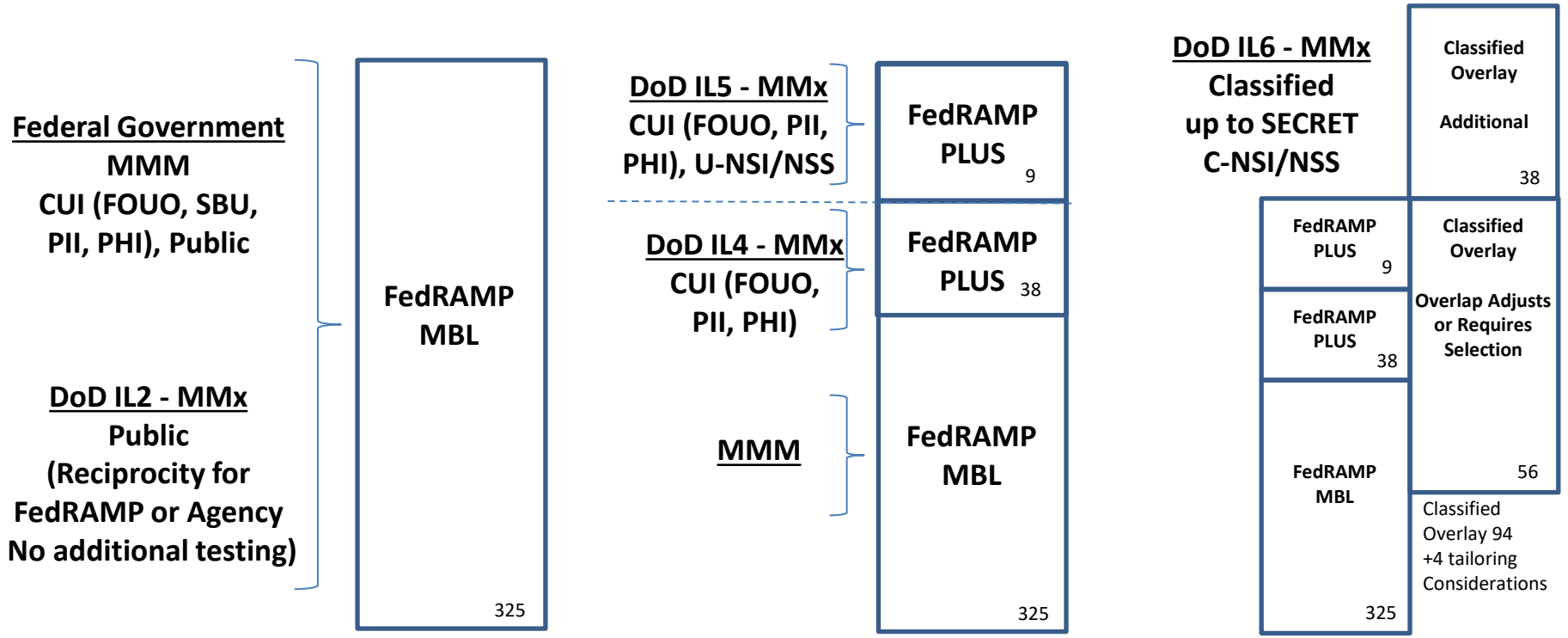
- **Cloud eMASS site: https://cloud.emass.apps.mil/**
- **A separate instance of eMASS is available for cloud services.**
- **It can be accessed by CSPs and their designated 3PAO POC.**
  - Medium Token Assurance Certificate or a Medium Hardware Assurance Certificate is required. More information on certificates and the External Certification Authority (ECA) is located at **https://public.cyber.mil/eca/**.
- **The CSPs will create/manage eMASS packages for their CSOs that will provide inheritance across to DoD MOs 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.**

- **All eMASS questions should be directed to DISA Ft Meade RE Mailbox DISA Cloud eMASS Team disa.meade.re.mbx.disa-cloud-emass-team@mail.mil**

Summary Requirements per Information Impact Level

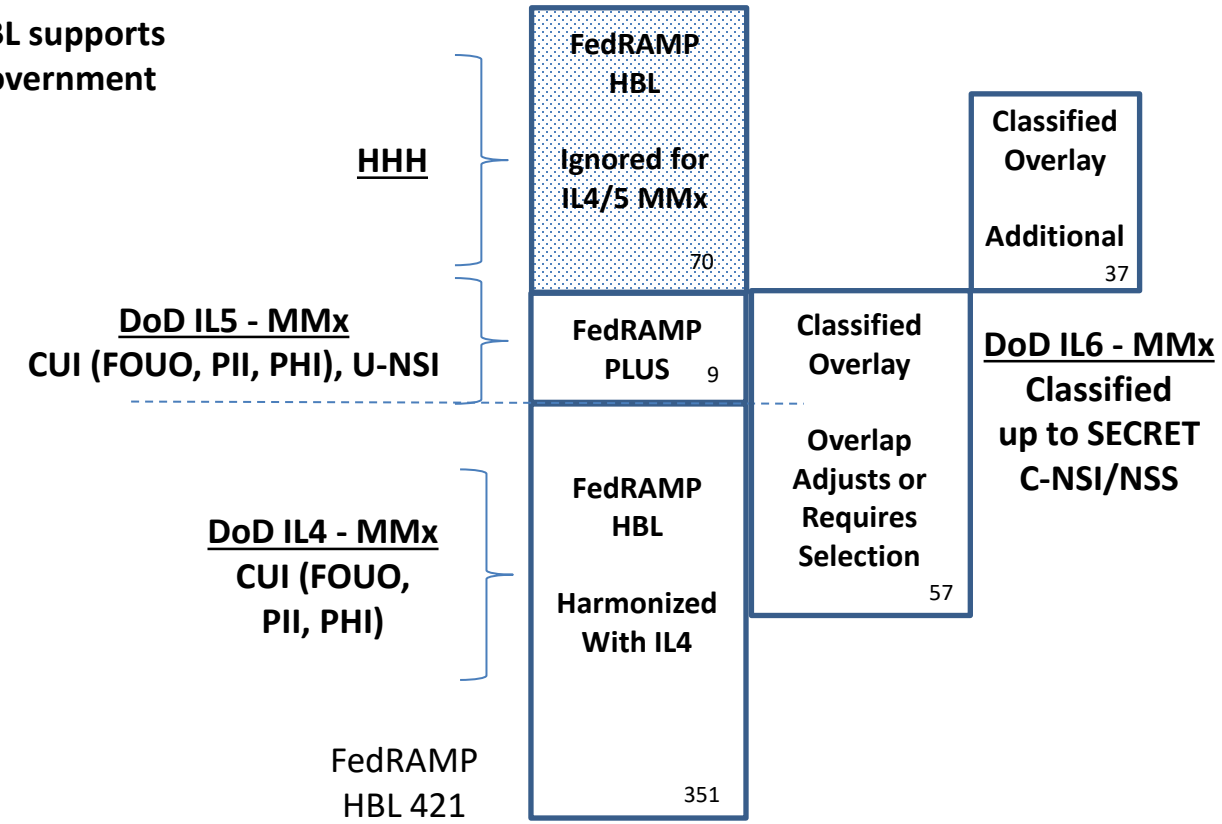
IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	CSP PERSONNEL REQUIREMENTS & INVESTIGATION EQUIVALENCY
2	PUBLIC	FedRAMP Moderate Baseline (MBL)	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	Tier 1 (T1)
4	CUI (FOUO, PII, PHI) or Non-CUI	Level 2 + CUI-Specific Tailored Set OR FedRAMP HBL	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 (IT-1) Tier 5 (T5) ADP-2 (IT-2) Tier 3 (T3) Non-Disclosure Agreement (NDA)
5	CUI (FOUO, PII, PHI), U-NSI/NSS	Level 4 + NSS-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	
6	Classified SECRET NSS	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated T5 & SECRET Clearance NDA

DoD IL 2/4/5/6 Based on FedRAMP MBL



DoD IL 4/5/6 Based on FedRAMP HBL

NOTE: FedRAMP HBL supports
- HHH for Federal Government
- MMM for DoD



Leveraging FedRAMP Authorized Services

- **The FedRAMP Plus (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. (CC SRG, Section 2.6)**
- **For IL4/IL5, DISA leverages the FedRAMP authorization and assesses the additional controls and requirements.**
- **For IL2, there are no additional security controls required for a DoD PA.**
- **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 CSO Packages

- Both the FedRAMP and DoD authorization processes promote reuse of security authorization packages.
- A CSO goes through the authorization process once, and after achieving authorization, 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.
- FedRAMP quick guide for reusing authorizations - https://www.fedramp.gov/assets/resources/documents/Reusing_Authorizations_for_Cloud_Products_Quick_Guide.pdf
- Review the DoD CC SRG for DoD-specific guidance.

Uplift/Leverage a JAB P-ATO

- **A FedRAMP JAB Provisional-Authorization to Operate (J-PATO) is issued by the JAB to a CSP for a CSO.**
- **The CSO's security authorization package is reviewed by JAB Reviewers from three agencies (DoD, DHS, GSA).**
- **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.**
- **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.**
  - This is not the only path to achieve a DoD PA.
  - ****Does not Require DoD Sponsor Analysts**

Uplift/Leverage an Agency ATO

- An Agency ATO is issued by a Federal Agency 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 Assessment Division for review and validation toward issuing a DoD PA.
- The DISA Cloud Assessment Division will request all baseline documentation and applicable continuous monitoring artifacts.

- **Does not Require DoD Sponsor Analysts

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 in order to be authorized.
  - If a DoD organization acting as a CSP develops and manages 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 Assessment Division.**
- **The CSP/3PAO submits assessment documentation (RAR/SSP/SAP/SAR/POAM, etc.) to the DISA Cloud Assessment Division.**
- **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.**

Mission Owner Considerations

- **The DoD MOs 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, Section 3, page 14.**

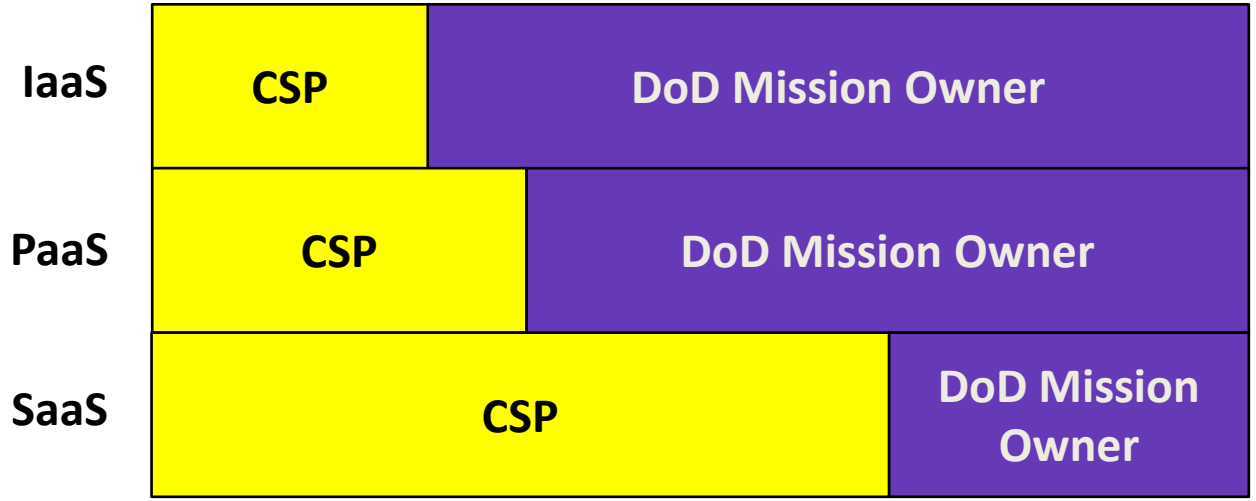
- **The DoD Component sponsoring the CSP must:**
  - Be committed to use
  - Align with a CSSP
  - Provide a minimum of two qualified support analysts to complete review of the CSP's security authorization package.
  - Understand and be capable of responsibility for the customer's portion of controls under the shared responsibility model for cloud use.
- **One DISA Joint Validation Team (JVT) Lead and the DoD Component-sponsored Support Analysts make up the JVT.**
- **A Mission Owner leveraging the DoD PA is responsible for MO requirements and responsibilities to include continuous monitoring.**

Mission Owner AO Responsibility

- **Maximize use 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 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 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



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

ATO

JVT Skill Requirements for all JVT Members

- **Specific skills needed:**
  - In-depth familiarity with NIST Risk Management Framework (RMF)
  - Knowledge of DoD RMF
  - Knowledge of DoD Cloud Computing Security Requirement Guide (CC SRG)
  - Familiarization with FIPS-199, NIST SP 800-53, NIST SP 800-53A, and 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 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.

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 JVT Lead 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 RMF.
- 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 Review Methodology

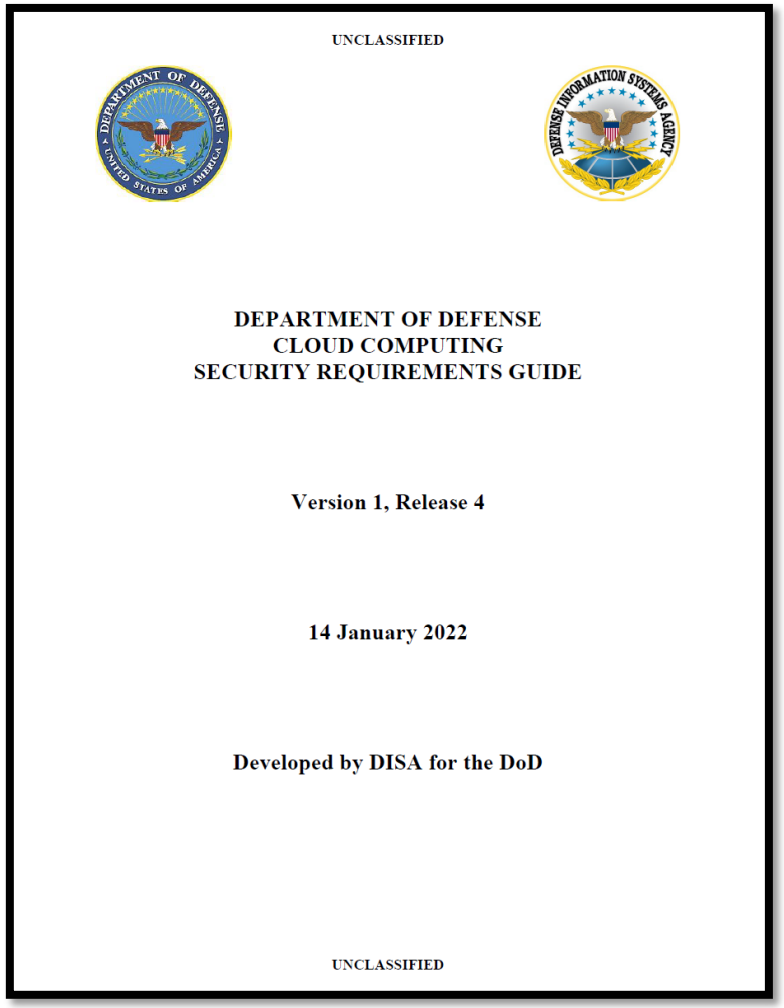
- **The JVT will perform a technical review and validation of the following CSP/3PAO completed and signed documentation, and any other relevant documents:**
  - Readiness Assessment Report (RAR)
  - Architecture/Network Topology
  - SSP & IL4/5/6 SSP Addendum for FedRAMP+ controls
  - FedRAMP baseline 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)**
    - The CSP is to provide review of risk remediation and mitigation plans from the POA&Ms
  - **All additional supporting documentation**

Continuous Monitoring

- FedRAMP & DoD Continuous Monitoring(ConMon) requirements apply until the DoD PA is revoked or expires.
- DISA Cloud JVT Lead 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.
- The CSPs maintain test results and evidence in eMASS.
- Mission Owners inherit security controls in eMASS.

- **CSOs with both a FedRAMP and DoD authorization can leverage the same ConMon Data.

Cloud Computing Security Requirements



UNCLASSIFIED

DEPARTMENT OF DEFENSE
CLOUD COMPUTING
SECURITY REQUIREMENTS GUIDE

Version 1, Release 4

14 January 2022

Developed by DISA for the DoD

UNCLASSIFIED

- **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/.**

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.
- 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.

Additional Considerations for IL4/IL5, cont'd

- **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.**

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://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

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

/DISA @USDISA /USDISA DISA.mil

Backup Slides

FedRAMP/FedRAMP+ Security Control Requirements

FedRAMP Moderate Baseline 325

325 Controls/Control Enhancements (C/CE) → **325**

FedRAMP High Baseline 421

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

*These 96 additional C/CEs include all 38 FedRAMP+ C/CEs required for IL4

DoD Impact Level 4 Baseline 325+38

FedRAMP MBL + 38 FedRAMP+ C/CE = 363 IL4 C/CE → **363**
+ 10 DoD General Readiness Requirements

DoD Impact Level 5 Baseline 325+38+9

IL4 + 9 FedRAMP+ C/CE = 372 IL5 C/CE / → **372**
+ 10 DoD General Readiness 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 V1R4.

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 offing. 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.

Prioritization for Security Assessment

- **Top Priority: CSOs 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 CSOs fall into this category, resolution of priorities will be determined by a designated SecDef or JCS senior.**
- **The CSO renewing an expiring PA that currently hosts DoD IT Projects.**
- **The CSO with a DoD sponsor with these prerequisites:**
  1) **CSO has completed the FedRAMP authorization process**
  2) **CSO has an existing contract**
  3) **CSO rates high on readiness checklist**
  4) **CSO Sponsor has reviewers to help with the analysis of the 3PAO's assessment products**
- **The CSO with DoD sponsor currently operating in a DoD private cloud scenario and has a second DoD sponsor seeking its services.**
- **The CSO with a DoD sponsor not meeting the above conditions.**
- **Least Priority: CSOs without a DoD sponsor but have a capability aligned to a recognized DoD interest.**