**SLIDES ONLY**

**NO SCRIPT PROVIDED**

# FedRAMP Authorization and Equivalency

Cloud requirements for the Defense Industrial Base

**February 2025**

# Agenda

- Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012: Overview of Cloud Service Requirements
- Federal Risk and Authorization Management Program (FedRAMP) Authorization Process Overview
- FedRAMP Equivalency Requirements for the Department of Defense (DoD)
- Recommendations for Cloud Service Providers (CSPs)
- Q&A

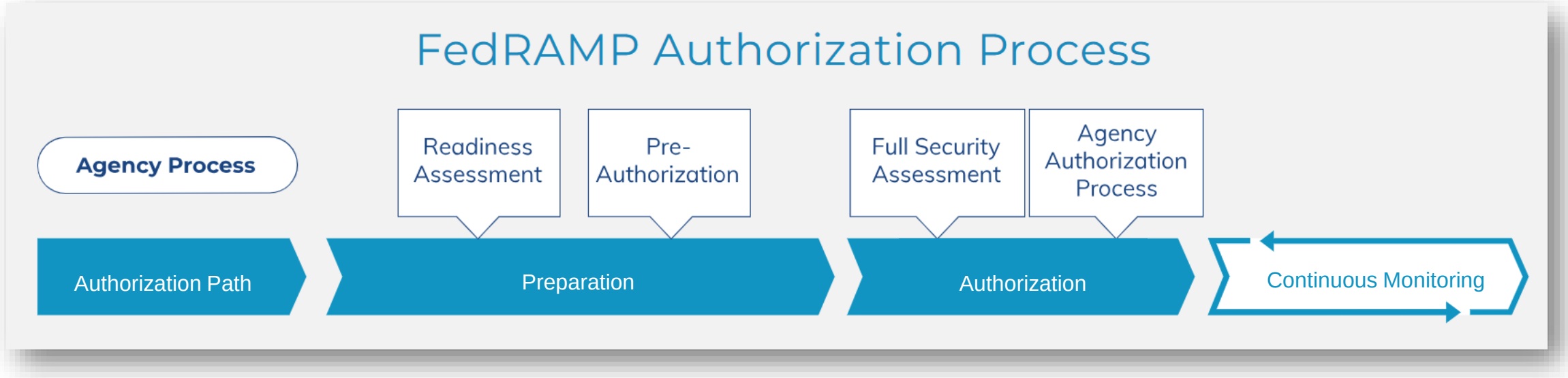
# DFARS 252.204-7012 Cloud Service Requirements

**Adequate Security:** "The Contractor shall provide adequate security on all covered contractor information systems."

Contractors that use external cloud service providers that store, process, or transmit any covered defense information shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the FedRAMP Moderate baseline.

# FedRAMP Overview

The **Federal Risk and Authorization Management Program (FedRAMP)** is a government-wide program that provides a standardized, reusable approach to security assessment, authorization and continuous monitoring for cloud products and services

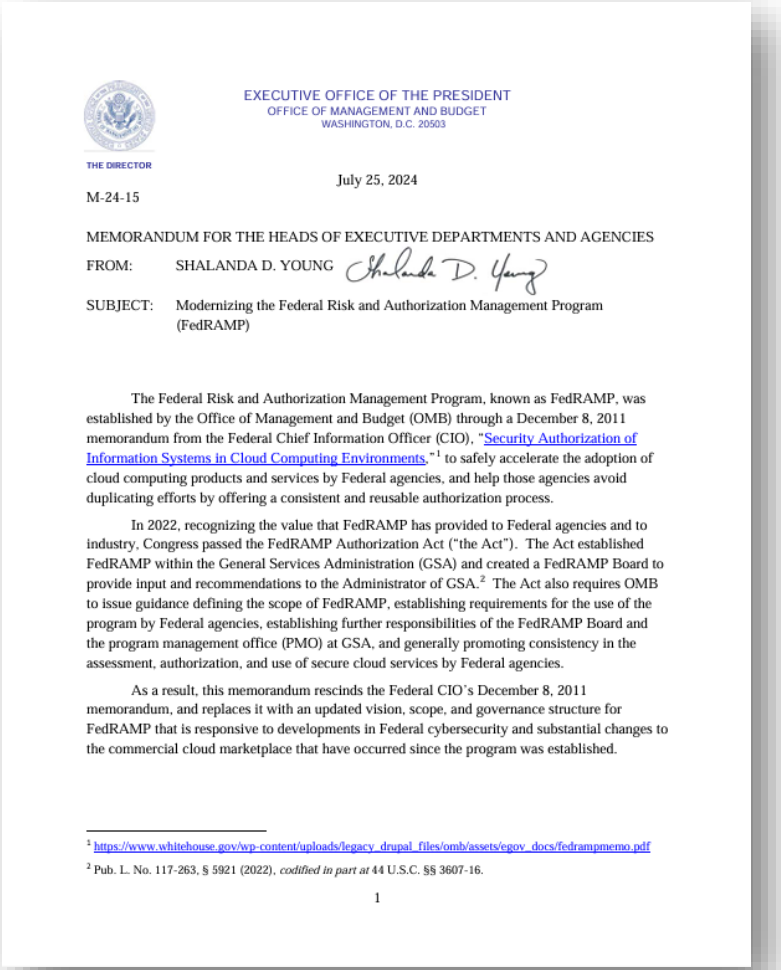


# FedRAMP Transition

- In 2022, Congress passed the FedRAMP Authorization Act, which replaced the Joint Authorization Board (JAB) with a **FedRAMP Board** to oversee the overall health and performance of FedRAMP and work within the Federal community to expand the authorization capacity of the FedRAMP ecosystem

- The Act also required the Office of Management and Budget (OMB) to issue guidance (**M-24-15**) to accelerate the adoption of secure cloud products and services across the Federal government

- Together, these actions began a series of shifts that altered the way FedRAMP operates as a program



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

July 25, 2024

M-24-15

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: SHALANDA D. YOUNG

SUBJECT: Modernizing the Federal Risk and Authorization Management Program (FedRAMP)

The Federal Risk and Authorization Management Program, known as FedRAMP, was established by the Office of Management and Budget (OMB) through a December 8, 2011 memorandum from the Federal Chief Information Officer (CIO), "Security Authorization of Information Systems in Cloud Computing Environments,"[1] to safely accelerate the adoption of cloud computing products and services by Federal agencies, and help those agencies avoid duplicating efforts by offering a consistent and reusable authorization process.

In 2022, recognizing the value that FedRAMP has provided to Federal agencies and to industry, Congress passed the FedRAMP Authorization Act ("the Act"). The Act established FedRAMP within the General Services Administration (GSA) and created a FedRAMP Board to provide input and recommendations to the Administrator of GSA.[2] The Act also requires OMB to issue guidance defining the scope of FedRAMP, establishing requirements for the use of the program by Federal agencies, establishing further responsibilities of the FedRAMP Board and the program management office (PMO) at GSA, and generally promoting consistency in the assessment, authorization, and use of secure cloud services by Federal agencies.

As a result, this memorandum rescinds the Federal CIO's December 8, 2011 memorandum, and replaces it with an updated vision, scope, and governance structure for FedRAMP that is responsive to developments in Federal cybersecurity and substantial changes to the commercial cloud marketplace that have occurred since the program was established.

[1] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/assets/egov_docs/fedrampmemo.pdf

[2] Pub. L. No. 117-263, § 5921 (2022), *codified in part at* 44 U.S.C. §§ 3607-16.

1

# FedRAMP Transition (Cont.)

- Historically, the JAB consisted of the Chief Information Officers of the DoD, the Department of Homeland Security (DHS), and the General Services Administration (GSA), along with their technical representatives, and approved cloud service offerings for FedRAMP authorization and monitored the security of offerings it authorized

- Today, the JAB is no longer monitoring cloud services as a unified entity or authorizing new cloud services. FedRAMP is providing the coordination for both the systems previously prioritized for potential JAB Authorization and the previously Authorized JAB Systems

# FedRAMP Way Ahead

- Two-phased approach to transition oversight of formerly JAB Authorized systems to the DoD, DHS, GSA, FedRAMP, or other agency customers

- **Phase I: (Complete)**
  - Transition began in late October 2024 and ran through December 2024
  - Assigned new designated lead from either one of the former JAB agencies or FedRAMP, which aligns with the agency currently using the system
  - 30-day transition period for each system

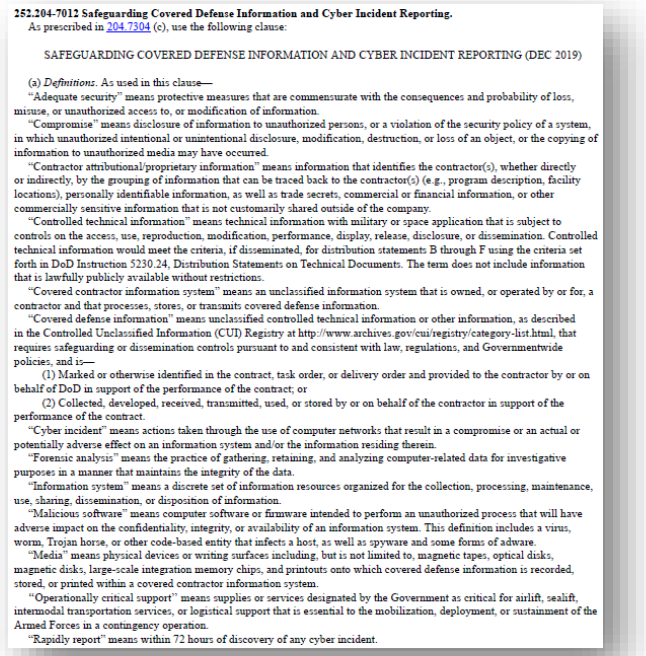
***Once a system transitions, the former P-ATO letters will terminate.***

# FedRAMP Way Ahead (Cont.)

- **Phase II: (In progress)**
  - Designated lead agencies to set up multi-agency continuous monitoring with support from the FedRAMP Program Management Office (PMO)
    - For systems transitioned to DoD, DHS, and GSA, the newly designated lead agency will be the primary on continuous monitoring activities going forward
    - FedRAMP will validate collaborative continuous monitoring, ensuring agency visibility into the security posture of the system
  - For systems that were initially transitioned to FedRAMP, the FedRAMP PMO will contact agency customers to identify a new designated lead

# FedRAMP Moderate Equivalency

- **Derives from DFARS clause 252.204-7012** "Safeguarding Covered Defense Information and Cyber Incident Reporting"
- Provides flexibility via an **additional pathway for DoD contractors to use Cloud Service Offerings (CSOs)** to process, store, and transmit covered defense information (CDI) in support of contract mission
- Does **not** confer FedRAMP Moderate Authorization for CSOs that meet the criteria for equivalency



**252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.**

As prescribed in 204.7304 (c), use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)

(a) *Definitions.* As used in this clause—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

"Malicious software" means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

"Operationally critical support" means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

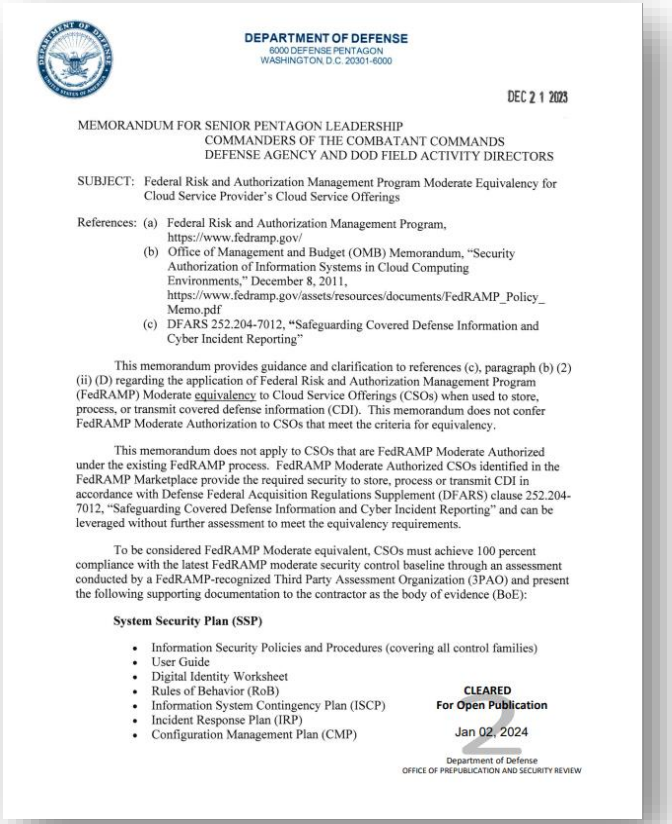
"Rapidly report" means within 72 hours of discovery of any cyber incident.

**FedRAMP Moderate Equivalency ≠ FedRAMP Moderate Authorization**

*https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf*

# FedRAMP Moderate Equivalency Memo Purpose

**Provides guidance and clarification for contractors to pursue FedRAMP Moderate Equivalency for CSOs that do not have an Authority to Operate (ATO), so that contractors can use the CSOs to store, process, or transmit CDI**



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

DEC 2 1 2023

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings

References: (a) Federal Risk and Authorization Management Program, https://www.fedramp.gov/
(b) Office of Management and Budget (OMB) Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," December 8, 2011, https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf
(c) DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting"

This memorandum provides guidance and clarification to references (c), paragraph (b) (2) (ii) (D) regarding the application of Federal Risk and Authorization Management Program (FedRAMP) Moderate equivalency to Cloud Service Offerings (CSOs) when used to store, process, or transmit covered defense information (CDI). This memorandum does not confer FedRAMP Moderate Authorization to CSOs that meet the criteria for equivalency.

This memorandum does not apply to CSOs that are FedRAMP Moderate Authorized under the existing FedRAMP process. FedRAMP Moderate Authorized CSOs identified in the FedRAMP Marketplace provide the required security to store, process or transmit CDI in accordance with Defense Federal Acquisition Regulations Supplement (DFARS) clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" and can be leveraged without further assessment to meet the equivalency requirements.

To be considered FedRAMP Moderate equivalent, CSOs must achieve 100 percent compliance with the latest FedRAMP moderate security control baseline through an assessment conducted by a FedRAMP-recognized Third Party Assessment Organization (3PAO) and present the following supporting documentation to the contractor as the body of evidence (BoE):

**System Security Plan (SSP)**

- Information Security Policies and Procedures (covering all control families)
- User Guide
- Digital Identity Worksheet
- Rules of Behavior (RoB)
- Information System Contingency Plan (ISCP)
- Incident Response Plan (IRP)
- Configuration Management Plan (CMP)

CLEARED
For Open Publication
Jan 02, 2024
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

# Roles and Responsibilities

- DIB Contractor
- 3PAO
- DIBCAC
- C3PAO

# Roles and Responsibilities

- DIB Contractor
- 3PAO
- DIBCAC
- C3PAO

- **Ensures the CSO meets security requirements** equivalent to FedRAMP Moderate baseline and complies with DFARS 252.204-7012 requirements
- **Validates the Body of Evidence (BoE)** provided by a Third Party Assessment Organization (3PAO) meets Moderate Equivalent standards
- If using a FedRAMP Moderate Equivalent CSO, **provides a Customer Responsibility Matrix (CRM) to DIBCAC and C3PAO assessors to aid assessments**
- **Acts as an approver** for the use of the CSO by their organization and confirms that CSP has an Incident Response Plan (IRP)
  - Ensures CSP follows the IRP and can notify contractor
  - **Responsible for reporting** in the event of a CSO compromise
  - Reports incidents IAW applicable **contract terms and conditions**

# Roles and Responsibilities

- DIB Contractor
- 3PAO
- DIBCAC
- C3PAO

Assesses CSO and provides FedRAMP Moderate Equivalency package to a contractor as a **BoE**, which includes:

***1. System Security Plan (SSP)***

- Information System Security Policy and Procedures
- Information System Contingency Plan (ISCP)
- Incident Response Plan (IRP)
- Configuration Management Plan (CMP)
- Federal Information Procession Standards (FIPS 199)

***2. Security Assessment Plan (SAP)***

- Security Test Case Procedures
- Penetration Testing Plan and Methodology conducted annually and validated

# Roles and Responsibilities

- DIB Contractor
- 3PAO
- DIBCAC
- C3PAO

Assesses CSO and provides FedRAMP Moderate Equivalency package to a contractor as a **BoE**, which includes:

***3. Security Assessment Report (SAR)***

- Risk Exposure Table
- Security Test Case Procedures
- Infrastructure Scan Results conducted monthly and validated annually
- Web Scan Results conducted monthly and validated annually
- Penetration Test Reports

***4. Plan Of Action and Milestones (POA&M)***

- Continuous Monitoring Strategy
- Continuous Monitoring monthly summary, validated annually

# Roles and Responsibilities

- DIB Contractor
- 3PAO
- DIBCAC
- C3PAO

- Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) **reviews the CSP's BoE** asserting to FedRAMP Moderate Equivalency
  - Validates compliance with DFARS clauses 252.204-7012 and 252.204-7020
  - Implements contractor-required controls

DCMA DEFENSE CONTRACT MANAGEMENT AGENCY

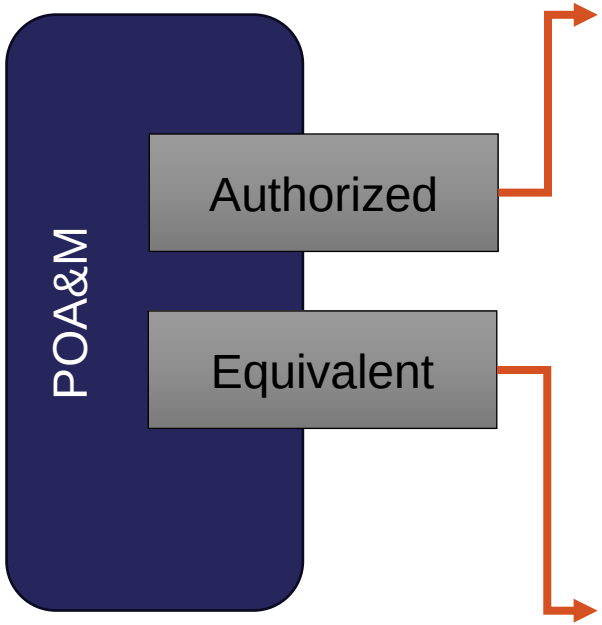
https://www.dcma.mil/DIBCAC/

# Roles and Responsibilities

- DIB Contractor
- 3PAO
- DIBCAC
- C3PAO

- For Cybersecurity Maturity Model Certification (CMMC) assessments, a CMMC 3rd Party Assessment Organization (C3PAO) **reviews the CSP's BoE** asserting to FedRAMP Moderate Equivalency
  - Validates compliance with DFARS clauses 252.204-7012 and 252.204-7020
  - Implements contractor-required controls

# FedRAMP Moderate Equivalency POA&Ms




- POA&Ms Allowed
  - Must have Remediation Plan
  - Must have Scheduled Completion Date
  - All high and critical risk findings must be remediated prior to receiving a FedRAMP Authorization
  - Must be remediated within 30/90/180 days based on criticality of POA&M item

- CSOs must achieve 100% compliance with the latest **FedRAMP Moderate Baseline** at the conclusion of assessment conducted by a FedRAMP-recognized 3PAO
  - Continuing Operational Plans of Action and Milestones (POA&Ms) after assessment and during CSO operation **are expected and acceptable**
  - **Complete risk avoidance is required,** as there is no government sponsor and therefore no Authorizing Official who can officially accept risk on behalf of the CSO in this situation

# Recommendations for CSPs

1. Engage a FedRAMP-recognized 3PAO early

2. Conduct a Readiness Assessment before formal testing

3. Maintain strong internal governance for security documentation and incident reporting

# Points of Contact

**Cybersecurity Maturity Model Certification Program Management Office**

*For inquiries regarding equivalency in the CMMC ecosystem*

osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil

**Risk Management Framework Technical Advisory Group**

osd.pentagon.dod-cio.mbx.rmf-tag-secretariat@mail.mil

# Questions?