



SLIDES ONLY  
NO SCRIPT PROVIDED

CLEARED  
For Open Publication

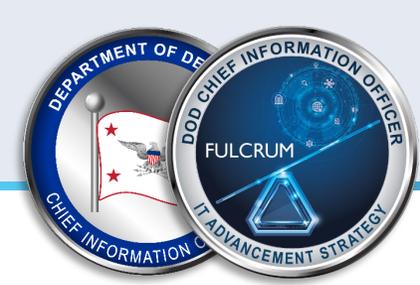
Jan 21, 2025

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW



# Introduction to the CMMC Enterprise Mission Assurance Support Service (eMASS)

February 12, 2025



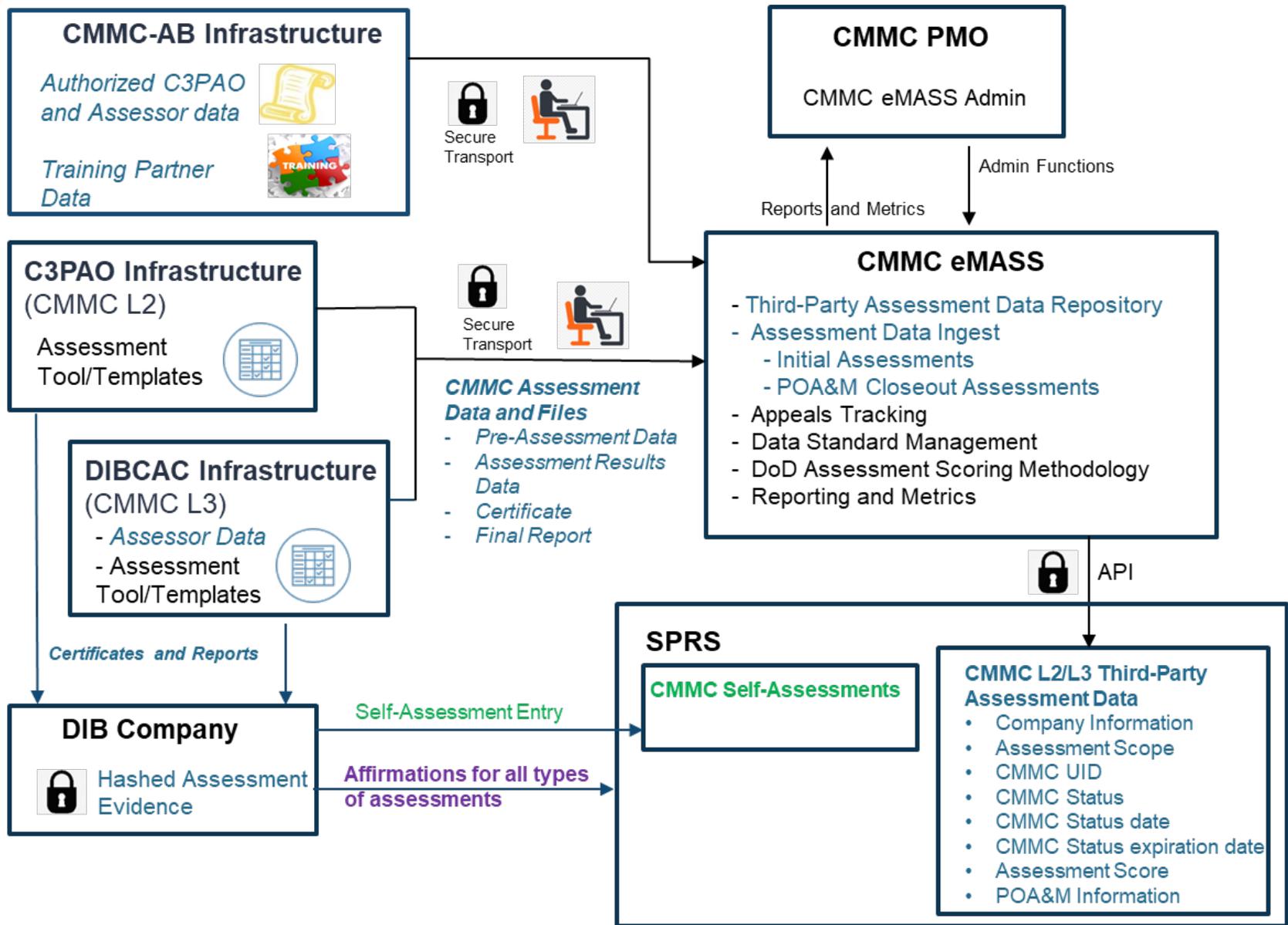
# CMMC eMASS Overview

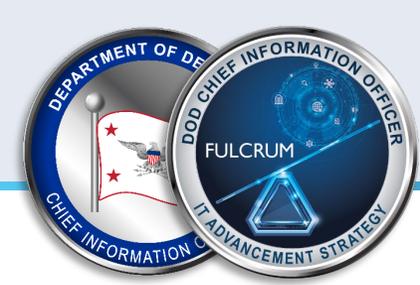
- The Cybersecurity Maturity Model Certification (CMMC) eMASS is a tailored version of DoD's eMASS that is used to store, track, and report on CMMC Level 2 and Level 3 assessment data
- CMMC eMASS is the data repository for CMMC assessment and supporting data. It does not contain proprietary data (e.g., assessment evidence)
- CMMC eMASS is also the engine for tracking assessments, Plans of Actions and Milestones (POA&Ms), and appeals actions, and is a mechanism used for reporting/tracking CMMC metrics

<https://cmmc.emass.apps.mil/>



# CMMC eMASS Assessment Data Flow





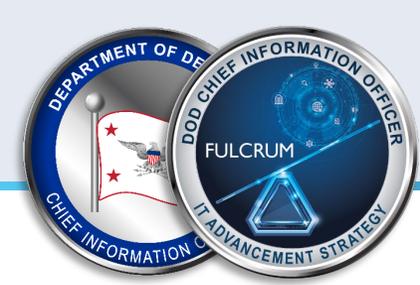
# CMMC eMASS Roles (1/2)

- CMMC Program Management Office (PMO) Role:
  - Government user. Can access all data in the system and run reports.
- CMMC PMO Administrator Role:
  - System administrator. Create and configure user accounts and access.
- CMMC Accreditation Body (AB) Role:
  - User from the CMMC AB that uploads data for authorized CMMC Third-Party Assessment Organizations (C3PAOs), authorized assessors, approved training partners, and approved partner publishers.



# CMMC eMASS Roles (2/2)

- C3PAO Role:
  - Ability to upload **CMMC Level 2** pre-assessment data, assessment results, and certificates for initial assessments and POA&M close-out assessments
  - Ability to track appeals
  - Has access to assessment data only of the companies they have assessed
- Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Role:
  - Ability to upload **CMMC Level 3** pre-assessment data, assessment results, and certificates for initial assessments and POA&M close-out assessments
  - Has access to all assessment data, reports, and metrics



# Non-Administrative Use of CMMC eMASS

## **AB action:**

- Upload authorized C3PAO and Level 2 assessor data

## **DIBCAC action:**

- Upload Level 3 assessor data

## **C3PAO and DIBCAC action:**

- Create assessment records and workflows
- Upload planning data (Pre-Assessment information)
- Upload assessment results
- Upload the CMMC certificate

## **CMMC eMASS System Application Programming Interface (API):**

- Subset of the data for completed assessment records pulled into SPRS

## **C3PAO and DIBCAC action:**

- Upload POA&M Closeout Assessment Data
- Track appeals actions

## **CMMC PMO and others:**

- View and download reports/metrics



# CMMC Assessment Data Standard

- **Assessment teams generate assessment data compliant with the CMMC assessment data standard, which is comprised of two JSON schemas—one for “pre-assessment,” or planning data, and one for assessment results:**
  - CMMC.PreAssessment.schema.json
  - CMMC.AssessmentResults.schema.json
- **C3PAOs may develop or purchase any tool that is compliant with the data standard and DoD security requirements to generate pre-assessment data and assessment results in the required JSON file format. C3PAOs may also use two spreadsheets that are compliant with the assessment data standard:**
  - CMMC\_Level2\_PreAssessment\_Template.xlsx
  - CMMC\_Level2\_AssessmentResults\_Template.xlsx

All assessment data standard files will be maintained by CMMC eMASS developers over the CMMC eMASS system’s lifecycle and are available on <https://cmmc.emass.apps.mil/>



# CMMC eMASS Process Flow (1 of 3)

## PREREQUISITES

- C3PAO/DIBCAC coordinates with Organization Seeking Certification (OSC) to determine assessment scope, team, and plan
- C3PAO/DIBCAC contacts the CMMC PMO Admin to configure “HQ record”
  - *A Defense Industrial Base (DIB) company may have multiple information systems requiring separate assessments. Each assessment aligns with a unique OSC. Multiple OSCs may align with a single DIB company*

DIB Company (“HQ Record”)

├ OSC 1  
└ OSC 2

- **CMMC eMASS Step 1:** Create Assessment Record/Package
- **CMMC eMASS Step 2:** Upload “Pre-Assessment” Information



# CMMC eMASS Process Flow (2 of 3)

## Conduct Assessment

- OSC hashes assessment artifacts
- Quality review and approval process (internal to the C3PAO and DIBCAC)
- Assessment results are reported using the data standard

## • CMMC eMASS Step 3: Upload “Assessment Results”

- If assessment results in Final or Conditional status:
  - CMMC eMASS calculates the score and CMMC Status (Final or Conditional Level 2 or 3)
  - CMMC eMASS autogenerates CMMC UID, Status Date (the date the results are uploaded), and Status Expiration Date (3 years for Final assessments, 180 days for Conditional assessments)
- If assessment does not result in a Final or Conditional status:
  - CMMC Status is “No CMMC Status”



## CMMC eMASS Process Flow (3 of 3)

- CMMC eMASS Step 4: Upload Certificate
  - Limited assessment data is transferred to SPRS
- CMMC eMASS Step 5: Upload Assessment Findings Report

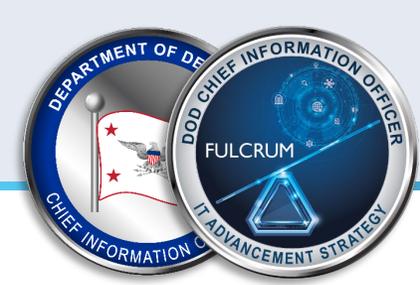
***ASSESSMENT WORKFLOW PROCESS COMPLETE***



# POA&M Closeout Assessment

## POA&M close-out assessment workflow is identical to that of an initial assessment

- The same data standard is used to report data (pre-assessment and results templates/JSON schemas)
- If the POA&M closeout assessment results in a CMMC Status of Final Level 2 or 3, then the CMMC Status is updated to reflect the change from Conditional to Final Level 2 or 3 with no change to the CMMC Status Date
- If the POA&M closeout assessment results in No CMMC Status, then the CMMC Status is updated from Conditional to No CMMC Status with no change to the CMMC Status Date
- There is no option for a POA&M closeout assessment to result in an updated Conditional status
- For Level 2 assessments, the same or a different C3PAO may conduct the POA&M closeout assessment



# References

- **C3PAO User Job Aid:** *eMASS\_CMMC\_C3PAO\_User\_Job\_Aid.pdf\**
- **C3PAO CMMC eMASS CONCEPT of OPERATIONS V. 5.12\***
- **CMMC eMASS site:** <https://cmmc.emass.apps.mil/>
- **CMMC eMASS PMO Administrator email:** [osd.pentagon.dod-cio.mbx.cmmc-emass-admin@mail.mil](mailto:osd.pentagon.dod-cio.mbx.cmmc-emass-admin@mail.mil)
- **CMMC Assessment Data Standard\*:**
  - **JSON schema:** CMMC.PreAssessment.schema.json
  - **JSON schema:** CMMC.AssessmentResults.schema.json
  - **Excel spreadsheet:** CMMC\_Level2\_PreAssessment\_Template.xlsx
  - **Excel spreadsheet:** CMMC\_Level2\_AssessmentResults\_Template.xlsx
- **CMMC Artifact Hashing Tool User Guide:** <https://dodcio.defense.gov/CMMC/>
- **Help Desk Ticketing:** *eMASS\_CMMC\_Help\_Desk\_Ticket\_Job\_Aid.pdf\**
- **New User Registration:** *eMASS\_CMMC\_New\_User\_Registration\_Job\_Aid.pdf\**

\* File available at <https://cmmc.emass.apps.mil/>



# Acronyms

**API** – Application Programming Interface

**C3PAO** - CMMC Third-Party Assessment Organization

**CAC** – Common Access Card

**CCA** – CMMC Certified Assessor

**CMMC** – Cybersecurity Maturity Model Certification

**DIB** – Defense Industrial Base

**DIBCAC** – Defense Industrial Base Cybersecurity Assessment Center

**DoD** – Department of Defense

**ECA** - External Certificate Authority

**eMASS** - Enterprise Mission Assurance Support Service

**IT** – Information Technology

**JSON** - JavaScript Object Notation

**OSC** - Organization Seeking Certification

**PIV** – Personal Identity Verification

**PKI** – Public Key Infrastructure

**POC** – Point of Contact

**PMO** – Program Management Office

**POA&M** - Plan of Actions and Milestones

**SPRS** – Supplier Performance Risk System

**UID** – Unique Identifier



# Points of Contact

## Cybersecurity Maturity Model Certification Program Management Office

*For inquiries regarding eMASS*

[osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil](mailto:osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil)



Questions?