~~Six~~ Three Months to CMMC?

Matthew Travis

25 September 2024

THE CYBER AB
CMMC CERTIFICATION

Discussion Points

1. Six Months or Three Months?...Where Are We with CMMC Rulemaking?
2. What the Start of CMMC Means for Defense Contractors
3. Decision for the DIB: CMMC Train or the Platform of Denial?
4. Managed Service Providers (MSPs/MSSPs) and CMMC Level 2 Certification
5. Cloud Service Providers and FedRAMP Moderate Equivalency
6. Building Ecosystem Capacity
7. What We Are Working On

CMMC Title 48

The CMMC **Title 48** Proposed Rule (the “DFARS Rule”) was published in the *Federal Register* on 15 August

- **Title 48 Proposed Rule implements the CMMC program as DoD contract requirements**
- **Gives direction to DoD contracting officers and program managers**
- **Addresses several comments/questions from the CMMC 1.0 Interim Final Rule (2020)**
- **Public Comment Period will be open through 15 October 2024**
- **Of Note:**
  - CMMC conformance will be placed on contract ***award***—not on proposal or performance
  - Primes *will not* have access to CMMC eMASS to verify subcontractor certification
  - DIB companies outside the U.S. will be held to the same standards as U.S. contractors

CMMC Title 32

The CMMC **Title 32 Final Rule** (the "CMMC Program Rule") was cleared by OMB/OIRA on 15 September

- **Title 32 Final Rule establishes CMMC as an official DoD program**
- **Final Rule likely undergoing final QA review, formatting, and DoD sign-out approval**
- **Upon sign-out, Final Rule goes to NARA for eventual publication in the Federal Register**
- **Published Final Rule will have an effective-in-force date: CMMC will begin on that date**
- **Of Note: What about the required Congressional review?**

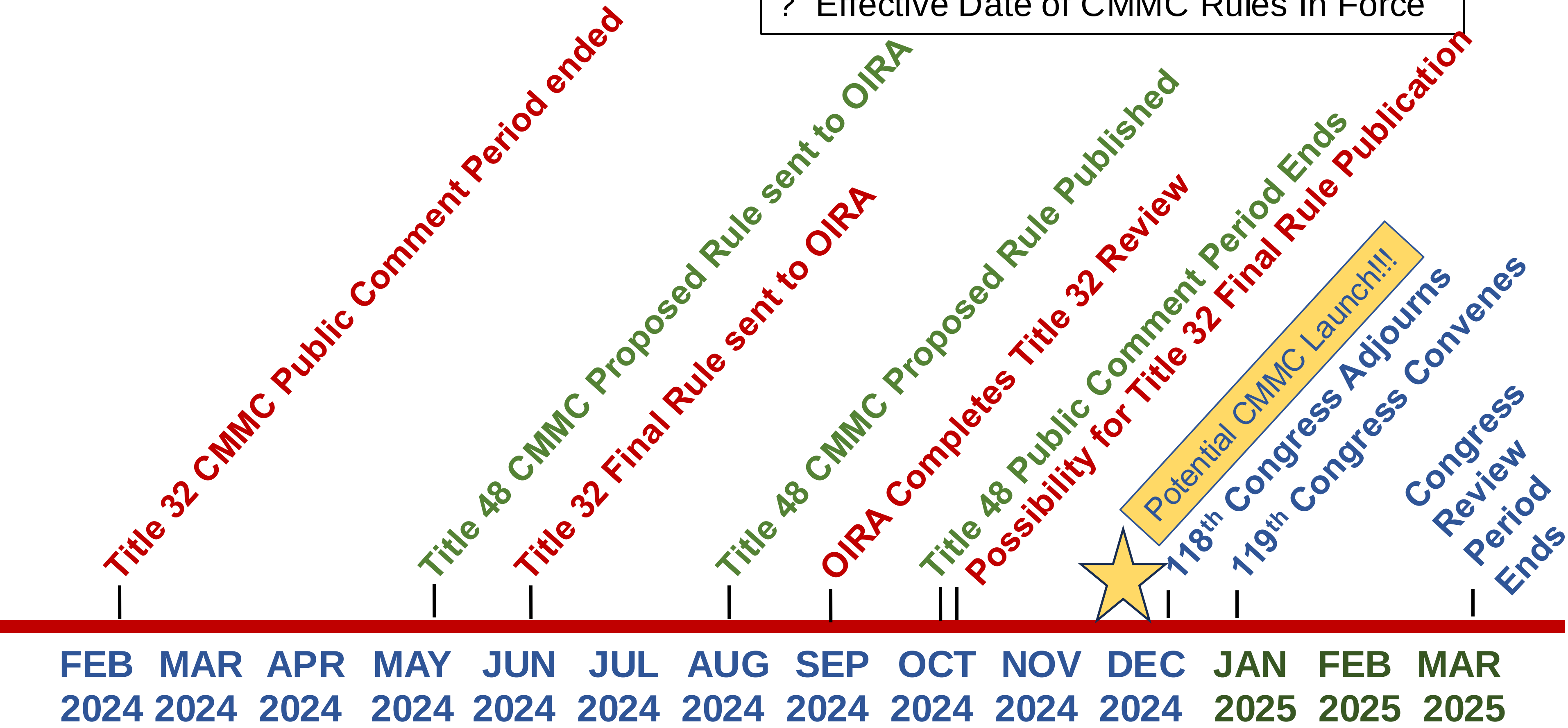
Anticipating the CMMC Timeline

Dates We Do Not Yet Know

? ~~Public Comment Period for Title 48 Rule~~

? ~~Completion of OIRA Interagency Review~~

? Effective Date of CMMC Rules In Force



Title 32 CMMC Public Comment Period ended

Title 48 CMMC Proposed Rule sent to OIRA

Title 32 Final Rule sent to OIRA

Title 48 CMMC Proposed Rule Published

OIRA Completes Title 32 Review

Title 48 Public Comment Period Ends

Possibility for Title 32 Final Rule Publication

Potential CMMC Launch!!!

118th Congress Adjourns

119th Congress Convenes

Congress Review Period Ends

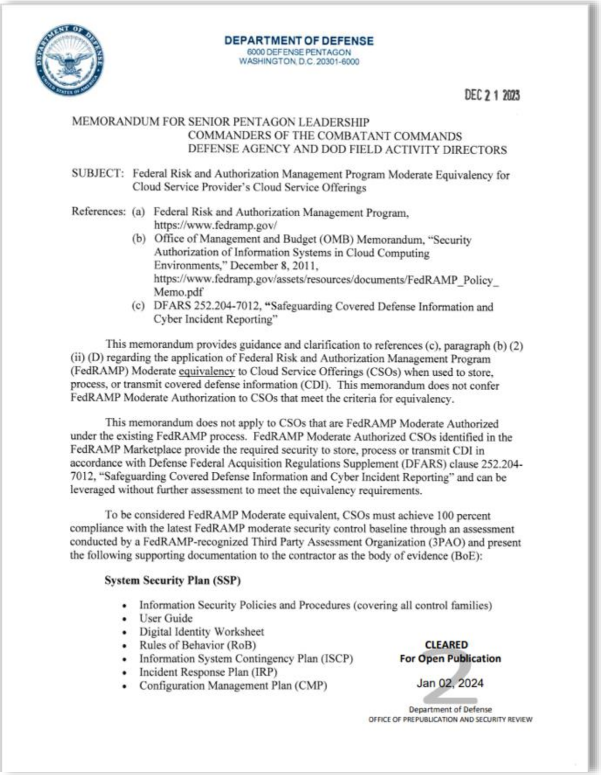
We do not necessarily expect CMMC to enter into force officially until late **Q4 2024** at the earliest

Program Update

1. Six Months or Three Months?...Where Are We with CMMC Rulemaking?
2. What the Start of CMMC Means for Defense Contractors
3. Decision for the DIB: CMMC Train or the Platform of Denial?
4. Managed Service Providers (MSPs/MSSPs) and CMMC Level 2 Certification
5. Cloud Service Providers and FedRAMP Moderate Equivalency
6. Building Ecosystem Capacity
7. What We Are Working On

FedRAMP Moderate Equivalency

All Ecosystem Members should be familiar with the 21 December 2023 DoD memorandum on FedRAMP equivalency for cloud service offerings



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.

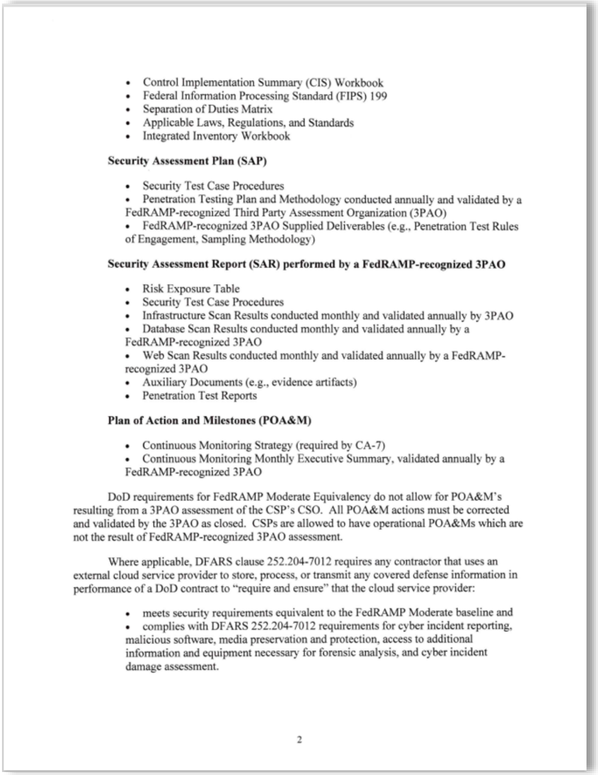
This memorandum does not apply to CSOs that are FedRAMP Moderate Authorized under the existing FedRAMP process. FedRAMP Moderate Authorized CSOs identified in the FedRAMP Marketplace provide the required security to store, process or transmit CDI in accordance with Defense Federal Acquisition Regulations 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



- Control Implementation Summary (CIS) Workbook
- Federal Information Processing Standard (FIPS) 199
- Separation of Duties Matrix
- Applicable Laws, Regulations, and Standards
- Integrated Inventory Workbook

Security Assessment Plan (SAP)

- Security Test Case Procedures
- Penetration Testing Plan and Methodology conducted annually and validated by a FedRAMP-recognized Third Party Assessment Organization (3PAO)
- FedRAMP-recognized 3PAO Supplied Deliverables (e.g., Penetration Test Rules of Engagement, Sampling Methodology)

Security Assessment Report (SAR) performed by a FedRAMP-recognized 3PAO

- Risk Exposure Table
- Security Test Case Procedures
- Infrastructure Scan Results conducted monthly and validated annually by 3PAO
- Database Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Web Scan Results conducted monthly and validated annually by a FedRAMP-recognized 3PAO
- Auxiliary Documents (e.g., evidence artifacts)
- Penetration Test Reports

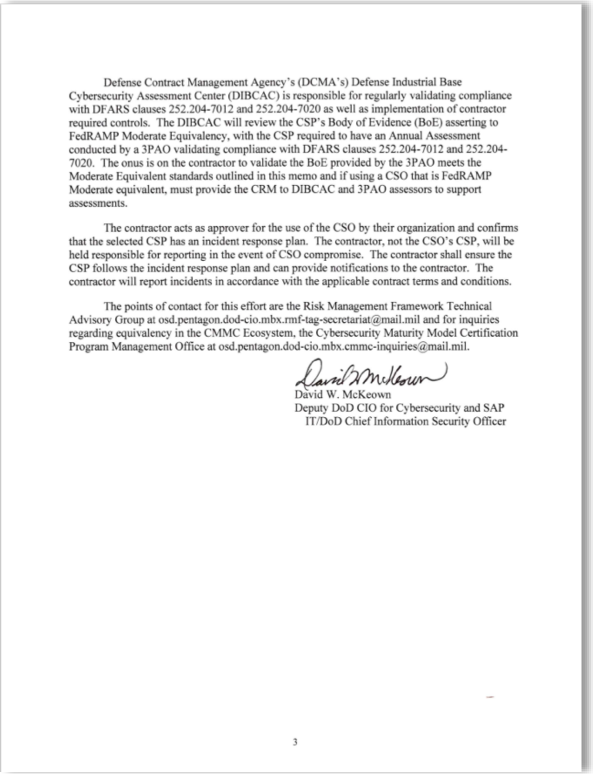
Plan of Action and Milestones (POA&M)

- Continuous Monitoring Strategy (required by CA-7)
- Continuous Monitoring Monthly Executive Summary, validated annually by a FedRAMP-recognized 3PAO

DoD requirements for FedRAMP Moderate Equivalency do not allow for POA&M's resulting from a 3PAO assessment of the CSP's CSO. All POA&M actions must be corrected and validated by the 3PAO as closed. CSPs are allowed to have operational POA&Ms which are not the result of FedRAMP-recognized 3PAO assessment.

Where applicable, DFARS clause 252.204-7012 requires any contractor that uses an external cloud service provider to store, process, or transmit any covered defense information in performance of a DoD contract to "require and ensure" that the cloud service provider:

- meets security requirements equivalent to the FedRAMP Moderate baseline and
- complies with DFARS 252.204-7012 requirements for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.



Defense Contract Management Agency's (DCMA's) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) is responsible for regularly validating compliance with DFARS clauses 252.204-7012 and 252.204-7020 as well as implementation of contractor required controls. The DIBCAC will review the CSP's Body of Evidence (BoE) asserting to FedRAMP Moderate Equivalency, with the CSP required to have an Annual Assessment conducted by a 3PAO validating compliance with DFARS clauses 252.204-7012 and 252.204-7020. The onus is on the contractor to validate the BoE provided by the 3PAO meets the Moderate Equivalent standards outlined in this memo and if using a CSO that is FedRAMP Moderate equivalent, must provide the CRM to DIBCAC and 3PAO assessors to support assessments.

The contractor acts as approver for the use of the CSO by their organization and confirms that the selected CSP has an incident response plan. The contractor, not the CSO's CSP, will be held responsible for reporting in the event of CSO compromise. The contractor shall ensure the CSP follows the incident response plan and can provide notifications to the contractor. The contractor will report incidents in accordance with the applicable contract terms and conditions.

The points of contact for this effort are the Risk Management Framework Technical Advisory Group at osd.pentagon.dod-cio.mbx.rmf-tag-secretariat@mail.mil and for inquiries regarding equivalency in the CMMC Ecosystem, the Cybersecurity Maturity Model Certification Program Management Office at osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil.

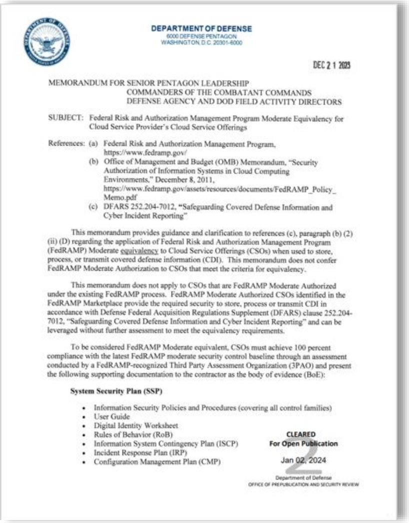
David W. McKeown
Deputy DoD CIO for Cybersecurity and SAP
IT/DoD Chief Information Security Officer

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

FedRAMP Moderate Equivalency and CMMC

- **Cloud Service Providers** must:
  - Achieve 100 percent compliance with the FedRAMP moderate security control baseline through an assessment conducted by a **FedRAMP 3PAO**
  - Present supporting documentation of equivalency—the “body of evidence”—to the **OSC**

- **OSCs** must:
  - Validate the body of evidence from the CSP
  - Possess a client responsibility matrix (CRM) from the CSP
  - Ensure the CSP has an incident response plan
  - **Approve the use of the CSO within its CMMC-scoped environment**



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

An assessment review of a CSO’s Body of Evidence to confirm FedRAMP Moderate Equivalency **is a point-in-time determination**

Program Update

1. Six Months or Three Months?...Where Are We with CMMC Rulemaking?
2. What the Start of CMMC Means for Defense Contractors
3. Decision for the DIB: CMMC Train or the Platform of Denial?
4. Managed Service Providers (MSPs/MSSPs) and CMMC Level 2 Certification
5. Cloud Service Providers and FedRAMP Moderate Equivalency
6. Building Ecosystem Capacity
7. What We Are Working On

CCA Requirements

Individuals currently certified under the CCP and CCA programs must complete all certification requirements prior to CMMC entering into force

CMMC Certified Professional (CCP)

- ✓ **NEW** Obtain Tier 3 Background Investigation Eligibility Determination

CMMC Certified Assessor (CCA)

- ✓ **NEW** Obtain Tier 3 Background Investigation Eligibility Determination or Equivalent
- ✓ **NEW** Have at least three (3) years of cybersecurity experience
- ✓ **NEW** Have at least one (1) year of assessment or audit experience
- ✓ **NEW** Possess at least one baseline certification aligned to the Intermediate, or above, Proficiency Level for Career Pathway Certified Assessor Job ID 612 from Directive 8140.03

Find the Matrix here: https://public.cyber.mil/dcwf-work-role/security-control-assessor/

Program Update

1. Six Months or Three Months?...Where Are We with CMMC Rulemaking?
2. What the Start of CMMC Means for Defense Contractors
3. Decision for the DIB: CMMC Train or the Platform of Denial?
4. Managed Service Providers (MSPs/MSSPs) and CMMC Level 2 Certification
5. Cloud Service Providers and FedRAMP Moderate Equivalency
6. Building Ecosystem Capacity
7. What We Are Working On

What We are Working On

The Cyber AB is decisively engaged in preparing for CMMC operations

- CMMC Assessment Process (CAP v2.0)
- Code of Professional Conduct (CoPC)
- Reauthorization of C3PAOs
- CMMC eMASS Access and Protocols
- Updates to CMMC Marketplace and Cyber AB Web Platform
- C3PAO Accreditation Scheme
- CMMC Level 2 Certificate Design

CEIC EAST 2024

CMMC Ecosystem Summit + CMMC **Implementation Conference**

21-22 November 2024

The Gaylord National Resort, National Harbor MD

“CMMC: CEIC and You Shall Find”

https://ceiceast.com