RADICL

CMMC 2.0 COMPLIANCE

WWW.RADICL.COM

Agenda

- Introductions
- What is CMMC?
- Why does CMMC matter?
- What is FCI/CUI
- CMMC scope
- Assessment frequency
- What's needed to become compliant
- What are our free resources?
- Q&A

RADICL AND THE COMPLIANCE LEADERSHIP TEAM

Victor Cich

Senior Compliance Consultant

- Passionate about compliance
- Helps organizations achieve CMMC Level 2, NIST 800-171, and NIST 800-53
- CMMC Certified Assessor and a Registered Practitioner with CYBER AB

What is CMMC?

- 15 cybersecurity requirements protecting Federal Contract Information (FCI)
  - **FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems.**
- 110 cybersecurity requirements protecting Controlled Unclassified Information (CUI)
  - **DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.**
    - **Subject to NIST SP 800-171 Rev 2**
    - **"Shall implement NIST SP 800-171 Rev 2 as soon as practical, but not later than December 31, 2017"**
- 32 Code of Federal Regulations(CFR) Part 170
  - Published October 15th, 2024
  - Effective date of December 16th, 2024
  - Phased rollout covering new and legacy contracts.

WHY DOES CMMC MATTER?

- DoD Contract clauses require compliance
  - FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems.
  - DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.
  - DFARS 252.204-7019 Notice of NISTSP 800-171 DoD Assessment Requirements.
- Nation State Threat Actors
  - NIST SP 800-171 Rev 2/CMMC covers the 110 cybersecurity requirements to improve security posture
  - Protects against IP theft and information aggregation
- Noncompliance could lead to contract/revenue loss
  - New contracts will most likely require certification starting Q3 of 2025

FEDERAL CONTRACT INFORMATION

- What is Federal Contract Information (FCI)?
  - FCI is defined as information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public or simple transactional information such as necessary to process payments.
- FCI examples
  - Contract Information
  - Emails exchanged with the DoD or defense contractor(s)
  - Contract performance reports
  - Process documentation
  - Solicitations or proposal responses
- Systems storing, processing or transmitting the above are considered "In Scope"

CONTROLLED UNCLASSIFIED INFORMATION

- What is Controlled Unclassified Information(CUI)?
  - Controlled Unclassified Information (CUI) is information that requires safeguarding, or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies but is not classified.
  - Examples:
    - Controlled Technical Information (CTI)
      - Technical data of computer software
    - Personally Identifiable Information (PII)
      - SSN, passport numbers, etc.
    - Protected Health Information (PHI)
    - For Official Use Only (FOUO)
  - Systems storing, processing or transmitting the above are considered "In Scope"

CMMC SCOPE

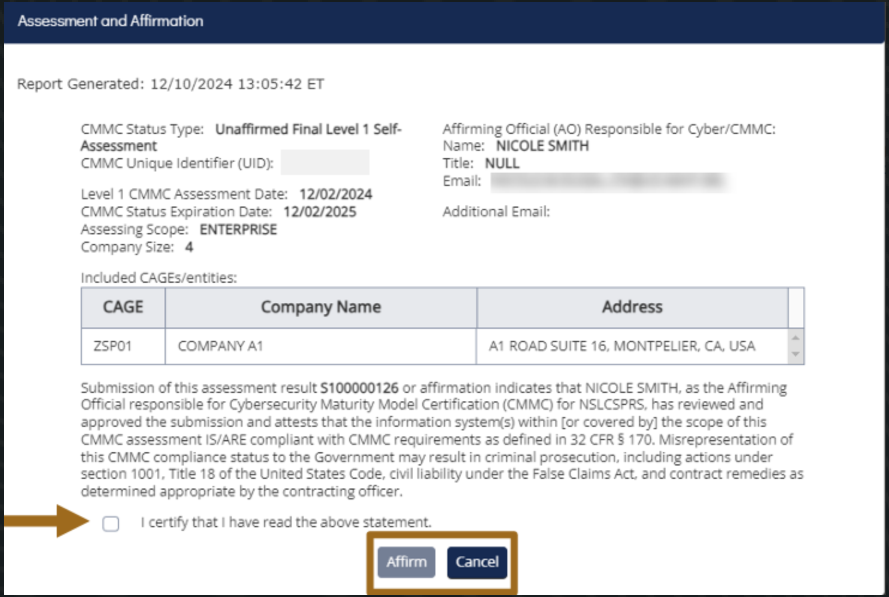
- When building out the CMMC scope, think about where the FCI/CUI will be stored physically, digitally, and who will be working with the data, or around it.
- The organization will often have a scope for FCI, and a completely different scope for CUI.
- People, Places, Systems
  - Process
  - Store
  - Transmit
- Scope Limitations
  - Logical separations: Firewalls, Virtual Local Area Networks (VLANs)
  - Physical separations: Gates, locks, badge access, guards, or air gapped systems.

ASSESSMENT FREQUENCY

- How often do you need to complete a level 1 assessment?
  - A self-assessment needs to be completed every year with an attestation submitted by the President/CEO.
    - Submitted to the Supplier Performance Risk System site.
- How often do you need to complete a level 2 assessment?
  - A self-assessment needs to be completed every year with an attestation submitted by the President/CEO.
    - Submitted to the Supplier Performance Risk System site.
  - A Certified Assessment completed by a C3PAO needs to be completed every 3 years, or upon any major change to the infrastructure.
    - Examples would be moving office locations, moving an enclave from cloud to on-prem.

CMMC LETTER OF ATTESTATION EXAMPLE

- When submitting your assessment and affirmation to the Supplier Performance Risk System, you will select who is the affirming official.
- https://www.sprs.csd.disa.mil
  - https://www.sprs.csd.disa.mil/videos/Tutorials/CMMCov/CMMCov.html



Assessment and Affirmation

Report Generated: 12/10/2024 13:05:42 ET

CMMC Status Type: **Unaffirmed Final Level 1 Self-Assessment**
CMMC Unique Identifier (UID):

Level 1 CMMC Assessment Date: **12/02/2024**
CMMC Status Expiration Date: **12/02/2025**
Assessing Scope: **ENTERPRISE**
Company Size: **4**

Affirming Official (AO) Responsible for Cyber/CMMC:
Name: **NICOLE SMITH**
Title: **NULL**
Email: [redacted]

Additional Email:

Included CAGEs/entities:

CAGE	Company Name	Address
ZSP01	COMPANY A1	A1 ROAD SUITE 16, MONTPELIER, CA, USA

Submission of this assessment result **S100000126** or affirmation indicates that NICOLE SMITH, as the Affirming Official responsible for Cybersecurity Maturity Model Certification (CMMC) for NSLCSPRS, has reviewed and approved the submission and attests that the information system(s) within [or covered by] the scope of this CMMC assessment IS/ARE compliant with CMMC requirements as defined in 32 CFR § 170. Misrepresentation of this CMMC compliance status to the Government may result in criminal prosecution, including actions under section 1001, Title 18 of the United States Code, civil liability under the False Claims Act, and contract remedies as determined appropriate by the contracting officer.

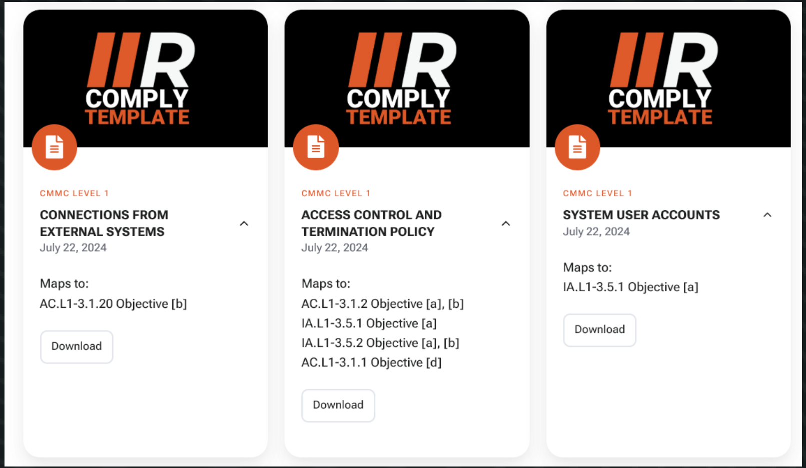
□ I certify that I have read the above statement.

WHAT IS NEEDED TO BECOME COMPLIANT?

- Give power to the CMMC readiness team
  - Executive leadership is ultimately responsible
- CMMC is a company-wide project, not just an IT project
  - Everyone is responsible for CMMC compliance
  - Every department will have their own role
  - CMMC is often a major culture change
- Company policy and procedure updates
  - Policies will need to be signed and in a final format(pdf) for the assessment
- System Security Plan
  - An assessment can't be completed without an SSP in place.

WHAT ARE THE RADICL FREE RESOURCES?

- CMMC quick-start toolkit
  - ○ Identify your needs
  - ○ Download templates
  - ○ Customize
  - ○ Implement



CMMC LEVEL 1

CONNECTIONS FROM EXTERNAL SYSTEMS

July 22, 2024

Maps to:
AC.L1-3.1.20 Objective [b]

CMMC LEVEL 1

ACCESS CONTROL AND TERMINATION POLICY

July 22, 2024

Maps to:
AC.L1-3.1.2 Objective [a], [b]
IA.L1-3.5.1 Objective [a]
IA.L1-3.5.2 Objective [a], [b]
AC.L1-3.1.1 Objective [d]

CMMC LEVEL 1

SYSTEM USER ACCOUNTS

July 22, 2024

Maps to:
IA.L1-3.5.1 Objective [a]

Q&A