February Tech Talk: CMMC is here!!

What You Must Do by March 15 and What's Coming Next

2/10/2026

John Bedford, TMM

Chris Wolfl, TMM

Ground Rules and Tips

Share With Your Colleagues and Network

- Sessions will be recorded and available on IAM Learning

Enhance Your Viewing Experience

- Toggle to “Speaker” View
- Microphones will be muted for this session

Make Connections:

- Share Comments and Questions in the Chat

IAM Antitrust Statement

- Discussions, comments, and presentations during IAM functions must not: (1) refer to any past, present, or future rates, prices or anything related thereto; (2) include any reference to marketing strategies that would reduce competition; (3) include any discussion of boycotts of any person, product, or firm; or (4) inhibit any member's employees from discussing employment with other member companies.

- If anyone feels like we are getting into an area we shouldn't be discussing based on the above statement, please interject, stop the conversation and we'll move on to a different topic.

Today’s Agenda

What are you seeing in the proposed DP3 Business Rules?

1. Introductions and Expectations
2. Why CMMC Exists and Why Movers Are Impacted
3. Understanding FCI vs CUI
4. CMMC Overview: Level 1 vs Level 2
5. CMMC Level 1 Control Families
6. Level 1 Controls Explained
   - Access Control
   - Identification & Authentication
   - Media Protection
   - Physical Protection
   - System & Communications Protection
   - System & Information Integrity
7. What Asserting Compliance Means and the March 15 Deadline
8. Subcontractors, Agents, and Flow-Down Responsibilities
9. Level 2 Preview and Planning Considerations
10. Wrap-Up and Questions

Introductions

John Bedford, VP Information Technology, TMM

John started with TMM in 2015 and has over 25 years of enterprise technology and leadership experience across regulated industries, including financial services, software, and over 10 years in logistics. He has held multiple certifications in technology, project management, and business continuity.

Chris Wolfl, Director Technical Services, TMM

Chris joined TMM in November 2025 with over 20 years of IT experience, a background in federal compliance frameworks since 1997, and more than a decade supporting multiple federal contract vehicles. He approaches compliance frameworks such as CMMC as a journey of maturity, helping organizations build practical foundations that support long-term security and compliance goals.

Expectations

This is NOT

- A technical deep dive
- Legal advice

This IS about

- Understanding the requirements
- Why we’re impacted
- What must be done

…and hopefully answering some of your questions.

Why CMMC Exists

- DoW developed framework based on NIST SP 800-171
- Published in the Code of Federal Regulations (CFR)
  - Codified in 32 CFR Part 170
  - It’s the law
- Sets foundational cybersecurity standards for the Defense Industrial Base (DIB)
- Required as a condition of contract award

Why the Moving Industry is in Scope

- Adopted for DP3 program in 2026 Tender of Service (Dec 2025)
- Formalizes/replaces “Information safeguarding requirements”
- Information provided by DPS falls under the protected status (FCI and CUI)
- Required as a condition of shipment award

The Clock is Real

Key Dates

- **March 15, 2026 (33 days)**
  Level 1 self-assessment due to receive shipment awards beginning May 15, 2026

*** Don't forget to provide your **CMMC UID from SPRS** to transcom.scott.tcj9.mbx.pp-quals@mail.mil*

- **March 15, 2027**
  Level 2 self-assessment due to receive shipment awards beginning May 15, 2027

Understanding FCI vs CUI

Federal Contract Information (FCI)

Defined as information, not intended for public release, which is provided by or generated for the U.S. Government under the terms of a service contract. Information created to deliver a service to the U.S. Government.

- **Shipment Locations**
  - Origin locations
  - Destination locations
- **Shipment Timing**
  - Pickup dates
  - Required Delivery Dates (RDD)
- **Contractual Service Data**
  - Information created to perform DP3 services
  - Non-public data generated under the Tender of Service

Understanding FCI vs CUI

Controlled Unclassified Information (CUI)

> Information that the U.S. Government creates or possesses, or that an entity creates or possesses on behalf of the U.S. Government, which requires safeguarding or dissemination controls as mandated by law, regulation, or U.S. Government-wide policy.

In practice this is primarily **personally identifiable information (PII)** of service members, DoW/USCG personnel, and their families

- **Personal Identifiers**
  - Service member, DoW, USCG, and family member names
- **Contact Information**
  - Origin and destination addresses
  - Personal and work phone numbers and/or email addresses
- **Identification Numbers**
  - Social Security Numbers (SSN)
  - DoD Identification Numbers (DoDID)
- **Shipment & Claims Information**
  - Household goods inventories (incl. photos, videos, and virtual surveys)
  - Claims documentation
  - Service member banking information

CMMC Framework Overview: Level 1 vs Level 2

Level 1

- 15 controls – 6 control families
- Protects FCI
- Annual self-attestation
- Completion by 03/15/2026

Level 2

- 110 controls – 14 control families
- Protects CUI
- Annual self-attestation (does NOT require a C3PAO)
- Completion by 03/15/2027

Level 1: Scoping

Consider the People, Technology, Facilities, and External Service Providers

- **People** – May include, but are not limited to, employees, contractors, vendors, and external service provider personnel.
- **Technology** – May include, but are not limited to, servers, client computers, mobile devices, network appliances (e.g., firewalls, switches, APs, and routers), VoIP devices, applications, virtual machines, and database systems.
- **Facilities** – May include, but are not limited to, physical office locations, satellite offices, server rooms, datacenters, manufacturing plants, and secured rooms.
- **External Service Provider (ESP)** – as defined in 32 CFR § 170.4, means external people, technology, or facilities that an OSA utilizes for provision and management of comprehensive IT and/or cybersecurity services on behalf of the OSA.

** CMMC Level 1 Scoping Guide*

Level 1: Control Families Overview

Six Buckets of Basic Cyber Hygiene

- Access Control (AC.1) – who can use systems
- Identification & Authentication (IA.1) – logins and passwords
- Media Protection (MP.1) – USB drives, laptops, PCs etc.
- Physical Protection (PE.1) – offices and facilities
- System & Communications Protection (SC.1) – basic network safety
- System & Information Integrity (SI.1) – keeping systems healthy

Level 1: Controls Explained

(17 Controls: NIST tells you what to secure, CMMC tells you how to demonstrate it and at what level.)

CMMC Practice	Short Name	NIST Description
AC.L1-3.1.1	Authorized Access Control	3.1.1 - Limit system access to authorized users, processes acting on behalf of users or devices.
AC.L1-3.1.2	Transaction & Function Control	3.1.2 - Limit system access to authorized transactions and functions.
AC.L1-3.1.20	External Connections	3.1.20 - Control connections to external information systems.
AC.L1-3.1.22	Control Public Information	3.1.22 - Control information posted or processed on publicly accessible systems.
IA.L1-3.5.1	Identification	3.5.1 - Identify system users, processes acting on behalf of users, and devices.
IA.L1-3.5.2	Authentication	3.5.2 - Authenticate identities before granting access to systems.
MP.L1-3.8.3	Media Disposal	3.8.3 - Sanitize or destroy media containing sensitive information before disposal or reuse.
PE.L1-3.10.1	Limit Physical Access	3.10.1 - Limit physical access to systems and facilities to authorized personnel.
PE.L1-3.10.3	Escort Visitors	3.10.3 - Escort visitors and monitor visitor activity.
PE.L1-3.10.4	Physical Access Logs	3.10.4 - Maintain logs of physical access to systems.
PE.L1-3.10.5	Manage Physical Access	3.10.5 - Manage physical access devices and mechanisms.
SC.L1-3.13.1	Boundary Protection	3.13.1 - Monitor, control, and protect communications at system boundaries.
SC.L1-3.13.5	Public-Access System Separation	3.13.5 - Separate publicly accessible systems from internal networks.
SI.L1-3.14.1	Flaw Remediation	3.14.1 - Identify, report, and correct system flaws in a timely manner.
SI.L1-3.14.2	Malicious Code Protection	3.14.2 - Provide protection from malicious code (e.g. malware).
SI.L1-3.14.4	Update Malicious Code Protection	3.14.4 - Update malware protection mechanisms as new releases become available.
SI.L1-3.14.5	System & File Scanning	3.14.5 - Perform periodic scanning and real-time scans for malicious content.

Level 1: Controls & How To Demonstrate Compliance

CMMC Practice	NIST Control	Short Name	Compliance Example
AC.L1-3.1.1	3.1.1	Authorized Access Control	Use Active Directory (AD) accounts; only assign user accounts to employees who need access. Maintain an access list.
AC.L1-3.1.2	3.1.2	Transaction & Function Control	Implement role-based permissions so only HR can access personnel files or finance can access invoices.
AC.L1-3.1.20	3.1.20	External Connections	Only allow VPN connections with MFA. Disable USB ports on sensitive workstations. Maintain a list of allowed external connections.
AC.L1-3.1.22	3.1.22	Control Public Information	Review the company website and cloud storage to ensure sensitive or FCI data is not publicly available.
IA.L1-3.5.1	3.5.1	Identification	Maintain unique user accounts in systems, don't use shared admin accounts. Log devices connecting to networks.
IA.L1-3.5.2	3.5.2	Authentication	Require passwords, PINs, or MFA before login. Document the authentication method in your policy.
MP.L1-3.8.3	3.8.3	Media Disposal	Physically shred or use certified wiping software on hard drives, USB drives, or paper with FCI. Keep a disposal log.
PE.L1-3.10.1	3.10.1	Limit Physical Access	Lock server rooms and sensitive offices. Issue keys/cards only to authorized staff. Keep a key/card access list.
PE.L1-3.10.3	3.10.3	Escort Visitors	Require visitors to sign in, wear badges, and be escorted in sensitive areas. Keep visitor logs.
PE.L1-3.10.4	3.10.4	Physical Access Logs	Use card readers or manual logs to track entry/exit. Retain logs for audit purposes.
PE.L1-3.10.5	3.10.5	Manage Physical Access	Regularly audit access cards, disable lost/stolen badges, and change door codes when staff leave.
SC.L1-3.13.1	3.13.1	Boundary Protection	Configure firewalls to only allow necessary traffic; log firewall events and review them periodically.
SC.L1-3.13.5	3.13.5	Public-Access System Separation	Keep web servers isolated from internal networks via VLANs or firewalls. Don't store internal files on public-facing servers.
SI.L1-3.14.1	3.14.1	Flaw Remediation	Apply operating system and application patches within 30 days of release. Track patching in a log.
SI.L1-3.14.2	3.14.2	Malicious Code Protection	Install antivirus/anti-malware software on all endpoints. Run daily scans.
SI.L1-3.14.4	3.14.4	Update Malicious Code Protection	Ensure anti-virus definitions are update automatically. Document last update date.
SI.L1-3.14.5	3.14.5	System & File Scanning	Schedule weekly full system scans and configure real-time scanning. Keep scan logs for review.

What Level 1 Compliance Looks Like Day-to-Day

- **Each employee has their own login**
  No shared accounts. You can tell who accessed what and when.
- **Access is removed when someone leaves or changes roles**
  Departing employees can't log back in later — intentionally or accidentally.
- **USB drives, PCs, and laptops are controlled**
  Company devices are tracked, protected, and not freely shared.
- **Visitors don't wander freely in offices**
  Guests are escorted; sensitive areas and systems aren't left unattended.
- **Antivirus and system updates are turned on**
  Devices automatically protect themselves against common threats.
- **Systems are monitored for problems or unusual behavior**
  Alerts from antivirus or systems are noticed and not ignored.
- **Issues are addressed in a reasonable timeframe**
  Infected machines, warnings, or errors are investigated and fixed.
- **Unauthorized changes are prevented or corrected**
  Employees can't install random software or change system settings without approval.

Submitting your self-assessment

To access SPRS and file your self-assessment

- TSPs should be registered in SAM.gov
- Confirm in SAM.gov
  - CAGE details and hierarchy
  - If multiple entities CAGE hierarchy should be set to define HLO
- Register in PIEE as a ‘SPRS Cyber Vendor User’ to secure SPRS credentials
  - This will require CAM approval
  - May need to submit request to or call PIEE helpdesk
  - Activate the user role(s)
- Access SPRS through PIEE
  - Select company CAGE
  - Complete your self-assessment in SPRS
  - Add and complete your assessment

What “Asserting Compliance” Means

- TSPs required to file a self-assessment asserting their compliance with CMMC Level 1 by March 15, 2026
- Security Requirement

  Defines the high-level control point (15 for level 1)
- Assessment Objectives

  A set of determination statements that altogether expresses the desired outcome of the security requirement
- Assessment Methods
  - Examine – review, inspect, observe assessment objects for understanding and clarification
  - Interview – discuss with individuals (IT security staff) for clarification of assessment objects
  - Test – exercise assessment objects to confirm expected outcome

What “Asserting Compliance” Means

- OSAs (TSPs) not expected to use all methods or deploy all assessment objects outlined in assessment guide
  - Flexibility to determine the level of effort
  - But, effort must support the determination that the requirement has been satisfied
- Assessment Findings
  - MET
  - NOT MET
  - NOT APPLICABLE
- Must be able to submit/check “MET” on ALL 15 security requirements

Subcontractors, Agents and Flow Down Responsibilities

- PCS JTF Personal Property Advisory ##26-0025A

  Subcontractor Compliance: TSPs will ensure all subcontractors and suppliers complete an affirmation of continuous compliance with the requirements applicable to the CMMC level required for the subcontract or other contractual instrument for each of the subcontractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the subcontract.

- TSP responsible for confirming flow down compliance
  - Request copy of CMMC 'Final Level 1' certification status (if a TSP)
  - Request copy of agent's security plan
  - Build into agent/comp agreement language
  - Add language to statement of work (BOL) for "one-off" agents

What's Next: Level 2 Preview and Planning

CMMC Level 2 incorporates 110 security requirements

- Includes the 15 requirements from level 1
- Protects CUI
- DP3 CUI data categorized as General Privacy (PRVCY) information
- Only requires annual self-assessment (not a C3PAO)
- Must assert compliance by March 15, 2027 for shipment awards beginning May 15, 2027
- Includes options for conditional compliance
  - Must meet 90 of the 110
  - Conditional certification (6 months)
  - POA&Ms

Helpful Resources

- Project Spectrum | Cybersecurity Readiness & Compliance - Project Spectrum

  A free resource for small to medium businesses (SMBs) looking to become CMMC Compliant, supported by the DoD Office of Small Business Programs.

- IAM CMMC Resource Center - IAM CMMC Resource Center - IAM

  A collection of curated guides, templates, and official DoD documentation

- Contact the IAM CMMC Working Group – cmmc@iamovers.org

QUESTIONS?