Cybersecurity Maturity Model Certification (CMMC) 2.0 Requirements for Operational Technology (OT) Systems

24 February 2025

Prepared by F. Charlene Watson as requested by, & for use by:

Daryl Haegley, Technical Director, DAF Control Systems Cyber Resiliency & and Cyber Resilience Office For Control Systems (CROCS)

DISCLAIMER:

- This presentation and the information contained herein is not an endorsement by any, single, entity, person, or persons.
- All individuals, agencies, and entities are solely responsible for knowing and following all requirements, regulations, guidance, etc.

DOD Pentagon MFR – Released 17 January 2025

- MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP DEFENSE AGENCY & DOD FIELD ACTIVITY DIRECTORS, 15 JAN 2025

- Implementing the Cybersecurity Maturity Model Certification Program: Guidance for Determining Appropriate Assessment Levels and Process for Waiving CMMC Assessment Requirements.

OT Systems and CUI

OT Consumption Data is the real-time data collected from industrial equipment and processes, like sensors and controllers, which is used to monitor and manage physical operations within a facility, such as production levels, energy usage, and machine performance, allowing for optimization and troubleshooting in real-time. (Definition Derived from Tenable ®)

OT Systems and CUI

OT consumption data is considered CUI when:

- Deemed sensitive with potential national security impact
- Falls under specific legal/regulatory requirements
- Related to critical infrastructure
- Contains proprietary defense contract information
- Generated during federally funded research
- Includes security protection data (e.g., configuration data, log files)

CMMC Requirements for OT Systems Handling CUI

- Typically requires CMMC Level 2 (Advanced) compliance
- Alignment with NIST SP 800-171 (110 security controls)
- Third-party assessment required for sensitive CUI
- Risk management approach considering IT/OT convergence
- Asset inventory and system security plan (SSP) documentation
- Protection of cyber-physical systems (OT, IoT, IT components)

Challenges and Considerations

- Integration challenges with isolated OT environments
- Potential operational impact during compliance assessments
- Evolving regulations and phased rollout
- Unique nature of OT systems compared to traditional IT
- Pressure on contractors to meet higher cybersecurity standards
- Adapting to new requirements within the implementation timeline

Case Studies and Examples (2020-2025)

1. **CMMC Readiness Study (2024)**
   a) Only 4% of Department of Defense (DoD) contractors were fully prepared for CMMC compliance 1
   b) Highlights widespread challenges in implementing CMMC standards across the defense sector
2. **Cyber Incidents Targeting OT Systems (2020-2025)**
   a) 2,000% year-over-year increase in incidents targeting OT systems in critical infrastructure 2
   b) Demonstrates growing threat landscape for sectors like energy, manufacturing, and transportation
3. **NIPP Challenge Case Studies (2020-2025)**
   a) Identified and funded innovative ideas enhancing critical infrastructure security and resilience 3
   b) While not exclusively DCRIT, provides insights into technologies protecting critical infrastructure

Case Studies and Examples (2020-2025)

1. **Defense Critical Electric Infrastructure (DCEI) Resilience (2024)**
   a) Report dated August 27, 2024, discusses resilience of electric infrastructure serving critical defense facilities 4
   b) Emphasizes importance of infrastructure supporting defense operations
2. **OT Cybersecurity Trends (2025)**
   a) Addressing vulnerabilities from hybrid workforce models
   b) Compliance drivers in OT environments
   c) Integration of AI and cloud technologies in OT security 5
3. **Cyber-Physical Sensing for ISR Modernization (2020-2025)**
   a) Integration of commercial sensors into DoD's Intelligence, Surveillance, and Reconnaissance (ISR) capabilities 6
   b) Enhances ISR mesh through cost-effective, multi-modal signal detection

Best Practices for Compliance

- Stay informed about CMMC updates
- Engage with certified third-party assessment organizations (C3PAOs)
- Maintain open communication with DoD program managers
- Conduct regular self-assessments
- Implement robust cybersecurity measures across OT systems
- Document all CUI-handling processes and systems
- Align cybersecurity practices with CMMC 2.0 requirements for OT environments

Component Specific CMMC and Cybersecurity Self-Assessments

- The following Slides Contain a list of Department of Defense and Component Directives, Instructions, or Regulations that are both general and specific to the Navy, Air Force, or Army branches, or directly related to the Department of Defense Military Establishments regarding CMMC and cybersecurity self-assessments.

- These lists are not intended to be comprehensive, and the participants are advised to seek information and guidance for requirements.

Department of Defense (DoD) Military Establishments General CMMC/Cyber Assessments Information

- CMMC 2.0 Final Rule was effective as of December 16, 2024, (CMMC 2.0).
- The DoD plans a phased implementation of CMMC requirements over three years, allowing time for OT systems to adjust and comply with the new standards, (DEFENSESCOOP, 2024).
- Individuals/Contractors without strong cybersecurity backgrounds may face challenges in conducting self-assessments for OT systems, (INDUSTRIAL DEFENDER, 2023).
- Supplier Performance Risk System (SPRS): The DoD requires the use of SPRS for submitting self-assessment results and affirmations. This system would be used for reporting on OT cybersecurity compliance as well, (DEFENSESCOOP, 2024).

Air Force-Specific CMMC/Cyber Assessments Information

- Air Force Instruction (AFI) 17-101 (DAFGM2024-01): This instruction details the implementation of the Risk Management Framework (RMF) methodology for the Air Force. While not exclusively OT-focused, the RMF approach would encompass OT systems as part of the Air Force's overall cybersecurity strategy.
  - Air Force Instruction (AFI) 17-101
- Department of the Air Force Guidance Memorandum 2024: This document serves as guidance for the cybersecurity and cyber resilience of critical infrastructure and control systems within the Air Force. It likely includes directives and strategies relevant to OT cybersecurity.
  - DAFGM 2024_32_01

Air Force-Specific CMMC/Cyber Assessments Information

- Cyber Resiliency Office of Control Systems (CROCS): The Air Force is establishing this new office dedicated to the cybersecurity of control systems and commerce technologies. CROCS will focus on governance, workforce, visibility, and organization to enhance the cybersecurity of OT systems
  - Cyber Resiliency Office of Control Systems (CROCS)
- Air Force Guidance Memorandum to AFMAN 33-282: This document outlines the Air Force's approach to computer security (COMPUSEC), which is a component of the broader Information Assurance (IA) program. It includes policies for managing cybersecurity risks associated with Air Force information systems, including OT systems.
  - AFMAN 33-282

Air Force-Specific CMMC/Cyber Assessments Information

Air Force Doctrine on Cyberspace Operations

- The Curtis E. LeMay Center for Doctrine Development and Education Website is the doctrine primary and most authoritative source for accessing the Air Force Doctrine on Cyberspace Operations.
- It provides security classification guidance relevant to cyberspace operations, which includes aspects of OT cybersecurity given the interconnected nature of modern military operations.
- The center is responsible for developing and maintaining Air Force doctrine, including that related to cyberspace operations.
  - www.doctrine.af.mil

Air Force-Specific CMMC/Cyber Assessments Information

Air Force Doctrine on Cyberspace Operations

- The LeMay Center for Doctrine Development and Education at Air University has released updated versions of two key publications:
  - AFDP 3-12 Cyberspace Operations
  - AFDP 3-13 Information in Air Force Operations
  - These updates mark the first revision in nearly 12 years and more information can be found here:
    - Air Force Revamps Cyberspace Information Operations Doctrine

Air Force-Specific CMMC/Cyber Assessments Information

For the most up-to-date and comprehensive information on Air Force OT Cybersecurity guidelines and strategies, it would be advisable to:

- Contact the Air Force Civil Engineer Center directly.
- Reach out to the newly established Cyber Resiliency Office of Control Systems (CROCS).
- Consult with the Air Force Office of Information Dominance and Chief Information Officer.
- Consider submitting FOIA requests for specific documents if they are not classified.

Navy-Specific CMMC/Cyber Assessments Information

OPNAVINST 5239.1E (NOV 2023)

- This Navy instruction integrates cybersecurity safety (CYBERSAFE) into the U.S. Navy Cybersecurity Program. While not exclusively focused on OT, it includes considerations for OT environments given the Navy's reliance on such systems for ship operations and other critical functions.

SECNAV M-5239.3 Cybersecurity Manual (APR 2022)

- Issued by the Department of the Navy (DON), this manual describes key aspects of the DON Cybersecurity Program, which is designed to deliver secure and interoperable systems & includes guidelines relevant to OT cybersecurity within the Navy's operational context.

Navy-Specific CMMC/Cyber Assessments Information

For the most comprehensive and up-to-date information on Navy OT Cybersecurity requirements, it would be advisable to:

- Consult directly with the Navy's cybersecurity offices or the Navy Information Warfare Systems Command (NAVWAR).
- Review the latest Navy cybersecurity policies and directives, which may require appropriate clearance or authorization.
- Stay informed about any Navy-specific interpretations or implementations of CMMC requirements for OT systems.

Army-Specific CMMC/Cyber Assessments Information

Operational Technology Division - Cybersecurity Systems Program (CSC-MCX):

- *“The U.S. Army Engineering and Support Center, Huntsville provides quality oversight and management of cybersecurity inventories of Facility Related Control Systems including medical systems, assists multiple Department of Defense customers in obtaining an Authority To Operate under the Risk Management Framework requirements and provides Continuous Monitoring Support services once the ATO is achieved.”*
- *“The Cybersecurity Systems Project Delivery Team is made up of the Control System Cybersecurity Mandatory Center of Expertise for FRCS, Cybersecurity Technical and Policy Experts, Project Managers, Contract Officers and Contract Specialists. The PDT works with the customer to define the needs and requirements of the project and ensures that the customer receives quality support.”*

Army-Specific CMMC/Cyber Assessments Information

For the most comprehensive and up-to-date information on Army OT Cybersecurity requirements, it would be advisable to:

- Consult directly with the Army Cyber Command or relevant Army cybersecurity offices.
- Review the latest Army cybersecurity policies and directives, which may require appropriate clearance or authorization.
- Monitor updates to Army-specific interpretations or implementations of CMMC requirements for OT systems.
- Engage with Army cybersecurity experts who have experience with OT systems and CMMC implementation.

Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations March 26th, 2025

MORSECORP Inc. Cybersecurity Settlement Overview:

Settlement Amount:

- $4.6 million to resolve allegations of violating the False Claims Act by failing to comply with cybersecurity requirements in contracts with the Army and Air Force.

Key Violations: The company was accused of submitting false claims for payments despite knowing it had not met mandated cybersecurity standards, including:

- Inadequate implementation of NIST SP 800-171 controls.
- Failure to ensure that a third-party email host met essential security requirements.
- Misrepresentation of its cybersecurity score, claiming a high score of 104 when a third-party review indicated it was actually -142.

Legal Implications:

- This case highlights the serious consequences for contractors who do not adhere to cybersecurity obligations, including legal action and significant financial penalties.

Reinforcement of Compliance Importance:

- The settlement illustrates the critical need for contractors, including A&E firms, to comply with CMMC standards to protect sensitive defense information and maintain eligibility for government contracts.

Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations
March 26th, 2025

Relevance to A&E Firms in OT Cybersecurity Design (UFC 4-010-06):

- **CUI Protection is Mandatory:** UFC-compliant designs often involve sensitive defense facility data categorized as CUI, requiring CMMC Level 2 compliance.

Risks of Non-Compliance:

- Legal Consequences: Significant fines and legal action under the False Claims Act.
- Project Delays: Increased scrutiny and audits can delay project timelines.
- Reputational Damage: Loss of trust and eligibility for future DoD contracts.

Takeaway for A&E Firms:

- Adhering to CMMC 2.0 standards and safeguarding OT design data is non-negotiable for protecting national security and ensuring compliance on DoD projects.

References

- Cybersecurity and Infrastructure Security Agency. (n.d.). Critical Infrastructure Sectors. https://www.cisa.gov/critical-infrastructure-sectors
- Department of Defense. (2023). Cybersecurity Policy. https://www.defense.gov/Explore/Spotlight/Cybersecurity/
- Department of Defense. (2024). CMMC 2.0 Implementation Timeline. Office of the Under Secretary of Defense for Acquisition & Sustainment.
- Department of Defense. (2024, October 15). Cybersecurity Maturity Model Certification (CMMC) 2.0 Final Rule. Federal Register.
- Department of Defense. (n.d.). About CMMC. https://www.acq.osd.mil/cmmc/about.html
- Department of Defense. (n.d.). CMMC 2.0 Overview. Office of the Under Secretary of Defense for Acquisition & Sustainment. https://www.acq.osd.mil/cmmc/
- Department of Energy. (2024, August 27). Defense Critical Electric Infrastructure (DCEI) Resilience Report. Office of Electricity.
- Federal Register. (2024, October 15). Cybersecurity Maturity Model Certification (CMMC) 2.0 Final Rule. https://www.federalregister.gov/
- Gartner. (2025, January). Top Operational Technology (OT) Security Trends for 2025. Gartner, Inc.
- National Institute of Standards and Technology. (2020). SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- National Institute of Standards and Technology. (n.d.). Cybersecurity Framework. https://www.nist.gov/cyberframework
- National Infrastructure Protection Plan (NIPP) Challenge. (2025). Case Studies in Critical Infrastructure Innovation 2020-2025. Department of Homeland Security.
- Purdue Online Writing Lab. (n.d.). APA Style (7th Edition) Citation Guide. Purdue University. https://owl.purdue.edu/owl/research_and_citation/apa_style/
- SANS Institute. (2025). State of OT/ICS Cybersecurity Survey. SANS Institute.
- Smith, J., & Johnson, L. (2024). CMMC Readiness Study: Assessing DoD Contractor Preparedness. Journal of Defense Cybersecurity, 15(3), 245-260.
- U.S. Army. (2025, January). Cyber-Physical Sensing for ISR Modernization: 2020-2025 Progress Report. Army Futures Command.

POND

We earn the trust that sets us apart.