AM GENERAL™
MISSION READY ★ FUTURE DRIVEN

Subcontractor Cybersecurity Compliance Guide

Contents

Change Log

Date	Description	Responsible
7/18/2024	Initial Release	A. Kassa
8/6/2024	Minor clarification to subcontractor requirements	A. Kassa
11/15/2024	Update to reflect CMMC 2.0 final rulemaking	A. Kassa
6/25/2025	Regulatory and requirement updates/clarifications	A. Kassa
8/19/2025	Additional resource links added	A. Kassa
10/27/2025	Updated guide to reflect November 10th date for CMMC to be added to contracts	A. Kassa

WHAT IS NIST COMPLIANCE?

- **What it is:** NIST Compliance refers to adhering to the security requirements outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 revision 2, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations." This NIST SP provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI). DoD contractors and subcontractors that handle CUI must comply with these standards as mandated by the Department of Defense (DoD) through the Defense Federal Acquisition Regulation Supplement (DFARS). Note that while revision 2 has been superseded by NIST 800-171 r3, CMMC and DFARS mandate compliance with NIST 800-171 r2 until a future date that will be determined by the DoD.

- **Purpose:** The purpose of NIST compliance for DoD contractors and subcontractors is to safeguard Controlled Unclassified Information (CUI). CUI is sensitive information that is not classified but could be detrimental to national security if disclosed or misused. By implementing these security controls, DoD aims to:
  - Reduce the risk of cyberattacks on contractor systems that store or process CUI.
  - Ensure the confidentiality, integrity, and availability of CUI.
  - Standardize cybersecurity practices across the DoD supply chain.

  - **Key Points:**
  - **DFARS Clauses:** DoD enforces NIST compliance through DFARS clauses 252.204-7012 and 252.204-7020. These clauses require contractors to:
    - Implement the security requirements in NIST SP 800-171 r2.
    - Flow down the NIST compliance requirement to subcontractors that handle CUI.
    - Undergo CMMC assessments at a designated level (Basic, Medium, or High) depending on the contract and the sensitivity of the CUI.
    - Rapidly report cyber incidents directly to the DoD (requirements are outlined in a separate section below).
  - **Focus on CUI:** NIST SP 800-171 r2 outlines a comprehensive set of security controls, but DoD contractors only need to implement those controls relevant to protecting CUI within their systems.
  - **Continuous Process:** NIST compliance is an ongoing process. Contractors need to maintain their security controls, update them as needed, and address any identified security vulnerabilities.

CMMC (CYBERSECURITY MATURITY MODEL CERTIFICATION):

- **What it is:** The Cybersecurity Maturity Model Certification (CMMC) 2.0 is a mandatory program established by the Department of Defense (DoD) to validate the level of maturity of contractors and sub-contractor’s cybersecurity programs based on NIST 800-171 r2 Controls. It implements a tiered structure so that the more sensitive data a DoD program has, the higher level of validation is required to ensure FCI and CUI are protected.

- **Purpose:** While Cybersecurity controls have long been required by DFARS 252.204-7012, DoD has found that real-world implementation of the controls is far from complete. Lacking the resources to assess the readiness of every contractor and sub-contractor - DoD has adopted CMMC, including the strategy to use third-party assessment organizations to do the validation that these requirements are being met.

- **Key Points:**
- **Regulatory Mandate:** CMMC 2.0 is a mandatory requirement for DoD contractors and subcontractors. The specific CMMC level required is determined by the type and sensitivity of data handled and is specified in DoD solicitations and contracts (e.g., through DFARS 252.204-7021).
- **Tiered Maturity Model:** CMMC 2.0 streamlines the previous framework into three distinct maturity levels, providing progressively advanced cybersecurity requirements:
    - **Level 1: Foundational Cyber Hygiene**
    - **Level 2: Advanced Cybersecurity**
    - **Level 3: Expert Cybersecurity**
- **NIST Alignment:** CMMC 2.0 is directly aligned with existing and widely accepted cybersecurity standards, significantly leveraging National Institute of Standards and Technology (NIST) Special Publications.
- **Assessment and Certification:** Depending on the CMMC level and contract type, certification requires either an annual self-assessment or a triennial independent assessment and certification by a CMMC-approved Certified Third-Party Assessment Organization (C3PAO). Subcontractors who are certified by a C3PAO will still need to complete an annual self-attestation between their triennial C3PAO assessments. Both types of assessment are conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology.
- **Focus on Security Practices and Processes:** CMMC emphasizes not just the implementation of security controls but also the establishment and maturity of security processes.

Understanding CMMC Levels for Subcontractors:

For most AM General Subcontractors, the focus will be on CMMC Levels 1 and 2:

- **CMMC Level 1: Foundational (Protecting Federal Contract Information - FCI)**
    - **Scope:** Applies to organizations that handle Federal Contract Information (FCI), which is information not intended for public release but not critical to national security (e.g., contract numbers, project timelines, etc.).
    - **Requirements:** Encompasses 15 basic cybersecurity practices derived from FAR 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems." These are fundamental cyber hygiene practices.

    - **Assessment:** Requires an **annual self-assessment uploaded to SPRS**. Organizations must document their compliance and have a senior official affirm compliance annually. The results are to be entered into the Subcontractor Performance Risk System (SPRS).
    - **POA&Ms:** Plans of Action & Milestones (POA&Ms) are generally **not permitted** for Level 1, meaning all controls must be fully implemented at the time of assessment.
- **CMMC Level 2: Advanced (Protecting Controlled Unclassified Information - CUI)**
    - **Scope:** Applies to organizations that process, store, or transmit Controlled Unclassified Information (CUI). CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.
    - **Requirements:** Aligns directly with all 110 security requirements outlined in **NIST SP 800-171 r2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."**
    - **Assessment:**
        - For acquisitions involving CUI, a **third-party assessment** by a C3PAO is required **every three years**. The results are entered into the CMMC Enterprise Mission Assurance Support Service (eMASS).
    - **POA&Ms:** Limited use of POA&Ms is permitted for some non-critical controls, provided they are closed out within 180 days. Specific critical requirements cannot be included in a POA&M. The definition of which controls can be included in a POA&M is provided in the NIST SP 800-171 DoD Assessment Methodology
- **CMMC Level 3: Expert (Protecting High-Priority CUI against Advanced Persistent Threats)**
    - **Scope:** For organizations handling high-priority, sensitive CUI, particularly those supporting critical DoD programs.
    - **Requirements:** Builds upon CMMC Level 2 requirements by adding a subset of advanced cybersecurity practices from **NIST SP 800-172**.
    - **Assessment:** Requires a **government-led assessment** by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every three years.

Regulatory Alignment & Timeline:

- **Final Rule Effective Date:** The CMMC Program final rule (32 CFR Part 170) became effective on **December 16, 2024**.
- **Contractual Implementation:** As part of the phased implementation outlined in 32 CFR Part 170, the Department of Defense (DoD) will start incorporating Cyber Maturity Model Certification (CMMC) 2.0 compliance requirements into select solicitations. **This change, which officially begins November 10, 2025,** will be executed by revising the DFARS 252-204-7021 clause. CMMC 2.0 requirements will also be added to select existing contracts through modification.

- **Phased Rollout:** CMMC requirements will be incorporated into DoD solicitations and contracts in a phased approach, beginning with high-priority contracts in Fiscal Year 2026, starting on November 10, 2025. Full implementation across all applicable contracts is expected by 2028. This means mandatory third-party assessments could begin sometime in 2025 or 2026 for relevant contracts.

NIST SP 800-171 r2 forms the critical foundation for CMMC. All the security controls outlined in NIST 800-171 r2 are directly incorporated into CMMC Level 2 requirements.

CMMC builds upon NIST 800-171 r2 by ensuring its implementation via mandatory third-party assessment.

Organizations already working towards or compliant with NIST 800-171 r2 will find their efforts directly contribute to CMMC Level 2 compliance. Leveraging existing NIST 800-171 r2 efforts is an excellent starting point for CMMC readiness.

Stay Informed: It is crucial to stay updated on the DoD's announcements and guidance regarding the CMMC implementation timeline and specific contract requirements. Regularly check the DoD's official CMMC website and associated resources for the latest information and updates- Chief Information Officer > CMMC. Engage with AM General to understand our specific CMMC expectations and timelines if you are a subcontractor.

Here's an analogy: Think of NIST 800-171 as a recipe book with various security measures and requirements as ingredients and their specific measurements. CMMC is the third-party validation that ensures all of the correct ingredients are there, in the correct measurements, and cooked in such a way that results in a well-rounded and complete dish.

SUPPLIER REQUIREMENTS (WHERE DFARS 252.204-7012 and 7020) ARE INCLUDED AS A CONTRACTUAL FLOWDOWN):

a) In accordance with NIST SP 800-171 r2, all Subcontractors with whom we exchange CUI are required to complete the following:

1.) *Site Security Plan (SSP)*

2.) *Self-assessment conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology, with score generated.*

3.) *Score uploaded to SPRS system.*

4.) *Written confirmation that self-assessment score is uploaded to SPRS system via the annual representations and certifications document.*

5.) *Plan of Action & Milestones (POA&M)*

b) **Subcontractors must indicate that they have completed the self-assessment and uploaded their score to SPRS or confirm they will comply with the requirement and provide an estimated date of completion on AM General's Annual Reps & Certs document (1ZF4001) to be eligible to receive an RFP or RFQ.**

c) **All <u>Subcontractors with whom we exchange CUI must have a self-assessment score uploaded to SPRS prior to a business award.</u>**

Please Note: Uploading a self-assessment score to the Supplier Performance Risk System (SPRS) is a minimum requirement to receive RFQs that involve Controlled Unclassified Information (CUI). While uploading a score on the SPRS demonstrates your current cybersecurity posture, it alone does not guarantee compliance with CMMC 2.0 requirements. Subcontractors should have an SSP and POA&M in place to address gaps in preparation for CMMC level 2 certification. Any Subcontractors handling FCI are required to meet the 15 minimum security control requirements as outlined in FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems) and in alignment with CMMC Level 1.

For business continuity and/or access to new business opportunities, the process is as follows:
NIST SP 800-171 Implementation → Self-attestation → Third Party Assessment

For resources to help you implement these controls, please visit the CMMC website:
https://cyberab.org/

SUPPLIER REQUIREMENTS (WHERE DFARS 252.204-7021 IS INCLUDED AS A CONTRACTUAL FLOWDOWN):

a) **Level 1: Foundational (Federal Contract Information)**

Applies to: Suppliers handling Federal Contract Information (FCI).

Requirements:

- Implement **15** basic security practices aligned with **FAR Clause 52.204-21**.
- Complete an **Annual Self-Assessment** of compliance.
- A senior company official must **annually affirm** compliance in the DoD's Supplier Performance Risk System (SPRS).
- **No Plan of Action and Milestones (POA&Ms)** are permitted; all 15 practices must be fully implemented.
- The subcontractor must confirm compliance with Level 1 requirements via AM General's annual representations and certifications form.

b) **Level 2: Advanced (Controlled Unclassified Information)**

Applies to: Suppliers handling Controlled Unclassified Information (CUI).

Requirements:

- Implement all **110** security requirements specified in **NIST SP 800-171 r2**.

- Maintain a **System Security Plan (SSP)** and a **POA&M** document.
- **Assessment is contract-dependent:**
  - **Critical CUI:** Requires a formal, triennial assessment by a Certified Third-Party Assessor Organization (C3PAO).
  - **Non-Critical CUI:** Permits an annual self-assessment uploaded to SPRS.
- POA&Ms are **permitted** for certain controls but must be closed out, either by the C3POA or documented as part of an updated self-assessment, within **180 days**.
- A senior company official must **annually affirm** compliance in SPRS.
- The subcontractor must confirm compliance with Level 2 requirements via AM General's annual representations and certifications form and provide us with a copy of your valid certification.

c) Level 3: Expert (Critical CUI/Advanced Persistent Threats)

Applies to: Suppliers handling CUI for the DoD's highest priority programs.

Requirements:

- Implement all **110 NIST SP 800-171** controls **plus 24 enhanced security controls** selected from **NIST SP 800-172**.
- Requires a **Government-Led Assessment** by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every **three years**.
- Achieving CMMC Level 2 is a **prerequisite**.
- POA&Ms are **permitted only** for the original 110 NIST 800-171 controls (with a 180-day deadline), but **not** for the 24 additional NIST 800-172 controls.
- A senior company official must **annually affirm** compliance in SPRS.

The subcontractor must confirm compliance with Level 2 requirements via AM General's annual representations and certifications form and provide us with a copy of your valid certification.

Cyber Incident Reporting Requirements

This section outlines the cyber incident reporting requirements for all subcontractors supporting AMG contracts that involve Controlled Unclassified Information (CUI) or Covered Defense Information (CDI), or that provide operationally critical support. These requirements are mandated by Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012.

1. Cyber Incident Definition and Reporting Timeline

- A "cyber incident" means actions taken using computer networks, to include cloud computing, that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

- Subcontractors are required to **rapidly report** cyber incidents impacting DoD contract performance **directly to the DoD** via https://dibnet.dod.mil/portal/intranet/. "Rapid reporting" means any cyber incident must be reported **within 72 hours of discovery**.

2. Required Submissions

When a cyber incident occurs, the entity that suffered the incident (e.g., the subcontractor) must submit the following to the Government as outlined in DFARS 252.204-7012:

- A cyber incident report.
- Malicious software, if detected and isolated, as required by DFARS 252.204-7012(d).
- Images of all known affected information systems and all relevant monitoring/packet capture data. (These images must be preserved and protected for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.)

3. DoD-Approved Medium Assurance Certificate

Prior to reporting cyber incidents to the DoD website, subcontractors must have or acquire a DoD-approved medium assurance certificate. More information on obtaining this certificate is available at: https://public.cyber.mil/eca/

4. Notification to AMG

In the event of a cyber incident experienced by a Subcontractor, AMG requires its Subcontractor to:

- Notify the DoD of the cyber incident as required by DFARS 252.204-7012(c).
- Provide your AMG buyer with the incident report number assigned in the DoD reporting system.

KEY TAKEAWAYS AND BEST PRACTICES:

Understanding and Alignment:

- **Identify FCI and/or CUI Flow:** First, understand if your work with the AM General involves handling FCI and/or Controlled Unclassified Information (CUI). Work with your AM General Buyer to confirm if FCI and/or CUI will be shared during procurement and during the period of contract performance. If you will not receive or handle FCI and/or CUI, CMMC certification may not be required.
- **Review Contract Requirements:** Carefully examine the subcontract to determine the specific CMMC level required by the AM General. This will dictate the rigor of your security controls and which level you will need to align your efforts with (Level 1,2 or 3).
- **Align with AM General:** Coordinate with the AM General on our CMMC compliance strategy. This ensures alignment in controls and reduces redundancy in efforts.

Self-Assessment and Gap Analysis:

- **NIST SP 800-171 r2 Baseline:** Since CMMC builds upon NIST SP 800-171 r2, assess your current cybersecurity posture against the NIST controls. Utilize resources like NIST Self-Assessment guides and tools for support. Links to these resources can be found in the "Additional Resources" section at the end of this guide.
- **Gap Analysis:** Identify any gaps between your existing controls and the required CMMC level. Prioritize these gaps based on severity and ease of implementation.

Implementation and Improvement:

- **Develop a System Security Plan (SSP):** Create a documented plan outlining your security controls and procedures to address the identified gaps. A template can be found at: https://csrc.nist.gov/files/pubs/sp/800/171/r2/upd1/final/docs/cui-ssp-template-final.docx
- **Implement Security Controls:** Address the gaps by implementing the necessary security controls as outlined in NIST SP 800-171 for your required CMMC level.
- **Focus on People, Processes, and Technology:** Enhance your cybersecurity posture across all aspects - train employees on security practices, establish clear security policies, and invest in appropriate security tools.

Additional Tips:

- **Seek Professional Guidance:** Consider engaging a Registered Practitioners Organization (RPO) for support with gap analysis, control implementation, and overall CMMC readiness. They can be found in the CMMC Marketplace on cyberab.org.
- **Leverage Resources:** Utilize resources from the CMMC Accreditation Body (CMMC-AB) marketplace, DoD CMMC website, and relevant industry associations.
- **Start Early:** The CMMC implementation timeline can be lengthy (typically 6 – 18 months). Starting early allows for a smoother and less stressful certification process.

FREQUENTLY ASKED QUESTIONS (FAQs):

1.) I am selling commercial items to AM General, am I exempt from these requirements?

a) Possibly. If you are providing Commercial Off-The-Shelf (COTS) items, per the definition in FAR 2.101, you are exempt. Please complete the Subcontractor Assertion of Commerciality - 1ZF2003 *(buyer should provide a copy of the template to complete*)

b) If you are providing commercial items to AM general (outside of COTS) requirements may depend on the relevant program security classification guide.

2.) I have completed the AM General FAR/DFARS Reps & Certs, but my company is not NIST compliant, what next steps should I take?

I. Obtain self-assessment score by completing the "survey" through the NIST Readiness Assessment Tool on the following website: Project Spectrum (FREE RESOURCE)

Subcontractors are not required to complete their self-assessment through Project Spectrum. This is a free resource, but you are welcome to choose whatever method you deem to be best aligned with your needs and will fulfill the *requirement.*

II. **Upload score to [Supplier Performance Risk System (disa.mil)]**

- **PLEASE NOTE:** You must be registered at SAM.gov and have an active CAGE code (assigned through SAM registration) to register in the SPRS system.
- **Follow the quick entry guide available on the SPRS site to register in PIEE and gain access to SPRS to upload your score:** SPRS NIST SP 800-171 Quick Entry Guide (disa.mil)

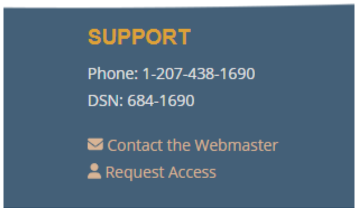
III. **Once complete, provide written confirmation that your organization's score is uploaded in SPRS.**

- A new assessment should be completed and uploaded every (3) years.

3.) I have tried to submit my scores, but I am having technical issues logging into SPRS. What should I do?

PLEASE NOTE: You must be registered in SAM.gov and have an active CAGE code (assigned through SAM registration) to register in the SPRS system where you will upload your company's score.

SPRS FAQs and Support: Follow link for FAQs (SPRS - Frequently Asked Questions (disa.mil)) and scroll to bottom left hand of page to contact SUPPORT.



SUPPORT

Phone: 1-207-438-1690

DSN: 684-1690

Contact the Webmaster

Request Access

PIEE Customer Support
Email: disa.global.servicedesk.mbx.eb-ticket-requests@mail.mil
Phone: 866-618-5988
Fax: 801-605-7453
Help Desk Hours: Monday-Friday 0630-2400 EST
Supplier Performance Risk System (SPRS)
PIEE
Email: webptsmh@navy.mil
Phone: 207-438-1690
DSN: 684-1690

4.) What level of CMMC Certification will I be required to achieve?

CMMC 2.0, the current iteration of the Cybersecurity Maturity Model Certification program, defines three levels of cybersecurity maturity that contractors must meet based on the type of information they handle in DoD contracts:

Level 1: Safeguarding FCI (Federal Contract Information)

- Focuses on basic cyber hygiene practices to protect Federal Contract Information (FCI).
- FCI is unclassified information that is not publicly releasable but could be harmful if mishandled.
- Leverages existing safeguard requirements outlined in FAR clause 52.204-21.
- Self-assessment is typically the primary method for demonstrating compliance at this level.

Level 2: Protecting CUI (Controlled Unclassified Information)

- Addresses a broader range of security controls compared to Level 1.
- Aims to safeguard Controlled Unclassified Information (CUI), which is sensitive but unclassified data that could be detrimental if disclosed.
- Aligns with the security requirements outlined in NIST SP 800-171 r2, a well-established cybersecurity standard.
- Depending on the criticality of the CUI and contract requirements, compliance might involve a self-assessment or a third-party assessment by an approved CMMC assessor.

Level 3: Addressing Advanced Persistent Threats (APTs)

- The most stringent level, designed for protecting highly sensitive CUI and programs critical to national security.
- Requires robust security controls to defend against sophisticated cyberattacks from Advanced Persistent Threats (APTs).
- Leverages a subset of controls from NIST SP 800-172, a more demanding cybersecurity standard focused on high-risk systems.
- Assessments for Level 3 are currently planned to be conducted by government officials.

Key takeaway: The level of CMMC certification a subcontractor needs depends on the type of information they handle in the DoD contract, as specified by the AM General. Level 1 focuses on basic protection, Level 2 covers a broader range for CUI, and Level 3 addresses the most sensitive information and advanced threats. As you work through your preparations for CMMC Certification, please work with your AM General buyer to make sure your approach is aligned with the type of sensitive information you are handling.

Urgent Notice on Certification: C3PAOs currently face a backlog. To avoid contract ineligibility, suppliers handling CUI must immediately begin engaging a C3PAO after meeting the necessary requirements. Find accredited C3PAOs on the CyberAB's Marketplace - CyberAB > Directory

5.) **I am a small to medium sized business and there are potentially high costs associated with me upgrading my cybersecurity competencies and protocols to meet DoD requirements. What options are out there for me?**

There are several resources, paid and free, which provide support to companies pursuing NIST compliance/CMMC Certification. There are also grants/funding available to small/medium enterprises, which vary by State/Region.

APEX Accelerators is a great resource that can help connect you with the right support your organization may need to help you with your NIST SP 800-171 Compliance/CMMC 2.0 certification journey. Go to the bottom of their main webpage to find a branch nearest to you.

ADDITIONAL RESOURCES:

- **NIST Special Publication 800-171 revision 2**: This is the core document outlining the security requirements for protecting CUI. See link to the NIST website where you can download this version: SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | CSRC
- **NIST Cybersecurity Framework (CSF)**: While not a mandatory requirement, the NIST Cybersecurity Framework provides a helpful guide for organizations to improve their overall cybersecurity posture. It can be a good resource for Subcontractors to use in conjunction with NIST SP 800-171. https://www.nist.gov/cyberframework
- **DoD CMMC Resources:** The DoD CMMC website provides a variety of resources for contractors on the CMMC program, including frequently asked questions (FAQs), training materials, and implementation guides. About CMMC
- **DLA JCP**: The JCP was established in 1985 to allow United States (U.S.)/Canadian contractors to apply for access to Department of Defense/Department of National Defense (DOD/DND) unclassified export controlled technical data/critical technology on an equally favorable basis in accordance with DODD 5230.25, “Withholding of Unclassified Technical Data and Technology from Public Disclosure,” and Canadian Technical Data Control Regulations. https://www.dla.mil/Logistics-Operations/Services/JCP/
- **Defense Industrial Base (DIB) Cybersecurity Portal:** https://dibnet.dod.mil/dibnet/#resources
- CyberAB's Marketplace: CyberAB > Directory