NIST SP 800-171 & CMMC LEVEL 2 ASSESSMENT SCOPING

NIST SP 800-171 Scope of Applicability[1]	Controlled Unclassified Information (CUI) Components "Components of nonfederal systems that process, store, or transmit CUI"[2]			Security Protection Components "Components of nonfederal systems that provide security protection for CUI components"[2]		Out-of-Scope "Components where isolation techniques have been applied"[2]
CMMC Level 2 Assessment Scope Asset Category	**CUI Assets** "Assets that process, store, or transmit CUI"	**Contractor Risk Managed Assets** "Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place. Assets are not required to be physically or logically separated from CUI assets"	**CUI Specialized Assets[3]** "Assets that may…process, store, or transmit CUI. Assets include government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment"	**Security Protection Assets** "Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI"	**Security Protection Specialized Assets[3]** "Assets that may…not process, store, or transmit CUI. Assets include government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment"	**Out-of-Scope** "Assets that cannot process, store, or transmit CUI"
Apply all applicable NIST SP 800-171 Requirements	✓	✓	✓	✓	✓	✗
Complete a DODAM Basic Self-Assessment	✓	✓	✓	✓	✓	✗
Requirements extend to Subcontractors & External Service Providers with access to or protect CUI	✓	✓	✓	✓	✓	✗
Subject to Examination, Interview, & Test by Assessor for all Requirements	✓	✗	✗	✓	✗	✗
Subject to Spot Checks by the Assessor Against all Requirements	✗	✓	✗	✗	✗	✗
Evaluated via the Organization's System Security Plan and supporting documents[4]	✗	✓	✓	✗	✓	✓[5]
Subject to Negative Testing by an Assessor to Validate Isolation Techniques	✗	✗	✗	✗	✗	✓

Notes:
1. NIST SP 800-171 establishes the Scope of Applicability in Para 1.1 and Para 3
2. See NIST SP 800-171 Para 1.1
3. The CMMC Assessment Scoping Guide for Level 2 only identifies a general category for Specialized Assets. This infographic separates them to depict their relationship to the NIST SP 800-171 Scope of Applicability
4. There is no flow down requirement in DFARS Clause 252.204-7019. While there is no flow down requirement in the clause, Primes are requiring their sub-contractors and suppliers at attest in the Supplier Performance Risk System (SPRS) anyway.
5. See CMMC Assessment Guide for Level 2 for CA.L2-3.12.4 and Table 1. CMMC Asset Categories Overview in the CMMC Assessment Level 2 Scoping Guide
6. Out-of-Scope components should be identified in the SSP along with an explanation on how logical or physical isolation techniques have been applied. This leads to negative testing to ensure techniques are working

Table of Contents

Commentary

This document was created on 6 November 2022 and has not been revised, yet.
This document and the infographic will be revised when the CMMC Interim Rule is published.

Foundational Premises of the Infographic

The foundational premises of this infographic are:

1. Department of Defense (DoD) contractors in the Defense Industrial Base (DIB) are legally and contractually obligated to implement NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" after signing a contract with Department of Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 included as a requirement.[i, ii] Per the clause, every time a subcontractor or external service provider is given access to CUI, they are obligated to flow down the clause.
2. DoD prime contractors in the DIB are legally and contractually obligated to self-attest to their implementation of NIST SP 800-171 in accordance with (IAW) DFARS Clause 252.204-7019 the Supplier Performance Risk System (SPRS). While there is no flow down requirement in the clause, Primes are required to "***not*** *award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government*." This has resulted in Primes generally requiring their sub-contractors and suppliers also self-attest in SPRS anyway.
3. DoD contractors in the DIB are legally and contractually obligated to "*provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology*" IAW DFARS Clause 252.204-7020. DFARS Clause 252.204-7020 does have a flow down requirement every time a subcontractor or external service provider is given access to CUI.
4. The DIB contractor (a.k.a., the Organization Seeking Certification (OSC)) is **not** required to implement the Cybersecurity Maturity Model Certification (CMMC). Per the rescinded DFARS Clause 252.204-7021, "Cybersecurity Maturity Model Certification Requirement," "*The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.*"

In summary:

- All DIB contractors are expected to implement NIST SP 800-171 upon signing a contract containing DFARS Clause 252.204-7012.
- DIB Prime Contractors are required to self-attest in SPRS using the DoD Assessment Methodology (DoDAM) for their implementation of NIST SP 800-171.
- All DIB non-prime contractors are also required to self-attest using the DoDAM for their implementation of NIST SP 800-171. Many primes are also requiring their sub-contractors to also self-attest in SPRS.

- All DIB contractors are required to provide access to its facilities, systems, and personnel if the DoD wants to validate the contractor implemented NIST SP 800-171.
- Presuming there is no significant change to the three previously cited clauses, all DIB contractors must implement NIST SP 800-171 and will be required to be CMMC accredited to receive future contracts.

In case the point was missed above, there is no standing legal and contractual requirement to "implement CMMC" today, just to be accredited using DOD's CMMC defined methodology in the future.

Purpose of the Infographic

The purpose of the infographic is to quickly sum up an OSC's legal and contractual requirements to implement NIST SP 800-171 and then to highlight expectations on how to categorize the organization's components into the CMMC Assessment Scoping categories.

Bifurcation of Specialized Asset Category

The CMMC Assessment Scope Level 2 "Guide," Version 2.0, December 2021[iii] defines Specialized Assets as:

- "Assets that may or may not process, store, or transmit CUI
- Assets include: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment"

As pointed out in our "White Paper | Debunking CMMC Assessment Scope Myths,"[iv] Specialized Assets, when put into context of the NIST SP 800-171 Scope of Applicability, the Specialized Asset category can span CUI & Security Protections Components.

This infographic is in-line with our interpretation of how CMMC Assessment Scoping resides within the legal and contractual obligation to apply the NIST SP 800-171 Scope of Applicability to the contractor's business.

Brief statement about the first column rows

NIST SP 800-171 Scope of Applicability

NIST SP 800-171, para 1.1 defines the "Scope of Applicability" as:

> *"The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components."*

Following this statement is NIST's guidance to take items out-of-scope:

> *"If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets."*

This row and related headers directly map to these statements.

CMMC Level 2 Assessment Scope Asset Category

These categories have been pulled directly from the CMMC Assessment Scope Level 2 "Guide," Version 2.0, December 2021. Creative license has been applied to Specialized Assets to illustrate that they can span CUI & Security Protections Components.

Apply all applicable NIST SP 800-171 Requirements

DIB contractors are required to apply all requirements to all applicable "facilities, systems, and personnel components."

However, based upon the DIB contract's scoping efforts to take items out-of-scope and based upon limitations for that component, the DIB contractor may not be able to apply all requirements to all components. This is acceptable and an "As the CMMC Churns" will address how to handle these instances.

Complete a DODAM Basic Self-Assessment

IAW DFARS Clauses 252.204-7019 and 252.204-7020, all DOD contractors with access to CUI are required to measure their implementation of NIST SP 800-171 using the DoDAM. At least, Prime contractors are required to report their self-assessment in SPRS.

Requirements extend to Subcontractors & External Service Providers with access to or protect CUI

Flow down to Subcontractors is specified in the DFARS Clauses.

Per DoD Cybersecurity FAQ Q&A #7:

> *"Outsourcing your IT to another company does not transfer your DFARS clause 252.204-7012 responsibilities or implementation of NIST SP 800-171 requirements. Your company is responsible and accountable for meeting the contractual obligations with the Government as per the contract. The key to successfully demonstrating compliance with DFARS clause 252.204-7012 and NIST SP 800-171 is having a well written contract with the third-party that describes your requirements, and includes deliverables that meet or exceed requirements to protect DoD CUI."*

Fundamentally, the DIB contractor extended their IT services to external Cloud Service Providers and if they too have access to CUI, they must implement NIST SP 800-171 requirements. This statement is the most conservative one based on the limited guidance provided by DOD at this point in time.

DoD has also further enhanced and specified in DFARS Clause 252.204-7012, para (b)(2)(ii)(D):

> *"If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause 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."*

Subject to Examination, Interview, & Test by Assessor for all Requirements

IAW CMMC Assessment Scope Level 2 "Guide," Version 2.0, December 2021, Table 1. CMMC Asset Categories Overview.

Subject to Spot Checks by the Assessor Against all Requirements

IAW CMMC Assessment Scope Level 2 "Guide," Version 2.0, December 2021, Table 1. CMMC Asset Categories Overview.

Evaluated via the Organization's System Security Plan and supporting documents

IAW CMMC Assessment Scope Level 2 "Guide," Version 2.0, December 2021, Table 1. CMMC Asset Categories Overview.

Subject to Negative Testing by an Assessor to Validate Isolation Techniques

This is normally done under the auspices of AC.L2-3.1.3, Control the flow of CUI in accordance with approved authorizations.

Most common checks are done against the guest wireless, which should not have access to the CUI networks. This would be in line with Assessment Objective (AO) "[e] approved authorizations for controlling the flow of CUI are enforced."

Hierarchy of Authorities

BUSINESS RULE: Lower-level entities in the hierarchy cannot contradict or override higher-level items

The following is the fundamental cascade of hierarchies that legally establish the requirement for Non-Federal Organizations to implement NIST SP 800-171:

1) Federal Information Security Modernization Act of 2014 [v]
   a) Executive Order 13556, Controlled Unclassified Information, November 4, 2010[vi]
      i) Title 32 Code of Federal Regulation (CFR) Part 2002, Controlled Unclassified Information (CUI) [vii, viii]
         (1) Code of Federal Regulations (CFR), Title 48 - Federal Acquisition Regulations System
            (a) 48 CFR CHAPTER 2 - DEPARTMENT DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS)[ix]
               - DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" [x]
               - DFARS Clause 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements.[xi, xii]
               - DFARS Clause 252.204-7020[xiii], NIST SP 800-171 DoD Assessment Requirements.[xiv,]
               - ~~DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirement.~~[xv, xvi]

            (i) Department of Defense (DoD) Instruction (DoDI) 5200.48, Controlled Unclassified Information (CUI) [xvii]
               1. DoD Guidance:
                  - NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020[xviii]
                  - CMMC Documentation [xix]
                  - Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 and DFARS Subpart 239.76 and PGI Subpart 239.76) (as of Nov 23, 2021)[xx] {a.k.a., Cybersecurity FAQs}

Requirements to Implement NIST SP 800-171

Federal Information Security Modernization Act of 2014

Inclusion of Non-Federal Organization needing to have cybersecurity when dealing with the Federal Government

Executive Order 13556 of November 4, 2010, Controlled Unclassified Information (CUI)

- No mention of NIST SP 800-171

32 CFR Part 2002, Controlled Unclassified Information

§2002.14 (h)(2), "NIST SP 800-171 (incorporated by reference, see § 2002.2) defines the requirements necessary to protect CUI Basic on non-Federal information systems in accordance with the requirements of this part. Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless the authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the CUI category or subcategory of the information involved prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality)."

Code of Federal Regulations (CFR), Title 48 - Federal Acquisition Regulations System

- No federal level acquisition requirement to enforce 32 CFR Part 2002
- NARA has one in draft since 2017

48 CFR CHAPTER 53 - DEPARTMENT OF THE AIR FORCE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS)

DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

(b)(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security

requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

DFARS Clause 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements.[xxi]

(b) Requirement. In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800-171 DoD Assessments are described in the NIST SP 800-171 DoD Assessment Methodology located at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171.[xxii]

DFARS Clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements.[xxiii]

(c) Requirements. The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171, if necessary.[xxiv]

Department of Defense (DoD) Instruction (DoDI) 5200.48, Controlled Unclassified Information (CUI)

- 2.3. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DSCA).
  - **"**b. Assesses contractor compliance with contractually established CUI system requirements in DoD classified contracts associated with the National Industrial Security Program (NISP) in accordance with Part 2003 of Title 32, CFR and National Institute of Standards and Technology Special Publication (NIST SP) 800-171 guidelines."
- 2.9. DOD CIO
  - "e. Coordinates with the USD(I&S), USD(A&S), USD(R&E), and DoD Component heads to develop uniform security requirements for industry partners' IS and network security controls adequate for the type of CUI identified in the contract in accordance with Part 2002 of Title 32, CFR, Section 252.204-7012 of the DFARS, and NIST SP 800-171."
- 3.10. GENERAL SYSTEM AND NETWORK CUI REQUIREMENTS.
  - "In accordance with DoDIs 8500.01 and 8510.01, security controls for systems and networks are set to the level required by the safeguarding requirements for the data or information being processed, as identified in Federal Information Processing Standards 199 and 200. For DoD CUI, the minimum security level will be moderate confidentiality in accordance with Part 2002 of Title 32, CFR and NIST SP 800-171."
- 5.1. GENERAL.
  - "a. The NIST SP 800-171 identifies the baseline CUI system security requirements for industry established by Part 2002 of Title 32, CFR. Additionally, Section 252.204-7012 of the DFARS specifies a waiver process for defense contractors in accordance with NIST SP 800-171 for contractor IT or networks."

DoD Guidance:

NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020[xxv]

- 1) Background

- a) “DFARS clause 252.204-7012 further states that to provide adequate security, the Contractor shall implement, at a minimum, the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations.”
- b) “DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, requires, among other things, offerors to represent they will implement the security requirements in NIST SP 800-171 in effect at the time the solicitation is issued or as authorized by the contracting officer. To document implementation of NIST SP 800-171, the contractor must develop, document, and periodically update a system security plan that describes system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. If implementation of the security requirements is not complete, companies must develop and implement plans of action to describe when and how any unimplemented security requirements will be met.”

- 2) Purpose
  - a) “The NIST SP 800-171 DoD Assessment Methodology, Version 1.2 documents a standard methodology that enables a strategic assessment of a contractor’s implementation of NIST SP 800-171, a requirement for compliance with DFARS clause 252.204-7012.”
  - c) “DoD will use this methodology to assess the implementation of NIST SP 800-171 by its prime contractors. Prime contractors may use this methodology to assess the implementation status of NIST SP 800-171 by subcontractors.”

CMMC Documentation

Cybersecurity Maturity Model Certification (CMMC) Model Overview, Version 2.0, December 2021[xxvi]

- 1. Introduction
  - “The model encompasses the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision (Rev) 2 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012. DFARS clause 252.204-7012 specifies additional requirements beyond the NIST SP 800-171 security requirements, such as incident reporting. CMMC is designed to provide assurance to the DoD that a DIB contractor can adequately protect CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain”
- 2. CMMC Model
  - 2.4 CMMC Practices
    - 2.4.1 Overview, “The CMMC model measures the implementation of the NIST SP 800-171 Rev 2 security requirements. The practices originate from the safeguarding requirements and security requirements specified in FAR Clause 52.204-21 [3] and DFARS Clause 252.204-7012 [5], respectively.
      - Level 1 is equivalent to all of the safeguarding requirements from FAR Clause 52.204-21.
      - Level 2 is equivalent to all of the security requirements in NIST SP 800-171 Revision 2.

CMMC Assessment Guide Level 2, Version 2.0, December 2021[xxvii]

- CMMC Level Descriptions
    - "CMMC Levels 1 and 2 consist of the security requirements specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

      …

      CMMC Level 2 addresses the protection of Controlled Unclassified Information (CUI), which the National Archives and Record Administration (NARA) defines as:

      > *Information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.*"

Cybersecurity FAQs

- **Q6: When must the requirements in DFARS clause 252.204-7012 be implemented?**
    - **A6:** [para 3] "You only have to implement the security requirements in NIST SP 800-171 if your contract includes DFARS clause 252.204-7012 AND you are provided covered defense information by DoD (or are developing covered defense information for DoD) AND you are processing, storing or transmitting that covered defense information on your information system/network."
- **Q7: Our Company has outsourced its IT support and systems to a third-party contractor. Are we still responsible for complying with DFARS clause 252.204-7012 and implementing NIST SP 800-171?"**
    - **A7:** Outsourcing your IT to another company does not transfer your DFARS clause 252.204-7012 responsibilities or implementation of NIST SP 800-171 requirements. Your company is responsible and accountable for meeting the contractual obligations with the Government as per the contract. The key to successfully demonstrating compliance with DFARS clause 252.204-7012 and NIST SP 800-171 is having a well written contract with the third-party that describes your requirements, and includes deliverables that meet or exceed requirements to protect DoD CUI. If your IT service support is deemed to be less than or non-compliant with the contract, the company contracting with DoD is ultimately responsible.
- **Q8: Can the requirements in DFARS clause 252.204-7012, specifically the NIST SP 800-171 security requirements, be waived?**
    - **A8:** DFARS clause 252.204-7012 does not allow for "waivers" to the NIST SP 800-171 security requirements. It does allow an offeror/contractor to propose variances from any of the security requirements specified by NIST SP 800-171. The offeror/contractor must submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of why a particular security requirement is not applicable, or how an alternative but equally effective security measure effectively meets the capability in order to satisfy a particular requirement and achieve equivalent protection. An authorized representative of the DoD CIO will adjudicate offeror/contractor requests to vary from NIST SP 800-171 requirements in writing (see DFARS clause 252.204-7012 (b)(2)(ii)(B) and FAQs 62-66).
- **Q15: Will the DOD certify that a contractor is compliant with the require security requirements?**
    - **A15:** No. No new oversight paradigm is created through this rule.
      Compliance with DFARS clause 252.204-7012 requires contractors/subcontractors to comply with all requirements in the clause. By signing the contract, the contractor agrees to comply

with the contract terms. If oversight related to these requirements is deemed necessary, then it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract. DoD can validate compliance in this way, but will not certify that a contractor is compliant with DFARS clause 252.204-7012.
An implemented system security plan and associated plans of action for any planned implementations or mitigations demonstrate implementation or planned implementation of the security requirements in NIST SP 800-171.
USD(A&S) memorandum, "Assessing Contractor Implementation of Cybersecurity Requirements," dated November 14, 2019, provides a standard DoD methodology to assess a contractor's implementation of the security requirements in NIST SP 800-171. The NIST SP 800-171 DoD Assessment Methodology, available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.1%20%203.13.2020.pdf, is intended for assessment purposes only and does not add any substantive requirements to either NIST SP 800-171 or DFARS clause 252.204-7012.

- **Q16: Is a 3rd Party assessment of compliance required?**
    - **A16:** 3rd party (that is, an outside commercial company) assessments or certifications are not required, authorized, or recognized by DoD to assert compliance with DFARS clause 252.204-7012. By signing the contract, the contractor agrees to comply with the terms of the contract. In order to safeguard covered defense information, companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with DFARS clause 252.204-7012.

There are many more citation to NIST SP 800-171 sprinkled throughout the Cybersecurity FAQS

Requirements to be Accredited Via CMMC

DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirement.

As prescribed in 204.7503(a) and (b), insert the following clause:

CYBERSECURITY MATURITY MODEL CERTIFICATION REQUIREMENTS (NOV 2020)

(a) *Scope*. The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see https://www.acq.osd.mil/cmmc/index.html).

(b) *Requirements*. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) *Subcontracts*. The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

(End of clause)

Infographic Revision Table

Date	Revisions	Link to version image
4 Nov 2022	Version 1.0 – Initial publication	https://peakinfosec.com/wp-content/uploads/2022/11/NIST-SP-800-171-and-CMMC-LEVEL-2-ASSESSMENT-SCOPING-v1-0.jpeg
4 Nov 2022	Version 1.1 • Vincent Scott at Defense Cybersecurity Group identified the infographic definitions for CRMA and CUI Specialized Asset were flip-flopped • Changed "Apply all 110 NIST SP 800-171 Requirements" "Apply all applicable NIST SP 800-171 Requirements" to reflect the reality of how applying "all 110 NIST SP 800-171 Requirements" is done	https://peakinfosec.com/wp-content/uploads/2022/11/NIST-SP-800-171-and-CMMC-LEVEL-2-ASSESSMENT-SCOPING-v1-1.png
5 Nov 2022	Version 1.2 • Added note to explain bifurcation of the Specialized Asset category	https://peakinfosec.com/wp-content/uploads/2022/11/NIST-SP-800-171-and-CMMC-LEVEL-2-ASSESSMENT-SCOPING-v1.2.png
6 Nov 2022	Version 1.3 • Added "Self-Attest against DODAM in SPRS" row • Clarified "Requirements extend to Subcontractors & External Service Providers" to "Requirements extend to Subcontractors & External Service Providers with access to or protect CUI"	https://peakinfosec.com/wp-content/uploads/2022/11/NIST-SP-800-171-and-CMMC-LEVEL-2-ASSESSMENT-SCOPING-v1.3.png

Endnotes

[i] C.f., DFARS Clause 252.204-7012 (m) *Subcontracts*.
[ii] C.f., DoD Cybersecurity FAQs, Q&A #6. If the DIB Contractor does not actually process, store, or t transmit CUI, the the contractor should have the clause struck form its contract. There is no such thing as a self-deleting clause, especially with regards to DFARS Clause 252.204-7012
[iii] C.f., https://www.acq.osd.mil/cmmc/docs/Scope_Level2_V2.0_FINAL_20211202_508.pdf
[iv] C.f., https://peakinfosec.com/information-security/compliance/white-paper-debunking-cmmc-assessment-scope-myths/
[v] C.f., https://www.congress.gov/bill/113th-congress/senate-bill/2521
[vi] C.f., https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information
[vii] C.f., https://www.ecfr.gov/current/title-32/part-2002
[viii] 32 CFR Part 2002 established the National Archives and Records Administration (NARA) as the Federal lead for the CUI program. Its Information Security Oversight Office (ISSO) is responsible for the program and publishes CUI Notices the supersede and Federal agency directives.
[ix] C.f., https://www.ecfr.gov/current/title-48/chapter-2. DFARS Clauses begin in Chapter H, Part 252 at https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252
[x] C.f., https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
[xi] C.f., https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7019
[xii] DFARS Clause 252.204-7019 is expected to become a final rule in December 2022. Final revision to the rule may drive changes to this diagram.
[xiii] DFARS Clause 252.204-7020 is expected to become a final rule in December 2022. Final revision to the rule may drive changes to this diagram.
[xiv] C.f., https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7020
[xv] DFARS 252.204-7021 is ~~struck through~~ on purpose because it was temporarily rescinded by the Department of Defense. It is expected to be republished for commentary February/March 2023 and go into effect as an Interim Rule in May/June 2023.
[xvi] C.f., https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7021
[xvii] C.f., https://www.dodcui.mil/Portals/109/Documents/Policy Docs/DoDI 5200.48 CUI.pdf
[xviii] C.f., https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf
[xix] C.f., https://www.acq.osd.mil/cmmc/documentation.html
[xx] C.f, https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2021-11/Cyber%20DFARS%20FAQs%20rev%203%20%207.30.2020%20%2B%20correction%2011.23.2021.pdf
[xxi] C.f., https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7019
[xxii] DFARS Clause 252.204-7019, para (b)
[xxiii] C.f., https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7020
[xxiv] DFARS Clause 252.204-7020, para (c)
[xxv] The DODAM is specifically cited in DGARS Clauses 252.204-7019 and 252.204-7020
[xxvi] C.f. Cybersecurity Maturity Model Certification - Model Overview (osd.mil)
[xxvii] C.f., https://www.acq.osd.mil/cmmc/docs/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf