DoD Enforces Cyber Security Measures Affecting All Defense Contractors

The Department of Defense (DoD) has embedded a set of cybersecurity clauses into every defense contract. These clauses are not optional IT requirements — they are binding contract terms with direct impact on revenue, cost, and eligibility for future awards.

Together, DFARS 252.204-7012, 7019, 7020, and 7021 form a phased progression:

- **7012 (Today):** You must already safeguard Controlled Unclassified Information (CUI) using NIST SP 800-171 and report cyber incidents to DoD within 72 hours. This is a current contractual obligation, enforceable now.
- **7019 (Today):** You cannot win new DoD work unless you have a current cybersecurity score (SPRS) on record. This score is based on your implementation of NIST SP 800-171.
- **7020 (Today):** DoD has the right to audit your systems and verify your score. Subcontractors must also have scores on file.
- **7021 (Starting Nov 2025):** You must hold an official CMMC certification (third-party validated) to receive contracts. Self-attestation will no longer be enough.

Why CEOs and CFOs should care

- **Revenue risk:** Without compliance, your company will be ineligible for new DoD awards. This can cut off critical revenue streams.
- **Cost exposure:** Non-compliance discovered mid-contract can create delays, re-competition, or termination, with associated financial penalties.
- **Budgeting:** Achieving compliance requires investment in people, process, and technology. Early budgeting avoids last-minute remediation costs and lost opportunities.

Why CIOs and CISOs should care

- **Operational risk:** You must implement and maintain all 110 controls of NIST SP 800-171 and prepare for formal third-party audits.
- **Incident readiness:** You must be capable of detecting, reporting, and preserving evidence for cyber incidents within 72 hours.
- **Supply chain risk:** Subs and partners must also be compliant. Weak links in your supply chain can disqualify you or increase oversight.

Does this mean your existing contracts are impacted?

Under the Christian Doctrine, mandatory contract clauses that reflect significant public policy are read into every DoD contract, whether or not they appear in the written terms. For companies handling Controlled Unclassified Information (CUI), this means that the safeguarding, reporting, and assessment requirements of DFARS 252.204-7012, 7019, and 7020 apply automatically. These obligations also flow down from primes to subcontractors, so even small suppliers cannot avoid compliance if their work touches CUI. In practice, all defense contractors are expected to already meet CMMC Level 1 (for FCI) or Level 2 (for CUI) self-certification requirements today, with posted scores in SPRS and documented System Security Plans. Beginning in November 2025, Level 2 contracts will additionally require third-party certification (C3PAO) under DFARS 252.204-7021. This phased approach makes it clear: compliance is not optional, and readiness must be treated as a present obligation — not a future goal — for every member of the Defense Industrial Base.

Bottom Line

This is not just an IT issue — it is a business survival issue for any company in the Defense Industrial Base. Leadership must understand that:

- These clauses are already in effect and apply to current contracts (not just future ones).
- Compliance gaps today create scope uncertainty, audit risk, and contract delays tomorrow.
- Preparing now for CMMC certification is significantly less expensive than scrambling later under contract pressure.

Reading and acting on this document is essential for protecting both DoD revenue streams and your organization's long-term position in the defense supply chain.

CyberFoundry: Building Compliance-Ready Cybersecurity Programs

At CyberFoundry, we specialize in guiding defense contractors and suppliers through the complex requirements of DFARS 252.204-7012/7019/7020/7021 and the Cybersecurity Maturity Model Certification (CMMC). These regulations are not abstract policies — they are contractual obligations that determine your eligibility to win and retain DoD business.

Our role is to help you build and document a cybersecurity program that is not only operationally effective but also assessment-ready. We bring a blend of technical expertise, compliance knowledge, and real-world defense industry experience to:

- Map your existing environment against NIST SP 800-171 and DFARS obligations.
- Identify and close gaps that would cause you to fail a CMMC assessment.
- Develop the policies, procedures, and technical controls that assessors will expect to see.
- Guide you through SPRS scoring, incident reporting readiness, and subcontractor flow-down requirements.
- Build a long-term compliance roadmap that balances security maturity with cost control.

For most companies — even those with a preexisting security program — achieving CMMC readiness is not a quick project. It typically requires 12–24 months of sustained effort to fully implement, test, and institutionalize the required practices before a third-party assessor will certify you. Attempting to shortcut this timeline often results in failed assessments, contract delays, or expensive rework.

With CyberFoundry, you gain a partner who understands both the letter of the regulations and the realities of the defense supply chain. Our goal is simple: to make sure your program is credible, compliant, and ready for assessment — so your business can focus on growth, not regulatory surprises.

DFARS & CMMC Clause Comparison (High-Level Summary)

Clause	What It Means	What You Must Do	Risk If Ignored
252.204-7012 *Safeguarding CDI & Cyber Incident Reporting*	If you handle **CUI/CDI**, you must protect it per **NIST SP 800-171** and report incidents.	• Implement all **110 controls** in NIST 800-171. • Report incidents to **DIBNet within 72 hrs**. • Preserve forensic data for **90 days**. • Use **FedRAMP Moderate-equivalent cloud**. • Flow down to all subs handling CUI.	• **Breach of contract**. • Loss of current/future work. • DCMA/DIBCAC audit findings. • Increased liability for incidents.
252.204-7019 *Notice of NIST 800-171 Assessment*	You must have a **current SPRS score** on file (≤ 3 years old) to be considered for award.	• Post at least a **Basic Assessment score** to SPRS. • Update SSP/POA&M and expected completion date. • Keep score current (≤ 3 yrs).	• **Ineligible for new awards**. • Contracting officer cannot move forward without SPRS score.
252.204-7020 *NIST 800-171 Assessment Requirements*	DoD may perform **Medium or High Assessments** to validate your score.	• Provide access to **systems, people, facilities** for DoD/DCMA review. • Prepare SSP, POA&M, and evidence. • Flow clause down: **subs must have an SPRS score**.	• Findings reduce your score. • **Negative impact on awardability**. • 14-day rebuttal window — if missed, findings stand.
252.204-7021 *CMMC Certification*	Future state: you must hold a **CMMC certificate** at the contract's required level.	• Achieve certification via a **C3PAO assessment** (Level 2 = NIST 800-171). • Keep certificate **current (≤ 3 years)**. • Ensure subs are certified at proper level.	• **Cannot win or perform contracts** requiring CMMC. • Excluded from defense supply chain if uncertified after rollout.

High-Level Clause Summaries (DFARS & CMMC)

252.204-7012

Safeguarding Covered Defense Information & Cyber Incident Reporting

What it requires:

- You must implement NIST SP 800-171 security requirements on any system that handles Covered Defense Information (CDI/CUI).
- You must report cyber incidents within 72 hours via DoD's DIBNet portal.
- You must preserve forensic data for 90 days and cooperate with DoD requests for analysis.
- If using cloud services, they must meet FedRAMP Moderate equivalency.
- You must flow this clause down to all subs that handle CDI/CUI.

What you must know:

- If you hold CUI, you already have this obligation, even before CMMC is applied.
- Noncompliance exposes you to contract breach or termination.
- You need an incident response plan, access to DIBNet, and forensic readiness.
- This clause is live today — not future, not optional.

252.204-7019

Notice of NIST SP 800-171 DoD Assessment Requirements

What it requires:

- To be eligible for award, you must have a current NIST 800-171 assessment score (≤3 years old) in the Supplier Performance Risk System (SPRS).
- At minimum, you can self-post a Basic Assessment (self-scored).
- DoD may conduct Medium or High Assessments for higher confidence.

What you must know:

- If you don't have a posted score in SPRS, you cannot win new DoD work.
- A Basic Assessment is acceptable short-term, but Medium/High may follow.
- Your SSP, POA&M, and expected remediation timeline are visible to DoD.

252.204-7020
NIST SP 800-171 DoD Assessment Requirements

What it requires:

- Establishes how assessments (Basic, Medium, High) are conducted and scored.
- Requires you to grant access to facilities, systems, and personnel for Government-led assessments.
- Requires you to flow this down to subs — subs must have their own current Basic Assessment (at minimum) posted in SPRS.

What you must know:

- You cannot subcontract to firms without an SPRS score (≥ Basic).
- Medium/High assessments by DCMA/DoD involve document review, interviews, and technical validation.
- You have a right to rebut assessment findings, but only in a 14-day window.
- Scores (not details) are visible to DoD buyers and affect award decisions.

252.204-702
Cybersecurity Maturity Model Certification (CMMC) Requirements

What it requires:

- Starting with contracts issued after Nov 2025, you must have a current CMMC certificate (≤3 years old) at the level required by the contract.
- Certification must be maintained throughout contract performance.
- Requires flow-down: all subs handling FCI or CUI must also be certified at the appropriate level.

What you must know:

- This is the “end state” — self-attestations end, third-party certification (C3PAO) begins.
- Level 1 = FCI only;
  Level 2 = CUI (NIST 800-171, assessed by C3PAO);
  Level 3 (rare) = critical programs (NIST 800-172).
- You must budget and plan early: certification can take months to prepare.
- If subs are not certified, you cannot use them for in-scope work.

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

As prescribed in 204.7304 (c), use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (MAY 2024)

(a) Definitions.

As used in this clause—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

“Operationally critical support” means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

“Rapidly report” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013 , Rights in Technical Data—Other Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Adequate security.

The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:
    (i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010 , Cloud Computing Services, of this contract.
    (ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(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 https://csrc.nist.gov/publications/sp800) 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.
C. If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.
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/documents-templates/) 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.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—
    (i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and
    (ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.

(3) Medium assurance certificate requirement.In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

(d) Malicious software.

When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) Media preservation and protection.

When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) Access to additional information or equipment necessary for forensic analysis.

Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) Cyber incident damage assessment activities.

If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) DoD safeguarding and use of contractor attributional/proprietary information.

The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) Use and release of contractor attributional/proprietary information not created by or for DoD.

Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

(1) To entities with missions that may be affected by such information;
(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
(3) To Government entities that conduct counterintelligence or law enforcement investigations;
(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009 , Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) Use and release of contractor attributional/proprietary information created by or for DoD.

Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) Other safeguarding or reporting requirements.

The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) Subcontracts.

The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and
(2) Require subcontractors to—
    (i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

252.204-7019 Notice of NISTSP 800-171 DoD Assessment Requirements.

As prescribed in 204.7304(d), use the following provision:

NOTICE OF NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2023)

(a) Definitions.

"Basic Assessment", "Medium Assessment", and **"High Assessment"** have the meaning given in the clause 252.204-7020, NIST SP 800-171 DoD Assessments.

"Covered contractor information system" has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this solicitation.

(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/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf .

(c) Procedures.

(1) The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) () for all covered contractor information systems relevant to the offer.

(2) If the Offeror does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the Offeror may conduct and submit a Basic Assessment to for posting to SPRS in the format identified in paragraph (d) of this provision.

(d) Summary level scores.

Summary level scores for all assessments will be posted 30 days post-assessment in SPRS to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) **Basic Assessments.**
An Offeror may follow the procedures in paragraph (c)(2) of this provision for posting Basic Assessments to SPRS.

(i) The email shall include the following information:

A. Cybersecurity standard assessed (e.g., NIST SP 800-171 Rev 1).

B. Organization conducting the assessment (e.g., Contractor self-assessment).

C. For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

1. All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and
2. A brief description of the system security plan architecture, if more than one plan exists.

D. Date the assessment was completed.
E. Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement).
F. Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(ii) If multiple system security plans are addressed in the email described at paragraph (d)(1)(i) of this section, the Offeror shall use the following format for the report:

- System Security Plan
- CAGE Codes supported by this plan
- Brief description of the plan architecture
- Date of assessment
- Total Score
- Date score of 110 will achieved

(2) **Medium and High Assessments.**

DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system assessed:

(i) The standard assessed (e.g., NIST SP 800-171 Rev 1).
(ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).
(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.
(iv) A brief description of the system security plan architecture, if more than one system security plan exists.
(v) Date and level of the assessment, i.e., medium or high.
(vi) Summary level score (e.g., 105 out of 110, not the individual value assigned for each requirement).
(vii) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(3) Accessibility.

(i) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).
(ii) Authorized representatives of the Offeror for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.
(iii) A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this section. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected

against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(End of provision)

252.204-7020 NIST SP 800-171DoD Assessment Requirements.

As prescribed in 204.7304 (e), use the following clause:

NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2023)

(a) Definitions.

"Basic Assessment" means a contractor's self-assessment of the contractor's implementation of NIST SP 800-171 that—

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);
(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and
(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.

"Covered contractor information system" has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

"High Assessment" means an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—
    (i) A review of a contractor's Basic Assessment;
    (ii) A thorough document review;
    (iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the contractor's system security plan; and
    (iv) Discussions with the contractor to obtain additional information or clarification, as needed; and
(2) Results in a confidence level of "High" in the resulting score.

"Medium Assessment" means an assessment conducted by the Government that—

1) Consists of—
    (i) A review of a contractor's Basic Assessment;
    (ii) A thorough document review; and
    (iii) Discussions with the contractor to obtain additional information or clarification, as needed; and
2) Results in a confidence level of "Medium" in the resulting score.

(b) Applicability.

This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, in accordance with Defense Federal Acquisition Regulation System (DFARS) clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

(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/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf , if necessary.

(d) Procedures.

Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) () to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) Basic Assessments. A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology to for posting to SPRS.
    (i) The email shall include the following information:
        (A) Version of NIST SP 800-171 against which the assessment was conducted.
        (B) Organization conducting the assessment (e.g., Contractor self-assessment).
        (C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—
            1. All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and
            2. A brief description of the system security plan architecture, if more than one plan exists.
        (D) Date the assessment was completed.
        (E) Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement).
        (F) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.
    (ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Contractor shall use the following format for the report:
        - System Security Plan
        - CAGE Codes supported by this plan
        - Brief description of the plan architecture
        - Date of assessment
        - Total Score
        - Date score of 110 will achieved

(2) Medium and High Assessments. DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:
    (i) The standard assessed (e.g., NIST SP 800-171 Rev 1).
    (ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).
    (iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.
    (iv) A brief description of the system security plan architecture, if more than one system security plan exists.
    (v) Date and level of the assessment, i.e., medium or high.

(vi) Summary level score (e.g., 105 out of 110, not the individual value assigned for each requirement).

(vii) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(e) Rebuttals.

(1) DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf).

(2) Upon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

(f) Accessibility.

(1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(3) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at .

(4) A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this clause. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(g) Subcontracts.

(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services (excluding commercially available off-the-shelf).

(2) The Contractor shall 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/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf , 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.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171

DoD Assessment Methodology, to mailto:webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.

(End of clause)

252.204-7021 Cybersecurity Maturity Model Certification Requirements.

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

CYBERSECURITY MATURITY MODEL CERTIFICATION REQUIREMENTS (JAN 2023)

(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 products or commercial services, 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)

References

Defense Federal Acquisition Regulation Supplement (DFARS). (2024). 252.204-7012, Safeguarding covered defense information and cyber incident reporting.
Retrieved from https://www.acquisition.gov/dfars/252.204-7012

Defense Federal Acquisition Regulation Supplement (DFARS). (2023). 252.204-7019, Notice of NIST SP 800-171 DoD assessment requirements.
Retrieved from https://www.acquisition.gov/dfars/252.204-7019

Defense Federal Acquisition Regulation Supplement (DFARS). (2023). 252.204-7020, NIST SP 800-171 DoD assessment requirements.
Retrieved from https://www.acquisition.gov/dfars/252.204-7020

Defense Federal Acquisition Regulation Supplement (DFARS). (2023). 252.204-7021, Cybersecurity Maturity Model Certification (CMMC) requirements.
Retrieved from https://www.acquisition.gov/dfars/252.204-7021

Defense Federal Acquisition Regulation Supplement (DFARS). (2023). 252.239-7010, Cloud computing services.
Retrieved from https://www.acquisition.gov/dfars/252.239-7010

National Institute of Standards and Technology (NIST). (2021). NIST SP 800-171 Rev. 2: Protecting controlled unclassified information in nonfederal systems and organizations.
Retrieved from https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

National Institute of Standards and Technology (NIST). (2018). NIST SP 800-171A: Assessing security requirements for controlled unclassified information.
Retrieved from https://csrc.nist.gov/publications/detail/sp/800-171a/final

National Institute of Standards and Technology (NIST). (2020). NIST SP 800-172: Enhanced security requirements for protecting controlled unclassified information.
Retrieved from https://csrc.nist.gov/publications/detail/sp/800-172/final

Office of the Under Secretary of Defense (OUSD A&S). (2020). NIST SP 800-171 DoD assessment methodology v1.2.1.
Retrieved from 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

Office of the Under Secretary of Defense (OUSD A&S). (2023). Cybersecurity Maturity Model Certification (CMMC) program.
Retrieved from https://www.acq.osd.mil/cmmc/index.html

Department of Defense, Chief Information Officer (DoD CIO). (2023). CMMC Level 2 scoping guide v2.13.
Retrieved from https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2v2.pdf

Department of Defense, Chief Information Officer (DoD CIO). (2023). CMMC Level 2 assessment guide v2.13.
Retrieved from https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL2v2.pdf

Department of Defense. (n.d.). Supplier Performance Risk System (SPRS).
Retrieved from https://www.sprs.csd.disa.mil/

Department of Defense. (n.d.). SPRS awardee user guide.
Retrieved from https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf

National Archives. (n.d.). Controlled Unclassified Information (CUI) registry.
Retrieved from https://www.archives.gov/cui

DoD Cyber Crime Center (DC3). (2025). Mandatory and voluntary cyber incident reporting.
Retrieved from https://dc3.mil/dcise

Federal Risk and Authorization Management Program (FedRAMP). (n.d.). FedRAMP program homepage.
Retrieved from https://www.fedramp.gov/

Defense Pricing and Contracting (DPC). (2020). DoDI 5000.79: Defense-wide sharing and use of supplier and product performance information.
Retrieved from https://www.esd.whs.mil/Directives/issuances/dodi/500079/

Glossary

Basic / Medium / High Assessment (NIST 800-171)
Self-score (Basic) or DoD/DCMA-run reviews (Medium/High) of your 800-171 implementation.
Why it matters: Your **score must be in SPRS** to be eligible for awards; Government can validate it.

C3PAO (CMMC Third-Party Assessor Organization)
Accredited firm that performs **CMMC Level 2** certifications.
Why it matters: Starting **Nov 2025**, many Level 2 contracts require a **C3PAO certificate** to award.

CAGE / UEI
Unique identifiers for contractors in federal systems (CAGE = entity code; UEI replaces DUNS).
Why it matters: Ties your assessments/scores and contracts to the correct legal entity.

Christian Doctrine
Legal principle: mandatory clauses that reflect significant procurement policy are **read into** DoD contracts even if omitted.
Why it matters: **7012/7019/7020** obligations can apply **whether or not** they're written in your T&Cs.

CMMC (Cybersecurity Maturity Model Certification)
DoD program requiring third-party certification of cybersecurity practices.
Why it matters: **7021** makes certification a **condition of award/performance** (phasing in from **Nov 2025**).

CRMA (Contractor Risk-Managed Asset)
Systems capable of handling CUI but managed (by policy/controls) so they **do not**.
Why it matters: Impacts scope, cost, and how large your assessed environment becomes.

CUI (Controlled Unclassified Information)
Unclassified data that requires safeguarding (e.g., technical drawings, specs).
Why it matters: Handling CUI triggers **NIST 800-171**, **7012/7019/7020**, and often **CMMC L2**.

DC3 (DoD Cyber Crime Center)
Receives malware/samples and supports incident forensics for DoD cases.
Why it matters: **7012** may require submission of malicious code/evidence to DC3.

DCMA / DIBCAC
DoD oversight bodies (Defense Contract Management Agency; its DIBCAC unit audits cybersecurity).
Why it matters: They conduct **Medium/High** assessments and can **impact awardability**.

DFARS 252.204-7012
Contract clause: safeguard CUI with **NIST 800-171**, **report incidents in 72 hours**, preserve evidence 90 days; cloud must meet **FedRAMP Moderate equivalency**; flow-down to subs.
Why it matters: **Active now**—breach risks contract loss and liability.

DFARS 252.204-7019
Requires a **current 800-171 score in SPRS** (≤3 years old) to be considered for award.
Why it matters: No SPRS score = no award.

DFARS 252.204-7020
Authorizes DoD/DCMA **validation** of your score (site visits, evidence); subs must also have scores.
Why it matters: Expect verification and a short rebuttal window (14 business days).

DFARS 252.204-7021
CMMC requirement clause: you must **hold and maintain** the contract-required **CMMC certificate**.
Why it matters: Certification becomes a **go/no-go** factor as CMMC phases in from **Nov 2025**.

DIB / DIBNet
Defense Industrial Base; DIBNet is the DoD portal for **72-hour incident reporting**.
Why it matters: You need accounts and a practiced **IR playbook** to meet **7012** timelines.

FedRAMP Moderate Equivalency
Security baseline for cloud services that store/process DoD CUI.
Why it matters: Using non-compliant cloud for CUI can **break 7012** and jeopardize contracts.

FCI (Federal Contract Information)
Non-public info provided for/contracts but **not** CUI.
Why it matters: Drives **CMMC Level 1** (foundational) scope for some suppliers.

Flow-Down
Prime must include clauses in subcontracts when subs handle FCI/CUI.
Why it matters: Your **supply chain** must also comply; non-compliant subs can disqualify you.

Forensic Preservation (90 Days)
Maintain system images/logs after a reportable incident.
Why it matters: **7012** requires it; failure undermines investigations and compliance.

Incident (72-Hour Reporting)
Cyber event affecting CUI or operationally critical support must be reported to DoD **within 72 hours**.
Why it matters: Requires **prepared IR process**, evidence capture, and executive notification paths.

NIST SP 800-171 / 171A / 172
Standards for protecting CUI (800-171), assessment procedures (171A), and enhanced protections (172).
Why it matters: **800-171 = 110 controls** you must implement for L2; **172** appears in rare Level 3 cases.

POA&M (Plan of Action & Milestones)
Your remediation plan for unmet 800-171 requirements.
Why it matters: Drives your **SPRS score** and credibility of your roadmap.

Prime / Subcontractor
Prime holds the contract with DoD; subs perform portions of the work.
Why it matters: Obligations and certification levels flow to subs handling in-scope data.

Scope / Enclave
The defined boundary (people, tech, processes) that handles FCI/CUI; an enclave is a segmented environment for it.
Why it matters: Smaller, well-designed enclaves reduce cost, risk, and audit surface.

SPRS (Supplier Performance Risk System) Score
Your reported **800-171 score** and completion date on a 0–110 scale (can be negative).
Why it matters: **Required for awards** (7019) and visible to DoD buyers.

SSP (System Security Plan)
Documentation of how you meet each 800-171 requirement and your system architecture.
Why it matters: Foundation for **assessments and certification**—auditors ask for it first.

72-Hour / 90-Day Requirements
Report incidents to DoD within **72 hours**; preserve forensic data **90 days**.
Why it matters: Hard deadlines with contractual consequences.