

**Defense Acquisition Regulations System, DoD****252.204-7020**

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](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)

[85 FR 61520, Sept. 29, 2020, as amended at 87 FR 15818, Mar. 18, 2022]

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

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

**NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (MAR 2022)****(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

**252.204-7020**

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/safe-guarding.html#nistSP800171>, if necessary.

(d) *Procedures.* Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) (<https://www.sprs.csd.disa.mil/>) 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 [webptsmh@navy.mil](mailto:webptsmh@navy.mil) for posting to SPRS.

(i) The email shall include the following information:

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 be 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 ac-

**48 CFR Ch. 2 (10-1-22 Edition)**

(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:

tion 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](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).

(2) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own

**Defense Acquisition Regulations System, DoD****252.204-7022**

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](https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf).

(3) 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 items (excluding COTS items).

(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/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.

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

(End of clause)

[85 FR 61520, Sept. 29, 2020, as amended at 87 FR 15818, Mar. 18, 2022]

**252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.**

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

**CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENT (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)

[85 FR 61520, Sept. 29, 2020]

**252.204-7022 Expediting Contract Closeout.**

As prescribed in 204.804-70, use the following clause:

**EXPEDITING CONTRACT CLOSEOUT (MAY 2021)**

(a) At the conclusion of all applicable closeout requirements of Federal Acquisition Regulation 4.804, the Government and Contractor shall mutually agree on the residual dollar amount remaining on the contract. Both the Government and Contractor agree to waive payment of any residual dollar amount of \$1,000 or less to which either party may be entitled at the time of contract closeout.

(b) A residual dollar amount includes all money owed to either party at the end of the contract and as a result of the contract, excluding amounts connected in any way with taxation or a violation of law or regulation.

(c) For purposes of determining residual dollar amounts, offsets (e.g., across multiple contracts or orders) may be considered only to the extent permitted by law.

(End of clause)

[86 FR 27277, May 20, 2021]