

Section H - Special Contract Requirements

CLAUSES INCORPORATED BY FULL TEXT

52.223-3 HAZARDOUS MATERIAL IDENTIFICATION AND SAFETY DATA (FEB 2026)

(a) Hazardous material, as used in this clause, includes any material defined as hazardous under the latest version of Federal Standard No. 313 (including revisions adopted during the term of the contract).

(b) The Offeror must list any hazardous material, as defined in paragraph (a) of this clause, to be delivered under this contract. The hazardous material shall be properly identified and include any applicable identification number, such as National Stock Number or Special Item Number. This information shall also be included on the Safety Data Sheet submitted under this contract.

Material (if none, insert None)	Identification No.
NONE	_____
_____	_____
_____	_____

(c) This list must be updated during performance of the contract whenever the Contractor determines that any other material to be delivered under this contract is hazardous.

(d) The apparently successful offeror agrees to submit, for each item as required prior to award, a Safety Data Sheet, meeting the requirements of 29 CFR 1910.1200(g) and the latest version of Federal Standard No. 313, for all hazardous material identified in paragraph (b) of this clause. Data shall be submitted in accordance with Federal Standard No. 313, whether or not the apparently successful offeror is the actual manufacturer of these items. Failure to submit the Safety Data Sheet prior to award may result in the apparently successful offeror being considered nonresponsible and ineligible for award.

(e) If, after award, there is a change in the composition of the item(s) or a revision to Federal Standard No. 313, which renders incomplete or inaccurate the data submitted under paragraph (d) of this clause, the Contractor shall promptly notify the Contracting Officer and resubmit the data.

(f) Neither the requirements of this clause nor any act or failure to act by the Government shall relieve the Contractor of any responsibility or liability for the safety of Government, Contractor, or subcontractor personnel or property.

(g) Nothing contained in this clause shall relieve the Contractor from complying with applicable Federal, State, and local laws, codes, ordinances, and regulations (including the obtaining of licenses and permits) in connection with hazardous material.

(h) The Government's rights in data furnished under this contract with respect to hazardous material are as follows:

(1) To use, duplicate and disclose any data to which this clause is applicable. The purposes of this right are to—

(i) Apprise personnel of the hazards to which they may be exposed in using, handling, packaging, transporting, or disposing of hazardous materials;

(ii) Obtain medical treatment for those affected by the material; and

(iii) Have others use, duplicate, and disclose the data for the Government for these purposes.

(2) To use, duplicate, and disclose data furnished under this clause, in accordance with subparagraph (h)(1) of this clause, in precedence over any other clause of this contract providing for rights in data.

(3) The Government is not precluded from using similar or identical data acquired from other sources.

(End of clause)

Section I - Contract Clauses

CLAUSES INCORPORATED BY REFERENCE

52.240-90	Security Prohibitions and Exclusions Representations and Certifications	FEB 2026
52.240-91	Security Prohibitions and Exclusions	FEB 2026
52.245-1	Government Property	SEP 2021
52.246-18	Warranty Of Supplies Of A Complex Nature	MAY 2001
252.204-7018	Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services	JAN 2023
252.245-7003	Contractor Property Management System Administration	JAN 2025
252.245-7005	Management and Reporting of Government Property	JAN 2024

CLAUSES INCORPORATED BY FULL TEXT

52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (APR 2026)

(a) Definitions. As used in this clause—

Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (e.g., vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

- (1) The Contractor will not engage in any racially discriminatory DEI activities.
- (2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause.
- (3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts.
- (4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer.
- (5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.
- (6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, for which the place of delivery or performance is in the United States.

(End of clause)

252.204-7021 CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENTS (NOV 2025)

(a) Definitions. As used in this clause-

Controlled unclassified information means information the Government creates or possesses, or information an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls (32 CFR 2002.4(h)).

Current means--

(1) With regard to Conditional Cybersecurity Maturity Model Certification (CMMC) Status--

(i) Not older than 180 days for Conditional Level 2 (Self) assessments and Conditional Level 2 (certified third-party assessment organization (C3PAO)) assessments, with--

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance by an affirming official (see 32 CFR 170.4); and

(ii) Not older than 180 days for Conditional Level 3 (Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)) assessments, with--

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance by an affirming official;

(2) With regard to Final CMMC Status--

(i) Not older than 1 year for Final Level 1 (Self), with--

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.15); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official;

(ii) Not older than 3 years for Final Level 2 (Self) assessments and Final Level 2 (C3PAO) assessments, with--

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.16 and 170.17); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(iii) Not older than 3 years for Final Level 3 (DIBCAC) assessments, with--

(A) No changes in compliance with the requirements at 32 CFR part 170 since the Final CMMC Status date (see 32 CFR 170.18); and

(B) A corresponding affirmation of continuous compliance, not older than 1 year, by an affirming official; and

(3) With regard to affirmation of continuous compliance (32 CFR 170.22), not older than 1 year with no changes in compliance with the requirements at 32 CFR part 170.

Cybersecurity Maturity Model Certification (CMMC) status means the result of meeting or exceeding the minimum required score for the corresponding assessment. The potential statuses are as follows:

(1) Final Level 1 (Self).

(2) Conditional Level 2 (Self).

(3) Final Level 2 (Self).

(4) Conditional Level 2 (C3PAO).

(5) Final Level 2 (C3PAO).

(6) Conditional Level 3 (DIBCAC).

(7) Final Level 3 (DIBCAC).

Cybersecurity Maturity Model Certification unique identifier (CMMC UID) means 10 alpha-numeric characters assigned to each CMMC assessment and reflected in the Supplier Performance Risk System (SPRS) for each contractor information system.

Federal contract information (FCI) means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. It does not include information provided by the Government to the public, such as on public websites, or simple transactional information, such as information necessary to process payments.

Plan of action and milestones means a document that identifies tasks to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones, as defined in National Institute of Standards and Technology Special Publication 800-115 (32 CFR 170.21).

- (b) Framework. The Cybersecurity Maturity Model Certification (CMMC) is a framework for assessing a contractor's compliance with applicable information security protections (see 32 CFR part 170).
- (c) Duplication. The CMMC assessments will not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a reassessment may be necessary, for example, when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.
- (d) Requirements. The Contractor shall--
- (1)(i) Have and maintain for the duration of the contract a current CMMC status at the following CMMC level, or higher: Level 1 for all information systems used in performance of the contract, task order, or delivery order that process, store, or transmit FCI or CUI; and
 - (ii) Consult 32 CFR 170.23 related to the flowdown of the CMMC requirements, and flow down the correct CMMC level to subcontracts and other contractual instruments;
- (2) Only process, store, or transmit FCI or CUI on contractor information systems that have a CMMC status at the CMMC level required in paragraph (d)(1) of this clause, or higher;
- (3) Complete on an annual basis, and maintain as current, an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance with the requirements associated with the CMMC level required in paragraph (d)(1) of this clause in the Supplier Performance Risk System (SPRS) (<https://piee.eb.mil>) for each CMMC UID applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract;
- (4) Ensure all subcontractors and suppliers complete prior to subcontract award, and maintain on an annual basis, an affirmation, by the affirming official (see 32 CFR 170.4), of continuous compliance with the requirements associated with the CMMC level required for the subcontract or other contractual instrument for each of the subcontractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the subcontract; and
- (5) If the Contractor has a CMMC Status of Conditional, successfully close out a valid plan of action and milestones (32 CFR 170.21) to achieve a CMMC Status of Final.
- (e) Reporting. The Contractor shall--
- (1) Submit to the Contracting Officer--
 - (i) The CMMC UID(s) issued by SPRS for contractor information systems that will process, store, or transmit FCI or CUI during performance of the contract; and
 - (ii) Any changes in the CMMC UIDs generated in SPRS throughout the life of the contract, task order, or delivery order, if applicable;
- (2) Enter into SPRS the results of a current self-assessment for each CMMC UID, not covered by a C3PAO assessment or DIBCAC assessment, applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract; and
- (3) Complete in SPRS on an annual basis and maintain as current an affirmation of continuous compliance by the affirming official (see 32 CFR 170.4) for each self-assessment, C3PAO assessment, or DIBCAC assessment required under the contract in SPRS.
- (f) Subcontracts. The Contractor shall--
- (1) Insert the substance of this clause, including this paragraph (f) and excluding paragraph (e)(1), in subcontracts and other contractual instruments, including those for the acquisition of commercial products and commercial services, excluding commercially available off-the-shelf items, if the subcontract or other contractual instrument will contain a requirement to process, store, or transmit FCI or CUI; and
 - (2) Prior to awarding a subcontract or other contractual instrument, ensure that the subcontractor has a current CMMC certificate or current CMMC status at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor based on the requirements at 32 CFR 170.23.
- (End of clause)

252.204-7025 NOTICE OF CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL
REQUIREMENTS (NOV 2025)

(a) Definitions. As used in this provision, controlled unclassified information (CUI), current, Cybersecurity Maturity Model Certification (CMMC) status, Cybersecurity Maturity Model Certification unique identifier (CMMC UID), Federal contract information (FCI), and Plan of action and milestones have the meaning given in the Defense Federal Acquisition Regulation Supplement 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements, clause of this solicitation.

(b)(1) Cybersecurity Maturity Model Certification (CMMC) level. The CMMC level required by this solicitation is: Level 1. This CMMC level, or higher (see 32 CFR part 170), is required prior to award for each contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) during performance of the contract.

(2) The Offeror will not be eligible for award of a contract, task order, or delivery order resulting from this solicitation if the Offeror does not have, for each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of a contract resulting from this solicitation--

(i) The current CMMC status entered in the Supplier Performance Risk System (SPRS) (<https://piee.eb.mil>) at the CMMC level required by paragraph (b)(1) of this provision; and

(ii) A current affirmation of continuous compliance with the security requirements identified at 32 CFR part 170 in SPRS.

(c) Plan of action and milestones. If the Offeror has a CMMC Status of Conditional, the Offeror shall successfully close out a valid plan of action and milestones (32 CFR 170.21) to achieve a CMMC Status of Final.

(d) CMMC unique identifiers. The Offeror shall provide, in the proposal, the CMMC unique identifier(s) (CMMC UIDs) issued by SPRS for each contractor information system that will process, store, or transmit FCI or CUI during performance of a contract, task order, or delivery order resulting from this solicitation. The Offeror also shall update the list when new CMMC UIDs are generated in SPRS. The CMMC UIDs are provided in SPRS after the Offeror enters the results of self-assessment(s) for each such information system.

(End of provision)