TABLE OF CONTENTS

(Revised November 10, 2025)

SUBPART 204.1—CONTRACT EXECUTION
204.101 Contracting officer's signature.

SUBPART 204.2—CONTRACT DISTRIBUTION
204.201 Procedures.
204.203 Taxpayer identification information.
204.270 Electronic Data Access.

SUBPART 204.4—SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY
204.402 General.
204.403 Responsibilities of contracting officers.
204.404 Contract clause.
204.404-70 Additional contract clauses.
204.470 U.S.-International Atomic Energy Agency Additional Protocol.
204.470-1 General.
204.470-2 National security exclusion.
204.470-3 Contract clause.

SUBPART 204.6—CONTRACT REPORTING
204.602 General.
204.604 Responsibilities.
204.606 Reporting data.

SUBPART 204.8—CONTRACT FILES
204.802 Contract files.
204.804 Closeout of contract files.
204.804-70 Contract clause.
204.805 Disposal of contract files.

SUBPART 204.9—TAXPAYER IDENTIFICATION NUMBER INFORMATION
204.902 General.

SUBPART 204.11—SYSTEM FOR AWARD MANAGEMENT
204.1103 Procedures.

SUBPART 204.12—ANNUAL REPRESENTATIONS AND CERTIFICATIONS
204.1202 Solicitation provision and contract clause.

SUBPART 204.16—UNIFORM PROCUREMENT INSTRUMENT IDENTIFIERS
204.1601 Policy.
204.1603 Procedures.
204.1670 Cross reference to Federal Procurement Data System.
204.1671 Order of application for modifications.

SUBPART 204.17—SERVICE CONTRACTS INVENTORY
204.1700 Scope of subpart.
204.1701 Definitions.

204.1703 Reporting requirements.
204.1705 Contract clauses.

SUBPART 204.18—COMMERCIAL AND GOVERNMENT ENTITY CODE
204.1870 Procedures.

SUBPART 204.21—PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT
204.2100 Scope of subpart.
204.2101 Definitions.
204.2102 Prohibition.
204.2103 Procedures.
204.2104 Waivers.
204.2105 Solicitation provisions and contract clause.

SUBPART 204.70—RESERVED

SUBPART 204.71—UNIFORM CONTRACT LINE ITEM NUMBERING SYSTEM
204.7100 Scope.
204.7101 Definitions.
204.7102 Policy.
204.7103 Contract line items.
204.7103-1 Criteria for establishing.
204.7103-2 Numbering procedures.
204.7104 Contract subline items.
204.7104-1 Criteria for establishing.
204.7104-2 Numbering procedures.
204.7105 Contract exhibits and attachments.
204.7106 Contract modifications.
204.7107 Contract accounting classification reference number (ACRN) and agency accounting identifier (AAI).
204.7108 Payment instructions.
204.7109 Contract clauses.

SUBPART 204.72—ANTITERRORISM AWARENESS TRAINING.
204.7200 Scope of subpart.
204.7201 Definition.
204.7202 Policy.
204.7203 Contract clause.

SUBPART 204.73—SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING
204.7300 Scope.
204.7301 Definitions.
204.7302 Policy.
204.7303 Procedures.
204.7304 Solicitation provision and contract clauses.

SUBPART 204.74—DISCLOUSURE OF INFORMATION TO LITIGATION SUPPORT CONTRACTORS

204.7400 Scope of subpart.
204.7401 Definitions.
204.7402 Policy.
204.7403 Contract clauses.

SUBPART 204.75—CYBERSECURITY MATURITY MODEL CERTIFICATION
204.7500 Scope of subpart.
204.7501 Definitions.
204.7502 Policy.
204.7503 Procedures.
204.7504 Solicitation provision and contract clause.

SUBPART 204.76—SUPPLIER PERFORMANCE RISK SYSTEM
204.7600 Scope of subpart.
204.7601 Definitions.
204.7602 Applicability.
204.7603 Procedures.
204.7604 Solicitation provision.

SUBPART 204.75—CYBERSECURITY MATURITY MODEL CERTIFICATION

(Revised November 10, 2025)

204.7500 Scope of subpart.

(a) This subpart prescribes policies and procedures for including the Cybersecurity Maturity Model Certification (CMMC) level requirements in DoD contracts. CMMC is a framework (see 32 CFR part 170) for assessing a contractor's information security protections.

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.

(c) This subpart applies to unclassified contractor information systems.

204.7501 Definitions.

As used in this subpart—

"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.

204.7502 Policy.

(a) *Award eligibility*.

(1) The contracting officer shall include in the solicitation the required CMMC level, if provided by the program office or the requiring activity.

(2) Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current CMMC status at the CMMC level required by the solicitation.

(3) Contractors are required to achieve, at time of award, a CMMC status at the level specified in the solicitation, or higher, for all information systems used in the performance of the contract, task order, or delivery order that will process, store, or transmit FCI or CUI. Contractors are required to maintain a current CMMC status at the specified CMMC level or higher, if required by the contract, task order, or delivery order, throughout the life of the contract, task order, or delivery order.

(b) *CMMC status.*

(1) Contracting officers may award a contract, task order, delivery order, or modification to exercise an option or extend a period of performance, if the offeror's or contractor's CMMC status is—

(i) Listed in the definition of "CMMC status"; and

(ii) Equal to or higher than the CMMC level required by the solicitation or contract, task order, or delivery order.

(2) CMMC levels 2 and 3 can be in a conditional level for a period not to exceed 180 days from the CMMC status date (32 CFR 170.21), and award can occur with a conditional CMMC level. CMMC level 1 requires a final CMMC level for award.

204.7503 Procedures.

(a) *CMMC level.* The contracting officer shall include the CMMC level (see 32 CFR 170.19) required by the program office or requiring activity in the solicitation provision and contract clause prescribed at 204.7504.

(b) *Award.* Contracting officers shall check SPRS and not award a contract, task order, or delivery order to an offeror that does not have a current CMMC status posted in SPRS at the CMMC level (see 32 CFR 170.15 through 170.18) required by the solicitation, or higher, for each CMMC UID provided by the offeror. The CMMC UIDs are applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract.

(c) *Option exercise or period of performance extension.* Contracting officers shall check SPRS and not exercise an option or extend the period of performance on a contract, task order, or delivery order, unless the contractor has a current CMMC status posted in SPRS at the CMMC level (see 32 CFR 170.15 through 170.18) required by the contract, task order, or delivery order, or higher, for each CMMC UID provided by the contractor. The contractor's CMMC UIDs are applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are or will be used in performance of the contract.

(d) *CMMC UIDs.* If the contractor provides new CMMC UIDs during performance of the contract, task order, or delivery order, the contracting officer shall check in SPRS, using the CMMC UIDs assigned by SPRS, that the contractor has a current CMMC status at the required CMMC level, or higher, for each of the contractor information systems identified that will process, store, or transmit FCI or CUI during contract performance.

204.7504 Solicitation provision and contract clause.

(a) Unless the requirements at 32 CFR 170.5(d) are met, use the clause at 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements, as follows:

(1) Until November 9, 2028, in solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf (COTS) items, if the program office or requiring activity determines that the contractor is required to have a specific CMMS level.

(2) On or after November 10, 2028, in solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for those solely for the acquisition of COTS items, if the program office or requiring activity determines that the contractor is required to use contractor information systems in the performance of the contract, task order, or delivery order to process, store, or transmit FCI or CUI.

(b) Use the provision at 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, in solicitations that include the clause at 252.204-7021.

SUBPART 212.3—SOLICITATION PROVISIONS AND CONTRACT CLAUSES FOR THE ACQUISITION OF COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

(Revised November 10, 2025)

212.301 Solicitation provisions and contract clauses for the acquisition of commercial products and commercial services.

See DoD Class Deviation 2023-O0008, Commercial Products and Commercial Services Omnibus Clause for Acquisitions Using the Procurement Desktop-Defense System, issued September 18, 2023. This class deviation allows the contracting officer to use the PD2 clause logic capability to automatically select the clauses that are applicable to the specific solicitation and contract. The contracting officer shall ensure that the deviation clause is incorporated into these solicitations and contracts because the deviation clause fulfills the statutory requirements on auditing and subcontract clauses applicable to commercial products and commercial services. The deviation also authorizes adjustments to the deviation clause required by future changes to the clause at FAR 52.212-5 that are published in the FAR. This deviation is effective for 3 years, or until otherwise rescinded.

(c) Include an evaluation factor regarding supply chain risk (see subpart 239.73) when acquiring information technology, whether as a service or as a supply, that is a covered system, is a part of a covered system, or is in support of a covered system, as defined in 239.7301.

(f) The following additional provisions and clauses apply to DoD solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services. If the offeror has completed any of the following provisions listed in this paragraph electronically as part of its annual representations and certifications at *https://www.sam.gov*, the contracting officer shall consider this information instead of requiring the offeror to complete these provisions for a particular solicitation. The contracting officer shall not use other FAR or DFARS provisions and clauses unless required by the FAR or DFARS or consistent with customary commercial practices (section 874(b)(1)(A), Pub. L. 114-328).

(i) *Part 203—Improper Business Practices and Personal Conflicts of Interest.*

(A) Use the FAR clause at 52.203-3, Gratuities, as prescribed in FAR 3.202, to comply with 10 U.S.C. 4651.

(B) Use the clause at 252.203-7000, Requirements Relating to Compensation of Former DoD Officials, as prescribed in 203.171-4(a), to comply with section 847 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(C) Use the clause at 252.203-7002, Requirement to Inform Employees of Whistleblower Rights, as prescribed in 203.970, to comply with 10 U.S.C. 4701.

(D) Use the provision at 252.203-7005, Representation Relating to Compensation of Former DoD Officials, as prescribed in 203.171-4(b).

(ii) *Part 204—Administrative and Information Matters.*

(A) Use the clause at 252.204-7004, Antiterrorism Awareness Training for Contractors, as prescribed in 204.7203.

(B) Use the provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, as prescribed in 204.7304(a), to comply with section 941 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and section 1632 of the National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291).

(C) Use the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, as prescribed in 204.7304(b), to comply with section 941 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and section 1632 of the National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291).

(D) Use the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, as prescribed in 204.7304(c), to comply with section 941 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and section 1632 of the National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291).

(E) Use the clause at 252.204-7014, Limitations on the Use or Disclosure of Information by Litigation Support Contractors, as prescribed in 204.7403(a), to comply with 10 U.S.C. 129d.

(F) Use the clause at 252.204-7015, Notice of Authorized Disclosure of Information for Litigation Support, as prescribed in 204.7403(b), to comply with 10 U.S.C. 129d.

(G) Use the provision at 252.204-7016, Covered Defense Telecommunications Equipment or Services—Representation, as prescribed in 204.2105(a), to comply with section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91).

(H) Use the provision at 252.204-7017, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services—Representation, as prescribed in 204.2105(b), to comply with section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91).

(I) Use the clause at 252.204-7018, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services, as prescribed in 204.2105(c), to comply with section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91).

(J) Use the provision at 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements, as prescribed in 204.7304(d).

(K) Use the clause at 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, as prescribed in 204.7304(e).

(L) Use the clause at 252.204-7021, Cybersecurity Maturity Model Certification Requirements, as prescribed in 204.7504(a).

(M) Use the clause at 252.204-7022, Expediting Contract Closeout, as prescribed in 204.804-70.

(N) Use the clause at 252.204-7023, Reporting Requirements for Contracted Services, to comply with 10 U.S.C. 4505.

(*1*) Use the basic clause as prescribed in 204.1705(a)(i) and (ii).

(*2*) Use the alternate I clause as prescribed in 204.1705(a)(i) and (iii).

(O) Use the provision at 252.204-7024, Notice on the Use of the Supplier Performance Risk System, as prescribed in 204.7604.

(P) Use the provision at 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, as prescribed in 204.7504(b).

(iii) *Part 205—Publicizing Contract Actions.* Use the clause at 252.205-7000, Provision of Information to Cooperative Agreement Holders, as prescribed in 205.470, to comply with 10 U.S.C. 4957.

(iv) *Part 209—Contractor Qualifications.*

(A) Use the provision at 252.209-7011, Representation for Restriction on the Use of Certain Institutions of Higher Education, as prescribed in 209.170-4, to comply with section 1062 of the National Defense Authorization Act for Fiscal Year 2021 (Pub. L. 116-283).

(B) Use the provision at 252.209-7012, Prohibition Relating to Conflicts of Interest in Consulting Services—Certification, as prescribed in 209.572(e), to comply with section 812 of the National Defense Authorization Act for Fiscal Year 2024 (Pub. L. 118-31).

(v) *Part 211—Describing Agency Needs.*

(A) Use the clause at 252.211-7003, Item Unique Identification and Valuation, as prescribed in 211.274-5(a).

(B) Use the clause at 252.211-7008, Use of Government-Assigned Serial Numbers, as prescribed in 211.274-5(b).

(vi) *Part 215—Contracting by Negotiation.*

(A) Use the provision at 252.215-7003, Requirements for Submission of Data Other Than Certified Cost or Pricing Data—Canadian Commercial Corporation, as prescribed at 215.408(2)(i).

(B) Use the clause at 252.215-7004, Requirement for Submission of Data other Than Certified Cost or Pricing Data—Modifications—Canadian Commercial Corporation, as prescribed at 215.408(2)(ii).

(C) Use the provision 252.215-7008, Only One Offer, as prescribed at 215.408(3).

(D) Use the provision 252.215-7010, Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data, as prescribed at 215.408(5)(i) to comply with section 831 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239) and sections 851 and 853 of the National Defense Authorization Act for Fiscal Year 2016 (Pub. L. 114-92).

(*1*) Use the basic provision as prescribed at 215.408(5)(i)(A).

(*2*) Use the alternate I provision as prescribed at 215.408(5)(i)(B).

(E) Use the provision at 252.215-7016, Notification to Offerors—Postaward Debriefings, as prescribed in 215.570, to comply with section 818 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91).

(vii) *Part 216—Types of Contracts.* Use the clause at 252.216-7010, Postaward Debriefings for Task Orders and Delivery Orders, as prescribed in 216.506-70(b), to comply with section 818 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91).

(viii) *Part 219—Small Business Programs.*

(A) Use the provision at 252.219-7000, Advancing Small Business Growth, as prescribed in 219.309(1), to comply with 10 U.S.C. 4959.

(B) Use the clause at 252.219-7003, Small Business Subcontracting Plan (DoD Contracts), to comply with 15 U.S.C. 637.

(*1*) Use the basic clause as prescribed in 219.708(b)(1)(A)(*1*).

(*2*) Use the alternate I clause as prescribed in 219.708(b)(1)(A)(*2*).

(*3*) Use the alternate II clause as prescribed in 219.708(b)(1)(A)(*3*).

(C) Use the clause at 252.219-7004, Small Business Subcontracting Plan (Test Program), as prescribed in 219.708(b)(1)(B), to comply with 15 U.S.C. 637 note.

(D) Use the provision at 252.219-7012, Competition for Religious-Related Services, as prescribed in 219.270-3, to comply with section 898 of the National Defense Authorization Act for Fiscal Year 2016 (Pub. L. 114-92).

(ix) *Part 223—Environment, Sustainable Acquisition, and Material Safety.*

(A) Use the clause at 252.223-7008, Prohibition of Hexavalent Chromium, as prescribed in 223.7306.

(B) Use the clause at 252.223-7009, Prohibition of Procurement of Fluorinated Fire-Fighting Agent for Use on Military Installations, as prescribed at 223.7404 to comply with section 322(b), (c), and (d) of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92).

(x) *Part 225—Foreign Acquisition.*

(A) Use the provision at 252.225-7000, Buy American—Balance of Payments Program Certificate, to comply with 41 U.S.C. chapter 83 and Executive Order 10582 of December 17, 1954, Prescribing Uniform Procedures for Certain Determinations Under the Buy-American Act.

(*1*) Use the basic provision as prescribed in 225.1101(1)(i).

(*2*) Use the alternate I provision as prescribed in 225.1101(1)(ii).

(B) Use the clause at 252.225-7001, Buy American and Balance of Payments Program, to comply with 41 U.S.C. chapter 83 and Executive Order 10582 of December 17, 1954, Prescribing Uniform Procedures for Certain Determinations Under the Buy-American Act.

(*1*) Use the basic clause as prescribed in 225.1101(2)(ii).

(*2*) Use the alternate I clause as prescribed in 225.1101(2)(iii).

(C) Use the clause at 252.225-7006, Acquisition of the American Flag, as prescribed in 225.7002-3(c), to comply with section 8123 of the DoD Appropriations Act, 2014 (Pub. L. 113-76, division C, title VIII), and the same provision in subsequent DoD appropriations acts.

(D) Use the clause at 252.225-7007, Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies, as prescribed in 225.1103(4), to comply with section 1211 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2006 (Pub. L. 109-163) as amended by the NDAAs for FY 2012 and FY 2017.

(E) Use the clause at 252.225-7008, Restriction on Acquisition of Specialty Metals, as prescribed in 225.7003-5(a)(1), to comply with 10 U.S.C. 4863.

(F) Use the clause at 252.225-7009, Restriction on Acquisition of Certain Articles Containing Specialty Metals, as prescribed in 225.7003-5(a)(2), to comply with 10 U.S.C. 4863.

(G) Use the provision at 252.225-7010, Commercial Derivative Military Article—Specialty Metals Compliance Certificate, as prescribed in 225.7003-5(b), to comply with 10 U.S.C. 4863.

(H) Use the clause at 252.225-7012, Preference for Certain Domestic Commodities, as prescribed in 225.7002-3(a), to comply with 10 U.S.C. 4862.

(I) Use the clause at 252.225-7015, Restriction on Acquisition of Hand or Measuring Tools, as prescribed in 225.7002-3(b), to comply with 10 U.S.C. 4862.

(J) Use the clause at 252.225-7016, Restriction on Acquisition of Ball and Roller Bearings, as prescribed in 225.7009-5, to comply with section 8065 of Public Law 107-117 and the same restriction in subsequent DoD appropriations acts.

(K) Use the clause at 252.225-7017, Photovoltaic Devices, as prescribed in 225.7017-4(a), to comply with section 846 of the National Defense Authorization Act for Fiscal Year 2011 (Pub. L. 111-383).

(L) Use the provision at 252.225-7018, Photovoltaic Devices—Certificate, as prescribed in 225.7017-4(b), to comply with section 846 of the National Defense Authorization Act for Fiscal Year 2011 (Pub. L. 111-383).

(M) Use the clause at 252.225-7019, Restriction on Acquisition of Anchor and Mooring Chain, as prescribed in 225.7004-7(a), to comply with 10 U.S.C. 4864 and section 8041 of the Fiscal Year 1991 DoD Appropriations Act (Pub. L. 101-511) and similar sections in subsequent DoD appropriations acts.

(N) Use the provision at 252.225-7020, Trade Agreements Certificate, to comply with 19 U.S.C. 2501-2518 and 19 U.S.C. 4501-4732. Alternate I also implements section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(*1*) Use the basic provision as prescribed in 225.1101(5)(i).

(*2*) Use the alternate I provision as prescribed in 225.1101(5)(ii).

(O) Use the clause at 252.225-7021, Trade Agreements, to comply with 19 U.S.C. 2501-2518 and 19 U.S.C. 4501-4732.

(*1*) Use the basic clause as prescribed in 225.1101(6)(i).

(*2*) Use the alternate II clause as prescribed in 225.1101(6)(iii).

(P) Use the provision at 252.225-7023, Preference for Products or Services from Afghanistan, as prescribed in 225.7703-4(a), to comply with section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(Q) Use the clause at 252.225-7024, Requirement for Products or Services from Afghanistan, as prescribed in 225.7703-4(b), to comply with section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(R) Use the clause at 252.225-7026, Acquisition Restricted to Products or Services from Afghanistan, as prescribed in 225.7703-4(c), to comply with section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(S) Use the clause at 252.225-7027, Restriction on Contingent Fees for Foreign Military Sales, as prescribed in 225.7307(a), to comply with 22 U.S.C. 2779.

(T) Use the clause at 252.225-7028, Exclusionary Policies and Practices of Foreign Governments, as prescribed in 225.7307(b), to comply with 22 U.S.C. 2755.

(U) Use the clause at 252.225-7029, Acquisition of Uniform Components for Afghan Military or Afghan National Police, as prescribed in 225.7703-4(d), to comply with section 826 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112–239).

(V) Use the provision at 252.225-7031, Secondary Arab Boycott of Israel, as prescribed in 225.7605, to comply with 10 U.S.C. 4659.

(W) Use the provision at 252.225-7035, Buy American—Free Trade Agreements—Balance of Payments Program Certificate, to comply with 41 U.S.C. chapter 83 and 19 U.S.C. 4501-4732. Alternates II, III, and V also implement section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(*1*) Use the basic provision as prescribed in 225.1101(9)(i).

(*2*) Use the alternate I provision as prescribed in 225.1101(9)(ii).

(*3*) Use the alternate II provision as prescribed in 225.1101(9)(iii).

(*4*) Use the alternate III provision as prescribed in 225.1101(9)(iv).

(*5*) Use the alternate IV provision as prescribed in 225.1101(9)(v).

(*6*) Use the alternate V provision as prescribed in 225.1101(9)(vi).

(X) Use the clause at 252.225-7036, Buy American—Free Trade Agreements—Balance of Payments Program, to comply with 41 U.S.C. chapter 83 and 19 U.S.C. 4501-4732. Alternates II, III, and V also implement section 886 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(*1*) Use the basic clause as prescribed in 225.1101(10)(i)(A).

(*2*) Use the alternate I clause as prescribed in 225.1101(10)(i)(B).

(*3*) Use the alternate II clause as prescribed in 225.1101(10)(i)(C).

(*4*) Use the alternate III clause as prescribed in 225.1101(10)(i)(D).

(*5*) Use the alternate IV clause as prescribed in 225.1101(10)(i)(E).

(*6*) Use the alternate V clause as prescribed in 225.1101(10)(i)(F).

(Y) Use the clause at 252.225-7039, Defense Contractors Performing Private Security Functions Outside the United States, as prescribed in 225.302-6, to comply with section 862 of the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

(Z) Use the clause at 252.225-7040, Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States, as prescribed in 225.371-5(a).

(AA) Use the clause at 252.225-7043, Antiterrorism/Force Protection Policy for Defense Contractors Outside the United States, as prescribed in225.372-2.

(BB) Use the provision at 252.225-7049, Prohibition on Acquisition of Certain Foreign Commercial Satellite Services—Representations, as prescribed in 225.772-5(a), to comply with 10 U.S.C. 2279.

(CC) Use the provision at 252.225-7050, Disclosure of Ownership or Control by the Government of a Country that is a State Sponsor of Terrorism, as prescribed in 225.771-5, to comply with 10 U.S.C. 4871(b).

(DD) Use the clause at 252.225-7051, Prohibition on Acquisition for Certain Foreign Commercial Satellite Services, as prescribed in 225.772-5(b), to comply with 10 U.S.C. 2279.

(EE) Use the clause at 252.225-7052, Restriction on the Acquisition of Certain Magnets, Tantalum, and Tungsten, as prescribed in 225.7018-5, to comply with 10 U.S.C. 4872.

(FF) Use the provision at 252.225-7053, Representation Regarding Prohibition on Use of Certain Energy Sourced from Inside the Russian Federation, as prescribed in 225.7019-4(a), to comply with section 2821 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92).

(GG) Use the clause at 252.225-7054, Prohibition on Use of Certain Energy Sourced from Inside the Russian Federation, as prescribed in 225.7019-4(b), to comply with section 2821 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92).

(HH) Use the provision at 252.225-7055, Representation Regarding Business Operations with the Maduro Regime, as prescribed in 225.7020-5(a), to comply with section 890 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92).

(II) Use the clause at 252.225-7056, Prohibition Regarding Business Operations with the Maduro Regime, as prescribed in 225.7020-5(b), to comply with section 890 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92).

(JJ) Use the provision at 252.225-7059, Prohibition on Certain Procurements from the Xinjiang Uyghur Autonomous Region—Representation, as prescribed in 225.7022-5(a), to comply with section 855 of the National Defense Authorization Act for Fiscal Year 2023 (Pub. L. 117-263) and 10 U.S.C. 4661.

(KK) Use the clause at 252.225-7060, Prohibition on Certain Procurements from the Xinjiang Uyghur Autonomous Region, as prescribed in 225.7022-5(b), to comply with section 855 of the National Defense Authorization Act for Fiscal Year 2023 (Pub. L. 117-263) and 10 U.S.C. 4661.

(LL) Use the clause at 252.225-7061, Restriction on the Acquisition of Personal Protective Equipment and Certain Other Items from Non-Allied Foreign Nations, as prescribed in 225.7023-4, to comply with 10 U.S.C. 4875.

(MM) Use the clause at 252.225-7062, Restriction on Acquisition of Large Medium-Speed Diesel Engines, as prescribed in 225.7004-7(b), to comply with 10 U.S.C. 4864.

(NN) Use the clause at 252.225-7063, Restriction on Acquisition of Components of T-AO 205 and T-ARC Class Vessels, as prescribed in 225.7004-7(c), to comply with 10 U.S.C. 4864.

(OO) Use the clause at 252.225-7064, Restriction on Acquisition of Certain Satellite Components, as prescribed in 225.7004-7(d), to comply with 10 U.S.C. 4864.

(PP) Use the provision at 252.225-7065, Restriction on Acquisition of Fuel for Overseas Contingency Operations, as prescribed in 225.7024-4, to comply with section 843 of the National Defense Authorization Act for Fiscal Year 2022 (Pub. L. 117-81).

(xi) *Part 226—Other Socioeconomic Programs.*

(A) Use the clause at 252.226-7001, Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns, as prescribed in 226.104, to comply with section 8021 of Public Law 107-248 and similar sections in subsequent DoD appropriations acts.

(B) Use the provision at 252.226-7002, Representation for Demonstration Project for Contractors Employing Persons with Disabilities, as prescribed in 226.7203, to comply with section 853 of the National Defense Authorization Act for Fiscal Year 2004 (Pub. L. 108-136).

(xii) *Part 227—Patents, Data, and Copyrights.*

(A) Use the clause at 252.227-7013, Rights in Technical Data–Other Than Commercial Products and Commercial Services, as prescribed in 227.7102-4(b) and 227.7103-6(a). Use the clause with its Alternate I as prescribed in 227.7103-6(b)(1). Use the clause with its Alternate II as prescribed in 227.7103-6(b)(2), to comply with 10 U.S.C. 8687 and 17 U.S.C. 1301, et. seq.

(B) Use the clause at 252.227-7015, Technical Data–Commercial Products and Commercial Services, as prescribed in 227.7102-4(a)(1), to comply with 10 U.S.C. 3772(a). Use the clause with its Alternate I as prescribed in 227.7102-4(a)(2), to comply with 10 U.S.C. 8687 and 17 U.S.C. 1301, et. seq.

(C) Use the clause at 252.227-7018, Rights in Other Than Commercial Technical Data and Computer Software—Small Business Innovation Research Program and Small Business Technology Transfer Program, as prescribed in 227.7104-4(a)(1).

(D) Use the clause at 252.227-7037, Validation of Asserted Restrictions on Technical Data, as prescribed in 227.7102-4(c), to comply with 10 U.S.C. 3781-3786.

(E) Use the provision at 252.227-7040, Additional Preaward Requirements for Small Business Technology Transfer Program, as prescribed in 227.7104-4(c)(1).

(F) Use the clause at 252.227-7041, Additional Postaward Requirements for Small Business Technology Transfer Program, as prescribed in 227.7104-4(c)(2).

(xiii) *Part 229—Taxes.* Use the clause at 252.229-7014, Full Exemption from Two-Percent Excise Tax on Certain Foreign Procurements, as prescribed in 229.402-70, to comply with 26 U.S.C. 5000C.

(xiv) *Part 232—Contract Financing.*

(A) Use the clause at 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports, as prescribed in 232.7004, to comply with 10 U.S.C. 4601.

(B) Use the clause at 252.232-7006, Wide Area WorkFlow Payment Instructions, as prescribed in 232.7004(b).

(C) Use the clause at 252.232-7009, Mandatory Payment by Governmentwide Commercial Purchase Card, as prescribed in 232.1110.

(D) Use the clause at 252.232-7010, Levies on Contract Payments, as prescribed in 232.7102, to comply with 26 U.S.C. 6331(h).

(E) Use the clause at 252.232-7011, Payments in Support of Emergencies and Contingency Operations, as prescribed in 232.908.

(F) Use the provision at 252.232-7014, Notification of Payment in Local Currency (Afghanistan), as prescribed in 232.7202.

(xv) *Part 237—Service Contracting.*

(A) Use the clause at 252.237-7010, Prohibition on Interrogation of Detainees by Contractor Personnel, as prescribed in 237.173-5, to comply with section 1038 of the National Defense Authorization Act for Fiscal Year 2010 (Pub. L. 111-84).

(B) Use the clause at 252.237-7019, Training for Contractor Personnel Interacting with Detainees, as prescribed in 237.171-4, to comply with section 1092 of the National Defense Authorization Act for Fiscal Year 2005 (Pub. L. 108-375).

(C) Use the provision at 252.237-7025, Preaward Transparency Requirements for Firms Offering to Support Department of Defense Audits—Representation and Disclosure, as prescribed in 237.270(e)(3), to comply with section 1006 of the National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) and section 1011 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92).

(D) Use the clause at 252.237-7026, Postaward Transparency Requirements for Firms that Support Department of Defense Audits, as prescribed in 237.270(e)(4), to comply with section 1006 of the National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) and section 1011 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92).

(E) Use the clause at 252.237-7027, Transfer and Adoption of Military Animals, as prescribed in 237.7804 to comply with 10 U.S.C. 2387.

(xvi) *Part 239—Acquisition of Information Technology*.

(A) Use the provision 252.239-7009, Representation of Use of Cloud Computing, as prescribed in 239.7604(a).

(B) Use the clause 252.239-7010, Cloud Computing Services, as prescribed in 239.7604(b).

(C) Use the provision at 252.239-7017, Notice of Supply Chain Risk, as prescribed in 239.7306(a), to comply with 10 U.S.C. 3252.

(D) Use the clause at 252.239-7018, Supply Chain Risk, as prescribed in 239.7306(b), to comply with 10 U.S.C. 3252.

(xvii) *Part 243—Contract Modifications.* Use the clause at 252.243-7002, Requests for Equitable Adjustment, as prescribed in 243.205-71, to comply with 10 U.S.C. 3862.

(xviii) *Part 244—Subcontracting Policies and Procedures.* Use the clause at 252.244-7000, Subcontracts for Commercial Products and Commercial Services, as prescribed in 244.403.

(xix) *Part 245—Government Property*. Use the clause at 252.245-7005, Management and Reporting of Government Property, as prescribed in 245.107(4).

(xx) *Part 246—Quality Assurance.*

(A) Use the clause at 252.246-7003, Notification of Potential Safety Issues, as prescribed in 246.370(a).

(B) Use the clause at 252.246-7004, Safety of Facilities, Infrastructure, and Equipment for Military Operations, as prescribed in 246.270-4, to comply with section 807 of the National Defense Authorization Act for Fiscal Year 2010 (Pub. L. 111-84).

(C) Use the clause at 252.246-7008, Sources of Electronic Parts, as prescribed in 246.870-3(b), to comply with section 818(c)(3) of Pub. L. 112-81, as amended by section 817 of the National Defense Authorization Act for Fiscal Year 2015 (Pub. L. 113-291) and section 885 of the National Defense Authorization Act for Fiscal Year 2016 (Pub. L. 114-92).

(xxi) *Part 247—Transportation.*

(A) Use the clause at 252.247-7003, Pass-Through of Motor Carrier Fuel Surcharge Adjustment to the Cost Bearer, as prescribed in 247.207, to comply with section 884 of the National Defense Authorization Act for Fiscal Year 2009 (Pub. L. 110-417).

(B) Use the basic or one of the alternates of the clause at 252.247-7023, Transportation of Supplies by Sea, as prescribed in 247.574(a), to comply with the Cargo Preference Act of 1904 (10 U.S.C. 2631(a)).

(*1*) Use the basic clause as prescribed in 247.574(a)(1).

(*2*) Use the alternate I clause as prescribed in 247.574(a)(2).

(*3*) Use the alternate II clause as prescribed in 247.574(a)(3).

(C) Use the clause 252.247-7025, Reflagging or Repair Work, as prescribed in 247.574(b), to comply with 10 U.S.C. 2631(b).

(D) Use the provision at 252.247-7026, Evaluation Preference for Use of Domestic Shipyards—Applicable to Acquisition of Carriage by Vessel for DoD Cargo in the Coastwise or Noncontiguous Trade, as prescribed in 247.574(c), to comply with section 1017 of the National Defense Authorization Act for Fiscal Year 2007 (Pub. L. 109-364).

(E) Use the clause at 252.247-7027, Riding Gang Member Requirements, as prescribed in 247.574(d), to comply with section 3504 of the National Defense Authorization Act for Fiscal Year 2009 (Pub. L. 110-417).

(F) Use the clause at 252.247-7028, Application for U.S. Government Shipping Documentation/Instructions, as prescribed in 247.207.

(xxii) *Part 270—Defense Contracting Programs.*

(A) Use the provision at 252.270-7000, Pilot Program to Incentivize Contracting with Employee-Owned Businesses—Representation, as prescribed at 270.105(a) to comply with section 874 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2022 (Pub. L. 117-81; 10 U.S.C. 3204 note) and section 872 of the NDAA for FY 2024 (Pub. L. 118-31; 10 U.S.C. 3204 note).

(B) Use the provision at 252.270-7001, Pilot Program to Incentivize Contracting with Employee-Owned Businesses—Subcontracting Certification, as prescribed at 270.105(b), to comply with section 874 of the NDAA for FY 2022 (Pub. L. 117-81; 10 U.S.C. 3204 note) and section 872 of the NDAA for FY 2024 (Pub. L. 118-31; 10 U.S.C. 3204 note).

(C) Use the clause at 252.270-7002, Pilot Program to Incentivize Contracting with Employee-Owned Businesses, as prescribed at 270.105(c), to comply with section 874 of the NDAA for FY 2022 (Pub. L. 117-81; 10 U.S.C. 3204 note) and section 872 of the NDAA for FY 2024 (Pub. L. 118-31; 10 U.S.C. 3204 note).

212.302 Tailoring of provisions and clauses for the acquisition of commercial products and commercial services.

(c) *Tailoring inconsistent with customary commercial practice.* The head of the contracting activity is the approval authority within the DoD for waivers under FAR 12.302(c).

212.370 Inapplicability of certain provisions and clauses to contracts and subcontracts for the acquisition of commercial products, commercial services, and commercially available off-the-shelf items.
The following provisions and clauses, not expressly authorized in law, are not applicable to contracts for the acquisition of commercial products and commercial services:

(a) FAR 52.204-22, Alternative Line Item Proposal.

(b) 252.203-7003, Agency Office of the Inspector General.

(c) 252.215-7007, Notice of Intent to Resolicit.

212.371 Inapplicability of certain provisions and clauses to contracts for the acquisition of commercially available off-the-shelf items.
Commercially available off-the-shelf (COTS) items are a subset of commercial products. Therefore, the provisions and clauses listed in 212.370 as not applicable to contracts or subcontracts for the acquisition of commercial products are also not applicable to contracts or subcontracts for the acquisition of COTS items. In addition, the following provisions and clauses published after October 13, 1994, not expressly authorized in law, are not applicable or are modified in their applicability to contracts for the acquisition of COTS items:

(a) FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

(b) 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls.

(c) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(d) 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements.

(e) 252.204-7020, NIST SP 800-171 DoD Assessment Requirements.

(f) 252.204-7021, Cybersecurity Maturity Model Certification Requirements.

(g) 252.205-7000, Provision of Information to Cooperative Agreement Holders.

(h) 252.270-7000, Pilot Program to Incentivize Contracting with Employee-Owned Businesses—Representation.

(i) 252.270-7001, Pilot Program to Incentivize Contracting with Employee-Owned Businesses—Subcontracting Certification.

(j) 252.270-7002, Pilot Program to Incentivize Contracting with Employee-Owned Businesses.

SUBPART 217.2—OPTIONS

(Revised November 10, 2025)

217.202 Use of options.

(1) See PGI 217.202 for guidance on the use of options.

(i) See PGI 217.202(1) for guidance on the use of options with foreign military sales (FMS).

(ii) See PGI 217.202(2) for the use of options with sole source major systems for U.S. and U.S./FMS combined procurements.

(2) For a contract that is initially awarded from the competitive selection of a proposal resulting from a broad agency announcement, see 234.005-1 for the use of contract options for the development and demonstration or initial production of technology developed under the contract or the delivery of initial or additional items.

217.204 Contracts.

(e)(i) Notwithstanding FAR 17.204(e), the ordering period of a task order or delivery order contract (including a contract for information technology) awarded by DoD pursuant to 10 U.S.C. 3403—

(A) May be for any period up to 5 years;

(B) May be subsequently extended for one or more successive periods in accordance with an option provided in the contract or a modification of the contract; and

(C) Shall not exceed 10 years unless the head of the agency determines in writing that exceptional circumstances require a longer ordering period.

(ii) Paragraph (e)(i) of this section does not apply to the following:

(A) Contracts, including task or delivery order contracts, awarded under other statutory authority.

(B) Advisory and assistance service task order contracts (authorized by 10 U.S.C. 3405 that are limited by statute to 5 years, with the authority to extend an additional 6 months (see FAR 16.505(c)).

(C) Definite-quantity contracts.

(D) GSA schedule contracts.

(E) Multi-agency contracts awarded by agencies other than NASA, DoD, or the Coast Guard.

(iii) Obtain approval from the senior procurement executive before issuing an order against a task or delivery order contract subject to paragraph (e)(i) of this section, if performance under the order is expected to extend more than 1 year beyond the 10-

year limit or extended limit described in paragraph (e)(i)(C) of this section (see FAR 37.106 for funding and term of service contracts).

217.207 Exercise of options.

(c) In addition to the requirements at FAR 17.207(c), exercise an option only after—

(1) Determining that the contractor's record in the System for Award Management database is active and the contractor's unique entity identifier, Commercial and Government Entity (CAGE) code, name, and physical address are accurately reflected in the contract document. See PGI 217.207 for the requirement to perform cost or price analysis of spare parts prior to exercising any option for firm-fixed-price contracts containing spare parts; and

(2) Working with the program office or requiring activity to verify in the Supplier Performance Risk System (*https://piee.eb.mil*) that—

(i) The summary level score 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) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted (see 204.7303); and

(ii) If there is a requirement for the contractor to have a Cybersecurity Maturity Model Certification (CMMC) status at a specific CMMC level, the contractor has a current CMMC status at the CMMC level required by the contract, or higher, for each of the CMMC unique identifiers applicable to each of the contractor information systems that process, store, or transmit Federal contract information or controlled unclassified information (see 204.7503(c)).

217.208 Solicitation provisions and contract clauses.

Sealed bid solicitations shall not include provisions for evaluations of options unless the contracting officer determines that there is a reasonable likelihood that the options will be exercised (10 U.S.C. 3206(e)). This limitation also applies to sealed bid solicitations for the contracts excluded by FAR 17.200.

217.208-70 Additional clauses.

(a) Use the basic or the alternate of the clause at 252.217-7000, Exercise of Option to Fulfill Foreign Military Sales Commitments, in solicitations and contracts when an option may be used for foreign military sales requirements. Do not use the basic or the alternate of this clause in contracts for establishment or replenishment of DoD inventories or stocks, or acquisitions made under DoD cooperative logistics support arrangements.

(1) Use the basic clause when the foreign military sales country is known at the time of solicitation or award.

(2) Use the alternate I clause when the foreign military sale country is not known at the time of solicitation or award.

(b) When a surge option is needed in support of industrial capability production planning, use the clause at 252.217-7001, Surge Option, in solicitations and contracts.

(1) Insert the percentage or quantity of increase the option represents in paragraph (a) of the clause to ensure adequate quantities are available to meet item requirements.

(2) Change 30 days in paragraphs (b)(2) and (d)(1) to longer periods, if appropriate.

(3) Change the 24-month period in paragraph (c)(3), if appropriate.

(Revised November 10, 2025)

252.204-7000 Disclosure of Information.
As prescribed in 204.404-70(a), use the following clause:

DISCLOSURE OF INFORMATION (OCT 2016)

(a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) The Contracting Officer has given prior written approval;

(2) The information is otherwise in the public domain before the date of release; or

(3) The information results from or arises during the performance of a project that involves no covered defense information (as defined in the clause at DFARS 252.204-7012) and has been scoped and negotiated by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental research (which by definition cannot involve any covered defense information), in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, in effect on the date of contract award and the Under Secretary of Defense (Acquisition, Technology, and Logistics) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008 (available at DFARS PGI 204.4).

(b) Requests for approval under paragraph (a)(1) shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 10 business days before the proposed date for release.

(c) The Contractor agrees to include a similar requirement, including this paragraph (c), in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

(End of clause)

252.204-7001 Reserved.

252.204-7002 Payment for Contract Line or Subline Items Not Separately Priced.
As prescribed in 204.7109(a), use the following clause:

PAYMENT FOR CONTRACT LINE OR SUBLINE ITEMS NOT SEPARATELY PRICED (APR 2020)

(a) If the schedule in this contract contains any contract line or subline items identified as not separately priced (NSP), it means that the unit price for the NSP line or subline item is included in the unit price of another, related line or subline item.

(b) The Contractor shall not invoice the Government for an item that includes in its price an NSP item until—

(1) The Contractor has also delivered the NSP item included in the price of the item being invoiced; and

(2) The Government has accepted the NSP item.

(c) This clause does not apply to technical data.

(End of clause)

252.204-7003 Control of Government Personnel Work Product.
As prescribed in 204.404-70(b), use the following clause:

CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992)

The Contractor's procedures for protecting against unauthorized disclosure of information shall not require Department of Defense employees or members of the Armed Forces to relinquish control of their work products, whether classified or not, to the Contractor.

(End of clause)

252.204-7004 Antiterrorism Awareness Training for Contractors.
As prescribed in 204.7203, use the following clause:

ANTITERRORISM AWARENESS TRAINING FOR CONTRACTORS
(JAN 2023)

(a) *Definition.* As used in this clause—

"Military installation" means a base, camp, post, station, yard, center, or other activity under the jurisdiction of the Secretary of a military department or, in the case of an activity in a foreign country, under the operational control of the Secretary of a military department or the Secretary of Defense (see 10 U.S.C. 2801(c)(4)).

(b) *Training.* Contractor personnel who require routine physical access to a Federally-controlled facility or military installation shall complete Level I antiterrorism awareness training within 30 days of requiring access and annually thereafter. In accordance with Department of Defense Instruction O-2000.16 Volume 1, DoD Antiterrorism (AT) Program Implementation: DoD AT Standards, Level I antiterrorism awareness training shall be completed—

(1) Through a DoD-sponsored and certified computer or web-based distance learning instruction for Level I antiterrorism awareness; or

(2) Under the instruction of a Level I antiterrorism awareness instructor.

(c) *Additional information*. Information and guidance pertaining to DoD antiterrorism awareness training is available at *https://jko.jten.mil/* or as otherwise identified in the performance work statement.

(d) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts, including subcontracts for commercial products and commercial services, when subcontractor performance requires routine physical access to a Federally-controlled facility or military installation.

(End of clause)

252.204-7005 Reserved.

252.204-7006 Billing Instructions—Cost Vouchers.
As prescribed in 204.7109(b), use the following clause:

BILLING INSTRUCTIONS—COST VOUCHERS (MAY 2023)

When submitting a request for payment using a cost voucher, the Contractor shall—

(a) Identify the contract line item(s) on the payment request that reasonably reflect contract work performance; and

(b) Separately identify a payment amount for each contract line item included in the payment request.

(End of clause)

252.204-7007 Alternate A, Annual Representations and Certifications.
As prescribed in 204.1202, use the following provision:

ALTERNATE A, ANNUAL REPRESENTATIONS AND CERTIFICATIONS (OCT 2025)

Substitute the following paragraphs (b), (d), and (e) for paragraphs (b) and (d) of the provision at FAR 52.204-8:

(b)(1) If the provision at FAR 52.204-7, System for Award Management, is included in this solicitation, paragraph (e) of this provision applies.

(2) If the provision at FAR 52.204-7, System for Award Management, is not included in this solicitation, and the Offeror has an active registration in the System for Award Management (SAM), the Offeror may choose to use paragraph (e) of this provision instead of completing the corresponding individual representations and certifications in the solicitation. The Offeror shall indicate which option applies by checking one of the following boxes:

___ (i) Paragraph (e) applies.

___ (ii) Paragraph (e) does not apply and the Offeror has completed the individual representations and certifications in the solicitation.

(d)(1) The following representations or certifications in the SAM database are applicable to this solicitation as indicated:

(i) 252.204-7016, Covered Defense Telecommunications Equipment or Services—Representation. Applies to all solicitations.

(ii) 252.216-7008, Economic Price Adjustment—Wage Rates or Material Prices Controlled by a Foreign Government. Applies to solicitations for fixed-price supply and service contracts when the contract is to be performed wholly or in part in a foreign country, and a foreign government controls wage rates or material prices and may during contract performance impose a mandatory change in wages or prices of materials.

(iii) 252.225-7042, Authorization to Perform. Applies to all solicitations when performance will be wholly or in part in a foreign country.

(iv) 252.225-7049, Prohibition on Acquisition of Certain Foreign Commercial Satellite Services—Representations. Applies to solicitations for the acquisition of commercial satellite services.

(v) 252.225-7050, Disclosure of Ownership or Control by the Government of a Country that is a State Sponsor of Terrorism. Applies to all solicitations expected to result in contracts of $200,000 or more.

(vi) 252.229-7012, Tax Exemptions (Italy)—Representation. Applies to solicitations and contracts when contract performance will be in Italy.

(vii) 252.229-7013, Tax Exemptions (Spain)—Representation. Applies to solicitations and contracts when contract performance will be in Spain.

(2) The following representations or certifications in SAM are applicable to this solicitation as indicated by the Contracting Officer: *[Contracting Officer check as appropriate.]*

___ (i) 252.209-7002, Disclosure of Ownership or Control by a Foreign Government.

___ (ii) 252.225-7000, Buy American—Balance of Payments Program Certificate.

___ (iii) 252.225-7020, Trade Agreements Certificate.

___ Use with Alternate I.

___ (iv) 252.225-7031, Secondary Arab Boycott of Israel.

___ (v) 252.225-7035, Buy American—Free Trade Agreements—Balance of Payments Program Certificate.

___ Use with Alternate I.

___ Use with Alternate II.

___ Use with Alternate III.

___Use with Alternate IV.

___ Use with Alternate V.

___ (vi) 252.226-7002, Representation for Demonstration Project for Contractors Employing Persons with Disabilities.

___ (vii) 252.232-7015, Performance-Based Payments—Representation.

(e) The Offeror has completed the annual representations and certifications electronically via the SAM website at *https://www.sam.gov*. After reviewing the SAM database information, the Offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in FAR 52.204-8(c) and paragraph (d) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer, and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below *[Offeror to insert changes, identifying change by provision number, title, date]*. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

FAR/DFARS Provision #	Title	Date	Change

Any changes provided by the Offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications located in the SAM database.

(End of provision)

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.
As prescribed in 204.7304(a), use the following provision:

COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)

(a) *Definitions.* As used in this provision—

"Controlled technical information," "covered contractor information system," "covered defense information," "cyber incident," "information system," and "technical information" are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(b) The security requirements required by contract clause 252.204-7012, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2)—

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

(2)(i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.
As prescribed in 204.7304(b), use the following clause:

LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (JAN 2023)

(a) *Definitions.* As used in this clause—

"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.

"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 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.

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

"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.

"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) *Restrictions.* The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject the Contractor to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) *Subcontracts.* The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial products and commercial services, without alteration, except to identify the parties.

(End of clause)

252.204-7010 Requirement for Contractor to Notify DoD if the Contractor's Activities are Subject to Reporting Under the U.S.-International Atomic Energy Agency Additional Protocol.

As prescribed in 204.470-3, use the following clause:

REQUIREMENT FOR CONTRACTOR TO NOTIFY DOD IF THE CONTRACTOR'S ACTIVITIES ARE SUBJECT TO REPORTING UNDER THE U.S.-INTERNATIONAL ATOMIC ENERGY AGENCY ADDITIONAL PROTOCOL (JAN 2009)

(a) If the Contractor is required to report any of its activities in accordance with Department of Commerce regulations (15 CFR Part 781 *et seq.*) or Nuclear Regulatory Commission regulations (10 CFR Part 75) in order to implement the declarations required by the U.S.-International Atomic Energy Agency Additional Protocol (U.S.-IAEA AP), the Contractor shall—

(1) Immediately provide written notification to the following DoD Program Manager:

[Contracting Officer to insert Program Manager's name, mailing address, e-mail address, telephone number, and facsimile number];

(2) Include in the notification—

(i) Where DoD contract activities or information are located relative to the activities or information to be declared to the Department of Commerce or the Nuclear Regulatory Commission; and

(ii) If or when any current or former DoD contract activities and the activities to be declared to the Department of Commerce or the Nuclear Regulatory Commission have been or will be co-located or located near enough to one another to result in disclosure of the DoD activities during an IAEA inspection or visit; and

(3) Provide a copy of the notification to the Contracting Officer.

(b) After receipt of a notification submitted in accordance with paragraph (a) of this clause, the DoD Program Manager will—

(1) Conduct a security assessment to determine if and by what means access may be granted to the IAEA; or

(2) Provide written justification to the component or agency treaty office for a national security exclusion, in accordance with DoD Instruction 2060.03, Application of the National Security Exclusion to the Agreements Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States of America. DoD will notify the Contractor if a national security exclusion is applied at the Contractor's location to prohibit access by the IAEA.

(c) If the DoD Program Manager determines that a security assessment is required—

(1) DoD will, at a minimum—

(i) Notify the Contractor that DoD officials intend to conduct an assessment of vulnerabilities to IAEA inspections or visits;

(ii) Notify the Contractor of the time at which the assessment will be conducted, at least 30 days prior to the assessment;

(iii) Provide the Contractor with advance notice of the credentials of the DoD officials who will conduct the assessment; and

(iv) To the maximum extent practicable, conduct the assessment in a manner that does not impede or delay operations at the Contractor's facility; and

(2) The Contractor shall provide access to the site and shall cooperate with DoD officials in the assessment of vulnerabilities to IAEA inspections or visits.

(d) Following a security assessment of the Contractor's facility, DoD officials will notify the Contractor as to—

(1) Whether the Contractor's facility has any vulnerabilities where potentially declarable activities under the U.S.-IAEA AP are taking place;

(2) Whether additional security measures are needed; and

(3) Whether DoD will apply a national security exclusion.

(e) If DoD applies a national security exclusion, the Contractor shall not grant access to IAEA inspectors.

(f) If DoD does not apply a national security exclusion, the Contractor shall apply managed access to prevent disclosure of program activities, locations, or information in the U.S. declaration.

(g) The Contractor shall not delay submission of any reports required by the Department of Commerce or the Nuclear Regulatory Commission while awaiting a DoD response to a notification provided in accordance with this clause.

(h) The Contractor shall incorporate the substance of this clause, including this paragraph (h), in all subcontracts that are subject to the provisions of the U.S.-IAEA AP.

(End of clause)

252.204-7011 Reserved.

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)

252.204-7013 Reserved.

252.204-7014 Limitations on the Use or Disclosure of Information by Litigation Support Contractors.

As prescribed in 204.7403(a), use the following clause:

LIMITATIONS ON THE USE OR DISCLOSURE OF INFORMATION BY LITIGATION SUPPORT CONTRACTORS (JAN 2023)

(a) *Definitions.* As used in this clause—

"Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or

recompiled. Computer software does not include computer data bases or computer software documentation.

"Litigation information" means any information, including sensitive information, that is furnished to the contractor by or on behalf of the Government, or that is generated or obtained by the contractor in the performance of litigation support work under a contract. The term does not include information that is lawfully, publicly available without restriction, including information contained in a publicly available solicitation.

"Litigation support" means administrative, technical, or professional services provided in support of the Government during or in anticipation of litigation.

"Litigation support contractor" means a contractor (including its experts, technical consultants, subcontractors, and suppliers) providing litigation support under a contract that contains this clause.

"Sensitive information" means controlled unclassified information of a commercial, financial, proprietary, or privileged nature. The term includes technical data and computer software, but does not include information that is lawfully, publicly available without restriction.

"Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.

(b) *Limitations on use or disclosure of litigation information.* Notwithstanding any other provision of this contract, the Contractor shall—

(1) Access and use litigation information only for the purpose of providing litigation support under this contract;

(2) Not disclose litigation information to any entity outside the Contractor's organization unless, prior to such disclosure the Contracting Officer has provided written consent to such disclosure;

(3) Take all precautions necessary to prevent unauthorized disclosure of litigation information;

(4) Not use litigation information to compete against a third party for Government or nongovernment contracts; and

(5) Upon completion of the authorized litigation support activities, destroy or return to the Government at the request of the Contracting Officer all litigation information in its possession.

(c) Violation of paragraph (b)(1), (b)(2), (b)(3), (b)(4), or (b)(5) of this clause, is a basis for the Government to terminate this contract.

(d) *Indemnification and creation of third party beneficiary rights.* The Contractor agrees—

(1) To indemnify and hold harmless the Government, its agents, and employees from any claim or liability, including attorneys' fees, court costs, and expenses, arising out of, or in any way related to, the misuse or unauthorized modification, reproduction, release, performance, display, or disclosure of any litigation information; and

(2) That any third party holding proprietary rights or any other legally protectable interest in any litigation information, in addition to any other rights it may have, is a third party beneficiary under this contract who shall have a right of direct action against the Contractor, and against any person to whom the Contractor has released or disclosed such litigation information, for any such unauthorized use or disclosure of such information.

(e) *Contractor employees.* The Contractor shall ensure that its employees are subject to use and nondisclosure obligations consistent with this clause prior to the employees being provided access to or use of any litigation information covered by this clause.

(f) *Subcontracts.* Include the substance of this clause, including this paragraph (f), in all subcontracts, including subcontracts for commercial products or commercial services.

(End of clause)

252.204-7015 Notice of Authorized Disclosure of Information for Litigation Support.

As prescribed in 204.7403(b), use the following clause:

NOTICE OF AUTHORIZED DISCLOSURE OF INFORMATION FOR LITIGATION SUPPORT (JAN 2023)

(a) *Definitions.* As used in this clause—

"Computer software" means computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, formulae, and related material that would enable the software to be reproduced, recreated, or recompiled. Computer software does not include computer data bases or computer software documentation.

"Litigation support" means administrative, technical, or professional services provided in support of the Government during or in anticipation of litigation.

"Litigation support contractor" means a contractor (including its experts, technical consultants, subcontractors, and suppliers) providing litigation support under a contract that contains the clause at 252.204-7014, Limitations on the Use or Disclosure of Information by Litigation Support Contractors.

"Sensitive information" means controlled unclassified information of a commercial, financial, proprietary, or privileged nature. The term includes technical data and computer software, but does not include information that is lawfully, publicly available without restriction.

"Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.

(b) *Notice of authorized disclosures.* Notwithstanding any other provision of this solicitation or contract, the Government may disclose to a litigation support contractor, for the sole purpose of litigation support activities, any information, including sensitive information, received--

(1) Within or in connection with a quotation or offer; or

(2) In the performance of or in connection with a contract.

(c) *Subcontracts.* Include the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for commercial products or commercial services.

(End of clause)

252.204-7016 Covered Defense Telecommunications Equipment or Services—Representation.
As prescribed in 204.2105(a), use the following provision:

COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (DEC 2019)

(a) *Definitions.* As used in this provision, "covered defense telecommunications equipment or services" has the meaning provided in the clause 252.204-7018, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov/) for entities excluded from receiving federal awards for "covered defense telecommunications equipment or services".

(c) *Representation.* The Offeror represents that it [ ] does, [ ] does not provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(End of provision)

252.204-7017 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services—Representation.
As prescribed in 204.2105(b), use the following provision:

PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES—REPRESENTATION (MAY 2021)

The Offeror is not required to complete the representation in this provision if the Offeror has represented in the provision at 252.204-7016, Covered Defense Telecommunications Equipment or Services—Representation, that it "does not provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument."

(a) *Definitions*. "Covered defense telecommunications equipment or services," "covered mission," "critical technology," and "substantial or essential component," as used in this provision, have the meanings given in the 252.204-7018 clause, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services, of this solicitation.

(b) *Prohibition*. Section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits agencies from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(c) *Procedures*. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at *https://www.sam.gov* for entities that are excluded when providing any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless a waiver is granted.

(d) *Representation*. If in its annual representations and certifications in SAM the Offeror has represented in paragraph (c) of the provision at 252.204-7016, Covered Defense Telecommunications Equipment or Services—Representation, that it "does" provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument, then the Offeror shall complete the following additional representation:

The Offeror represents that it [ ] will [ ] will not provide covered defense telecommunications equipment or services as a part of its offered products or services to DoD in the performance of any award resulting from this solicitation.

(e) *Disclosures*. If the Offeror has represented in paragraph (d) of this provision that it "will provide covered defense telecommunications equipment or services," the Offeror shall provide the following information as part of the offer:

(1) A description of all covered defense telecommunications equipment and services offered (include brand or manufacturer; product, such as model number, original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable).

(2) An explanation of the proposed use of covered defense telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition referenced in paragraph (b) of this provision.

(3) For services, the entity providing the covered defense telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known).

(4) For equipment, the entity that produced or provided the covered defense telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

(End of provision)

252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services.
As prescribed in 204.2105(c), use the following clause:

PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (JAN 2023)

(a) *Definitions*. As used in this clause—

"Covered defense telecommunications equipment or services" means—

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities;

(2) Telecommunications services provided by such entities or using such equipment; or

(3) Telecommunications equipment or services produced or provided by an entity that the Secretary of Defense reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Covered foreign country" means—

(1) The People's Republic of China; or

(2) The Russian Federation.

"Covered missions" means—

(1) The nuclear deterrence mission of DoD, including with respect to nuclear command, control, and communications, integrated tactical warning and attack assessment, and continuity of Government; or

(2) The homeland defense mission of DoD, including with respect to ballistic missile defense.

"Critical technology" means—

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled—

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition*. In accordance with section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91), the contractor shall not provide to the Government any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless the covered defense telecommunication equipment or services are covered by a waiver described in Defense Federal Acquisition Regulation Supplement 204.2104.

(c) *Procedures*. The Contractor shall review the list of excluded parties in the System for Award Management (SAM) at *https://www.sam.gov* for entities that are excluded when providing any equipment, system, or service, to carry out covered missions, that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless a waiver is granted.

(d) *Reporting*.

(1) In the event the Contractor identifies covered defense telecommunications equipment or services used as a substantial or essential

component of any system, or as critical technology as part of any system, during contract performance, the Contractor shall report at *https://dibnet.dod.mil* the information in paragraph (d)(2) of this clause.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:

(i) Within 3 business days from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 30 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered defense telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts*. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services.

(End of clause)

252.204-7019 Notice of NIST SP 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) (https://www.sprs.csd.disa.mil/) 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 webptsmh@navy.mil 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 800-171 DoD 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) (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 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).

(2) 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 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 products or commercial services (excluding commercially available off-the-shelf 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/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 webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.

(End of clause)

252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements.
As prescribed in 204.7504(a), use the following clause:

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: _____ *Contracting Officer insert: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC)* 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 or 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)

252.204-7022 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)

252.204-7023 Reporting Requirements for Contracted Services.
Basic. As prescribed in 204.1705(a)(i) and (ii), use the following clause:

REPORTING REQUIREMENTS FOR CONTRACTED SERVICES—BASIC
(JUL 2021)

(a) *Definition.* As used in this clause—

"First-tier subcontract" means a subcontract awarded directly by the contractor for the purpose of acquiring services for performance of a prime contract. It does not include the contractor's supplier agreements with vendors, such as long-term arrangements for materials or supplies or services that benefit multiple contracts and/or the costs of which are normally applied to a contractor's general and administrative expenses or indirect costs.

(b) The Contractor shall report annually, by October 31, at *https://www.sam.gov*, on the services performed under this contract or order, including any first-tier subcontracts, during the preceding Government fiscal year (October 1 - September 30).

(c) The Contractor shall report the following information for the contract or order:

(1) The total dollar amount invoiced for services performed during the preceding Government fiscal year under the contract or order.

(2) The number of Contractor direct labor hours, to include first-tier subcontractor direct labor hours, as applicable, expended on the services performed under the contract or order during the previous Government fiscal year.

(d) The Government will review the Contractor's reported information for reasonableness and consistency with available contract information. In the event the Government believes that revisions to the Contractor's reported information are warranted, the Government will notify the Contractor. Upon notification, the Contractor shall revise the reported information or provide the Government with a supporting rationale for the information.

(End of clause)

Alternate I. As prescribed in 204.1705(a)(i) and (iii), use the following clause, which substitutes "contract or agreement for each order" in lieu of "contract or order" in paragraph (b) and "order" in lieu of "contract or order" in paragraphs (c) and (c)(1) and (2), and identifies the dollar threshold and service acquisition portfolio groups for which orders under the contract or agreement require service contract reporting.

REPORTING REQUIREMENTS FOR CONTRACTED SERVICES—ALTERNATE I (JUL 2021)

(a) *Definition.* As used in this clause—

"First-tier subcontract" means a subcontract awarded directly by the contractor for the purpose of acquiring services for performance of a prime contract. It does not include the contractor's supplier agreements with vendors, such as long-term arrangements for materials or supplies or services that benefit multiple contracts and/or the costs of which are normally applied to a contractor's general and administrative expenses or indirect costs.

(b) The contractor shall report annually, by October 31, at https://www.sam.gov, on services performed during the preceding Government fiscal year (October 1 - September 30) under this contract or agreement for each order, including any first-tier subcontract, which exceeds $3 million for services in the following service acquisition portfolio groups:

(1) Logistics management services.

(2) Equipment-related services.

(3) Knowledge-based services.

(4) Electronics and communications services.

(c) The Contractor shall report the following information for the order:

(1) The total dollar amount invoiced for services performed during the preceding Government fiscal year under the order.

(2) The number of Contractor direct labor hours, to include first-tier subcontractor direct labor hours, as applicable, expended on the services performed under the order during the previous Government fiscal year.

(d) The Government will review the Contractor's reported information for reasonableness and consistency with available contract information. In the event the Government believes that revisions to the Contractor's reported information are warranted, the Government will notify the Contractor. Upon notification, the Contractor shall revise the reported information or provide the Government with a supporting rationale for the information.

(End of clause)

252.204-7024 Notice on the Use of the Supplier Performance Risk System.
As prescribed in 204.7604, use the following provision:

NOTICE ON THE USE OF THE SUPPLIER PERFORMANCE RISK SYSTEM
(MAR 2023)

(a) *Definitions.* As used in this provision—

"Item risk" means the probability that a product, based on intended use, will introduce performance risk resulting in safety issues, mission degradation, or monetary loss.

"Price risk" means a measure of whether a proposed price for a product or service is consistent with historical prices paid for that item or service.

"Supplier risk" means the probability that an award may subject the procurement to the risk of unsuccessful performance or to supply chain risk (see Defense Federal Acquisition Regulation Supplement 239.7301).

(b) The Supplier Performance Risk System (SPRS), available at *https://piee.eb.mil/*, will be used in the evaluation of the Quoter or Offeror's performance. SPRS retrieves item, price, quality, delivery, and contractor information on contracts from Government reporting systems in order to develop risk assessments.

(c) The Contracting Officer will consider SPRS risk assessments during the evaluation of quotations or offers received in response to this solicitation as follows:

(1) Item risk will be considered to determine whether the procurement represents a high performance risk to the Government.

(2) Price risk will be considered in determining if a proposed price is consistent with historical prices paid for a product or a service or otherwise creates a risk to the Government.

(3) Supplier risk, including but not limited to quality and delivery, will be considered to assess the risk of unsuccessful performance and supply chain risk.

(d) SPRS risk assessments are generated daily. Quoters or Offerors are able to access their risk assessments by following the access instructions in the SPRS user's guide available at *https://www.sprs.csd.disa.mil/reference.htm*. Quoters and Offerors are granted access to SPRS for their own risk assessment classifications only. SPRS reporting procedures and risk assessment methodology are detailed in the SPRS user's guide. The method to challenge a rating generated by SPRS is also provided in the user's guide. SPRS evaluation criteria are available at *https://www.sprs.csd.disa.mil/pdf/SPRS_DataEvaluationCriteria.pdf*.

(e) The Contracting Officer may consider any other available and relevant information when evaluating a quotation or an offer.

(End of provision)

252.204-7025 Notice of Cybersecurity Maturity Model Certification Level Requirements.
As prescribed in 204.7504(b), use the following provision:

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: _____ *[Contracting Officer insert: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC)].* 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)