OFFICE OF THE ASSISTANT SECRETARY OF WAR
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

In reply refer to
DARS Tracking Number: 2026-O0025

MEMORANDUM FOR COMMANDER, UNITED STATES CYBER COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND (ATTN: ACQUISITION EXECUTIVE)
COMMANDER, UNITED STATES TRANSPORTATION COMMAND (ATTN: ACQUISITION EXECUTIVE)
DEPUTY ASSISTANT SECRETARY OF THE ARMY (PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE NAVY (PROCUREMENT)
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE (CONTRACTING)
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Class Deviation—Revolutionary Federal Acquisition Regulation (FAR) Overhaul Part 40, Defense FAR Supplement (DFARS) Part 240

Effective February 1, 2026, contracting officers shall use—

- The revised FAR Part 40, Information Security and Supply Chain Security published on the Revolutionary FAR Overhaul web page at https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-40 in lieu of the text codified at 48 CFR chapter 1 (https://www.ecfr.gov).

- The attached new DFARS Part 240, Information Security and Supply Chain Security; and

- The attached new DFARS Procedures, Guidance, and Information (PGI) 240, Information Security and Supply Chain Security.

This class deviation implements the following:

- Section 2 of E.O. 14275, Restoring Common Sense to Federal Procurement, which establishes the policy that the FAR "should only contain provisions required by statute or essential to sound procurement, and any FAR provisions that do not advance these objectives should be removed.

- Section 4(a) of E.O. 14265, Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base which requires the Secretary of War to

eliminate or revise any unnecessary supplemental regulations or any other internal guidance, such as relevant parts of the Financial Management Regulation and Defense Federal Acquisition Regulation Supplement.

- The Office of Management and Budget memorandum, M-25-26 issued on May 2, 2025, titled, Overhauling the Federal Acquisition Regulation, which provided additional guidance to federal agencies regarding the FAR overhaul.

This class deviation remains in effect until rescinded or incorporated into the FAR, DFARS, and DFARS PGI. Inquiries regarding this class deviation can be addressed to osd.pentagon.ousd-a-s.mbx.dfars@mail.mil.

TENAGLIA.JOHN.M.1154945926 Digitally signed by TENAGLIA.JOHN.M.1154945926 Date: 2025.12.18 14:18:45 -05'00'

John M. Tenaglia
Principal Director,
Defense Pricing, Contracting, and Acquisition Policy

Attachments:
As stated

PART 240—INFORMATION SECURITY AND SUPPLY CHAIN SECURITY

SUBPART 240.2—SECURITY PROHIBITIONS AND EXCLUSIONS

240.270 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

240.270-1 Scope.
This section implements section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) and section 889(a)(1)(A) of the National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232).

240.270-2 Definitions.
As used in this section—

"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.

240.270-3 Prohibition.
In addition to the prohibition at FAR 40.202(d), unless the covered defense telecommunications equipment or services are subject to a waiver described in 240.270-5 the contracting officer must not procure or obtain, or extend or renew a contract (*e.g.,* exercise an option) 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.

240.270-4 Procedures.

(a) *Representations.*

(1) (i) If the offeror selects "does not" in response to the provision at DFARS 252.204-7016, the contracting officer may rely on the representation, unless the contracting officer has an independent reason to question the representation. If the contracting officer has a reason to question the "does not" representation in 252.204-7016, then the contracting officer must consult with the requiring activity and legal counsel.

(ii) If the offeror selects "does" in paragraph (c) of the provision at DFARS 252.204-7016, the offeror must complete the representation at DFARS 252.204-7017.

(2)(i) If the offeror selects "will not" in paragraph (d) of the provision at DFARS 252.204-7017, the contracting officer may rely on the representation, unless the contracting officer has an independent reason to question the representation. If the contracting officer has a reason to question the "will not" representation in FAR 52.240-90 or DFARS 252.204-7017, then the contracting officer must consult with the requiring activity and legal counsel.

(ii) If an offeror selects "will" in paragraph (d) of the provision at DFARS 252.204-7017, the offeror must provide the information required by paragraph (e) of the provision. When an offeror completes paragraph (e) of either of the provisions at FAR 52.240-90 or DFARS 252.204-7017, the contracting officer must—

(A) Forward the offeror's representation and disclosure information to the requiring activity; and

(B) Not award to the offeror unless the requiring activity advises—

(*1*) For equipment, systems, or services that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, that a waiver as described at FAR 40.203-3 has been granted; or

(*2*) For equipment, systems, or services to be used to carry out covered missions that use covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, that a waiver as described at DFARS 240.270-5 has been granted.

(b) *Reporting.* If a contractor reports information to *https://dibnet.dod.mil* in accordance with the clause at FAR 52.240-91 or DFARS 252.204-7018, the Defense Cyber Crime Center will notify the contracting officer, who will consult with the requiring activity on how to proceed with the contract.

240.270-5 Waivers.

The Secretary of Defense may waive the prohibition in 240.270-3 on a case-by-case basis for a single, one-year period, if the Secretary—

(a) Determines such waiver to be in the national security interests of the United States; and

(b) Certifies to the Congressional defense committees that—

(1) There are sufficient mitigations in place to guarantee the ability of the Secretary to carry out the covered missions; and

(2) The Secretary is removing the use of covered defense telecommunications equipment or services in carrying out such missions.

240.270-6 Solicitation provisions and contract clause.

(a) Insert the provision at 252.204-7016, Covered Defense Telecommunications Equipment or Services—Representation, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial products and commercial services, and solicitations for task orders and delivery orders, basic ordering agreements (BOAs), orders against BOAs, blanket purchase agreements (BPAs), and calls against BPAs.

(b) Insert the provision at 252.204-7017, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services—Representation, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial products and commercial services, and solicitations for task orders and delivery orders, BOAs, orders against BOAs, BPAs, and calls against BPAs.

(c) Insert the clause at 252.204-7018, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services, in all solicitations and resultant awards, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, and solicitations and awards for task orders and delivery orders, BOAs, orders against BOAs, BPAs, and calls against BPAs.

240.271 Requirements for Information Relating to Supply Chain Risk.

240.271-1 Scope.
This subpart implements 10 U.S.C. 3252 and elements of DoD Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), at *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=2018-11-08-075800-903.*

240.271-2 Definitions.

As used in this section—

"Covered item of supply" means an item of information technology that is purchased for inclusion in a covered system, and the loss of integrity of which could result in a supply chain risk for a covered system (see 10 U.S.C. 3252).

"Covered system" means a national security system, as that term is defined at 44 U.S.C. 3552(b) (see 10 U.S.C. 3252). It is any information system, including any telecommunications system, used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(1) The function, operation, or use of which—

(i) Involves intelligence activities;

(ii) Involves cryptologic activities related to national security;

(iii) Involves command and control of military forces;

(iv) Involves equipment that is an integral part of a weapon or weapons system; or

(v) Is critical to the direct fulfillment of military or intelligence missions but this does not include a system that is to be used for routine administrative and business applications, including payroll, finance, logistics, and personnel management applications; or

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

"Information technology" (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—

(i) Its use; or

(ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(2) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(3) The term "information technology" does not include any equipment acquired by a contractor incidental to a contract.

"Supply chain risk" means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (see 10 U.S.C. 3252).

240.271-3 Applicability.

Notwithstanding FAR part 39.001, apply this section to acquisition of information technology for covered systems (see 10 U.S.C. 3252), for procurements involving—

(a) A source selection for a covered system or a covered item of supply involving either a performance specification (see 10 U.S.C. 3206(a)(3)(B)), or an evaluation factor (see 10 U.S.C. 3206(b)(1)), relating to supply chain risk;

(b) The consideration of proposals for and issuance of a task or delivery order for a covered system or a covered item of supply where the task or delivery order contract concerned includes a requirement relating to supply chain risk (see 10 U.S.C. 3406(d)(3) and FAR 16.507-5(b)(2); or

(c) Any contract action involving a contract for a covered system or a covered item of supply where such contract includes a requirement relating to supply chain risk.

240.271-4 Authorized individuals.

(a) Subject to 240.271-5, the following individuals are authorized to take the actions authorized by 240.271-6:

(1) The Secretary of Defense.

(2) The Secretary of the Army.

(3) The Secretary of the Navy.

(4) The Secretary of the Air Force.

(b) The individuals authorized at paragraph (a) may not delegate the authority to take the actions at 240.271-6 or the responsibility for making the determination required by 240.271-5 to an official below the level of—

(1) For the Department of Defense, the Under Secretary of Defense for Acquisition and Sustainment; and,

(2) For the military departments, the service acquisition executive for the department concerned.

240.271-5 Determination and notification.

The individuals authorized in 240.271-4 may exercise the authority provided in 240.271-6 only after—

(a) Obtaining a joint recommendation by the Under Secretary of Defense for Acquisition and Sustainment and the Chief Information Officer of the Department of Defense, on the basis of a risk assessment by the Under Secretary of Defense for Intelligence, that there is a significant supply chain risk to a covered system;

(b) Making a determination in writing, in unclassified or classified form, with the concurrence of the Under Secretary of Defense for Acquisition and Sustainment, that—

(1) Use of the authority in 240.271-6(a), (b), or (c) is necessary to protect national security by reducing supply chain risk;

(2) Less intrusive measures are not reasonably available to reduce such supply chain risk; and

(3) In a case where the individual authorized in 240.271-4 plans to limit disclosure of information under 240.271-6(d), the risk to national security due to the disclosure of such information outweighs the risk due to not disclosing such information; and

(c)(1) Providing a classified or unclassified notice of the determination made under paragraph (b) of this section—

(i) In the case of a covered system included in the National Intelligence Program or the Military Intelligence Program, to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the congressional defense committees; and

(ii) In the case of a covered system not otherwise included in paragraph (a) of this section, to the congressional defense committees; and

(2) The notice must include—

(i) The following information (see 10 U.S.C. 3204(e)(2)):

(A) A description of the agency's needs.

(B) An identification of the statutory exception from the requirement to use competitive procedures and a demonstration, based on the proposed

contractor's qualifications or the nature of the procurement, of the reasons for using that exception.

(C) A determination that the anticipated cost will be fair and reasonable.

(D) A description of the market survey conducted or a statement of the reasons a market survey was not conducted.

(E) A listing of the sources, if any, that expressed in writing an interest in the procurement.

(F) A statement of the actions, if any, the agency may take to remove or overcome any barrier to competition before a subsequent procurement for such needs;

(ii) The joint recommendation by the Under Secretary of Defense for Acquisition and Sustainment and the Chief Information Officer of the Department of Defense as specified in paragraph (a) of this section;

(iii) A summary of the risk assessment by the Under Secretary of Defense for Intelligence that serves as the basis for the joint recommendation specified in paragraph (a) of this section; and

(iv) A summary of the basis for the determination, including a discussion of less intrusive measures that were considered and why they were not reasonably available to reduce supply chain risk.

240.271-6 Exclusion and limitation on disclosure.

Subject to 240.271-5, the individuals authorized in 240.271-4 may, in the course of procuring 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—

(a) Exclude a source that fails to meet qualification standards established in accordance with the requirements of 10 U.S.C. 3243, for the purpose of reducing supply chain risk in the acquisition of covered systems;

(b) Exclude a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order;

(c) Withhold consent for a contractor to subcontract with a particular source or direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract; and

(d) Limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information relating to the basis for carrying out any of the actions

authorized by paragraphs (a) through (c) of this section, and if such disclosures are so limited—

(1) No action undertaken by the individual authorized under such authority must be subject to review in a bid protest before the Government Accountability Office or in any Federal court; and

(2) The authorized individual must—

(i) Notify appropriate parties of action taken under paragraphs (a) through (d) of this section and the basis for such action only to the extent necessary to effectuate the action;

(ii) Notify other Department of Defense components or other Federal agencies responsible for procurements that may be subject to the same or similar supply chain risk, in a manner and to the extent consistent with the requirements of national security; and

(iii) Ensure the confidentiality of any such notifications.

240.271-7 Solicitation provision and contract clause.

(a) Insert the provision at 252.239-7017, Notice of Supply Chain Risk, in solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology, whether acquired 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 at 240.271-2.

(b) Insert the clause at 252.239-7018, Supply Chain Risk, in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology, whether acquired 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 at 240.271-2.

240.272 Prohibited Sources.

240.272-1 Restrictions administered by the Department of the Treasury on acquisitions of supplies or services from prohibited sources.
DoD personnel are authorized to make emergency acquisitions in direct support of U.S. or allied forces deployed in military contingency, humanitarian, or peacekeeping operations in a country or region subject to economic sanctions administered by the Department of the Treasury, Office of Foreign Assets Control.

240.272-2 Prohibition on acquisition of certain items from Communist Chinese military companies.
This section implements section 1211 of the National Defense Authorization Act for Fiscal Year 2006 (Pub. L. 109-163), section 1243 of the National Defense

Authorization Act for Fiscal Year 2012 (Pub. L. 112-81), and section 1296 of the National Defense Authorization Act for Fiscal Year 2017 (Pub. L. 114-328). See PGI 240.272-2 for additional information relating to this statute, the terms used in this section, the United States Munitions List (USML), and the 600 series of the Commerce Control List (CCL).

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

"Component" means an item that is useful only when used in conjunction with an end item (15 CFR 772.1 and 22 CFR 120.45(b)).

"Item" means—

(1) A USML defense article, as defined at 22 CFR 120.6;

(2) A USML defense service, as defined at 22 CFR 120.9; or

(3) A 600 series item, as defined at 15 CFR 772.1.

"Part" means any single unassembled element of a major or minor component, accessory, or attachment, that is not normally subject to disassembly without the destruction or impairment of designed use (15 CFR 772.1 and 22 CFR 120.45(d)).

(b) *Prohibition.* Do not acquire items covered by the USML or the 600 series of the CCL, through a contract or subcontract at any tier, from any Communist Chinese military company. This prohibition does not apply to components and parts of covered items unless the components and parts are themselves covered by the USML or the 600 series of the CCL.

(c) *Exceptions.* The prohibition in paragraph (b) of this section does not apply to items acquired—

(1) In connection with a visit to the People's Republic of China by a vessel or an aircraft of the U.S. armed forces;

(2) For testing purposes; or

(3) For the purpose of gathering intelligence.

(d) *Identifying items covered by the USML or the 600 series of the CCL.*

(1) Before issuance of a solicitation, the requiring activity will notify the contracting officer in writing whether the items to be acquired are covered by the USML or the 600 series of the CCL. The notification will identify any covered item(s) and will provide the pertinent USML reference(s) from 22 CFR part 121 or the 600 series of the CCL references from 15 CFR part 774, Supplement No. 1.

(2) The USML includes defense articles and defense services that fall into 21 categories. The CCL includes ten categories and five product groups in each category, many of which contain 600 series items. Since not all items covered by the

USML or 600 series of the CCL are themselves munitions (e.g., protective personnel equipment, military training equipment), the requiring activity should consult the USML and the 600 series of the CCL before concluding that an item is or is not covered. See PGI 240.272-2(d).

(e) *Waiver of prohibition.*

(1) The prohibition in paragraph (b) of this section may be waived, on a case-by-case basis, if an official identified in paragraph (b) of this section determines that a waiver is necessary for national security purposes.

(2) The following officials are authorized, without power of delegation, to make the determination specified in paragraph (a) of this section:

(i) The Under Secretary of Defense (Acquisition and Sustainment).

(ii) The Secretaries of the military departments.

(iii) The Component Acquisition Executive of the Defense Logistics Agency.

(3)(i) The official granting a waiver must submit a report to the congressional defense committees, with a copy to the Principal Director, Defense Pricing, Contracting, and Acquisition Policy (see PGI 240.272-2), not less than 15 days before issuing the waiver.

(ii) In the report, the official must—

(A) Identify the specific reasons for the waiver; and

(B) Include recommendations as to what actions may be taken to develop alternative sourcing capabilities in the future.

(f) *Contract clause.* Unless an exception in paragraph (c) of this section applies, insert the clause at 252.225-7007 , Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies, in solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, involving the delivery of items covered by the United States Munitions List or the 600 series of the Commerce Control List.

240.272-3 Prohibition on contracting or subcontracting with a firm that is owned or controlled by the government of a country that is a state sponsor of terrorism.

(a) *Scope.* This section implements 10 U.S.C. 4871(b).

(b) *Definition.* As used in this section—

"State sponsor of terrorism," is defined in the provision at 252.225-7050, Disclosure of Ownership or Control by the Government of a Country that is a State Sponsor of Terrorism.

(c) *Prohibition.*

(1) Do not award a contract of $200,000 or more to a firm when a foreign government that is a state sponsor of terrorism owns or controls, either directly or indirectly, a significant interest in—

(i) The firm;

(ii) A subsidiary of the firm; or

(iii) Any other firm that owns or controls the firm.

(2) For restrictions on subcontracting with a firm, or a subsidiary of a firm, that is identified by the Secretary of Defense as being owned or controlled by the government of a country that is a state sponsor of terrorism, see part 209.

(d) *Notification.* Forward any disclosure that the government of a country that is a state sponsor of terrorism has a significant interest in an offeror, a subsidiary of an offeror, or any other firm that owns or controls an offeror through agency channels to the address at PGI 240.272-3(d).

(e) *Waiver of prohibition.* The prohibition in paragraph (c) of this section may be waived if the Secretary of Defense determines that a waiver is not inconsistent with the national security objectives of the United States in accordance with 10 U.S.C. 4871(c).

(e) *Solicitation provision.* Insert the provision at 252.225-7050, Disclosure of Ownership or Control by the Government of a Country that is a State Sponsor of Terrorism, in solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial products and commercial services (other than commercial satellite services), that are expected to result in contracts of $200,000 or more. If the solicitation includes the provision at FAR 52.204-7, do not separately list the provision 252.225-7050 in the solicitation.

240.272-4 Prohibition on acquisition of certain foreign commercial satellite services.

(a) *Scope.* This section implements 10 U.S.C. 2279.

(b) *Definitions.* As used in this section—

"Covered foreign country" means—

(1) The People's Republic of China;

(2) North Korea;

(3) The Russian Federation; or

(4) Any country that is a state sponsor of terrorism. (10 U.S.C. 2279)

"Cybersecurity risk" means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism. (10 U.S.C. 2279)

"Foreign entity" means—

(1) Any branch, partnership, group or sub-group, association, estate, trust, corporation or division of a corporation, or organization organized under the laws of a foreign state if either its principal place of business is outside the United States or its equity securities are primarily traded on one or more foreign exchanges.

(2) Notwithstanding paragraph (1) of this definition, any branch, partnership, group or sub-group, association, estate, trust, corporation or division of a corporation, or organization that demonstrates that a majority of the equity interest in such entity is ultimately owned by U.S. nationals is not a foreign entity. (31 CFR 800.212)

"Government of a covered foreign country" includes the state and the government of a covered foreign country, as well as any political subdivision, agency, or instrumentality thereof.

"Launch vehicle" means a fully integrated space launch vehicle. (10 U.S.C. 2279)

"Satellite services" means communications capabilities that utilize an on-orbit satellite for transmitting the signal from one location to another.

"State sponsor of terrorism" means a country determined by the Secretary of State, under section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (Title XVII, Subtitle B, of the National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232), to be a country the government of which has repeatedly provided support for acts of international terrorism. As of December 14, 2020, state sponsors of terrorism include Iran, North Korea, and Syria. (10 U.S.C. 4871).

(c) *Prohibitions.*
Except as provided in paragraph (e) of this section, do not award a contract for commercial satellite services to—

(1)(i) A foreign entity if the Under Secretary of Defense for Acquisition and Sustainment or the Under Secretary of Defense for Policy reasonably believes that—

(A) The foreign entity is an entity in which the government of a covered foreign country has an ownership interest that enables the government to affect satellite operations;

(B) The foreign entity plans to or is expected to provide satellite services under the contract from a covered foreign country; or

(C) Entering into such contract would create an unacceptable cybersecurity risk for DoD, as determined by the Under Secretary of Defense for Acquisition and Sustainment or the Under Secretary of Defense for Policy; or

(ii) An offeror that is offering commercial satellite services provided by a foreign entity as described in paragraph (1) of this section; or

(2)(i) Any entity, except as provided in paragraph (c)(2)(ii) of this section, for a launch that occurs on or after December 31, 2022, if the Under Secretary of Defense for Acquisition and Sustainment or the Under Secretary of Defense for Policy reasonably believes that such satellite services will be provided using satellites that will be—

(A) Designed or manufactured—

(*1*) In a covered foreign country; or

(*2*) By an entity controlled in whole or in part by, or acting on behalf of, the government of a covered foreign country; or

(B) Launched outside the United States using a launch vehicle that is—

(*1*) Designed or manufactured in a covered foreign country; or

(*2*) Provided by—

(i) The government of a covered foreign country; or

(ii) An entity controlled in whole or in part by, or acting on behalf of, the government of a covered foreign country.

(ii) The prohibition in paragraph (c)(2)(i) of this section does not apply with respect to launch services for which a satellite service provider has a contract or other agreement that, prior to June 10, 2018, was either fully paid for by the satellite service provider or covered by a legally binding commitment of the satellite service provider to pay for such services.

(d) *Procedures.*

(1)(ii) Do not award to any source that is a foreign satellite service provider or is offering satellite services provided by a foreign entity if such award presents an unacceptable cybersecurity risk, as determined by the Under Secretary of Defense for Acquisition and Sustainment or the Under Secretary of Defense for Policy.

(ii) When procuring commercial satellite services from a foreign entity, the contracting officer must review the exclusion records in the System for Award Management (SAM) database as required at FAR 9.405, to ensure that an entity identified in, or otherwise known to be involved in, the otherwise successful offer is not listed as ineligible in the SAM database (see FAR 9.405).

(2) If an offeror discloses information in accordance with paragraph (c) of the provision 252.225-7049, Prohibition on Acquisition of Certain Foreign Commercial Satellite Services—Representations, the contracting officer—

(i) Must forward the information regarding the offeror through agency channels to the address at PGI 240.272-4(d); and

(ii) Must not award to that offeror, unless an exception is determined to apply in accordance with paragraph (e) of this section.

(3)(i) If the otherwise successful offeror provides negative responses to all representations in the provision at 252.225-7049, the contracting officer may rely on the representations, unless the contracting officer has an independent reason to question the representations.

(1ii) If the contracting officer has an independent reason to question a negative representation of the otherwise successful offeror, the contracting officer must consult with the office specified in PGI 240.272-4(d), prior to deciding whether to award to that offeror.

(e) *Exception.*

(1) The prohibitions in 240.272-4(c)(1) and (c)(2) do not apply if–

(i) The Under Secretary of Defense for Acquisition and Sustainment, or the Under Secretary of Defense for Policy, without power of redelegation, determines that it is in the national security interest of the United States to enter into such contract; and

(ii) Not later than seven days before entering into such contract, the Under Secretary of Defense making the determination in paragraph (e)(1)(i) of this section, in consultation with the Director of National Intelligence, submits to the congressional defense committees a national security assessment, in accordance with 10 U.S.C. 2279.

(2) If requesting an exception pursuant to paragraph (e)(1) of this section, the contracting officer must forward the request through agency channels to the address at PGI 240.272-4, providing any available information necessary for the Under Secretary of Defense making the determination in paragraph (e)(1)(i) of this section to evaluate the request and perform a national security assessment, in accordance with 10 U.S.C. 2279.

(f) *Solicitation provision and contract clauses.*

(1) Insert the provision at 252.225-7049, Prohibition on Acquisition of Certain Foreign Commercial Satellite Services—Representations, in solicitations that include the clause at 252.225-7051, Prohibition on Acquisition of Certain Foreign Commercial Satellite Services. If the solicitation includes the provision at FAR 52.204-7, do not separately list the provision 252.225-7049 in the solicitation.

(2) Insert the clause at 252.225-7051, Prohibition on Acquisition of Certain Foreign Commercial Satellite Services, in solicitations and contracts for the acquisition of commercial satellite services, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services.

(3) Insert the clause at 252.239-7018, Supply Chain Risk, as prescribed at 240.271-7(b), when applicable.

SUBPART 240.3—SAFEGUARDING INFORMATION

240.370 Safeguarding Covered Defense Information and Cyber Incident Reporting.

240.370-1 Scope.

(a) This section applies to contracts and subcontracts requiring contractors and subcontractors to safeguard covered defense information that resides in or transits through covered contractor information systems by applying specified network security requirements. It also requires reporting of cyber incidents.

(b) This section 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.

240.370-2 Definitions.

As used in this section—

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

"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.

"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 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.

"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 the 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.

240.370-3 Policy.

(a)(1) Contractors and subcontractors are required to provide adequate security on all covered contractor information systems in accordance with 32 CFR 2002 and the clause at 252.204-7012.

(2) High NIST SP 800-171 DoD Assessments will be conducted by Government personnel using NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information."

(3) The Medium or High NIST SP 800-171 DoD Assessments will use the scoring methodology described in 32 CFR 170.24.

(4) The Medium or High NIST SP 800-171 DoD Assessments will not duplicate efforts from any other DoD assessment or the Cybersecurity Maturity Model Certification (CMMC) (see 240.371), except for rare circumstances when a new assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a new assessment to ensure current compliance.

(b) Contractors and subcontractors are required to rapidly report cyber incidents directly to DoD at *http://dibnet.dod.mil*. Subcontractors provide the incident report number automatically assigned by DoD to the prime contractor. Lower-tier subcontractors likewise report the incident report number automatically assigned by DoD to their higher-tier subcontractor, until the prime contractor is reached.

(1) If a cyber incident occurs, contractors and subcontractors submit to DoD—

(i) A cyber incident report;

(ii) Malicious software, if detected and isolated; and

(iii) Media (or access to covered contractor information systems and equipment) upon request.

(2) Contracting officers must refer to PGI 240.370-9(c) for instructions on contractor submissions of media and malicious software.

(c) Information shared by the contractor may include contractor attributional/proprietary information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the contractor that reported the information. The Government must protect against the unauthorized use or release of information that includes contractor attributional/proprietary information.

(d) A cyber incident that is reported by a contractor or subcontractor must not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems or has otherwise failed to meet the requirements of the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. When a cyber incident is reported, the contracting officer must consult with the DoD component Chief Information Officer/cyber security office prior to assessing contractor compliance (see PGI 240.370-8(a)(3)). The contracting officer must consider such cyber incidents in the context of an overall assessment of a contractor's compliance with the requirements of the clause at 252.204-7012.

(e) Support services contractors directly supporting Government activities related to safeguarding covered defense information and cyber incident reporting (*e.g.,* forensic analysis, damage assessment, or other services that require access to data from another contractor) are subject to restrictions on use and disclosure of reported information.

240.370-4 Procedures.
Follow the procedures relating to safeguarding covered defense information at PGI 240.370.

240.370-5 Solicitation provisions and contract clauses.

(a) Insert the provision at 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(b) Insert the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting.

(c) Insert the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial products and commercial services, except for solicitations and contracts solely for the acquisition of COTS items.

(d) Insert the clause at 252.240-7997, NIST SP 800-171 DoD Assessment Requirements, in all 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 that are solely for the acquisition of COTS items.

240.371 Cybersecurity Maturity Model Certification

240.371-1 Scope.

(a) This section 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 section 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 section applies to unclassified contractor information systems.

240.371-2 Definitions.
As used in this section—

"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.

240.371-3 Policy.

(a) Award eligibility.

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

(2) Contracting officers must 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 CMMC 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.

240.371-4 Procedures.

(a) *CMMC level.* The contracting officer must 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 240.371-5.

(b) *Award.* Contracting officers must 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 must 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 must 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.

240.371-5 Solicitation provision and contract clause.

(a) Unless the requirements at 32 CFR 170.5(d) are met, insert 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 those 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 CMMC 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) Insert the provision at 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements, in solicitations that include the clause at 252.204-7021.

240.372 Safeguarding classified information within industry.

240.372-1 General.
DoD employees or members of the Armed Forces who are assigned to or visiting a contractor facility and are engaged in oversight of an acquisition program will retain control of their work products, both classified and unclassified (see PGI 240.372-1).

240.372-2 Responsibilities of contracting officers.

(a) Contracting officers must ensure that solicitations comply with PGI 240.372-2(1).

(b) For additional guidance on determining a project to be fundamental research in accordance with 252.204-7000(a)(3), see PGI 240.372-2(2).

240.372-3 Contract clauses.

(a) Insert the clause at 252.204-7000, Disclosure of Information, in solicitations and contracts when the contractor will have access to or generate unclassified information that may be sensitive and inappropriate for release to the public.

(b) Insert the clause at 252.204-7003, Control of Government Personnel Work Product, in all solicitations and contracts.

240.373 Security and Privacy for Computer Systems

240.373-1 Scope.
This section includes information assurance and Privacy Act considerations. Information assurance requirements are in addition to provisions concerning protection of privacy of individuals (see FAR Subpart 24.1).

240.373-2 Definition.
As used in this section—

"Information assurance" means measures that protect and defend information, that is entered, processed, transmitted, stored, retrieved, displayed, or destroyed, and information systems, by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

240.373-3 Policy and responsibilities.

(a) *General.*

(1) Agencies must ensure that information assurance is provided for information technology.

(2) For all acquisitions, the contracting officer must receive from the requiring activity—

(i) Statements of work, specifications, or statements of objectives that meet information assurance requirements as specified in paragraph (a) of this section;

(ii) Inspection and acceptance contract requirements; and

(iii) A determination as to whether the information technology requires protection against compromising emanations.

(b) *Compromising emanations—TEMPEST or other standard.*

For acquisitions requiring information assurance against compromising emanations, the requiring activity is responsible for providing to the contracting officer—

(1) The required protections, *i.e.,* an established National TEMPEST standard (e.g., NSTISSAM TEMPEST 1-92) or a standard used by other authority;

(2) The required identification markings to include markings for TEMPEST or other standard, certified equipment (especially if to be reused);

(3) Inspection and acceptance requirements addressing the validation of compliance with TEMPEST or other standards; and

(4) A date through which the accreditation is considered current for purposes of the proposed contract.

(c) *Information assurance contractor training and certification.*

(1) For acquisitions that include information assurance functional services for DoD information systems, or that require any appropriately cleared contractor personnel to access a DoD information system to perform contract duties, the contracting officer must receive from the requiring activity—

(i) A list of information assurance functional responsibilities for DoD information systems by category (e.g., technical or management) and level (e.g., computing environment, network environment, or enclave); and

(ii) The information assurance training, certification, certification maintenance, and continuing education or sustainment training required for the information assurance functional responsibilities.

(2) The responsibilities specified in paragraph (c)(1) of this section apply to all DoD information assurance duties supported by a contractor, whether performed full-time or part-time as additional or embedded duties, and when using a DoD contract, or a contract or agreement administered by another agency (e.g., under an interagency agreement).

(d) *Contract clause.* Insert the clause at 252.239-7000, Protection Against Compromising Emanations, in solicitations and contracts involving information technology that requires protection against compromising emanations.

Part 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

SUBPART 252.2—TEXT OF PROVISIONS AND CLAUSES

252.204-7000 Disclosure of information.
As prescribed in 240.372-3(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, Safeguarding Covered Defense Information and Cyber Incident Reporting) 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 240.372).

(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)

252.204-7003 Control of government personnel work product.
As prescribed in 240.372-3(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)

252.204-7008 Compliance with safeguarding covered defense information controls.
As prescribed in 240.370-5(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 240.370.5(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)

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.
As prescribed in 240.370-5(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)

252.204-7016 Covered Defense Telecommunications Equipment or Services—Representation.
As prescribed in 240.270-6(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 240.270-6(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 240.270-6(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)

252.240-7997 NIST SP 800-171 DoD Assessment Requirements.
As prescribed in 240.370-5(e), use the following clause:

NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS
(DEVIATION 2026-O0025)(FEB 2026)

(a) *Definitions.*

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, trained in accordance with DoD policy and procedures, using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a contractor's previous assessment(s), as applicable;

(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 Government personnel, trained in accordance with DoD policy and procedures, using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a contractor's previous assessment(s), as applicable;

(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, using the methodology described at 32 CFR 170.24, if necessary. The results of Medium or High NIST SP 800-171 DoD Assessments, when conducted by DCMA, will take precedence over any other assessment, in accordance with 32 CFR 170.16(a)(1)(iv), 32 CFR 170.17(a)(1)(iv), and 32 CFR 170.18(a)(1)(iv).

(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.

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, *i.e.,* DCMA.

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) Date and level of the assessment, *i.e.,* medium or high.

(v) Summary level score (overall numerical score, not the individual value assigned for each requirement).

(vi) Date that all requirements are expected to be implemented 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*. 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).

(End of clause)

252.204-7021 Compliance with the Cybersecurity Maturity Model Certification Level Requirements.
As prescribed in 240.371-5(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)

252.204-7025 Notice of Cybersecurity Maturity Model Certification Level Requirements.
As prescribed in 240.371-5(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)

252.225-7007 Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies.
As prescribed in 240.272-2(f), use the following clause:

PROHIBITION ON ACQUISITION OF CERTAIN ITEMS FROM COMMUNIST CHINESE MILITARY COMPANIES (DEC 2018)

(a) Definitions. As used in this clause—

"600 series of the Commerce Control List" means the series of 5-character export control classification numbers (ECCNs) of the Commerce Control List of the Export Administration Regulations in 15 CFR part 774, supplement No. 1. that have a "6" as the third character. The 600 series constitutes the munitions and munitions related ECCNs within the larger Commerce Control List. (See definition of "600 series" in 15 CFR 772.)

"Communist Chinese military company" means any entity, regardless of geographic location that is—

(1) A part of the commercial or defense industrial base of the People's Republic of China including a subsidiary or affiliate of such entity; or

(2) Owned or controlled by, or affiliated with, an element of the Government or armed forces of the People's Republic of China.

"Item" means—

(1) A USML defense article, as defined at 22 CFR 120.6;

(2) A USML defense service, as defined at 22 CFR 120.9; or

(3) A 600 series item, as defined at 15 CFR 772.1.

"United States Munitions List" means the munitions list of the International Traffic in Arms Regulation in 22 CFR part 121.

(b) Any items covered by the United States Munitions List or the 600 series of the Commerce Control List that are delivered under this contract may not be acquired, directly or indirectly, from a Communist Chinese military company.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts for items covered by the United States Munitions List or the 600 series of the Commerce Control List.

(End of clause)

252.225-7049 Prohibition on Acquisition of Certain Foreign Commercial Satellite Services—Representations.
As prescribed in 240.272-4(f)(1),use the following provision:

PROHIBITION ON ACQUISITION OF CERTAIN FOREIGN COMMERCIAL SATELLITE SERVICES—REPRESENTATIONS (DEC 2018)

(a) Definitions. As used in this provision—

"Covered foreign country," "foreign entity," "government of a covered foreign country," "launch vehicle," "satellite services," and "state sponsor of terrorism" are defined in the clause at Defense Federal Acquisition Regulation Supplement (DFARS) 252.225-7051, Prohibition on Acquisition of Certain Commercial Satellite Services.

"Cybersecurity risk" means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism. (10 U.S.C. 2279)

(b) Prohibition on award. In accordance with 10 U.S.C. 2279, unless an exception is determined to apply in accordance with DFARS 240.272-21, no contract for commercial satellite services may be awarded to—

(1)(i) A foreign entity if the Under Secretary of Defense for Acquisition and Sustainment or the Under Secretary of Defense for Policy reasonably believes that—

(A) The foreign entity is an entity in which the government of a covered foreign country has an ownership interest that enables the government to affect satellite operations;

(B) The foreign entity plans to, or is expected to, provide or use launch or other satellite services under the contract from a covered foreign country; or

(C) Entering into such contract would create an unacceptable cybersecurity risk for DoD; or

(ii) An offeror that is offering to provide the commercial satellite services of a foreign entity as described in paragraph (b)(1) of this section; or

(2)(i) Any entity, except as provided in paragraph (b)(2)(ii) of this provision, for a launch that occurs on or after December 31, 2022, if the Under Secretary of Defense for Acquisition and Sustainment or the Under Secretary of Defense for Policy reasonably believes that such satellite service will be provided using satellites that will be—

(A) Designed or manufactured—

(1) In a covered foreign country; or

(2) By an entity controlled in whole or in part by, or acting on behalf of, the government of a covered foreign country; or

(B) Launched outside the United States, using a launch vehicle that is—

(1) Designed or manufactured in a covered foreign country; or

(2) Provided by—

(i) The government of a covered foreign country; or

(ii) An entity controlled in whole or in part by, or acting on behalf of, the government of a covered foreign country.

(ii) The prohibition in paragraph (b)(2)(i)(B) of this provision does not apply with respect to launch vehicles for which the satellite service provider has a contract or other agreement relating to launch services that, prior to June 10, 2018, was either fully paid for by the satellite service provider or covered by a legally binding commitment of the satellite service provider to pay for such services.

(c) Representations. The Offeror represents that—

(1) It [ ] is, [ ] is not a foreign entity in which the government of a covered foreign country has an ownership interest that enables the government to affect satellite operations. If affirmative, identify the covered foreign country:_____;

(2) It [ ] is, [ ] is not a foreign entity that plans to provide satellite services under the contract from a covered foreign country. If affirmative, identify the covered foreign country:_____;

(3) It [ ] is, [ ] is not offering commercial satellite services provided by a foreign entity in which the government of a covered foreign country has an

ownership interest that enables the government to affect satellite operations. If affirmative, identify the foreign entity and the covered foreign country:_____;

(4) It [ ] is, [ ] is not offering commercial satellite services provided by a foreign entity that plans to or is expected to provide satellite services under the contract from a covered foreign country. If affirmative, identify the foreign entity and the covered foreign country:_____;

(5) It [ ] is, [ ] is not offering commercial satellite services that will use satellites, launched on or after December 31, 2022, that will be designed or manufactured in a covered foreign country. If affirmative, identify the covered foreign country:_____;

(6) It [ ] is, [ ] is not offering commercial satellite services that will use satellites, launched on or after December 31, 2022, that will be designed or manufactured by an entity controlled in whole or in part by, or acting on behalf of, the government of a covered foreign country. If affirmative, identify the entity, the covered foreign country, and the relationship of the entity to the government of the covered foreign country:_____;

(7) It [ ] is, [ ] is not offering commercial satellite services that will use satellites, launched outside the United States on or after December 31, 2022, using a launch vehicle that is designed or manufactured in a covered foreign country. If affirmative, identify the covered foreign country:_____;

(8) It [ ] is, [ ] is not offering commercial satellite services that will use satellites, launched outside the United States on or after December 31, 2022, using a launch vehicle that is provided by the government of a covered foreign country. If affirmative, identify the covered foreign country:_____; and

(9) It [ ] is, [ ] is not offering commercial satellite services that will use satellites, launched outside the United States on or after December 31, 2022, using a launch vehicle that is provided by an entity controlled in whole or in part by, or acting on behalf of, the government of a covered foreign country. If affirmative, identify the entity, the covered foreign country, and the relationship of the entity to the government of the covered foreign country:_____.

(d) Disclosure. If the Offeror has responded affirmatively to any representation in paragraphs (c)(7) through (c)(9) of this provision, and if such launches are covered in whole or in part by a contract or other agreement relating to launch services that, prior to June 10, 2018, was either fully paid for by the satellite service provider or covered by a legally binding commitment of the satellite service provider to pay for such services, provide the following information:

(1) The entity awarded the contract or other agreement:_____.

(2) The date the contract or other agreement was awarded:_____.

(3) The period of performance for the contract or other agreement:_____.

(e) The representations in paragraph (c) of this provision are a material representation of fact upon which reliance will be placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous representation, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

(End of provision)

252.225-7050 Disclosure of Ownership or Control by the Government of a Country that is a State Sponsor of Terrorism.
As prescribed in 240.272-3(e), use the following provision:

DISCLOSURE OF OWNERSHIP OR CONTROL BY THE GOVERNMENT OF A COUNTRY THAT IS A STATE SPONSOR OF TERRORISM (DEC 2022)

(a) Definitions. As used in this provision—

"Government of a country that is a state sponsor of terrorism" includes the state and the government of a country that is a state sponsor of terrorism, as well as any political subdivision, agency, or instrumentality thereof.

"Significant interest" means—

(1) Ownership of or beneficial interest in 5 percent or more of the firm's or subsidiary's securities. Beneficial interest includes holding 5 percent or more of any class of the firm's securities in "nominee shares," "street names," or some other method of holding securities that does not disclose the beneficial owner;

(2) Holding a management position in the firm, such as a director or officer;

(3) Ability to control or influence the election, appointment, or tenure of directors or officers in the firm;

(4) Ownership of 10 percent or more of the assets of a firm such as equipment, buildings, real estate, or other tangible assets of the firm; or

(5) Holding 50 percent or more of the indebtedness of a firm.

"State sponsor of terrorism" means a country determined by the Secretary of State, under section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (Title XVII, Subtitle B, of the National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232), to be a country the government of which has repeatedly provided support for acts of international terrorism. As of the date of this provision, state sponsors of terrorism include Iran, North Korea, and Syria.

(b) Prohibition on award. In accordance with 10 U.S.C. 4871, unless a waiver is granted by the Secretary of Defense, no contract may be awarded to a firm if the

government of a country that is a state sponsor of terrorism owns or controls a significant interest in—

(1) The firm;

(2) A subsidiary of the firm; or

(3) Any other firm that owns or controls the firm.

(c) Representation. Unless the Offeror submits with its offer the disclosure required in paragraph (d) of this provision, the Offeror represents, by submission of its offer, that the government of a country that is a state sponsor of terrorism does not own or control a significant interest in—

(1) The Offeror;

(2) A subsidiary of the Offeror; or

(3) Any other firm that owns or controls the Offeror.

(d) Disclosure.

(1) The Offeror shall disclose in an attachment to its offer if the government of a country that is a state sponsor of terrorism owns or controls a significant interest in the Offeror; a subsidiary of the Offeror; or any other firm that owns or controls the Offeror.

(2) The disclosure shall include—

(i) Identification of each government holding a significant interest; and

(ii) A description of the significant interest held by each government.

(End of provision)

252.225-7051 Prohibition on Acquisition of Certain Foreign Commercial Satellite Services.
As prescribed in 240.272-4(f)(2), use the following clause:

PROHIBITION ON ACQUISITION OF CERTAIN FOREIGN COMMERCIAL SATELLITE SERVICES (DEC 2022)

(a) Definitions. As used in this clause—

"Covered foreign country" means—

(1) The People's Republic of China;

(2) North Korea;

(3) The Russian Federation; or

(4) Any country that is a state sponsor of terrorism. (10 U.S.C. 2279)

"Foreign entity" means—

(1) Any branch, partnership, group or sub-group, association, estate, trust, corporation or division of a corporation, or organization organized under the laws of a foreign state if either its principal place of business is outside the United States or its equity securities are primarily traded on one or more foreign exchanges.

(2) Notwithstanding paragraph (1) of this definition, any branch, partnership, group or sub-group, association, estate, trust, corporation or division of a corporation, or organization that demonstrates that a majority of the equity interest in such entity is ultimately owned by U.S. nationals is not a foreign entity. (31 CFR 800.212)

"Government of a covered foreign country" includes the state and the government of a covered foreign country, as well as any political subdivision, agency, or instrumentality thereof.

"Launch vehicle" means a fully integrated space launch vehicle. (10 U.S.C. 2279)

"Satellite services" means communications capabilities that utilize an on-orbit satellite for transmitting the signal from one location to another.

"State sponsor of terrorism" means a country determined by the Secretary of State, under section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (Title XVII, Subtitle B, of the National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232), to be a country the government of which has repeatedly provided support for acts of international terrorism. As of the date of this provision, state sponsors of terrorism include Iran, North Korea, and Syria. (10 U.S.C. 4871)

(b) Limitation. Unless specified in its offer, the Contractor shall not provide satellite services under this contract that—

(1) Are from a covered foreign country; or

(2) Except as provided in paragraph (c), use satellites that will be—

(i) Designed or manufactured—

(A) In a covered foreign country; or

(B) By an entity controlled in whole or in part by, or acting on behalf of, the government of a covered foreign country; or

(ii) Launched outside the United States using a launch vehicle that is designed or manufactured—

(A) In a covered foreign country; or

(B) Provided by—

(1) The government of a covered foreign country; or

(2) An entity controlled in whole or in part by, or acting on behalf of, the government of a covered foreign country.

(c) Exception. The limitation in paragraph (b)(2) shall not apply with respect to—

(1) A launch that occurs prior to December 31, 2022; or

(2) A satellite service provider that has a contract or other agreement relating to launch services that, prior to June 10, 2018, was either fully paid for by the satellite service provider or covered by a legally binding commitment of the satellite service provider to pay for such services.

(End of clause)

252.239-7000 Protection against compromising emanations.
As prescribed in 240.373-3(d), use the following clause:

PROTECTION AGAINST COMPROMISING EMANATIONS (OCT 2019)

(a) The Contractor shall provide or use only information technology, as specified by the Government, that has been accredited to meet the appropriate information assurance requirements of—

(1) The National Security Agency National TEMPEST Standards (NSTISSAM TEMPEST 1-92, Compromising Emanations Laboratory Test Requirements, Electromagnetics (U)); or

(2) Other standards specified by this contract, including the date through which the required accreditation is current or valid for the contract.

(b) Upon request of the Contracting Officer, the Contractor shall provide documentation supporting the accreditation.

(c) The Government may, as part of its inspection and acceptance, conduct additional tests to ensure that information technology delivered under this contract satisfies the information assurance standards specified. The Government may conduct additional tests—

(1) At the installation site or contractor's facility; and

(2) Notwithstanding the existence of valid accreditations of information technology prior to the award of this contract.

(d) Unless otherwise provided in this contract under the Warranty of Supplies or Warranty of Systems and Equipment clause, the Contractor shall correct or replace accepted information technology found to be deficient within 1 year after proper installations.

(1) The correction or replacement shall be at no cost to the Government.

(2) Should a modification to the delivered information technology be made by the Contractor, the 1-year period applies to the modification upon its proper installation.

(3) This paragraph (d) applies regardless of f.o.b. point or the point of acceptance of the deficient information technology.

(End of clause)

252.239-7017 Notice of Supply Chain Risk.
As prescribed in 240.271-7(a), use the following provision:

NOTICE OF SUPPLY CHAIN RISK (DEC 2022)

(a) *Definition. Supply chain risk,* as used in this provision, means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (see 10 U.S.C. 3252).

(b) In order to manage supply chain risk, the Government may use the authorities provided by 10 U.S.C. 3252. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to an offeror and its supply chain.

(c) If the Government exercises the authority provided in 10 U.S.C. 3252 to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

(End of provision)

252.239-7018 Supply Chain Risk.
As prescribed in 240.271-7(b), use the following clause:

SUPPLY CHAIN RISK (DEC 2022)

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

Information technology (see 40 U.S.C 11101(6)) means, in lieu of the definition at FAR 2.1, any equipment, or interconnected system(s) or subsystem(s) of equipment,

that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

(1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires—

(i) Its use; or

(ii) To a significant extent, its use in the performance of a service or the furnishing of a product.

(2) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

(3) The term "information technology" does not include any equipment acquired by a contractor incidental to a contract.

Supply chain risk means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (see 10 U.S.C. 3252).

(b) The Contractor shall mitigate supply chain risk in the provision of supplies and services to the Government.

(c) In order to manage supply chain risk, the Government may use the authorities provided by 10 U.S.C. 3252. In exercising these authorities, the Government may consider information, public and non-public, including all-source intelligence, relating to a Contractor's supply chain.

(d) If the Government exercises the authority provided in 10 U.S.C. 3252 to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

(End of clause)

PGI 240—INFORMATION SECURITY AND SUPPLY CHAIN SECURITY

PGI 240.2—SECURITY PROHIBITIONS AND EXCLUSIONS

PGI 240.272 Prohibited Sources.

PGI 240.272-2 Prohibition on acquisition of certain items from Communist Chinese military companies.

(1) The Department of State is the lead agency responsible for the regulations governing the export of defense articles, which are identified on the United States Munitions List. The Department of State has issued the International Traffic in Arms Regulations, which implement the Arms Export Control Act (22 U.S.C. 2751) and include the United States Munitions List.

(2) The official version of the International Traffic in Arms Regulations can be found in Title 22, Parts 120 through 130, of the Code of Federal Regulations (22 CFR 120-130), published by the U.S. Government Printing Office and available at https://catalog.gpo.gov/F/SGDS5TUGPX9MMUK3XX2JKHLK2XA9FQBKGK5H86HIG5R89LDY66-18351?func=full-set-set&set_number=002106&set_entry=000002&format=999. The Department of State also publishes an on-line version at https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987#:~:text=The%20ITAR%20is%20available%20from%20the%20Government%20Printing,Federal%20Regulations%20%28CFR%29%20and%20as%20an%20updated%20e-document.

(a) Definitions. In accordance with 22 CFR 121.8—

(1) A major component includes any assembled element that forms a portion of an end item without which the end item is inoperable. Examples of major components are airframes, tail sections, transmissions, tank treads, and hulls;

(2) A minor component includes any assembled element of a major component; and

(3) Examples of parts are rivets, wires, and bolts.

(d) Identifying USML items.

(1) The 21 categories of items on the United States Munitions List (USML) can be found at https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121. Where applicable, the categories also contain a statement with regard to the coverage of components and parts of items included in a category. For example, a category may include all components and parts of covered items, or only those components and parts specifically designed or modified for military use.

(2) In addition to the list of covered items, the USML provides explanation of terms needed to determine whether a particular item is or is not covered by the USML.

(3) Within DoD, the experts on export control and the USML are in the Defense Technology Security Administration (DTSA).

(i) Official authorities and responsibilities of DTSA are in DoD Directive 5105.72, available at *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510572p.pdf*.

(ii) Additional information on DTSA and a correspondence link are available at https://www.dtsa.mil/SitePages/default.aspx.

(e) Waiver of prohibition**.**

(3(i)) Send a copy of the report to the Office of the Principal Director, Defense Pricing, Contracting, and Acquisition Policy (Contract Policy) (DPCAP/CP) via email at osd.pentagon.ousd-a-s.mbx.asda-dp-c-contractpolicy@mail.mil.

PGI 240.272-3 Prohibition on contracting or subcontracting with a firm that is owned or controlled by the government of a country that is a state sponsor of terrorism.

(d) Notification**.** Forward any information indicating that a firm, a subsidiary of a firm, or any other firm that owns or controls the firm, may be owned or controlled by the government of a country that is a state sponsor of terrorism, through agency channels, to DPCAP/CP via email at osd.pentagon.ousd-a-s.mbx.asda-dp-c-contractpolicy@mail.mil.

PGI 240.272-4 Prohibition on acquisition of certain foreign commercial satellite services.

(d) Procedures.

(1) Forward any information required in accordance with 225.772-3 or requests for an exception to DPCAP/CP via email at osd.pentagon.ousd-a-s.mbx.asda-dp-c-contractpolicy@mail.mil.

(2) Consult with DPCAP/CP, as required in accordance with 225.772-3(c)(2), via email at osd.pentagon.ousd-a-s.mbx.asda-dp-c-contractpolicy@mail.mil.

PGI 240.3—SAFEGUARDING INFORMATION

PGI 240.370 Safeguarding Covered Defense Information and Cyber Incident Reporting.

PGI 240.370-6 General.

(a) The contracting officer will be notified by the requiring activity when a solicitation is expected to result in a contract, task order, or delivery order that will involve—

(1) Covered defense information; or

(2) Operationally critical support.

(b) The contracting officer shall—

(1) Ensure that the requiring activity provides a work statement or specification that includes the identification of covered defense information or operationally critical support consistent with paragraph (a).

(2) Ensure that the solicitation and resultant contract, task order, or delivery order includes the requirement (such as a contract data requirements list), as provided by the requiring activity, for the contractor to apply markings, when appropriate, on covered defense information.

PGI 240.370-7 Safeguarding controls and requirements.

(a) When an offeror proposes to vary from any of 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," in accordance with paragraph (c)(2) of the solicitation provision at DFARS 252.204-7008, or in accordance with paragraphs (b)(2)(ii)(B) of DFARS clause 252.204-7012, the contracting officer shall submit the offeror's explanation of the proposed variance to the DoD Chief Information Officer via email at osd.dibcsia@mail.mil for adjudication.

(b) For additional information on safeguarding controls and requirements, see the Frequently Asked Questions document at http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contracting.html.

PGI 240.370-8 Cyber incident and compromise reporting.

(a) When a cyber incident is reported by a contractor, the DoD Cyber Crime Center (DC3) will send an unclassified encrypted email containing the cyber incident report to the contracting officer(s) identified on the Incident Collection Format (ICF). The DC3 may request the contracting officer send a digitally signed e-mail to DC3.

(1) The procuring contracting officer (PCO) shall notify the requiring activities that have contracts identified in the ICF. In cases where an administrative contracting officer (ACO) receives the cyber incident report, in lieu of the PCO, the ACO shall notify the PCO for each affected contract, who will then notify the requiring activity.

(2) In cases of cyber incidents involving multiple contracts, the DoD components will collaboratively designate a single contracting officer to coordinate additional actions required of the contractor, on behalf of the affected DoD components. The requiring activity will notify the contracting officer once a lead is designated.

(3) If the requiring activity requests an assessment of compliance with the requirements of the clause at DFARS 252.204-7012 related to the cyber incident, the contracting officer shall—

(i) Consult with the DoD component Chief Information Officer (CIO)/cyber security office;

(ii) Request a description of the contractor's implementation of the security requirements in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) in order to support evaluation of whether any of the controls were inadequate, or if any of the controls were not implemented at the time of the incident; and

(iii) Provide a copy of the assessment of contractor compliance to the requiring activity, the DoD CIO at osd.dibcsia@mail.mil, and the other contracting officers listed in the cyber incident report.

(b) When requested by the contractor, the contracting officer shall provide the contractor with the "Instructions for Malware Submission" document available at http://www.acq.osd.mil/dpap/pdi/docs/Instructions_for_Malware_Submission.docx. The contracting officer should never receive malicious software directly from the contractor.

(c) If the requiring activity requests access to contractor information or equipment, in accordance with DFARS 252.204-7012(f), the contracting officer shall provide a written request to the contractor.

(d) For additional information on cyber incident reporting, see the Frequently Asked Questions document at http://www.acq.osd.mil/dpap/pdi/network_penetration_reporting_and_contracting.html.
PGI 204.7303-4 DoD damage assessment activities.

PGI 240.370-9 DoD damage assessment activities.

(a) Prior to initiating damage assessment activities, the contracting officer shall verify that any contract identified in the cyber incident report includes the clause at DFARS 252.204-7012. If the contracting officer determines that a contract identified in the report does not contain the clause, the contracting officer shall notify the requiring activity that damage assessment activities, if required, may be determined to constitute a change to the contract.

(b) In cases of cyber incidents involving multiple contracts, a single contracting officer will be designated to coordinate with the contractor regarding media submission (see 204.7303-3(a)(2)).

(c) If the requiring activity requests the contracting officer to obtain media, as defined in DFARS 252.204-7012, from the contractor, the contracting officer shall—

(1) Provide a written request for the media;

(2) Provide the contractor with the "Instructions for Media Submission" document available at http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx; and

(3) Provide a copy of the request to DC3, electronically via email at dcise@dc3.mil, and the requiring activity.

(d) If the contracting officer is notified by the requiring activity that media are not required, the contracting officer shall notify the contractor and simultaneously provide a copy of the notice to DC3 and the requiring activity.

(e) The contracting officer shall document the action taken as required by paragraph (c) or (d) of this section, in the contract file.

(f) Upon receipt of the contractor media, DC3 will confirm receipt in writing to the contractor and the requesting contracting officer.

(g) Once the requiring activity determines that the damage assessment activities are complete, the requiring activity will provide the contracting officer with a report documenting the actions taken to close out the cyber incident.

PGI 240.372—Safeguarding Classified Information Within Industry.

PGI 240.372-1 General.

(1) The use of "Not Releasable to Foreign Nationals" (NOFORN) caveat on Department of Defense (DoD) Information, to include contract documents, shall not be applied to non-intelligence information except for Naval Nuclear Propulsion Information and the National Disclosure Policy document (NDP-1).

(2) Agencies shall not restrict procurements on the basis of foreign origin but rather on the level of security clearance required by industry to submit an offer and perform on the contract.

PGI 240.372-2 Responsibilities of contracting officers.

(1) Consistent with the requirements at FAR 4.403, contracting officers shall ensure that solicitations, to include any broad agency announcement (BAA), commercial solutions opening (CSO), or notice to industry that requires industry access to classified information and/or controlled unclassified information (see policy memos), shall contain one or more of the following:

(i) Draft DoD Form DD 254, DoD Contract Security Classification Specification. For guidance on completing the DD 254, see "Instructions for Completing DD Form 254, Department of Defense Contract Security Classification Specification" at *https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0254-Inst.pdf*. For information on the National Industrial Security Program Contract Classification System, see *https://www.dcsa.mil/is/nccs/*.

(ii) The clause at FAR 52.204-2, Security Requirements.

(iii) Detailed agency instructions for industry requirements to request access to classified information and/or controlled unclassified information. Agency instructions shall clearly reference and be in accordance with the National Industrial Security Program Operating Manual (NISPOM) (32 CFR part 117).

(iv) The following is a template of agency instructions to industry:

> "Offerors must have a valid U.S. security clearance of *[to be filled in by the contracting officer]* or higher in order to respond to this RFP (Announcement), because the RFP (Announcement) includes an annex (information) classified at the *[to be filled in by the contracting officer]* level which will be released only to offerors possessing the appropriate clearance. All classified material must be handled in accordance with the National Industrial Security Program Operating Manual (NISPOM) (32 CFR part 117)."

(2) Fundamental research project determination.

(i) Projects being scoped as fundamental research may include the entire contract effort or a specified portion of the statement of work, and must be documented in the written determination and in the contract.

(ii) The determination of fundamental research shall occur when the project is added to the statement of work, either prior to award or during a contract modification that modified the statement of work.

(iii) Fundamental research is defined in the USD(AT&L) memorandum on Fundamental Research, dated May 24, 2010.

(iv) See clause 252.204-7000(a)(3), concerning disclosure of information for fundamental research projects.