

costs of constructing the facilities or equipment. A mutually accepted communications service authorization may provide for exceptions.

(b) The Contractor shall operate and maintain all telecommunication facilities and equipment used under this agreement/contract whether the Government or the Contractor has title.

(End of clause)

252.239-7013 Term of Agreement and Continuation of Services.

Basic. As prescribed in 239.7411(c)(1), use the following clause:

TERM OF AGREEMENT AND CONTINUATION OF SERVICES—BASIC (OCT 2019)

(a) This basic agreement is not a contract. The Government incurs liability only upon issuance of a communication service authorization, which is a contract that incorporates the terms and conditions of this basic agreement.

(b) This agreement shall continue in force from year to year, unless terminated by either party by 30 days' written notice. Termination of this basic agreement does not terminate or cancel any communication service authorizations issued under this basic agreement prior to the termination.

(c) Communication service authorizations issued under this basic agreement may be modified to incorporate the terms and conditions of a new basic agreement negotiated with the Contractor.

(End of clause)

Alternate I. As prescribed in 239.7411(c)(2), use the following clause, which uses a different paragraph (c) than the basic clause and adds a new paragraph (d).

TERM OF AGREEMENT AND CONTINUATION OF SERVICES—ALTERNATE I (OCT 2019)

(a) This basic agreement is not a contract. The Government incurs liability only upon issuance of a communication service authorization, which is a contract that incorporates the terms and conditions of this basic agreement.

(b) This agreement shall continue in force from year to year, unless terminated by either party by 30 days' written notice. Termination of this basic agreement does not terminate or cancel any communication service authorizations issued under this basic agreement prior to the termination.

(c) The Contractor's current communication services authorizations have been modified to incorporate the terms and conditions of this basic agreement.

(1) All current communication service authorizations issued by _____ that incorporate Basic Agreement Number _____, dated _____, are modified to incorporate this basic agreement.

(2) Current communication service authorizations, issued by the activity in paragraph (c)(1) of this clause, that incorporate other agreements with the Contractor may also be modified to incorporate this basic agreement.

(d) Communication service authorizations issued under this basic agreement may be modified to incorporate a new basic agreement with the Contractor.

(End of clause)

[84 FR 58338, Oct. 31, 2019]

252.239-7015 [Reserved]

252.239-7016 Telecommunications security equipment, devices, techniques, and services.

As prescribed in 239.7411(d), use the following clause:

TELECOMMUNICATIONS SECURITY EQUIPMENT, DEVICES, TECHNIQUES, AND SERVICES (DEC 1991)

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

(1) *Securing* means the application of Government-approved telecommunications security equipment, devices, techniques, or services to contractor telecommunications systems.

(2) *Sensitive information* means any information the loss, misuse, or modification of which, or unauthorized access to, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy.

(3) *Telecommunications systems* means voice, record, and data communications, including management information systems and local data networks that connect to external transmission media, when employed by Government agencies, contractors, and subcontractors to transmit—

(i) Classified or sensitive information;

(ii) Matters involving intelligence activities, cryptologic activities related to national security, the command and control of military forces, or equipment that is an integral part of a weapon or weapons system; or

(iii) Matters critical to the direct fulfillment of military or intelligence missions.

(b) This solicitation/contract identifies classified or sensitive information that requires securing during telecommunications

252.239-7017

and requires the Contractor to secure telecommunications systems. The Contractor agrees to secure information and systems at the following location: (Identify the location.)

(c) To provide the security, the Contractor shall use Government-approved telecommunications equipment, devices, techniques, or services. A list of the approved equipment, etc. may be obtained from (identify where list can be obtained). Equipment, devices, techniques, or services used by the Contractor must be compatible or interoperable with (list and identify the location of any telecommunications security equipment, device, technique, or service currently being used by the technical or requirements organization or other offices with which the Contractor must communicate).

(d) Except as may be provided elsewhere in this contract, the Contractor shall furnish all telecommunications security equipment, devices, techniques, or services necessary to perform this contract. The Contractor must meet ownership eligibility conditions for communications security equipment designated as controlled cryptographic items.

(e) The Contractor agrees to include this clause, including this paragraph (e), in all subcontracts which require securing telecommunications.

(End of clause)

252.239-7017 Notice of supply chain risk.

As prescribed in 239.7306(a), use the following provision:

NOTICE OF SUPPLY CHAIN RISK (FEB 2019)

(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. 2339a).

(b) In order to manage supply chain risk, the Government may use the authorities provided by 10 U.S.C. 2339a. 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. 2339a 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.

48 CFR Ch. 2 (10-1-21 Edition)

(End of provision)

[78 FR 69272, Nov. 18, 2013, as amended at 84 FR 4370, Feb. 15, 2019]

252.239-7018 Supply chain risk.

As prescribed in 239.7306(b), use the following clause:

SUPPLY CHAIN RISK (FEB 2019)

(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. 2339a).

(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. 2339a. 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. 2339a to limit disclosure of information, no action undertaken by the Government under such authority shall be subject to review in a bid protest before