(b) Communication service authorizations currently in effect which were issued by the activity in paragraph (a) of this clause incorporating other agreements with the Contractor may also be modified to incorporate this agreement.

(c) This basic agreement is not a contract.

(End of clause)

[71 FR 39011, July 11, 2006]

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 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 (NOV 2013)

(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 national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

(b) In order to manage supply chain risk, the Government may use the authorities provided by section 806 of Public Law 111–383. 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 section 806 of Pub. L. 111–383 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)

[78 FR 69272, Nov. 18, 2013]

252.239–7018 Supply chain risk.

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

SUPPLY CHAIN RISK (NOV 2013)

(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 national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

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

(c) In order to manage supply chain risk, the Government may use the authorities provided by section 806 of Public Law 111–383. 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 section 806 of Public Law 111–383 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.

(e) The Contractor shall include the substance of this clause, including this paragraph (e), in all subcontracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

(End of clause)

[78 FR 69272, Nov. 18, 2013]

252.241–7000 Superseding contract.

As prescribed in 241.501–70(a), use the following clause:

SUPERSEDING CONTRACT (DEC 1991)

This contract supersedes contract No. _____, dated ____ which provided similar services. Any capital credits accrued to the Government, any remaining credits due to the Government under the connection charge, or any termination liability are transferred to this contract, as follows:

CAPITAL CREDITS

(List years and accrued credits by year and separate delivery points.)

OUTSTANDING CONNECTION CHARGE CREDITS

(List by month and year the amount credited and show the remaining amount of outstanding credits due the Government.)

TERMINATION LIABILITY CHARGES

(List by month and year the amount of monthly facility cost recovered and show the remaining amount of facility cost to be recovered.)

(End of clause)

[56 FR 36479, July 31, 1991, as amended at 63 FR 11549, Mar. 9, 1998]

252.241–7001 Government access.

As prescribed in 241.501–70(b), use the following clause:

GOVERNMENT ACCESS (DEC 1991)

Authorized representatives of the Government may have access to the Contractor's on-base facilities upon reasonable notice or in case of emergency.

(End of clause)

[56 FR 36479, July 31, 1991, as amended at 63 FR 11549, Mar. 9, 1998]

252.242–7000—252.242–7002 [Reserved]

252.242–7004 Material Management and Accounting System.

As prescribed in 242.7204, use the following clause: