Part 239 - ACQUISITION OF INFORMATION TECHNOLOGY

239.001 Applicability.

Subpart 239.1 - GENERAL

239.101 Policy.

Subpart 239.70 - EXCHANGE OR SALE OF INFORMATION TECHNOLOGY

239.7001 Policy.

Subpart 239.71 - SECURITY AND PRIVACY FOR COMPUTER SYSTEMS

239.7100 Scope of subpart.

239.7101 Definition.

239.7102 Policy and responsibilities.

239.7102-1 General.

239.7102-2 Compromising emanations—TEMPEST or other standard.

239.7102-3 Information assurance contractor training and certification.

239.7103 Contract clauses.

Subpart 239.72 - STANDARDS

239.7201 Solicitation requirements.

Subpart 239.73 - REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK

239.7300 Scope of subpart.

239.7301 Definitions.

239.7302 Applicability.

239.7303 Authorized individuals.

239.7304 Determination and notification.

239.7305 Exclusion and limitation on disclosure.

239.7306 Solicitation provision and contract clause.

Subpart 239.74 - TELECOMMUNICATIONS SERVICES

239.7400 Scope.

239.7401 Definitions.

239.7402 Policy.

239.7403 Reserved.

239.7404 Reserved.

239.7405 Delegated authority for telecommunications resources.

239.7406 Certified cost or pricing data and data other than certified cost or pricing data.

239.7407 Type of contract.

239.7408 Special construction.

239.7408-1 General.

239.7408-2 Applicability of construction labor standards for special construction.

239.7409 Special assembly.

239.7410 Cancellation and termination.

239.7411 Contract clauses.

Subpart 239.75 - Reserved

Subpart 239.76 - CLOUD COMPUTING

239.7600 Scope of subpart.

239.7601 Definitions.

239.7602 Policy and responsibilities.

239.7602-1 General.

239.7602-2 Required storage of data within the United States or outlying areas.

239.7603 Procedures.

239.7604 Solicitation provision and contract clause.

Parent topic: Defense Federal Acquisition Regulation

239.001 Applicability.

Notwithstanding FAR 39.001, this part applies to acquisitions of information technology, including national security systems.

Subpart 239.1 - GENERAL

239.101 Policy.

(1) A contracting officer may not enter into a contract in excess of the simplified acquisition threshold for information technology products or services that are not commercial products or commercial services unless the head of the contracting activity determines in writing that no commercial products or commercial services are suitable to meet the agency's needs, as determined through the use of market research appropriate to the circumstances (see FAR 10.001(a)(3)) (section 855 of the National Defense Authorization Act for Fiscal Year 2016 (Pub. L. 114-92)).

(2) See subpart 208.74 when acquiring commercial software or software maintenance.

(3) See 227.7202 for policy on the acquisition of commercial computer software and commercial computer software documentation.

(4) See 227.7203 for policy on the acquisition of other than commercial computer software and other than commercial computer software documentation.

Subpart 239.70 - EXCHANGE OR SALE OF INFORMATION TECHNOLOGY

239.7001 Policy.

Agencies shall follow the procedures in DoD Manual 4140.01, Volume 9, DoD Supply Chain Materiel Management Procedures: Materiel Programs, when considering the exchange or sale of Government-owned information technology.

Subpart 239.71 - SECURITY AND PRIVACY FOR COMPUTER SYSTEMS

239.7100 Scope of subpart.

This subpart 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).

239.7101 Definition.

“Information assurance,” as used in this subpart, 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.

239.7102 Policy and responsibilities.

239.7102-1 General.

(a) Agencies shall ensure that information assurance is provided for information technology in accordance with current policies, procedures, and statutes, to include—

(1) The National Security Act;

(2) The Clinger-Cohen Act;

(3) National Security Telecommunications and Information Systems Security Policy No. 11;

(4) Federal Information Processing Standards;

(5) DoD Directive 8500.1, Information Assurance;

(6) DoD Instruction 8500.2, Information Assurance Implementation;

(7) DoD Directive 8140.01, Cyberspace Workforce Management; and

(8) DoD Manual 8570.01-M, Information Assurance Workforce Improvement Program.

(b) For all acquisitions, the requiring activity is responsible for providing to the contracting officer—

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

(2) Inspection and acceptance contract requirements; and

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

239.7102-2 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—

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

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

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

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

239.7102-3 Information assurance contractor training and certification.

(a) 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 requiring activity is responsible for providing to the contracting officer—

(1) 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

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

(b) After contract award, the requiring activity is responsible for ensuring that the certifications and certification status of all contractor personnel performing information assurance functions as described in DoD 8570.01-M, Information Assurance Workforce Improvement Program, are in compliance with the manual and are identified, documented, and tracked.

(c) The responsibilities specified in paragraphs (a) and (b) 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) See PGI 239.7102-3 for guidance on documenting and tracking certification status of contractor personnel, and for additional information regarding the requirements of DoD 8570.01-M.

239.7103 Contract clauses.

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

(b) Use the clause at 252.239-7001 , Information Assurance Contractor Training and Certification, in solicitations and contracts involving contractor performance of information assurance functions as described in DoD 8570.01-M.

Subpart 239.72 - STANDARDS

239.7201 Solicitation requirements.

Contracting officers shall ensure that all applicable Federal Information Processing Standards are incorporated into solicitations.

Subpart 239.73 - REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK

239.7300 Scope of subpart.

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.

239.7301 Definitions.

As used in this subpart—

“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).

239.7302 Applicability.

Notwithstanding FAR 39.001, this subpart shall be applied 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 16.505(b)(1)(iv)(D)); 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.

239.7303 Authorized individuals.

(a) Subject to 239.7304 , the following individuals are authorized to take the actions authorized by 239.7305 :

(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 239.7305 or the responsibility for making the determination required by 239.7304 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.

239.7304 Determination and notification.

The individuals authorized in 239.7303 may exercise the authority provided in 239.7305 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 239.7305 (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 239.7303 plans to limit disclosure of information under 239.7305 (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 shall 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.

239.7305 Exclusion and limitation on disclosure.

Subject to 239.7304 , the individuals authorized in 239.7303 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 shall be subject to review in a bid protest before the Government Accountability Office or in any Federal court; and

(2) The authorized individual shall—

(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 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.

239.7306 Solicitation provision and contract clause.

(a) Insert the provision at 252.239-7017, Notice of Supply Chain Risk, in all 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 239.7301 .

(b) Insert the clause at 252.239-7018, Supply Chain Risk, in all 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 239.7301 .

Subpart 239.74 - TELECOMMUNICATIONS SERVICES

239.7400 Scope.

This subpart prescribes policy and procedures for acquisition of telecommunications services and maintenance of telecommunications security. Telecommunications services meet the definition of information technology.

239.7401 Definitions.

As used in this subpart—

“Common carrier” means any entity engaged in the business of providing telecommunications services which are regulated by the Federal Communications Commission or other governmental body.

“Foreign carrier” means any person, partnership, association, joint-stock company, trust, governmental body, or corporation not subject to regulation by a U.S. governmental regulatory body and not doing business as a citizen of the United States, providing telecommunications services outside the territorial limits of the United States.

“Governmental regulatory body” means the Federal Communications Commission, any statewide regulatory body, or any body with less than statewide jurisdiction when operating under the State authority. The following are not “governmental regulatory bodies”—

(1) Regulatory bodies whose decisions are not subject to judicial appeal; and

(2) Regulatory bodies which regulate a company owned by the same entity which creates the regulatory body.

“Long-haul telecommunications” means all general and special purpose long-distance telecommunications facilities and services (including commercial satellite services, terminal equipment, and local circuitry supporting the long-haul service) to or from the post, camp, base, or

station switch and/or main distribution frame (except for trunk lines to the first-serving commercial central office for local communications services).

“Noncommon carrier” means any entity other than a common carrier offering telecommunications facilities, services, or equipment for lease.

“Securing,” “sensitive information,” and “telecommunications systems” have the meaning given in the clause at 252.239-7016 , Telecommunications Security Equipment, Devices, Techniques, and Services.

“Telecommunications” means the transmission, emission, or reception of signals, signs, writing, images, sounds, or intelligence of any nature, by wire, cable, satellite, fiber optics, laser, radio, or any other electronic, electric, electromagnetic, or acoustically coupled means.

“Telecommunications services” means the services acquired, whether by lease or contract, to meet the Government's telecommunications needs. The term includes the telecommunications facilities and equipment necessary to provide such services.

239.7402 Policy.

(a) *Acquisition.* DoD policy is to acquire telecommunications services from common and noncommon telecommunications carriers—

(1) On a competitive basis, except when acquisition using other than full and open competition is justified;

(2) Recognizing the regulations, practices, and decisions of the Federal Communications Commission (FCC) and other governmental regulatory bodies on rates, cost principles, and accounting practices; and

(3) Making provision in telecommunications services contracts for adoption of—

(i) FCC approved practices; or

(ii) The generally accepted practices of the industry on those issues concerning common carrier services where—

(A) The governmental regulatory body has not expressed itself;

(B) The governmental regulatory body has declined jurisdiction; or

(C) There is no governmental regulatory body to decide.

(b) *Security.*

(1) The contracting officer shall ensure, in accordance with agency procedures, that purchase requests identify—

(i) The nature and extent of information requiring security during telecommunications;

(ii) The requirement for the contractor to secure telecommunications systems;

(iii) The telecommunications security equipment, devices, techniques, or services with which the contractor's telecommunications security equipment, devices, techniques, or services must be interoperable; and

(iv) The approved telecommunications security equipment, devices, techniques, or services, such as found in the National Security Agency's Information Systems Security Products and Services Catalogue.

(2) Contractors and subcontractors shall provide all telecommunications security techniques or services required for performance of Government contracts.

(3) Except as provided in paragraph (b)(4) of this section, contractors and subcontractors shall normally provide all required property, to include telecommunications security equipment or related devices, in accordance with FAR 45.102. In some cases, such as for communications security (COMSEC) equipment designated as controlled cryptographic item (CCI), contractors or subcontractors must also meet ownership eligibility conditions.

(4) The head of the agency may authorize provision of the necessary property as Government-furnished property or acquisition as contractor-acquired property, as long as conditions of FAR 45.102(b) are met.

(c) *Foreign carriers*. For information on contracting with foreign carriers, see PGI 239.7402 (c).

(d) *Long-haul telecommunications services*. When there is a requirement for procurement of long-haul telecommunications services, follow PGI 239.7402 (d).

239.7403 Reserved.

239.7404 Reserved.

239.7405 Delegated authority for telecommunications resources.

The contracting officer may enter into a telecommunications service contract on a month-to-month basis or for any longer period or series of periods, not to exceed a total of 10 years. See PGI 239.7405 for documents relating to this contracting authority, which the General Services Administration has delegated to DoD.

239.7406 Certified cost or pricing data and data other than certified cost or pricing data.

(a) Common carriers are not required to submit certified cost or pricing data before award of contracts for tariffed services. Rates or preliminary estimates quoted by a common carrier for tariffed telecommunications services are considered to be prices set by regulation within the provisions of 10 U.S.C. 3703. This is true even if the tariff is set after execution of the contract.

(b) Rates or preliminary estimates quoted by a common carrier for nontariffed telecommunications services or by a noncommon carrier for any telecommunications service are not considered prices set by law or regulation.

(c) Contracting officers shall obtain sufficient data to determine that the prices are reasonable in accordance with FAR 15.403-3 or 15.403-4. See PGI 239.7406 for examples of instances where additional data may be necessary to determine price reasonableness.

239.7407 Type of contract.

When acquiring telecommunications services, the contracting officer may use a basic agreement (see FAR 16.702) in conjunction with communication service authorizations. When using this method, follow the procedures at PGI 239.7407 .

239.7408 Special construction.

239.7408-1 General.

(a) “Special construction” normally involves a common carrier giving a special service or facility related to the performance of the basic telecommunications service requirements. This may include—

(1) Moving or relocating equipment;

(2) Providing temporary facilities;

(3) Expediting provision of facilities; or

(4) Providing specially constructed channel facilities to meet Government requirements.

(b) Use this subpart instead of FAR Part 36 for acquisition of “special construction.”

(c) Special construction costs may be—

(1) A contingent liability for using telecommunications services for a shorter time than the minimum to reimburse the contractor for unamortized nonrecoverable costs. These costs are usually expressed in terms of a termination liability, as provided in the contract or by tariff;

(2) A onetime special construction charge;

(3) Recurring charges for constructed facilities;

(4) A minimum service charge;

(5) An expediting charge; or

(6) A move or relocation charge.

(d) When a common carrier submits a proposal or quotation which has special construction requirements, the contracting officer shall require a detailed special construction proposal. Analyze all special construction proposals to—

(1) Determine the adequacy of the proposed construction;

(2) Disclose excessive or duplicative construction; and

(3) When different forms of charge are possible, provide for the form of charge most advantageous to the Government.

(e) When possible, analyze and approve special construction charges before receiving the service. Impose a ceiling on the special construction costs before authorizing the contractor to proceed, if prior approval is not possible. The contracting officer must approve special construction charges before final payment.

239.7408-2 Applicability of construction labor standards for special construction.

(a) The construction labor standards in FAR Subpart 22.4 ordinarily do not apply to special construction. However, if the special construction includes construction, alteration, or repair (as defined in FAR 22.401) of a public building or public work, the construction labor standards may apply. Determine applicability under FAR 22.402.

(b) Each CSA or other type contract which is subject to construction labor standards under FAR 22.402 shall cite that fact.

239.7409 Special assembly.

(a) Special assembly is the designing, manufacturing, arranging, assembling, or wiring of equipment to provide telecommunications services that cannot be provided with general use equipment.

(b) Special assembly rates and charges shall be based on estimated costs. The contracting officer should negotiate special assembly rates and charges before starting service. When it is not possible to negotiate in advance, use provisional rates and charges subject to adjustment, until final rates and charges are negotiated. The CSAs authorizing the special assembly shall be modified to reflect negotiated final rates and charges.

239.7410 Cancellation and termination.

(a)(1) Cancellation is stopping a requirement after placing of an order but before service starts.

(2) Termination is stopping a requirement after placing an order and after service starts.

(b) Determine cancellation or termination charges under the provisions of the applicable tariff or agreement/contract.

239.7411 Contract clauses.

(a) In addition to other appropriate FAR and DFARS clauses, use the following clauses in solicitations, contracts, and basic agreements for telecommunications services. Modify the clauses only if necessary to meet the requirements of a governmental regulatory agency.

(1) 252.239-7002 , Access.

(2) 252.239-7004 , Orders for Facilities and Services.

(3) 252.239-7007 , Cancellation or Termination of Orders.

(b) Use the following clauses in solicitations, contracts, and basic agreements for telecommunications services when the acquisition includes or may include special construction. Modify the clauses only if necessary to meet the requirements of a governmental regulatory agency—

(1) 252.239-7011 , Special Construction and Equipment Charges; and

(2) 252.239-7012 , Title to Telecommunication Facilities and Equipment.

(c) Use the basic or alternate of the clause at 252.239-7013 , Term of Agreement and Continuation of Services, in basic agreements for telecommunications services.

(1) Use the basic clause in basic agreements that do not supersede an existing basic agreement with the contractor.

(2) Use the alternate I clause in basic agreements that supersede an existing basic agreement with the contractor. Complete paragraph (c)(1) of the clause with the basic agreement number, date, and contacting office that issued the basic agreement being superseded.

(d) Use the clause at 252.239-7016 , Telecommunications Security Equipment, Devices, Techniques, and Services, in solicitations and contracts when performance of a contract requires secure telecommunications.

Subpart 239.75 - Reserved

Subpart 239.76 - CLOUD COMPUTING

239.7600 Scope of subpart.

This subpart prescribes policies and procedures for the acquisition of cloud computing services.

239.7601 Definitions.

As used in this subpart—

“Authorizing official,” as described in DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

“Cloud computing” means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications,

and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

“Government data” means any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained by the Government in the course of official Government business.

“Government-related data” means any information, document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. This does not include a contractor’s business records (e.g., financial records, legal records, etc.) or data such as operating procedures, software coding, or algorithms that are not uniquely applied to the Government data.

“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 information is recorded, stored, or printed within an information system.

239.7602 Policy and responsibilities.

239.7602-1 General.

(a) Generally, DoD shall acquire cloud computing services using commercial terms and conditions that are consistent with Federal law, and an agency’s needs, including those requirements specified in this subpart. Some examples of commercial terms and conditions are license agreements, End User License Agreements (EULAs), Terms of Service (TOS), or other similar legal instruments or agreements. Contracting officers shall incorporate any applicable service provider terms and conditions into the contract by attachment or other appropriate mechanism. Contracting officers shall carefully review commercial terms and conditions and consult counsel to ensure these are consistent with Federal law, regulation, and the agency’s needs.

(b)(1) Except as provided in paragraph (b)(2) of this section, the contracting officer shall only award a contract to acquire cloud computing services from a cloud service provider (e.g., contractor or subcontractor, regardless of tier) that has been granted provisional authorization by Defense Information Systems Agency, at the level appropriate to the requirement, to provide the relevant cloud computing services in accordance with the Cloud Computing Security Requirements Guide (SRG) (version in effect at the time the solicitation is issued or as authorized by the contracting officer) found at *https://public.cyber.mil/dccs/* .

(2) The contracting officer may award a contract to acquire cloud computing services from a cloud service provider that has not been granted provisional authorization when—

(i) The requirement for a provisional authorization is waived by the DoD Chief Information Officer; or

(ii) The cloud computing service requirement is for a private, on-premises version that will be

provided from U.S. Government facilities. Under this circumstance, the cloud service provider must obtain a provisional authorization prior to operational use.

(c) When contracting for cloud computing services, the contracting officer shall ensure the following information is provided by the requiring activity:

(1) Government data and Government-related data descriptions.

(2) Data ownership, licensing, delivery and disposition instructions specific to the relevant types of Government data and Government-related data (e.g., DD Form 1423, Contract Data Requirements List; work statement task; line item). Disposition instructions shall provide for the transition of data in commercially available, or open and non-proprietary format (and for permanent records, in accordance with disposition guidance issued by National Archives and Record Administration).

(3) Appropriate requirements to support applicable inspection, audit, investigation, or other similar authorized activities specific to the relevant types of Government data and Government-related data, or specific to the type of cloud computing services being acquired.

(4) Appropriate requirements to support and cooperate with applicable system-wide search and access capabilities for inspections, audits, investigations.

239.7602-2 Required storage of data within the United States or outlying areas.

(a) Cloud computing service providers are required to maintain within the 50 states, the District of Columbia, or outlying areas of the United States, all Government data that is not physically located on DoD premises, unless otherwise authorized by the authorizing official, as described in DoD Instruction 8510.01, in accordance with the SRG.

(b) The contracting officer shall provide written notification to the contractor when the contractor is permitted to maintain Government data at a location outside the 50 States, the District of Columbia, and outlying areas of the United States. See PGI 239.7602-2 for additional guidance.

239.7603 Procedures.

Follow the procedures relating to cloud computing at PGI 239.7603 .

239.7604 Solicitation provision and contract clause.

(a) Use the provision at 252.239-7009 , Representation of Use of Cloud Computing, in solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial products and commercial services, for information technology services.

(b) Use the clause at 252.239-7010 , Cloud Computing Services, 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 services.