

Subpart 38.1—Federal Supply Schedule Program

38.101 General.

(a) The Federal Supply Schedule program, pursuant to 41 U.S.C. 152(3), provides Federal agencies with a simplified process of acquiring commercial supplies and commercial services in varying quantities while obtaining volume discounts. Indefinite-delivery contracts are awarded using competitive procedures to firms. The firms provide supplies and services at stated prices for given periods of time, for delivery within a stated geographic area such as the 48 contiguous states, the District of Columbia, Alaska, Hawaii, and overseas. The schedule contracting office issues Federal Supply Schedule publications that contain a general overview of the Federal Supply Schedule (FSS) program and address pertinent topics.

(b) Each schedule identifies agencies that are required to use the contracts as primary sources of supply.

(c) Federal agencies not identified in the schedules as mandatory users may issue orders under the schedules. Contractors are encouraged to accept the orders.

(d) Although GSA awards most Federal Supply Schedule contracts, it may authorize other agencies to award schedule contracts and publish schedules. For example, the Department of Veterans Affairs awards schedule contracts for certain medical and non-perishable subsistence items.

(e) When establishing Federal Supply Schedules, GSA, or an agency delegated that authority, is responsible for complying with all applicable statutory and regulatory requirements (*e.g.*, Parts 5, 6, and 19). The requirements of parts 5, 6, and 19 apply at the acquisition planning stage prior to issuing the schedule solicitation and, generally, do not apply to orders and BPAs placed under resulting schedule contracts except see 8.404 and 8.405-5.

[65 FR 36025, June 6, 2000, as amended at 69 FR 34239, June 18, 2004; 76 FR 14559, Mar. 16, 2011; 76 FR 68036, Nov. 2, 2011; 79 FR 24213, Apr. 29, 2014; 86 FR 61030, Nov. 4, 2021]

Subpart 38.2—Establishing and Administering Federal Supply Schedules

38.201 Coordination requirements.

(a) Subject to interagency agreements, contracting officers having responsibility for awarding Federal Supply Schedule contracts shall coordinate and obtain approval of the General Services Administration's Federal Supply Service (FSS) before—

(1) Establishing new schedules;

(2) Discontinuing existing schedules;

(3) Changing the scope of agency or geographical coverage of existing schedules; or

(4) Adding or deleting special item numbers, national stock numbers, or revising their description.

(b) Requests should be forwarded to the General Services Administration, Federal Supply Service, Office of Acquisition (FC), Washington, DC 20406.

[48 FR 42368, Sept. 19, 1983, as amended at 54 FR 29282, July 11, 1989; 56 FR 55372, Oct. 25, 1991; 59 FR 53718, Oct. 25, 1994; 62 FR 40237, July 25, 1997]

PART 39—ACQUISITION OF INFORMATION TECHNOLOGY

Sec.

39.000 Scope of part.

39.001 Applicability.

39.002 Definitions.

Subpart 39.1—General

39.101 Policy.

39.102 Management of risk.

39.103 Modular contracting.

39.104 Information technology services.

39.105 Privacy.

39.106 Contract clause.

Subpart 39.2—Information and Communication Technology

39.201 Scope of subpart.

39.202 Definition.

39.203 Applicability.

39.204 Exceptions.

39.205 Exemptions.

AUTHORITY: 40 U.S.C. 121(c); 10 U.S.C. chapter 4 and 10 U.S.C. chapter 137 legacy provisions (see 10 U.S.C. 3016); and 51 U.S.C. 20113.

SOURCE: 61 FR 41470, Aug. 8, 1996, unless otherwise noted.

39.000

48 CFR Ch. 1 (10–1–24 Edition)

39.000 Scope of part.

This part prescribes acquisition policies and procedures for use in acquiring—

(a) Information technology, including financial management systems, consistent with other parts of this regulation, OMB Circular No. A–127, Financial Management Systems, and OMB Circular No. A–130, Management of Federal Information Resources; and

(b) Information and communication technology (see 2.101).

[66 FR 20897, Apr. 25, 2001, as amended at 86 FR 44232, Aug. 11, 2021; 89 FR 30254, Apr. 22, 2024]

39.001 Applicability.

This part applies to the acquisition of—

(a) Information technology by or for the use of agencies except for acquisitions of information technology for national security systems. However, acquisitions of information technology for national security systems shall be conducted in accordance with 40 U.S.C. 11302 with regard to requirements for performance and results-based management; the role of the agency Chief Information Officer in acquisitions; and accountability. These requirements are addressed in OMB Circular No. A–130; and

(b) Information and communication technology by or for the use of agencies or for the use of the public, unless an exception (see 39.204) or an exemption (see 39.205) applies. See 36 CFR 1194.1.

[86 FR 44232, Aug. 11, 2021]

39.002 Definitions.

As used in this part—

Modular contracting means use of one or more contracts to acquire information technology systems in successive, interoperable increments.

National security system means any telecommunications or information system operated by the United States Government, the function, operation, or use of which—

- (1) Involves intelligence activities;
- (2) Involves cryptologic activities related to national security;
- (3) Involves command and control of military forces;

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

(5) Is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management applications.

[61 FR 41470, Aug. 8, 1996, as amended at 62 FR 274, Jan. 2, 1997; 62 FR 44830, Aug. 22, 1997; 63 FR 9068, Feb. 23, 1998; 66 FR 2133, Jan. 10, 2001; 79 FR 70344, Nov. 25, 2014]

Subpart 39.1—General

39.101 Policy.

(a)(1) In acquiring information technology, agencies shall identify their requirements pursuant to—

(i) OMB Circular A–130, including consideration of security of resources, protection of privacy, national security and emergency preparedness, accessibility for individuals with disabilities, and energy efficiency;

(ii) The requirements for sustainable products and services (as defined in 2.101) in accordance with subpart 23.1;

(iii) Policies to enable power management and other energy-efficient or environmentally preferable features on all agency electronic products; and

(iv) Best management practices for energy-efficient management of servers and Federal data centers.

(2) When developing an acquisition strategy, contracting officers should consider the rapidly changing nature of information technology through market research (see Part 10) and the application of technology refreshment techniques.

(b) Agencies must follow OMB Circular A–127, Financial Management Systems, when acquiring financial management systems. Agencies may acquire only core financial management software certified by the Joint Financial Management Improvement Program.

(c) In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's

Web site at <http://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

(d) When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with 11.002(g).

(e) Contracting officers shall not purchase any hardware, software, or services developed or provided by Kaspersky Lab that the Government will use on or after October 1, 2018. (See 4.2002.)

(f)(1) On or after August 13, 2019, contracting officers shall not procure or obtain, or extend or renew a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system on or after August 13, 2019, unless an exception applies or a waiver is granted. (See subpart 4.21.)

(2) On or after August 13, 2020, agencies are prohibited from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception applies or a waiver is granted (see subpart 4.21). This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(g) See the prohibition in 4.2202 on the presence or use of a covered application (“TikTok”).

(h) Executive agencies are prohibited from procuring or obtaining, or extending or renewing a contract to procure or obtain, any covered article, or any products or services produced or provided by a source, including contractor use of covered articles or sources, if prohibited from doing so by an applicable FASCSA order issued by the Director of National Intelligence, Secretary

of Defense, or Secretary of Homeland Security (see 4.2303).

[61 FR 41470, Aug. 8, 1996, as amended at 64 FR 32748, June 17, 1999; 64 FR 72446, Dec. 27, 1999; 70 FR 57452, Sept. 30, 2005; 72 FR 73217, Dec. 26, 2007; 73 FR 10968, Feb. 28, 2008; 74 FR 65607, Dec. 10, 2009; 76 FR 31401, May 31, 2011; 79 FR 70344, Nov. 25, 2014; 80 FR 26427, May 7, 2015; 83 FR 28144, June 15, 2018; 84 FR 40221, Aug. 13, 2019; 85 FR 42678, July 14, 2020; 86 FR 44232, Aug. 11, 2021; 88 FR 36434, June 2, 2023; 88 FR 69513, Oct. 5, 2023; 89 FR 30245, Apr. 22, 2024]

39.102 Management of risk.

(a) Prior to entering into a contract for information technology, an agency should analyze risks, benefits, and costs. (See part 7 for additional information regarding requirements definition.) Reasonable risk taking is appropriate as long as risks are controlled and mitigated. Contracting and program office officials are jointly responsible for assessing, monitoring and controlling risk when selecting projects for investment and during program implementation.

(b) Types of risk may include schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or systems, the number of simultaneous high risk projects to be monitored, funding availability, and program management risk.

(c) Appropriate techniques should be applied to manage and mitigate risk during the acquisition of information technology. Techniques include, but are not limited to: prudent project management; use of modular contracting; thorough acquisition planning tied to budget planning by the program, finance and contracting offices; continuous collection and evaluation of risk-based assessment data; prototyping prior to implementation; post implementation reviews to determine actual project cost, benefits and returns; and focusing on risks and returns using quantifiable measures.

39.103 Modular contracting.

(a) This section implements 41 U.S.C. 2308. Modular contracting is intended to reduce program risk and to incentivize contractor performance while meeting the Governments need

for timely access to rapidly changing technology. Consistent with the agency's information technology architecture, agencies should, to the maximum extent practicable, use modular contracting to acquire major systems (see 2.101) of information technology. Agencies may also use modular contracting to acquire non-major systems of information technology.

(b) When using modular contracting, an acquisition of a system of information technology may be divided into several smaller acquisition increments that—

(1) Are easier to manage individually than would be possible in one comprehensive acquisition;

(2) Address complex information technology objectives incrementally in order to enhance the likelihood of achieving workable systems or solutions for attainment of those objectives;

(3) Provide for delivery, implementation, and testing of workable systems or solutions in discrete increments, each of which comprises a system or solution that is not dependent on any subsequent increment in order to perform its principal functions;

(4) Provide an opportunity for subsequent increments to take advantage of any evolution in technology or needs that occur during implementation and use of the earlier increments; and

(5) Reduce risk of potential adverse consequences on the overall project by isolating and avoiding custom-designed components of the system.

(c) The characteristics of an increment may vary depending upon the type of information technology being acquired and the nature of the system being developed. The following factors may be considered:

(1) To promote compatibility, the information technology acquired through modular contracting for each increment should comply with common or commercially acceptable information technology standards when available and appropriate, and shall conform to the agency's master information technology architecture.

(2) The performance requirements of each increment should be consistent with the performance requirements of the completed, overall system within

which the information technology will function and should address interface requirements with succeeding increments.

(d) For each increment, contracting officers shall choose an appropriate contracting technique that facilitates the acquisition of subsequent increments. Pursuant to parts 16 and 17 of the Federal Acquisition Regulations, contracting officers shall select the contract type and method appropriate to the circumstances (e.g., indefinite delivery, indefinite quantity contracts, single contract with options, successive contracts, multiple awards, task order contracts). Contract(s) shall be structured to ensure that the Government is not required to procure additional increments.

(e) To avoid obsolescence, a modular contract for information technology should, to the maximum extent practicable, be awarded within 180 days after the date on which the solicitation is issued. If award cannot be made within 180 days, agencies should consider cancellation of the solicitation in accordance with 48 CFR 14.209 or 15.206(e). To the maximum extent practicable, deliveries under the contract should be scheduled to occur within 18 months after issuance of the solicitation.

[63 FR 9068, Feb. 23, 1998, as amended at 79 FR 24213, Apr. 29, 2014]

39.104 Information technology services.

When acquiring information technology services, solicitations must not describe any minimum experience or educational requirement for proposed contractor personnel unless the contracting officer determines that the needs of the agency—

(a) Cannot be met without that requirement; or

(b) Require the use of other than a performance-based acquisition (see subpart 37.6).

[66 FR 22085, May 2, 2001; 71 FR 218, Jan. 3, 2006]

39.105 Privacy.

Agencies shall ensure that contracts for information technology address protection of privacy in accordance

Federal Acquisition Regulation

39.203

with the Privacy Act (5 U.S.C. 552a) and part 24. In addition, each agency shall ensure that contracts for the design, development, or operation of a system of records using commercial information technology services or information technology support services include the following:

(a) Agency rules of conduct that the contractor and the contractor's employees shall be required to follow.

(b) A list of the anticipated threats and hazards that the contractor must guard against.

(c) A description of the safeguards that the contractor must specifically provide.

(d) Requirements for a program of Government inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

39.106 Contract clause.

The contracting officer shall insert a clause substantially the same as the clause at 52.239-1, Privacy or Security Safeguards, in solicitations and contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services.

[61 FR 41470, Aug. 8, 1996. Redesignated at 62 FR 274, Jan. 2, 1997. Redesignated at 79 FR 70344, Nov. 25, 2014]

Subpart 39.2—Information and Communication Technology

SOURCE: 66 FR 20897, Apr. 25, 2001, unless otherwise noted.

39.201 Scope of subpart.

(a) This subpart implements section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board's (U.S. Access Board) information and communication technology (ICT) accessibility standards at 36 CFR 1194.1.

(b) Further information on section 508 is available via the Internet at <http://www.section508.gov>.

(c) When acquiring ICT, agencies must ensure that—

(1) Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities; and

(2) Members of the public with disabilities seeking information or services from an agency have access to and use of information and data that is comparable to the access to and use of information and data by members of the public who are not individuals with disabilities.

[66 FR 20897, Apr. 25, 2001, as amended at 86 FR 44232, Aug. 11, 2021]

39.202 Definition.

Undue burden, as used in this subpart, means a significant difficulty or expense.

39.203 Applicability.

(a) *General*. Unless an exception at 39.204 or an exemption at 39.205 applies, acquisitions for ICT supplies and services shall meet the applicable ICT accessibility standards at 36 CFR 1194.1.

(b) *Indefinite-quantity contracts*. Confirmation of an exception or a determination of an exemption is not required prior to award of an indefinite-quantity contract, except for requirements that are to be satisfied by initial award. The contract must identify which supplies and services the contractor indicates as compliant and show where full details of compliance can be found (*e.g.*, vendor's or other exact website location).

(c) *Task order or delivery order*. At the time of issuance of a task order or delivery order under an indefinite-quantity contract, the requiring and ordering activities shall ensure compliance with the ICT accessibility standards and document an exception or exemption if applicable. Any task order or delivery order, or portion thereof, issued for a noncompliant ICT item shall be supported by the appropriate exception or exemption documented by the requiring activity.

39.204

(d) *Commercial products and commercial services.* When acquiring commercial products and commercial services, an agency must comply with those ICT accessibility standards that can be met with supplies or services that are available in the commercial marketplace and that best address the agency's needs, but see 39.205(a)(3).

(e) *Legacy ICT.* Any component or portion of existing ICT (*i.e.*, ICT that was procured, maintained, or used on or before January 18, 2018) is not required to comply with the current ICT accessibility standards if it—

(1) Complies with an earlier standard issued pursuant to section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), which is set forth in Appendix D to 36 CFR 1194.1); and

(2) Has not been altered (*i.e.*, a change that affects interoperability, the user interface, or access to information or data) after January 18, 2018.

(f) *Alterations of legacy ICT.* When altering any component or portion of existing ICT, after January 18, 2018, the component or portion must be modified to conform to the current ICT accessibility standards in 36 CFR 1194.1.

[86 FR 44232, Aug. 11, 2021, as amended at 86 FR 61030, Nov. 4, 2021]

39.204 Exceptions.

(a) The requirements in 39.203 do not apply to acquisitions for—

(1) *National security systems.* ICT operated by agencies as part of a national security system, as defined by 40 U.S.C. 11103(a);

(2) *Incidental contract items.* ICT acquired by a contractor incidental to a contract, *i.e.*, for in-house use by the contractor to perform the contract; or

(3) *Maintenance or monitoring spaces.* The portions of ICT that are operable parts (*i.e.*, hardware-based user controls for activating, deactivating, or adjusting ICT) or status indicators, and that are located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment.

(b) The contracting officer shall receive, as a part of the requirements documentation, written confirmation from the requiring activity that an exception, in accordance with paragraph (a)(1), (2), or (3) of this section, applies

48 CFR Ch. 1 (10–1–24 Edition)

to the ICT supply or service (see 7.105(b)(5)(iv)). This documentation shall be maintained in the contract file.

[86 FR 44232, Aug. 11, 2021]

39.205 Exemptions.

(a) *Allowable exemptions.* An agency may grant an exemption for the following:

(1) *Undue burden.* When an agency determines the acquisition of ICT conforming with all the applicable ICT accessibility standards would impose an undue burden on the agency, compliance with the ICT accessibility standards is only required to the extent that it would not impose an undue burden. In determining whether conformance to one or more ICT accessibility standards would impose an undue burden, an agency shall consider the extent to which conformance would impose significant difficulty or expense considering the agency resources available to the program or component for which the ICT supply or service is being procured.

(2) *Fundamental alteration.* When an agency determines that acquisition of ICT that conforms with all applicable ICT accessibility standards would result in a fundamental alteration in the nature of the ICT, such acquisition is required to conform only to the extent that conformance will not result in a fundamental alteration in the nature of the ICT.

(3) *Nonavailability of conforming commercial products and commercial services.* Where there are no commercial products and commercial services that fully conform to the ICT accessibility standards, the agency shall procure the supplies or service available in the commercial marketplace that best meets the ICT accessibility standards consistent with the agency's needs.

(b) *Alternative means of access.* An agency shall provide individuals with disabilities access to and use of information and data by an alternative means to meet the identified needs when an exemption in paragraphs (a)(1), (2), or (3) of this section applies.

(c) *Documentation.* When an exemption applies, the contracting officer

shall obtain, as part of the requirements documentation, a written determination from the requiring activity explaining the basis for the exemption in paragraphs (a)(1), (2) or (3) of this section. This documentation shall be maintained in the contract file.

(1) *Undue burden.* A determination of undue burden shall address why and to what extent compliance with applicable ICT accessibility standards constitutes an undue burden.

(2) *Fundamental alteration.* A determination of fundamental alteration shall address the extent to which compliance with the applicable ICT accessibility standards would result in a fundamental alteration in the nature of the ICT.

(3) *Nonavailability of conforming commercial products and commercial services.* A determination of commercial products and commercial services nonavailability shall include—

(i) A description of the market research performed;

(ii) A listing of the requirements that cannot be met; and

(iii) The rationale for determining that the ICT to be procured best meets the ICT accessibility standards in 36 CFR 1194.1, consistent with the agency's needs.

[86 FR 44232, Aug. 11, 2021, as amended at 86 FR 61030, Nov. 4, 2021]

PART 40—INFORMATION SECURITY AND SUPPLY CHAIN SECURITY

Sec.
40.000 Scope of part.

Subpart 40.1 [Reserved]

Subpart 40.2 [Reserved]

Subpart 40.3 [Reserved]

AUTHORITY: 40 U.S.C. 121(c); 10 U.S.C. chapter 4 and 10 U.S.C. chapter 137 legacy provisions (see 10 U.S.C. 3016); and 51 U.S.C. 20113.

SOURCE: 89 FR 22605, Apr. 1, 2024, unless otherwise noted.

40.000 Scope of part.

(a) This part addresses broad security requirements that apply to acquisitions of products and services. It prescribes policies and procedures for

managing information security and supply chain security when acquiring products and services that include, but are not limited to, information and communications technology (ICT).

(b) See part 39 for security-related policies and procedures that only apply to ICT.

(c) See parts 4, 24, and 46 for additional policies and procedures related to managing information security and supply chain security.

(d) Information and supply chain policies and procedures that are unrelated to security are covered in other parts of the FAR (*e.g.*, part 22 for labor and human trafficking risks and part 23 for climate-related risks).

Subpart 40.1 [Reserved]

Subpart 40.2 [Reserved]

Subpart 40.3 [Reserved]

PART 41—ACQUISITION OF UTILITY SERVICES

Subpart 41.1—General

Sec.
41.100 Scope of part.
41.101 Definitions.
41.102 Applicability.
41.103 Statutory and delegated authority.

Subpart 41.2—Acquiring Utility Services

41.201 Policy.
41.202 Procedures.
41.203 GSA assistance.
41.204 GSA areawide contracts.
41.205 Separate contracts.
41.206 Interagency agreements.

Subpart 41.3—Requests for Assistance

41.301 Requirements.

Subpart 41.4—Administration

41.401 Monthly and annual review.
41.402 Rate changes and regulatory intervention.

Subpart 41.5—Solicitation Provision and Contract Clauses

41.501 Solicitation provision and contract clauses.