Subpart 39.1 - General

Parent topic: Part 39 - Acquisition of Information Technology

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) Electronic Product Environmental Assessment Tool (EPEAT®) standards (see 23.704);

(iii) Policies to enable power management, double-sided printing, 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 website 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).

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 Government's 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* Regulation, *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 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*.

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).

39.105 Privacy.

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