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 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).

(i) *Executive agencies must* comply with the prohibitions on unmanned aircraft systems (e.g., drones) in accordance with 40.202.

Parent topic: Subpart 39.1 - General