510.002 Pre-Award Procedures.

(a) Market research must be conducted in accordance with 523.104(a)(1).

(b) Ensure statement of work includes sustainability requirements in accordance with 523.104(a)(2).

(c) *Market research activities related to cyber-supply chain risk management for information technology, GSA-funded acquisitions*.

(1) The acquisition planning team must include the GSA Chief Information Security Officer (CISO), or representative, in market research activities and ensure that entities' cyber-supply chain risk management capabilities are considered, as much as possible, before developing requirement documents for an acquisition and before soliciting offers if the acquisition is to acquire a--

(i) *Federal Information Processing Standard (FIPS) 199 High-Impact Information System*. A high-impact information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals if there was a breach of security resulting in a potential loss of confidentiality, integrity, or availability; or

(ii) *FIPS 199 Moderate-Impact Information System*. A moderate-impact information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals if there was a breach of security resulting in a potential loss of confidentiality, integrity, or availability.

(iii) *FIPS 199 Low-Impact Information System*. This paragraph (c)(1) does not apply to acquisitions of low-impact information systems.

(2)The acquisition planning team should:

(i) *Search the System for Award Management (SAM)*. As potential capable sources are identified, and when determining the acquisition strategy, consider searching SAM (https://www.sam.gov) to review self-certifications, submitted in response to the provision at FAR 52.204-26 (or FAR 52.212-3(v) for commercial items or commercial services), as to whether the source provides covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument and whether the source uses covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(ii) *Review the Cyber-Supply Chain Risk Management Page*. The C-SCRM page on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm) is frequently updated to include guides, samples and templates, and other considerations to assist acquisition teams during market research related to C-SCRM. The page also includes helpful points of contacts within the agency that may be able to provide additional information.

(iii) *Review GEAR*. As the acquisition team is determining the availability of certain commercial products or commercial services, the GSA Enterprise Architecture Analytics and Reporting (GEAR) application (https://ea.gsa.gov/), which comprises the authoritative list of approved and denied Commercial-off-the-shelf (COTS) software within GSA, should be reviewed.

(iv) *Review the FedRAMP Marketplace*. If the acquisition may include cloud services, the acquisition team should review the Federal Risk and Authorization Management Program (FedRAMP)

Marketplace (https://marketplace.fedramp.gov/) for potential cloud services solutions.

(v) *Review Governmentwide Vehicles and Shared Services*. Consider Government-wide Acquisition Contracts (GWACs), Multi-Agency Contracts (MACs), or GSA Schedules that have already evaluated their awardees for Supply Chain Risk Management process and procedures at the master contract level and have incorporated relevant provisions and clauses. Additionally, shared services, such as Quality Service Management Offices (QSMOs), provide an online platform for acquiring high-quality, cost-efficient services that may help reduce the time and cost involved in sourcing and maintaining cybersecurity solutions.

(vi) *Other Sources*. If a compliant supplier cannot be identified, the acquisition planning team should look for other ways to satisfy the requirement, including identifying other acquisition strategies, changing the requirement description, changing the requirement, insourcing, or determining another solution.

(d) *Market research activities related to cyber-supply chain risk management for non-information technology, GSA-funded acquisitions. The acquisition planning team should*:

(1) *Search the System for Award Management (SAM)*. As potential capable sources are identified, and when determining the acquisition strategy, consider searching SAM (https://www.sam.gov) to review self-certifications, submitted in response to the provision at FAR 52.204-26 (or FAR 52.212-3(v) for commercial items or commercial services), as to whether the source provides covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument and whether the source uses covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(2) *Review the Cyber-Supply Chain Risk Management Page*. The C-SCRM page on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm) is frequently updated to include guides, samples and templates, and other considerations to assist acquisition teams during market research related to C-SCRM. The page also includes helpful points of contacts within the agency that may be able to provide additional information.

(3) *Review Government-wide Vehicles and Shared Services*. Consider Government-wide Acquisition Contracts (GWACs), Multi-agency Contracts (MACs), or GSA Schedules that have already evaluated their awardees for Supply Chain Risk Management process and procedures at the Master Contract Level and have incorporated relevant provisions and clauses. Additionally, shared services, such as Quality Service Management Offices (QSMOs), provide an online platform for acquiring high-quality, cost-efficient services that may help reduce the time and cost involved in sourcing and maintaining cybersecurity solutions.

(4) *Other Sources*. If a compliant supplier cannot be identified, the acquisition planning team should look for other ways to satisfy the requirement, including identifying other acquisition strategies, changing the requirement description, changing the requirement, or determining another solution.

Parent topic: Part 510 - Market Research