General Services Administration
Washington, DC 20405

ADM 2800.12B, Change 136
September 29, 2021

GSA ORDER

Subject: General Services Administration Acquisition Manual; GSAM Case 2021-G512, Cyber-Supply Chain Risk Management (C-SCRM) Pre-Award Activities

1. Purpose. This order transmits a revision to the General Services Administration Acquisition Manual (GSAM) to provide acquisition considerations related to Cyber-Supply Chain Risk Management (C-SCRM).

2. Background. A series of recent policy changes internal and external to GSA have highlighted the importance of the Federal Government's goal to improve its focus on C-SCRM acquisition. This order reflects GSA's commitment to help meet that goal by establishing GSA-specific acquisition considerations related to C-SCRM during various stages of the acquisition.

   Internal Policies:

   In April 2021, GSA issued it's Cyber-Supply Chain Risk Management (C-SCRM) Strategic Plan[1] (the "Plan"). As outlined in the Plan, acquisition policy (in addition to IT governance) must continually be updated to address the changing and growing nature of supply chain risks, including cyber supply chain risks. This GSAM amendment reflects another step in considering C-SCRM during an acquisition.

   On June 18, 2021, the GSA Office of the Chief Information Security Officer (OCISO) released *IT Security Procedural Guide: OCISO C-SCRM Program (CIO-IT Security-21-117)* that states, in part, "by integrating with the acquisition processes for GSA IT, supply chain risks (including cyber-related) can be considered in procurement decisions based on C-SCRM evaluations of providers; and can prevent the award of contracts to product or IT service providers who pose an unacceptable level of risk to the organization."

   External Policies:

   On May 12, 2021, Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, was issued. This EO states, "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." It highlights that the Federal Government must improve its efforts to identify, deter, project against, detect, and respond to these cyber threats. While additional

[1] Version 1.3, dated March 29, 2021, approved April 13, 2021

rulemaking and guidance from the Federal Acquisition Regulatory Council and other responsible agencies will be forthcoming as a result of this EO, GSA is taking a proactive approach to amending our specific acquisition policy to help meet the requirements of the EO.

3. Effective date. September 29, 2021

4. Explanation of changes. The amendment changes are non-regulatory changes. For full text changes of the amendment see Attachment A, GSAM Text Line-In/Line-Out.

   This amendment revises the language of the following GSAM subparts (titles reflect amended changes). Specific amendments are explained below.

   Amend section 504.7004 by:

   - Removing “reserved” in the title and adding “Acquisition Considerations” in its place.
   - Adding a new paragraph (a) that cross-references to Acquisition Planning (507.105(f))
   - Adding a new paragraph (b) that cross-references to Market Research (510.002(c))
   - Adding a new paragraph (c) that highlights evaluation considerations related to C-SCRM.
   - Adding a new paragraph (d) that highlights considerations prior to award.

   Amend section 507.105 by:

   - Adding a new paragraph at (g) that highlights what the acquisition planner must address and should address related to acquisitions for information technology and acquisitions that are not for information technology.

   Amend section 510.002 by:

   - Adding new paragraphs at (c) and (d) that highlights what the acquisition planning team must do and should do during market research as it relates to Supply Chain Risk Management (cyber and non-cyber related).

5. Cancellations. Not applicable.

6. Point of contact. For clarification of content, contact Stephen Carroll, GSA Acquisition Policy Division, at gsarpolicy@gsa.gov.

JEFFREY KOSES

Digitally signed by JEFFREY KOSES
Date: 2021.09.27 12:17:39 -04'00'

Jeffrey Koses
Senior Procurement Executive
Office of Acquisition Policy
Office of Government-wide Policy

GSAM Baseline: Change 135 effective 09/28/2021

- Additions to baseline made by rule are indicated by **[bold text in brackets]**
- Deletions to baseline made by rule are indicated by ~~strikethroughs~~
- Five asterisks (*****) indicate that there are no revisions between the preceding and following sections
- Three asterisks (***) indicate that there are no revisions between the material shown within a subsection

PART 504—ADMINISTRATIVE MATTERS

* * * * *

Subpart 504.70—[Cyber-]Supply Chain Risk Management

* * * * *

504.7004 ~~reserved~~[Acquisition Considerations

(a) *Acquisition Planning*. For cyber-supply chain risk management acquisition planning considerations, see 507.105(f).

(b) *Market Research*. For cyber-supply chain risk management market research considerations, see 510.002(c) and (d).

(c) *Evaluation*. As part of evaluating past performance, review the Contractor Performance Assessment Reporting System (CPARS) for any reported noncompliance with supply chain requirements and/or otherwise evaluate similar past performance information in accordance with the policies and procedures contained in the applicable subpart.

(d) *Pre-award*. *Apparent successful offeror*. If the apparent successful offeror responds that it "will" provide or "does" use covered telecommunications equipment or services in response to the representation provision at FAR 52.204-24 then, regardless of the offeror's response to the SAM representation provision(s) (e.g., FAR 52.204-26, FAR 52.212-3(v)), clarify with the apparent successful offeror to ensure that it accurately completed the representation(s). After clarifying the apparent successful offeror accurately completed the representation(s), follow the procedures at 504.7005(c) and consider the following:

(1) If the contracting officer determines that awarding to the apparent successful offeror will result in a violation of the prohibition at FAR 52.204-24(b), the contracting officer should determine that the offeror is not eligible for award and should move to the next offeror in line for award.

(2) If the contracting officer does not identify an eligible offeror, the acquisition team should explore other acquisition strategies, making a partial award, cancelling the solicitation, changing the requirement, or finding another approach that does not involve the use of covered telecommunications equipment or services.

(3) As a last resort, the acquisition team may consider pursuing a waiver for an offeror. The acquisition team should contact the appropriate Cyber-Supply Chain Risk Management Policy Advisor (see 504.7003(a)) for assistance and coordination. Instructions for requesting a waiver are available on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm).]

* * * * *

PART 507 - ACQUISITION PLANNING

* * * * *

507.105 Contents of written acquisition plans.

* * *

[(f) *Cyber-supply chain risk management for GSA-funded acquisitions*.

(1) The acquisition planner must discuss the scope of involvement (or planned involvement) of the GSA Chief Information Security Officer (CISO), or representative, as part of the acquisition planning team, to ensure cyber-supply chain risk considerations are addressed on a best effort basis based on availability of resources if the acquisition may involve GSA information systems and any of the following are applicable:

(i) *Hardware Devices*. Hardware devices that connect to the GSA enterprise network (wired or wireless).

(ii) *Critical Software*. Critical software that meets the current definition of Critical Software Under Executive Order (EO) 14028, *Improving the*

***Nation's Cybersecurity*, as defined by the National Institute of Standards and Technology (NIST).**

(iii) *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.

(iv) *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.

(v) *FIPS 199 Low-Impact Information Systems*. Unless 507.105(g)(1)(iii) or (iv) applies, this paragraph (g)(1) does not apply to the acquisition of low-impact information systems.

(2) For any other procurement requiring a written acquisition plan, the acquisition planner should discuss efforts to mitigate risks associated with cyber-supply chain risk management. Efforts and considerations could include:

(i) Market research efforts (see 510.002(c) and (d));

(ii) Procuring products or services already approved in GSA's Enterprise Architecture Analytics and Reporting (GEAR) system;

(iii) Procuring products or services with a current GSA IT Assessment and Authorization (A&A, or Authority to Operate (ATO)) or Federal Risk and Authorization Management Program (FedRAMP) Authorization;

(iv) Considering contracting vehicles that have already evaluated awardees supply chain methods and assurances; or

(v) Planning efforts with the GSA CISO.]

*** * * * ***

PART 510 - MARKET RESEARCH

* * * * *

510.002 Pre-Award Procedures

(a) * * *

(b) * * *

[(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, 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 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.]