General Services Administration
Washington, DC 20405

ADM 2800.12B, Change 168
August 17, 2023

GSA ORDER

Subject: General Services Administration Acquisition Manual; GSAM Case 2023-G509, Cyber-Supply Chain Risk Management (C-SCRM) Information Sharing

1. Purpose. This order transmits revisions to the General Services Administration Acquisition Manual (GSAM) regarding cyber-supply chain risk management (C-SCRM) to:

   - Reflect additional security-related risks that may require notification to GSA's Office of Mission Assurance (OMA).
   - Require notification of any change to the relevant Cyber-Supply Chain Risk Management Policy Advisor(s).
   - Clarify the Office of Governmentwide Policy's (OGP) role sharing supply chain risk information with relevant GSA offices and personnel, as appropriate, and with the Federal Acquisition Security Council (FASC), as appropriate.
   - Make editorial changes.

2. Background. General Services Administration Acquisition Manual (GSAM) Case 2021-G511 (Change 135) provided implementing instructions highlighting the process the acquisition workforce must go through to notify the responsible GSA office of a cyber-supply chain event. Contracting officers and acquisition team members were provided with a single location (the GSA IT service desk) to report events.

   Cyber-supply chain risks are constantly evolving. This revision builds on Change 135 to clarify roles, processes, and risk types.

3. Effective date. August 17, 2023

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

   This amendment revises the language of the following GSAM subparts. Specific amendments are explained below.

   - 504.7001 (Definitions)
   - 504.7003 (General Procedures)

- 504.7005 (Notification Procedures for Cyber-Supply Chain Events)

Amend section 504.7001 by-

a. Amending the definition of “Supply Chain Risk Information” to reflect the most current Code of Federal Regulations (C.F.R.) citation.

Amend section 504.7003 by-

b. Amending (a) to add a requirement that changes to the list of Cyber-Supply Chain Risk Management Policy Advisor(s) listed on the GSA Acquisition Portal are reported to spe.request@gsa.gov.
c. Amending (b) to identify GSA’s Office of Mission Assurance (OMA) as the office that acquisition teams must contact for the identification of events requiring notification to the GSA Emergency Operations Center or OMA’s Insider Threat Program.

Amend section 504.7005 by-

a. Reorganizing (d)(1), (d)(2), (d)(3), and (d)(4).
b. Amending (d)(1) to identify and clarify that the GSA Information Technology Office (GSA IT) is a member of the acquisition team for purposes related to the identification of supply chain risk information.
c. Amending (d)(4) to clarify GSA’s Office of Governmentwide Policy (OGP) role sharing supply chain risk information with relevant GSA offices and personnel, as appropriate, and with the Federal Acquisition Security Council (FASC), as appropriate.

5. 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: 2023.08.16 10:38:11 -04'00'

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

GSAM Case 2023-G509

GSAM Text, Line-In/Line-Out

GSAM Baseline: Change 167 effective 08/07/2023
• 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

504.7001 Definitions.

* * *

"Supply chain risk information" is defined at ~~41 C.F.R. 201.102(q)~~**[41 C.F.R. 201-1.101]**. Failure of an offeror to meet a solicitation's requirements, including security requirements, will not by itself constitute supply chain risk information.

* * * * *

504.7003 General procedures.

(a) GSA contracting activities may discuss supply chain concerns with the relevant Cyber-Supply Chain Risk Management Policy Advisor(s) listed on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm) at any time, including during acquisition planning, requirements development, and post award. **[Changes to this list shall be reported to spe.request@gsa.gov.]**

(b) ~~The following groups are responsible for resolving~~**[In addition to the]** Cyber-Supply Chain Events listed in 504.7005**[, additional risks**

may require notification to GSA's Office of Mission Assurance (OMA)]:

(1) [Any law enforcement or criminal activity, suspicious packages, or damage to GSA infrastructure should be reported to the GSA Emergency Operations Center (as specified under GSA Order 2400.2) at EOC@gsa.gov or 202-219-0338]~~Occurrence of an IT security incident. Office of GSA IT~~.

(2) [Insider threats, including acts of commission or omission by an insider who intentionally or unintentionally compromises an agency's ability to accomplish its mission (e.g., espionage, unauthorized disclosure of information, any activity resulting in the loss or degradation of departmental resources or capabilities) should be reported to the OMA Insider Threat Program at insider-threat-program@gsa.gov]~~Discovery of a prohibited article or source. GSA Supply Chain Risk Management Review Board~~.

~~(3) Identification of supply chain risk information. GSA Office of Government-wide Policy.~~

* * * * *

504.7005 Notification procedures for cyber-supply chain events.

(a) * * *
(b) * * *
(c) * * *

(d) *Identification of supply chain risk information.*

~~(1) GSA will share supply chain risk information with the FASC when:~~

~~(i) The FASC requests information associated with a particular source, a covered article, or a covered procurement (as defined at 41 U.S.C. 4713(k));~~

~~(ii) GSA determines that a substantial supply chain risk associated with a source, a covered article, or a covered procurement exists; or~~

~~(iii) GSA identifies supply chain risk management information (including both C-SCRM and non-C-SCRM risks) associated with a source, a covered article, or a covered procurement action and such information is deemed relevant to share with the FASC~~.

~~(2)~~**[(1)]** If substantial supply chain risk information is identified, or the contracting officer or another acquisition team member**[including the GSA Information Technology Office (GSA IT) (e.g., Chief Information Officer, Chief Information Security Officer)]** thinks supply chain risk information should be**[voluntarily]** shared with the FASC, the contracting officer or another acquisition team member must contact the GSA IT Service Desk ~~who~~**[. The GSA IT Service Desk]** will gather relevant information and share it with the appropriate Cyber-Supply Chain Risk Management Policy Advisor.

(i) Service-level policy may adopt additional procedures to provide acquisition team members with guidance prior to notifying the GSA IT Service Desk.

~~(3)~~**[(2)]** After initial notification, the appropriate Cyber-Supply Chain Risk Management Policy Advisor may request additional information and will work with the notifier to resolve the issue.

~~(4)~~**[(3)]** The Cyber-Supply Chain Risk Management Policy Advisors will share information with the Office of Acquisition Policy within OGP. ~~If deemed appropriate, OGP will share the information with the FASC~~

~~(i) The Office of Acquisition Policy within OGP will disseminate any supply chain risk information shared by the FASC to the relevant GSA offices and personnel.~~

~~(1)~~**[(4) OGP will share supply chain risk information with relevant GSA offices and personnel, as appropriate, and with the FASC when:**

(i) The FASC requests information associated with a particular source, a covered article, or a covered procurement (as defined at 41 U.S.C. 4713(k));

(ii) GSA determines that a substantial supply chain risk associated with a source, a covered article, or a covered procurement exists as described in 41 C.F.R. 201-1.101; or

(iii) GSA identifies supply chain risk management information (including both C-SCRM and non-C-SCRM risks) associated with a source, a covered article, or a covered procurement action and deems such information relevant to share with the FASC.]

* * * * *