General Services Administration
Washington, DC 20405

ADM 2800.12B, Change 135
September 28, 2021

GSA ORDER

Subject: General Services Administration Acquisition Manual; GSAM Case 2021-G511, Cyber-Supply Chain Risk Management (C-SCRM) Incident Response and Risk Information Sharing

1. Purpose. This order transmits a revision to the General Services Administration Acquisition Manual (GSAM) to improve acquisition-related incident response procedures and notification processes, outline GSA's Supply Chain Risk Information sharing process, and to update the GSAM to reflect a focus on 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 C-SCRM response and preparedness. This order reflects GSA's commitment to help meet that goal by establishing GSA-specific procedures for coordinating and assessing additional supply chain risks on GSA contracts.

   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, though GSA already has a robust information technology (IT) governance scheme, acquisition policy (in addition to the 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 one step in updating our acquisition policy to address C-SCRM.

   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, protect against, detect, and respond to these cyber threats. While additional 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.

   On December 21, 2018, the Federal Acquisition Supply Chain Security Act of 2018 (the "Act") was signed into law. The Act requires all Executive Branch agencies to

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

establish a formal program and to conduct supply chain risk assessments[2]. While implementation guidance from the Federal Acquisition Security Council (FASC) - established through the Act - is forthcoming, GSA is again taking proactive steps to start an information sharing process.

3. Effective date. September 28, 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.

   - 504.70 (Cyber-Supply Chain Risk Management)
   - 504.7000 (Scope of Subpart)
   - 504.7001 (Definitions)
   - 504.7002 (Policy)
   - 504.7003 (General Procedures)
   - 504.7005 (Notification Procedures for Cyber-Supply Chain Events)

   Amend subpart 504.70 by:

   - Amending the subpart heading by adding “Cyber-” in front of “Supply Chain Risk Management”. GSAM subpart 504.70 is updated to reflect a focus on C-SCRM.

   Amend section 504.7000 by:

   - Updating to reflect the focus on “cyber” supply chain management, remove the concentration on only the post-award phase, and specify the types of contracts and orders to which these procedures apply.

   Amend section 504.7001 by:

   - This section is updated to add or amend the following definitions:
     - Adding a definition for “Cyber-Supply Chain Event”.
     - Adding a definition for “Cyber-Supply Chain Risk Management”.
     - Adding a definition for “Cyber-Supply Chain Management Policy Advisor”.
     - Adding a definition for “IT security incident”.
     - Updating the definition of “Prohibited article”.
     - Adding a definition for “Prohibited source”.
     - Adding a cross-reference to the definition of “Supply chain risk information”.
     - Adding a definition for “Substantial supply chain risk information”.

   Amend section 504.7002 by:

[2] The Federal Acquisition Supply Chain Security Act of 2018 is Title II of the SECURE Technology Act (P.L. 115-390) (Dec. 21, 2018).

- Updating to reflect new policies applicable to C-SCRM.

Amend section 504.7003 by:

- Updating to reflect the responsible groups for resolving Cyber-Supply Chain Events.

Amend section 504.7005 by:

- Simplifying the process the acquisition workforce must go through to notify the responsible GSA office of a cyber-supply chain event[3]. Instead of acquisition workforce members having to determine the proper definition, or identifying the proper location to submit a notification, new language added at 504.7005 highlights the utilization of a "one-entry-point" system. In short, a notification - for any event recognized in the subpart - will go to the GSA IT Service Desk. The IT Service Desk technician will help identify the type of event and notify the responsible party. This will alleviate the acquisition workforce from the responsibility of determining where to submit various notifications.
- Adding requirements to share supply chain risk information (including for both C-SCRM and non-C-SCRM risks), to reflect GSA's commitment to sharing relevant information with the FASC.

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: 2021.09.27 12:21:10 -04'00'

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

[3] "Cyber-Supply Chain Event" is now defined through this amendment at GSAM 504.7001.

GSAM Case 2021-G511
GSAM Text, Line-In/Line-Out

GSAM Baseline: Change 134 effective 09/08/2021

- 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

504.7000 Scope of subpart.

This subpart prescribes acquisition policies and procedures **[for]**mitigating **[cyber-]**~~-~~supply chain risks ~~in the post-award phase~~ of ~~a~~ procurement**[s]** funded by GSA. Procedures in this subpart apply to all GSA**[-]** funded contracts and orders**[,]**~~. These procedures apply~~ regardless of the estimated value of the **[solicitation,]** contract**[or order, including purchases under the micro-purchase threshold and purchases using a Government Purchase Card]**.

504.7001 Definitions.

["Cyber-Supply Chain Event" means any situation or occurrence in or to a network, information system, or within the supply chain, not purchased on behalf of another agency, that has the potential to cause undesirable consequences or impacts. Cyber-Supply Chain Events, as they relate to this subpart, can include:

(a) Occurrence of an IT security incident;
(b) Discovery of a prohibited article or source; and
(c) Identification of supply chain risk information.

“Cyber-Supply Chain Risk Management”, or “C-SCRM”, means management of cyber-related (or, more generally, technology-related) risks in all phases of the acquisition lifecycle and at all levels of the supply chain, regardless of the product(s) or service(s) procured.

“Cyber-Supply Chain Risk Management Policy Advisor” means the identified lead of the Service-level acquisition management (e.g., the Federal Acquisition Service’s Office of Policy and Compliance (OPC), the Public Building Service’s Office of Acquisition Management (OAM), the Office of Administrative Services).

“IT security incident” means an occurrence that:

(a) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system;

(b) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

(c) Results in lost, stolen, or inappropriately accessed Controlled Unclassified Information (CUI) (including Personally Identifiable Information (PII)), lost or stolen GSA-owned devices (mobile phones, laptops, Personal Identity Verification (PIV) cards), and any other incident included in CIO-IT-Security-01-02); or

(d) Results in a situation that severely impairs, manipulates, or shuts down the operation of a system or group of systems (e.g., Building Automation Systems, Heating, Ventilation, Air Conditioning (HVAC) systems, Physical Access Control Systems (PACS), Advanced Metering Systems, Lighting Control Systems).]

“Prohibited article” means any prohibited product, system, or service that the contractor **[offers or]**provides **[to the Government]**that conflicts with the supply chain terms or conditions of the **[solicitation or]**contract (e.g., **[Federal Acquisition Security Council (FASC) exclusion order,]**GSA CIO Order, counterfeit items, ~~a~~ FAR **[provision or]**clause, including**[,]** without limitation**[,]** ~~the~~ FAR Clause at 52.204-23, Prohibition on Contracting for Hardware, Software, Products and Services Developed or Provided by Kaspersky Lab and Other

Covered Entities**[, FAR Provision at 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, and FAR Clause at 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment]**).

["Prohibited source" means any entity with which the Government may not enter into or renew a contract or from which the Government may not purchase products or services due to conflicts with the supply chain terms or conditions of the solicitation or contract (e.g., FASC exclusion order, GSA CIO Order, FAR provision or clause, contract-specific provision or clause).]

"Supply chain" means a linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

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

"Substantial supply chain risk information" means supply chain risk information that leads to any of the following:

(a) Removal of a presumptive awardee from pre-award consideration or competition;
(b) Rejection of a proposed subcontractor;
(c) Removal of a subcontractor from a contract; or
(d) Termination of a contract.]

504.7002 Policy.

(a) The Federal Information Security Modernization Act of 2014 **[(Public Law 113-283)]**and associated National Institute of Standards and Technology (NIST) guidance requires Federal agencies to manage supply chain risks for Federal information systems**[and to ensure the effectiveness of information security controls and risks]**.

(b) ~~OMB Circular A-130, "Managing Information as a Strategic Resource," directs agencies to implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle.~~

~~(c)~~ The SECURE Technology Act (Public Law 115-390)**[, which includes the Federal Acquisition Supply Chain Security Act of 2018, established the Federal Acquisition Security Council (FASC) to improve executive branch coordination, supply chain information sharing, and actions to address supply chain risks and]** requires GSA to have a lead representative **[for]** ~~of~~ the agency ~~on the Federal Acquisition Security Council as well as address supply chain risks posed by the acquisition of covered articles~~.

[(c) OMB Circular A-130, "Managing Information as a Strategic Resource," directs agencies to implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, and poor manufacturing and development practices throughout the system development life cycle.

(d) GSA Information Technology (IT) Security Procedural Guide CIO-IT Security-01-02, "Incident Response (IR)" (including successor policies), provides additional processes and procedures for incident response, as outlined by GSA's Office of the Chief Information Security Officer (OCISO).

(e) GSA Information Technology (IT) Security Procedural Guide CIO-IT Security-21-117, "Office of the Chief Information Security Officer (OCISO) Cyber Supply Chain Risk Management (C-SCRM) Program" (including successor policies), establishes a C-SCRM program within GSA's OCISO and serves as the Tier 2 plan for GSA.

(f) GSA CIO Order 2100.1, "GSA Information Technology (IT) Security Policy" (including successor policies), sets forth GSA's IT security policy and establishes controls required to comply with Federal laws and regulations.]

504.7003 General Procedures.

~~(a) Each service and staff office must provide a supply chain risk management point of contact to GSA's representative to the Federal Acquisition Security Council or designee to assist in providing recommended guidance to mitigate supply chain risks.~~

(**[a]**~~b~~) GSA contracting activities may discuss supply chain concerns with the relevant **[Cyber-]**Supply Chain Risk Management **[Policy Advisor(s)]**~~Point(s) of Contact~~ listed on the GSA Acquisition Portal (http://insite.gsa.gov/**[c]**scrm) at any time, including during acquisition planning**[,]** ~~and~~ requirements development**[, and post-award**.

(b) The following groups are responsible for resolving Cyber-Supply Chain Events listed in 504.7005:

(1) *Occurrence of an IT security incident*. Office of GSA IT.

(2) *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 ~~Post-award procedures~~[Notification procedures for cyber-supply chain events].

[(a) *General.*

(1) For any potential cyber-supply chain event, including occurrence of an IT security incident, discovery of a prohibited article or source, or identification of supply chain risk information, the contracting officer or another acquisition team member must contact the GSA IT Service Desk by phone at 866-450-5250 or by email at ITServiceDesk@gsa.gov.

(i) Do not include source selection sensitive information in the notification to the GSA IT Service Desk.

(ii) Do not include other sensitive information (e.g., IP address, access information such as an account login and password) in the notification to the GSA IT Service Desk. The notification should state that

additional information is sensitive and will be provided in person or via a secured method.

(iii) Determining whether the identified issue or potential issue is applicable under the procedures for each event type should not delay the acquisition team member from submitting a notification. When unsure, it is better to notify quickly rather than delay the event notification. The GSA IT Service Desk can assist in defining the event type once submitted.

(b) ***Occurrence of an IT security incident.***

(1) If an IT security incident occurs, concerning any GSA information system or data (owned or operated by GSA or by a contractor or other organization on behalf of GSA), regardless of the estimated value of the contract or order, including purchases under the micro-purchase threshold and purchases using a Government Purchase Card, the contracting officer or another acquisition team member must immediately contact the GSA IT Service Desk.

(2) The notification to the GSA IT Service Desk - whether via phone or email - should document as much information as possible, including:

(i) Description, date and time of the incident;

(ii) Whether any PII or contractor-attributional information is affected; and

(iii) Contract information (contract number, contractor name, name of GSA contracting office), as applicable.

(3) Do not delay notifying the GSA IT Service Desk even if all the information requested or considered to be relevant is not available.

(4) Additional guidance is available from the GSA IT Security Procedural Guide CIO-IT Security-01-02, "Incident Response (IR)", and GSA IT Security Procedural Guide CIO-IT Security-21-117, "OCISO Cyber Supply Chain Risk Management (C-SCRM) Program".

(5) After initial notification, GSA IT may request additional information and will work with the notifier to resolve the issue.]

~~(a) *Supply Chain Event Report.*~~**[(c) *Discovery of a prohibited article or source.*]**

(1) If a prohibited article **[or source]**is discovered within the supply chain of a procurement, **[regardless of the estimated value of the solicitation, contract, or order, including purchases under the micro-purchase threshold and purchases using a Government Purchase Card,]**the contracting officer **[or another acquisition team member must]**~~shall~~ immediately **[contact the GSA IT Service Desk]**~~submit a supply chain event report using the online form on the GSA Acquisition Portal (http://insite.gsa.gov/scrm) to ensure appropriate service and staff offices within GSA are notified~~.

(2) The **[notification to the GSA IT Service Desk - whether via phone or email - should document as much information as possible, including]**~~supply chain event report must include the following information~~:

(i) Contract **[or solicitation]**information, including contract **[or solicitation]** number**[,]** ~~and~~ contractor **[or offeror]** name**[, and]**~~;~~

~~(ii)~~ **[name of]**GSA contracting office;

(ii~~i~~) Prohibited article **[or source]**name;~~ and~~

(i**[ii]**~~v~~) Reason why prohibited article **[or source]**is banned on contract; **[and**

(iv) A "critical date," no less than three (3) business days in the future, for when a response from GSA's Supply Chain Review Board is requested.

(3) Do not delay notifying the GSA IT Service Desk even if all the information requested or considered to be relevant is not available.

(4) **After initial notification, GSA's Supply Chain Review Board may request additional information and will work with the notifier to resolve**

the issue.]~~The contracting officer shall provide as much information as is available at the time of report submission.~~

[(i) If the SCRM Review Board has not responded by the "critical date" required by 504.7005(c)(2)(iv), the contracting officer may make a determination without the SCRM Review Board's input, but should seek input and guidance from the appropriate Cyber-Supply Chain Risk Management Policy Advisor (see GSAM 504.7003(a)) and review additional guidance available on the GSA Acquisition Portal (http://insite.gsa.gov/cscrm) prior to making the determination.]

~~(4) GSA's representative to the Federal Acquisition Security Council or designee will notify the contracting officer to confirm receipt of the report.~~

[(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) If substantial supply chain risk information is identified, or the contracting officer or another acquisition team member thinks supply chain risk information should be shared with the FASC, the contracting officer or another acquisition team member must contact the GSA IT Service Desk who 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) 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) 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.]

(**[e]**~~b~~) **[Cyber-]**Supply Chain Event Risk Mitigation. The contract administration procedures under FAR part 49 (e.g., cure notice, termination for cause, past performance review) can be u**[s]**~~tiliz~~ed as needed to address immediate or future supply chain event concerns. Additional guidance on contract administration procedures is available on the GSA Acquisition Portal (http://insite.gsa.gov/**[c]**scrm)

(**[f]**~~c~~) *Past Performance Evaluation.* The contracting officer **[must]**~~shall~~ report any contractor non-compliance with supply chain requirements within the "Other Areas" portion of any applicable past performance evaluation form.

* * * * *