Subpart 504.70 - Cyber-Supply Chain Risk Management

Parent topic: Part 504 - Administrative Matters

504.7000 Scope of subpart.

This subpart prescribes acquisition policies and procedures for mitigating cyber-supply chain risks of procurements funded by GSA. Procedures in this subpart apply to all GSA-funded contracts and orders, 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, or FAR provision or clause, including, without limitation, 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 risk information” is defined at 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.

“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)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 the agency.

(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) 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)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.

(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

504.7004 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).

504.7005 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.

(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 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)Contract or solicitation information, including contract or solicitation number, contractor or offeror name, and name of GSA contracting office;

(ii)Prohibited article or source name; and

(iii)Reason why prohibited article or source is banned on contract.

(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.

(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.

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

(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. 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.

(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.

(3) The Cyber-Supply Chain Risk Management Policy Advisors will share information with the Office of Acquisition Policy within OGP.

(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.

(e) *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 used 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/cscrm).

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