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.

Parent topic: Subpart 504.70 - Cyber-Supply Chain Risk Management