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

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