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.

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