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.

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