

## Fed. Acquisition Security Council

## § 201-1.102

part 9 of the Federal Acquisition Regulation (48 CFR part 9).

*Source* means a non-Federal supplier, or potential supplier, of products or services, at any tier.

*Supply chain risk* means the risk that any person may sabotage, maliciously introduce unwanted functionality, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted by or through covered articles.

*Supply chain risk information* includes, but is not limited to, information that describes or identifies:

- (1) Functionality and features of covered articles, including access to data and information system privileges;
- (2) The user environment where a covered article is used or installed;
- (3) The ability of a source to produce and deliver covered articles as expected;
- (4) Foreign control of, or influence over, a source or covered article (e.g., foreign ownership, personal and professional ties between a source and any foreign entity, legal regime of any foreign country in which a source is headquartered or conducts operations);
- (5) Implications to government mission(s) or assets, national security, homeland security, or critical functions associated with use of a source or covered article;
- (6) Vulnerability of Federal systems, programs, or facilities;
- (7) Market alternatives to the covered source;
- (8) Potential impact or harm caused by the possible loss, damage, or compromise of a product, material, or service to an organization's operations or mission;
- (9) Likelihood of a potential impact or harm, or the exploitability of a system;
- (10) Security, authenticity, and integrity of covered articles and their supply and compilation chain;
- (11) Capacity to mitigate risks identified;

(12) Factors that may reflect upon the reliability of other supply chain risk information; and

(13) Any other considerations that would factor into an analysis of the security, integrity, resilience, quality, trustworthiness, or authenticity of covered articles or sources.

### § 201-1.102 Federal Acquisition Security Council (FASC).

(a) *Composition.* The following agencies and agency components shall be represented on the FASC:

- (1) Office of Management and Budget;
- (2) General Services Administration;
- (3) Department of Homeland Security;
- (4) Cybersecurity and Infrastructure Security Agency;
- (5) Office of the Director of National Intelligence;
- (6) National Counterintelligence and Security Center;
- (7) Department of Justice;
- (8) Federal Bureau of Investigation;
- (9) Department of Defense;
- (10) National Security Agency;
- (11) Department of Commerce;
- (12) National Institute of Standards and Technology; and
- (13) Any other executive agency, or agency component, as determined by the Chairperson of the FASC.

(b) *FASC information requests.* The FASC may request such information from executive agencies as is necessary for the FASC to carry out its functions, including evaluation of sources and covered articles for purposes of determining whether to recommend the issuance of removal or exclusion orders, and the receiving executive agency shall provide the requested information to the fullest extent possible.

(c) *Consultation and coordination with other councils.* The FASC will consult and coordinate, as appropriate, with other relevant councils and inter-agency committees, including the Chief Information Officers Council, the Chief Acquisition Officers Council, the Federal Acquisition Regulatory Council, and the Committee on Foreign Investment in the United States, with respect to supply chain risks posed by the acquisition and use of covered articles.

(d) *Program office and committees.* The FASC may establish a program office and any committees, working groups, or other constituent bodies the FASC deems appropriate, in its sole and unreviewable discretion, to carry out its functions. Such a committee, working group, or other constituent body is authorized to perform any function lawfully delegated to it by the FASC.

### Subpart B—Supply Chain Risk Information Sharing

#### § 201–1.200 Information sharing agency (ISA).

The Act requires the FASC to identify an appropriate executive agency—the FASC’s information sharing agency (ISA)—to perform administrative information sharing functions on behalf of the FASC, as provided at 41 U.S.C. 1323(a)(3). The ISA facilitates and provides administrative support to a FASC supply chain and risk management Task Force, and serves as the liaison to the FASC on behalf of the Task Force, as the Task Force develops the processes under which the functions described in 41 U.S.C. 1323(a)(3) are implemented on behalf of the FASC. The Department of Homeland Security (DHS), acting primarily through the Cybersecurity and Infrastructure Security Agency, is named the appropriate executive agency to serve as the FASC’s ISA. The ISA’s administrative functions shall not be construed to limit or impair the authority or responsibilities of any other Federal agency with respect to information sharing.

(a) *Submission of information.* Information should be submitted to the FASC by sending it to the ISA, acting on behalf of the FASC.

(b) *Receipt and dissemination functions.* The ISA, the Task Force, and support personnel at the FASC member agencies will carry out administrative information receipt and dissemination functions on behalf of the FASC.

(c) *Interagency supply chain risk management task force.* The FASC may identify members for an interagency supply chain risk management (SCRM) task force (the Task Force) to assist the FASC with implementing its informa-

tion sharing, analysis, and risk assessment functions as described in 41 U.S.C. 1323(a)(3). The purpose of the Task Force is to allow the FASC to capitalize on the various supply chain risk management and information sharing efforts across the Federal enterprise. This Task Force includes technical experts in SCRM and related interdisciplinary experts from agencies identified in § 201–1.102 and any other agency, or agency component, the FASC Chairperson identifies. The ISA facilitates the efforts of, and provide administrative support to, the Task Force and periodically reports to the FASC on Task Force efforts.

(d) *Processes and procedures.* The FASC will adopt and, as it deems necessary, revise:

(1) Processes and procedures describing how the ISA operates and supports FASC recommendations issued pursuant to 41 U.S.C. 1323(c);

(2) Processes and procedures describing how Federal and non-Federal entities must submit supply chain risk information (both mandatory and voluntary submissions of information) to the FASC, including any necessary requirements for information handling, protection, and classification;

(3) Processes and procedures describing the requirements for the dissemination of classified, controlled unclassified, or otherwise protected information submitted to the FASC by executive agencies;

(4) Processes and procedures describing how the ISA facilitates the sharing of information to support supply chain risk analyses under 41 U.S.C. 1326, recommendations issued by the FASC, and covered procurement actions under 41 U.S.C. 4713;

(5) Processes and procedures describing how the ISA will provide to the FASC and to executive agencies on behalf of the FASC information regarding covered procurement actions and any issued removal or exclusion orders; and

(6) Any other processes and procedures determined by the FASC Chairperson.