4.2301 Definitions.

As used in this subpart—

Covered article as defined in 41 U.S.C. 4713(k), means—

(1) *Information technology*, as defined in 40 U.S.C. 11101, including cloud computing services of all types;

(2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);

(3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or

(4) Hardware, systems, devices, software, or services that include embedded or incidental *information technology*.

FASCSA order means any of the following orders issued under the Federal *Acquisition* Supply Chain Security Act (FASCSA) requiring the removal of *covered articles* from *executive agency* information systems or the exclusion of one or more named *sources* or named *covered articles* from *executive agency procurement* actions, as described in 41 CFR 201–1.303(d) and (e):

(1) The Secretary of Homeland Security *may* issue *FASCSA orders* applicable to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of *FASCSA order may* be referred to as a Department of Homeland Security (DHS) *FASCSA order*.

(2) The Secretary of Defense *may* issue *FASCSA orders* applicable to the Department of Defense (DoD) and national security systems other than *sensitive compartmented information systems*. This type of *FASCSA order may* be referred to as a DoD *FASCSA order*.

(3) The Director of National Intelligence (DNI) *may* issue *FASCSA orders* applicable to the intelligence community and *sensitive compartmented information systems*, to the extent not covered by paragraph (2) of this definition. This type of *FASCSA order may* be referred to as a DNI *FASCSA order*.

Federal Acquisition Security Council (FASC) means the Council established pursuant to 41 U.S.C. 1322(a).

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;

(8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;

(9) The Bureau of Intelligence and Research of the Department of State;

(10) The Office of Intelligence and Analysis of the Department of the Treasury;

(11) The Office of Intelligence and Analysis of the Department of Homeland Security; or

(12) Such other elements of any department or agency as *may* be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of *national defense* or foreign policy.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of any *covered articles*, or any *products* or services produced or provided by a *source*. This applies when the *covered article* or the *source* is subject to an applicable *FASCSA order*. A *reasonable inquiry* excludes the need to include an internal or third-party audit.

Sensitive compartmented information means *classified information* concerning or derived from intelligence *sources*, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive compartmented information system means a national security system authorized to process or store *sensitive compartmented information*.

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

Supply chain risk, as defined in 41 U.S.C. 4713(k), 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 on the *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 covered *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; and

(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*.

Parent topic: Subpart 4.23 Federal Acquisition Security Council.