52.204-28 Federal Acquisition Supply Chain Security Act Orders—Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts.

As prescribed in 4.2306(a), insert the following clause:

Federal *Acquisition* Supply Chain Security Act Orders—Federal Supply Schedules, Governmentwide *Acquisition* Contracts, and Multi-Agency Contracts (Dec 2023)

(a) *Definitions*. As used in this clause—

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.

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

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.

(b) *Notice*. During contract performance, the Contractor *shall* be required to comply with any of the following that apply: DHS FASCSA orders, DoD FASCSA orders, or DNI FASCSA orders. The applicable FASCSA order(s) will be identified in the request for quotation (see 8.405-2), or in the

notice of intent to place an order (see 16.505(b)). FASCSA orders will be identified in paragraph (b)(1) of FAR 52.204-30, Federal *Acquisition* Supply Chain Security Act Orders—Prohibition, with its *Alternate* II.

(c) *Removal.* Upon notification from the *contracting officer*, during the performance of the contract, the Contractor *shall* promptly make any necessary changes or modifications to remove any covered article or any product or service produced or provided by a *source* that is subject to an applicable Governmentwide FASCSA order (see FAR 4.2303(b)).

(End of clause)

Parent topic: 52.204 [Reserved]