Billing Code 3110-05

OFFICE OF MANAGEMENT AND BUDGET

41 CFR Part 201

Federal Acquisition Supply Chain Security Act

AGENCY: Office of Management and Budget, OMB.

ACTION: Interim final rule with request for comments.

SUMMARY: As authorized by the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA), the Federal Acquisition Security Council (FASC) is issuing this interim final rule to implement the requirements of the laws that govern the operation of the FASC, the sharing of supply chain risk information, and the exercise of its authorities to recommend issuance of removal and exclusion orders to address supply chain security risks.

DATES: Effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Written comments must be received on or before [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties should provide comments via electronic mail to the following inbox: OFCIO@omb.eop.gov. The Office of Management and Budget is located at 725 17th Street, NW, Washington, DC 20503. No physical copies will be accepted.

Instructions: Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered. Comments submitted in response to this notice may be made publically available and are subject to disclosure under the Freedom of Information Act. For this reason, please do not include in your comments information of a

confidential nature, such as sensitive personal information or proprietary information, or any information that you would not want publicly disclosed. Summary information of the public comments received, including any specific comments, may be posted on *regulations.gov*.

FOR FURTHER INFORMATION CONTACT: Lisa N. Barr, 202-395-3015, Lisa.N.Barr@omb.eop.gov

SUPPLEMENTARY INFORMATION:

I. Background

Information and communications technology and services (ICTS) are essential to the proper functioning of U.S. government information systems. The U. S. government's efforts to evaluate threats to and vulnerabilities in ICTS supply chains have historically been undertaken by individual or small groups of agencies to address specific supply chain security risks. Because of the scale of supply chain risks faced by government agencies, and the need for better coordination among a broader group of agencies, there was an organized effort within the executive branch to support Congressional efforts in 2018 to pass new legislation to improve executive branch coordination, supply chain information sharing, and actions to address supply chain risks.

The Federal Acquisition Supply Chain Security Act of 2018 (FASCSA or Act) (Title II of Pub. L. No. 115-390), signed into law on December 21, 2018, established the Federal Acquisition Security Council (FASC). The FASC is an executive branch interagency council, chaired by a senior-level official from the Office of Management and Budget (OMB), and includes representatives from the General Services Administration (GSA); Department of Homeland Security (DHS); Office of the Director of National Intelligence (ODNI); Department of Justice; Department of Defense (DoD); and Department of Commerce (Commerce).

Pursuant to subsection 202(d) of the FASCSA, the FASC is required to prescribe this IFR to implement subchapter III of chapter 13 of title 41, U.S. Code. This IFR is organized in three subparts. Subpart A explains the scope of this IFR, provides definitions for relevant terms, and establishes the membership of the FASC. Subpart B establishes the role of the FASC's Information Sharing Agency (ISA). DHS, acting primarily through the Cybersecurity and Infrastructure Security Agency, will serve as the ISA. The ISA will standardize processes and procedures for submission and dissemination of supply chain information, and will facilitate the operations of a Supply Chain Risk Management (SCRM) Task Force under the FASC. This FASC Task Force (hereafter referred to as "Task Force") will be comprised of designated technical experts that will assist the FASC in implementing its information sharing, risk analysis, and risk assessment functions. Subpart B also prescribes mandatory and voluntary information sharing criteria and associated information protection requirements. Subpart C provides the criteria and procedures by which the FASC will evaluate supply chain risk from sources and covered articles and recommend issuance of orders requiring removal of covered articles from executive agency information systems (removal orders) and orders excluding sources or covered articles from future procurements (exclusion orders). Subpart C also provides the process for issuance of removal orders and exclusion orders and agency requests for waivers from such orders.

II. Analysis of Part 201

Subpart A – General

Subpart A establishes regulations generally applicable to the operations of the FASC. Subpart A, § 201.101(a) summarizes the scope of subparts A, B, and C, which generally govern the activities of federal agencies, and not non-federal entities. § 201.101(b) clarifies that nothing

in these regulations require non-federal entities to share supply chain risk information with the federal government. In addition, because subpart C provides for the issuance of exclusion orders and removal orders, which affect the supply and use of products and services supplied by non-federal entities, § 201.101(b)(2) explains that subpart C does not require the removal or a covered article from a non-federal information system or the exclusion of a covered article from procurement by a non-federal entity except to the extent that an exclusion order or a removal order applies to a prime contractor or subcontractor of a federal agency. This applicability to non-federal entities is addressed in § 201.303(e).

Subpart A, § 201.102 provides definitions applicable to the part. Subpart A, § 201.103 describes the membership of the FASC, the authority of the FASC to request information from executive agencies, and the authority of the FASC to establish a program office, committees, working groups, or other constituent bodies. These bodies are authorized to perform any function lawfully delegated to them by the FASC.

Subpart B – Supply Chain Risk Information Sharing

Subpart B identifies DHS as the executive agency for information sharing (or the ISA) and provides for the creation and establishment of a supply chain risk management and information sharing Task Force under the FASC. The ISA will facilitate and provide the administrative support to the FASC Task Force and serve as the liaison to the FASC. The Task Force will develop processes and procedures to be approved by the FASC that describe: (1) how the ISA and Task Force will operate and support the FASC; (2) how federal and non-federal entities submit supply chain risk information to the FASC, including any necessary requirements for information handling, protection and classification; (3) how to share information to support supply chain risk analyses under § 1326 of the Act, recommendations issued by the FASC, and

covered procurement actions under § 4713 of the Act; (4) how to provide information to the FASC and to executive agencies regarding removal orders and covered procurement actions; and (5) any other processes and procedures describing the operations of the FASC as determined by the FASC Chairperson. Subpart B, § 201.202 describes additional details of the mechanics of submitting information to the FASC (including mandatory and voluntary submissions) and dissemination of information by the FASC.

Subpart C – Removal Orders and Exclusion Orders

Subpart C describes the process by which the FASC will evaluate one or more sources and/or one or more covered articles to determine whether to recommend that the Secretary of Homeland Security, Secretary of Defense, and/or Director of National Intelligence issue a removal order and/or an exclusion order. Initiation of the process can begin either by referral of the FASC or any member of the FASC; upon the written request of any U.S. Government body; or based on information submitted to the FASC by any individual or non-federal entity that the FASC determines to be credible.

The FASC will evaluate sources and covered articles pursuant to a common set of non-exclusive factors that are listed in this IFR. Allowing for the evaluation of additional information provides the FASC with the needed flexibility to evaluate additional considerations and information on a case-by-case basis.

As part of the analysis of sources and/or covered articles, the FASC will conduct appropriate due diligence regarding the information that it is considering. This due diligence may include reviewing any information made available to the FASC; ensuring, to the extent possible, that the information is credible or that the level of confidence in the information is appropriately taken into consideration; and examining other relevant publicly-available information as

necessary and appropriate. In addition, the FASC will consult with the National Institute of Standards and Technology (NIST), before recommending issuance of an exclusion or removal order, to ensure that recommended orders do not conflict with existing federal standards and guidelines.

If the FASC does not find that recommending a removal or exclusion order is warranted, risk information received and analyzed by the FASC may be shared, as appropriate, pursuant to the procedures in Subpart B.

If the FASC decides to issue a recommendation, that recommendation will include the information necessary for the Secretary of Homeland Security, the Secretary of Defense, or the Director of National Intelligence, as appropriate, to determine whether to issue an exclusion order and/or a removal order. The recommendation must include the risk information and summaries specified in Subpart B, § 201.202(e). The recommendation will be directed to the Secretary of Homeland Security, Secretary of Defense, and/or Director of National Intelligence based on the scope of federal systems, identified in 41 U.S.C. 1323(c)(5), for which the FASC is recommending removal or exclusion from future procurements. The FASC or its designee will provide notice of the recommendation, along with the contents specified in Subpart C, § 201.302(b), to any source named in the recommendation. This due process procedure is intended to provide the named source(s) with the information needed for the source(s) to respond to the recommendation. If named source(s) wishes to respond to the notice, the source(s) should prepare a thorough and complete written response, submitting the response as directed in the notice. The FASC encourages source(s) to provide any information that it believes relevant in responding to the recommendation, including additional technical information about the covered article(s), details about the relationship between the source(s) and any foreign government, and a

detailed mitigation proposal that the source(s) believes would satisfy the concerns identified in the notice. The source(s) should submit such information and materials in writing before any request for a meeting to enable the FASC and the Secretary of Homeland Security, Secretary of Defense, and Director of National Intelligence, as applicable, to fully consider the source's written submission. The FASC may choose to rescind the recommendation based on the information provided by the source(s). The FASC does not intend to publicly disclose communications with the source(s) except to the extent required by law. The FASC welcomes comment on the adequacy or specific improvements to these procedures.

The Secretary of Homeland Security, the Secretary of Defense, or the Director of National Intelligence, as applicable, will review the recommendation and accompanying risk information and materials provided by the FASC, and any information and response submitted by a source, and determine whether to issue a removal order, an exclusion order, or both, for the agencies and systems within the scope of the authority of 41 U.S.C. § 1323(c)(5)(A)(i)–(iii). If one of these officials or an authorized designee issues an exclusion order or removal order, the named source(s) will be notified, among other required and discretionary notifications.

Once a removal or exclusion order is issued, all agencies to which the order applies would be required to comply with the order pursuant to 41 U.S.C. 1323(c)(7) and 44 U.S.C. 3554(a)(1)(B)(vi). If orders applying to the same source(s) or covered articles were issued by the Secretaries of Homeland Security and Defense and the Director of National Intelligence (i.e., effectively an executive branch-wide removal and/or exclusion order), the Administrator of General Services and officials at other executive agencies responsible for management of the Federal Supply Schedules, government-wide acquisition contracts, and multi-agency contracts

would facilitate implementation of such orders by removing the covered articles or sources identified in the orders from such contracts.

The regulation provides procedures for agencies to submit requests to the issuing official for an exception to an issued order. An agency may request an exception to an issued order for various reasons, such as need for additional time to comply with the order, or for a complete waiver based on issues of national security. The FASC will establish procedures for requesting waivers and criteria for approving or disapproving such requests, as appropriate.

All issued exclusion and removal orders must be reviewed at least annually pursuant to procedures which will be established by the FASC. Furthermore, an authorized official of the issuing agency may modify or rescind an issued exclusion or removal order, so long as a modified order does not apply more broadly than the order before modification.

III. Request for Comment

The FASC invites comments on all aspects of this IFR. Any non-public (oral and written) communications with FASC officials regarding the substance of this rule would be considered an ex-parte presentation, and a summary of the substance of the ex-parte presentation will be placed on the public record and become part of this docket. Not later than two (2) business days after an oral communication or meeting, the party which engaged in such communication or meeting must submit a memorandum to OMB summarizing the substance of the communication. OMB reserves the right to supplement the memorandum with additional information as necessary, or to request that the party making the filing do so, if a FASC official believes that important information was omitted or characterized incorrectly. Any written presentation provided in support of the oral communication or meeting will also be placed on the public record and become part of this docket. Such ex-parte communications must be submitted to this docket as

provided in the **ADDRESSES** section above and clearly labeled as an ex-parte presentation. Federal entities are not subject to these procedures.

IV. Classification

Executive Orders 12866 and 13563: Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a significant regulatory action under E.O. 12866. Accordingly, the Office of Information and Regulatory Affairs has reviewed this rule.

Executive Order 13771: This rule is not subject to the requirements of E.O. 13771, because the rule is issued with respect to a national security function of the United States. As highlighted by sections I and II of this preamble, national security is a primary direct benefit of this rule. Application of the national security exemption under E.O. 13771 requires assessing the application of the "good cause" exception under 5 U.S.C. 533. This rule meets the "good cause" exception, as FASCSA requires publication of an interim final rule to effectuate the authorities of the FASC in a timely manner, and the one-year deadline Congress established for publication of such rule would not provide sufficient time for notice and comment in light of the complex nature of the rule and interagency process.

Regulatory Flexibility Act: Because the FASC is not required to publish a notice of proposed rulemaking for this interim final rule under 5 U.S.C. 553, no Regulatory Flexibility Analysis is required. *See* 5 U.S.C. 603(a), 604(a).

Paperwork Reduction Act: The Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA) provides that an agency generally cannot conduct or sponsor a collection of information, and no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, unless that collection has obtained OMB approval and displays a currently valid OMB Control Number. This rule does not contain a collection of information and is therefore not subject to the PRA.

Congressional Review Act: The FASC has determined that this rule will take effect upon publication pursuant to 5 U.S.C. 808(2). The FASC finds that notice and public procedure before this rule takes effect is unnecessary and contrary to the public interest under 5 U.S.C. 808(2) in light of Congress's direction to issue an interim final rule to address the critical supply chain security issues covered by this rule and to respond to public comments when issuing a final rule. *See* 41 U.S.C. 1321 note.

Unfunded Mandates Reform Act of 1995: This rule does not contain any unfunded mandate or significantly or uniquely affect small governments, as described in the Unfunded Mandates Reform Act of 1995.

Executive Order 13132 (Federalism): This rule does not have Federalism implications as specified in Executive Order 13132.

Executive Order 12630 (Governmental Actions and Interference with Constitutionally Protected Property Rights): This rule does not implement policies that have takings implications as identified in Executive Order 12630.

Executive Order 13175 (Consultation and Coordination with Indian Tribes): The rule does not have tribal implications and will not impose substantial direct costs on tribal governments or preempt tribal law as specified by Executive Order 13175.

National Environmental Policy Act: This IFR does not require a detailed environmental analysis as the establishment and operation of FASC will not "individually or cumulatively have a significant effect on the human environment" (40 CFR 1508.4).

List of Subjects in 41 CFR Part 201

Cybersecurity, Federal acquisition, Government procurement, Information sharing, Information technology, National security, Removal and exclusion orders, Security measures, Supply chain, Supply chain risk information, Technology.

Grant Schneider,
Federal Chief Information Security Officer.

For the reasons set out in the preamble, 41 CFR part 201 is added to read as follows:

PART 201—FEDERAL ACQUISITION SUPPLY CHAIN SECURITY

Subpart A—General

Sec.

201.304 Executive agency compliance with exclusion and removal orders.

Authority: 41 U.S.C. 1321–1328, 4713.

Subpart A—General

§ 201.101 Scope.

(a) Except as provided in paragraph (b) of this section, this part applies to the following:

(1) The membership and operations of the FASC, including all U.S. and contractor personnel supporting the FASC's operations;

(2) Submission and dissemination of supply chain risk information; and

(3) Recommendations for, issuance of, and associated procedures related to removal orders and exclusion orders.

(b) This part does not require the following:

(1) Mandatory submission of supply chain risk information by non-federal entities.

(2) The removal or exclusion of any covered article by non-federal entities, except to the extent that an exclusion or removal order issued pursuant to subpart C of this Part applies to prime contractors and subcontractors to federal agencies.

§ 201.102 Definitions

For purposes of this part:

(a) *Appropriate congressional committees and leadership* means:

(1) The Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Select Committee on Intelligence, and the majority and minority leader of the Senate; and

(2) The Committee on Oversight and Government Reform, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Homeland Security, the Committee on

Armed Services, the Committee on Energy and Commerce, the Permanent Select Committee on Intelligence, and the Speaker and minority leader of the House of Representatives.

(b) *Council or FASC* means the Federal Acquisition Security Council.

(c) *Covered article* means any of the following:

(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 or subsequent U.S. government program for controlling sensitive unclassified information; or

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

(d) *Covered procurement* means:

(1) A source selection for a covered article involving either a performance specification, as provided in subsection (a)(3)(B) of title 41 U.S.C. 3306, or an evaluation factor, as provided in subsection (b)(1)(A) of title 41 U.S.C. 3306, relating to a supply chain risk, or where supply chain risk considerations are included in the agency's determination of whether a source is a responsible source;

(2) The consideration of proposals for and issuance of a task or delivery order for a covered article, as provided in title 41 U.S.C. 4106(d)(3), where the task or delivery order contract includes a contract clause establishing a requirement relating to a supply chain risk;

(3) Any contract action involving a contract for a covered article where the contract includes a clause establishing requirements relating to a supply chain risk; or

(4) Any other procurement in a category of procurements determined appropriate by the Federal Acquisition Regulatory Council, with the advice of the Federal Acquisition Security Council.

(e) *Covered procurement action* means any of the following actions, if the action takes place in the course of conducting a covered procurement:

(1) The exclusion of a source that fails to meet qualification requirements established under 41 U.S.C. 3311, for the purpose of reducing supply chain risk in the acquisition or use of covered articles;

(2) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order;

(3) The determination that a source is not a responsible source, based on considerations of supply chain risk; and

(4) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source from consideration for a subcontract under the contract.

(f) Exclusion order means any of the following orders requiring the exclusion of sources or covered articles from executive agency procurement actions:

(1) An order issued by Secretary of Homeland Security applicable to federal executive branch civilian agencies;

(2) An order issued by the Secretary of Defense applicable to Department of Defense and national security systems other than sensitive compartmented information systems; or

(3) An order issued by the Director of National Intelligence applicable to the Intelligence Community and sensitive compartmented information systems.

(g) *Executive agency* means:

(1) An executive department specified in 5 U.S.C. 101;

(2) A military department specified in 5 U.S.C. 102;

(3) An independent establishment as defined in 5 U.S.C. 104(1); and

(4) A wholly owned Government corporation fully subject to chapter 91 of title 3 U.S.C.

(h) *Information and communications technology* means:

(1) Information technology as defined in 40 U.S.C. 11101;

(2) Information systems, as defined in 44 U.S.C. 3502; and

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

(i) *Information technology* has the definition provided in 40 U.S.C. 11101.

(j) *Intelligence Community* includes 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;

(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.

(k) *National security system* has the definition given to it in 44 U.S.C. 3552 and 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 subject to paragraph (j)(1)(3) of this section, 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.

(3) Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(l) *Removal order* means any of the following orders, issued pursuant to 41 U.S.C. 1323(c)(5), requiring the removal of covered articles from executive agency information systems:

(m) An order issued by Secretary of Homeland Security applicable to federal executive branch civilian agencies;

(2) An order issued by the Secretary of Defense applicable to Department of Defense and national security systems other than sensitive compartmented information systems; or

(3) An order issued by the Director of National Intelligence applicable to the intelligence community and sensitive compartmented information systems.

(n) *Responsible source* means a responsible prospective contractor and subcontractors, at any tier, as defined in part 9 of the Federal Acquisition Regulation.

(o) *Source* means a non-federal supplier, or potential supplier, of products or services, at any tier.

(p) *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.

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

(1) Functionality of covered articles, including access to data and information system privileges;

(2) Information on the user environment where a covered article is used or installed;

(3) The ability of the source to produce and deliver covered articles as expected (i.e., supply chain assurance);

(4) Foreign control of, or influence over, the source (e.g., foreign ownership, personal and professional ties between the source and any foreign entity, legal regime of any foreign country in which the source is headquartered or conducts operations);

(5) Implications to national security, homeland security, and/or national critical functions associated with use of the covered source;

(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) Credibility of and confidence in other supply chain risk information;

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

(14) A summary of the above information, including: summary of the threat level on 1 (low) to 5 (high) scale; and summary of the vulnerability level on 1 (low) to 5 (high) scale; and, any other information determined to be relevant to the determination of supply chain risk.

§ 201.103 Federal Acquisition Security Council (FASC).

(a) 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) 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 the Chief Information Officers Council, the Chief Acquisition Officers Council, the Federal Acquisition Regulatory Council, the Committee on Foreign Investment in the United States, and other relevant councils and interagency committees 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

§ 201.201 Information Sharing Agency (ISA).

The Act requires the FASC to identify an appropriate executive agency—the FASC's Information Sharing Agency (ISA)—to perform the administrative information sharing functions on behalf of the FASC, as enumerated in the law at 41 U.S.C. 1323(a)(3). The ISA will facilitate and provide the administrative support to a FASC supply chain and risk management Task Force; and serve as the liaison to the FASC to communicate the Task Force efforts, as the Task Force develops the processes under which the functions in 41 U.S.C. 1323(a)(3) will be 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

are not construed to limit or impair the authority or responsibilities of any other federal agency with respect to information sharing.

(a) All references in this part to the "submission of information to the FASC" mean the submission of information to the ISA and the Task Force, on behalf of the FASC, pursuant to the FASC-approved processes and procedures described in this Section.

(b) The ISA and the Task Force will carry out administrative information dissemination functions on behalf of the FASC, and any references to the "dissemination of information by the FASC" mean dissemination of information by the ISA, on behalf of the FASC, pursuant to the FASC-approved processes and procedures described in this Section.

(c) *Interagency Supply Chain Risk Management Task Force.* The FASC will identify members for an interagency supply chain risk management (SCRM) task force (the Task Force) to assist the FASC with implementing its information sharing, risk 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 will include technical experts in SCRM and related interdisciplinary experts from agencies identified in § 201.103 and any other agency, or agency component, the FASC Chairperson identifies. The ISA will facilitate the efforts of and provide administrative support to the Task Force and periodically report to the FASC on the Task Force efforts. The ISA will convene the Task Force, including providing a physical location/facility to host the Task Force.

(d) The ISA, in consultation with the Task Force, will submit to the FASC for approval:

(1) Processes and procedures describing how the ISA and the Task Force will operate and support the FASC;

(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 for the ISA to notify the federal entity that provided classified information to the ISA, prior to disseminating that classified information;

(4) Processes and procedures describing how the ISA and the Task Force will facilitate 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) Process and procedures describing how the ISA and Task Force will provide information to the FASC and to executive agencies regarding covered procurement actions by agencies and any issued removal orders and covered procurement actions; and

(6) Any other processes and procedures describing the operations of the Task Force as determined by the FASC Chairperson.

(e) The ISA will also identify to the FASC any ISA resource gaps, including, but not limited to, gaps in staffing, budget, organization, training, materials, and facility needs that may be necessary to implement its duties pursuant to this part.

§ 201.202 Submitting Information to the FASC.

(a) *Requirements for Submission of Information.* All submissions of information to the FASC must be accomplished through the processes and procedures approved by the FASC in § 201.201. Any information submission to the FASC must comply with information sharing protections described in § 201.202 and be consistent with applicable law and regulations.

(b) *Mandatory Information Submission Requirements*. Executive agencies must expeditiously submit supply chain risk information to the ISA using procedures approved by the FASC in § 201.201 when:

(1) The FASC requests information relating to a particular source, covered article or covered procurement; or

(2) An executive agency has determined there is a reasonable basis to conclude a substantial supply chain risk associated with a source, covered procurement, or covered article exists. In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including:

(i) Supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying or managing its supply chain risk;

(ii) Supply chain risk information regarding covered procurement actions by the agency under 41 U.S.C. 4713; and any orders issued by the agency under 41 U.S.C. 4713.

(c) *Voluntary Information Submission Requirements.* All federal and non-federal entities may submit information relevant to SCRM, covered articles, sources, or covered procurement actions to the FASC not described in paragraph (b) in this section, *Mandatory Information Submission Requirements*.

(d) *Information Protections.* To the extent that information submitted to the FASC must be protected in accordance with applicable law and regulation, agencies providing such information must ensure the information contains proper marking, handling, dissemination, or use restrictions, including but not limited to the following:

(1) For classified information, the transmitting and receiving agencies shall ensure that information is provided to designated ISA personnel, who have an appropriate security

clearance and a need to know the information. The ISA, Task Force, and the FASC will handle such information consistent with the applicable restrictions.

(2) Other protected information submitted to the FASC must be marked in accordance with any applicable intellectual property, business confidentiality, contractual, or other applicable dissemination rules. The FASC, the ISA, and the Task Force, will handle such information in a manner consistent with such markings.

(3) To the extent supply chain risk information submitted to the FASC includes information protected by the Procurement Integrity Act, agencies shall submit such information consistent with the FASC approved processes and procedures described in § 201.201. The FASC will handle such information consistent with the identified restrictions.

(d) *Dissemination of Information by the FASC.* The FASC maintains the responsibility, at its sole discretion to disclose its recommendations and any supply chain risk information relevant to its recommendation with any federal or non-federal entities when the FASC determines that such sharing may facilitate identification or mitigation of supply chain risk to information systems and to the extent consistent with the following paragraphs:

(1) The FASC may maintain its recommendations and any supply chain risk information as nonpublic, to the extent permitted by law, or otherwise release such information to impacted entities and appropriate stakeholders if circumstances warrant such an approach including but not limited to exercising its discretion regarding the timing of any such release of information, the scope of information to be released, and the intended recipients of such information.

(2) Any release by the FASC of recommendations and supply chain risk information will be in accordance title 41 U.S.C. 1323 and with § 201.202(d), (e), (f) and (g)..

(3) The FASC will not release a recommendation to a non-federal entity, unless a decision on whether or not to issue an exclusion or removal order has been made, and the affected source has been notified.

(e) *Reliance on Shared information*. Executive agencies and the officials identified in § 201.103(a)(1) may consider and rely upon supply chain risk information and any other information the FASC determines appropriate, received pursuant to this subpart and the criteria established under § 201.201, to exercise the authorities and responsibilities in 41 U.S.C. 1323, 1326, and 4713.

(f) *Limitation on further dissemination of the information.* The FASC (including the ISA, Task Force, and any other FASC constituent bodies) shall comply with applicable limitations on dissemination of supply chain risk information submitted pursuant to this subpart, including but not limited to the following restrictions:

(1) Controlled Unclassified Information, such as Law Enforcement Sensitive, Proprietary, Privileged, or Personally Identifiable Information, may only be disseminated in compliance with the safeguarding and dissemination controls applicable for that category of information and consistent with any additional administrative markings applied to this specific information as laid out in Executive Order 13556, *Controlled Unclassified Information*, 32 CFR part 2002.

(2) Classified Information may only be disseminated consistent with the restrictions applicable to the information and in accordance with the FASC's processes and procedures for disseminating classified information as required by this part.

Subpart C—Removal Orders and Exclusion Orders

§ 201.301 Recommending removal orders and exclusion orders.

(a) *Referral Procedure*. The FASC may commence an evaluation of one or more sources and one or more covered articles, pursuant to the criteria in paragraph (b) of this section and for the purpose of determining whether to recommend that the source(s) or covered article(s) be subject to a removal order or exclusion order, in any of the following ways:

(1) Upon the referral of the FASC or any member of the FASC;

(2) Upon the request, in writing, of the head of an executive agency or designee, accompanied by a submission of relevant information; or

(3) Based on information submitted to the FASC by any federal or non-federal entity that the FASC deems, in its discretion, to be credible.

(b) *Criteria*. The FASC will evaluate sources and covered articles, including by analyzing available information, and considering the following, non-exclusive factors, as appropriate:

(1) Functionality of the covered articles, including the source's access to data and information system privileges;

(2) Security, authenticity, and integrity of covered articles and their supply and compilation chains, including for embedded, integrated, and bundled software;

(3) The ability of the source to produce and deliver the covered articles as expected (i.e., supply chain assurance);

(4) Ownership of, control of, or influence over the source or covered article(s) by a foreign government or parties owned or controlled by a foreign government, or other ties between the source and a foreign government, which may include the following considerations:

(i) Whether the U.S. government has identified the country as a foreign adversary or country of special concern;

(ii) Whether the source or its component suppliers have headquarters, research, development, manufacturing, test, distribution, or service facilities or other operations in a foreign country, including a country of special concern or a foreign adversary;

(iii) Personal and professional ties between the source—including its officers, directors or similar officials, employees, consultants, or contractors— and any foreign government; and

(iv) Laws and regulations of any foreign country in which the source has headquarters, research development, manufacturing, testing, packaging, distribution, or service facilities or other operations.

(5) Implications to national, homeland security, or critical functions associated with use of the source(s) or covered article(s);

(6) Vulnerabilities of federal systems, programs, or facilities;

(7) Capacity of the source or the U.S. Government to mitigate risks;

(8) Credibility of, and confidence in available information used to formulate assessment(s) of risk associated with proceeding, with using alternatives, and/or with adopting range of mitigations;

(9) Any transmission of information or data by a covered article to a country outside of the U.S.; and

(10) Any other information that would factor into an assessment of supply chain risk, including any impact to agency mission critical functions, and other information as the FASC deems appropriate.

(c) *Due Diligence*. As part of the analysis conducted pursuant to paragraph (b) of this section, the FASC will conduct appropriate due diligence. Such due diligence may include but need not be limited to the following actions:

(1) Review any information made available by the executive agency identified in § 202.201(a), and any other information the FASC determines appropriate;

(2) Ensure, to the extent possible, that the level of confidence in the information is appropriately taken into consideration; and

(3) Examine other relevant public or commercially available information as necessary or appropriate.

(d) *Consultation with NIST*. NIST will participate in FASC activities as a member and will advise the FASC on NIST standards and guidelines issued under 40 U.S.C. 11331, including ensuring that any recommended orders do not conflict with such standards and guidelines.

(e) *Content of recommendation*. (1) The FASC shall include the following in any recommendation to the Secretary of Homeland Security, Secretary of Defense, and/or Director of National Intelligence:

(i) Information necessary to positively identify any source(s) or covered article(s) recommended for exclusion or removal;

(ii) Information regarding the scope and applicability of the recommended exclusion order, removal order, or both, including whether any such order should apply to all executive agencies or a subset of executive agencies;

(iii) A summary of the supply chain risk assessment reviewed or conducted in support of the recommended exclusion or removal order, including material conflicting or contrary information, if any;

(iv) A summary of the basis for the recommendation, including a discussion of less intrusive measures that were considered and why such measures were not reasonably available to reduce supply chain risk;

(v) A description of the actions necessary to implement the recommended exclusion or removal order; and,

(vi) Where practicable, in the FASC's sole and unreviewable discretion, a description of the mitigation steps that could be taken by the source that may result in the FASC rescinding the recommendation.

(2) *Information sharing in absence of recommendation:* If the FASC decides not to issue a recommendation, information received and analyzed pursuant to the procedures in this section may be shared, as appropriate, pursuant to the procedures in subpart B of this chapter.

§ 201.302 Notice of recommendation to source and opportunity to respond.

(a) *Notice to source*. The FASC shall provide a notice of the FASC's recommendation to any source named in the recommendation.

(b) *Content of notice*. The notice under paragraph (a) of this section shall advise the source:

(1) That a recommendation has been made;

(2) Of the criteria the FASC relied upon and, to the extent consistent with national security and law enforcement interests, the information that forms the basis for the recommendation;

(3) That, within 30 days after receipt of the notice, the source may submit information in response to the recommendation;

(4) Of the procedures governing the review and possible issuance of an exclusion or removal order; and

(5) Where practicable, in the FASC's sole and unreviewable discretion, a description of the mitigation steps that could be taken by the source that may result in the FASC rescinding the recommendation.

(c) *Confidentiality of notice issued to source*. U.S. government personnel shall:

(1) Keep confidential and not make available outside of the executive branch, except to the extent required by law, any notice issued to a source under paragraph (b) of this section until an exclusion order or removal order is issued and the source has been notified pursuant to § 201.303(f)(1); and

(2) Keep confidential and not make available outside of the executive branch, except to the extent required by law, any notice issued to a source under paragraph (b) of this section if the FASC rescinds a recommendation or the Secretary of Homeland Security, Secretary of Defense, and Director of National Intelligence, as applicable, decide not to issue the recommended exclusion order and/or removal order.

(d) *Confidentiality of information submitted by source*. The FASC and its member agencies shall treat information that the source marks as confidential, private, or closely held, when marked by the source as Confidential and Not to be Publicly Shared. The FASC and its member agencies will not disclose such information to the public except to the extent required by law.

§ 201.303 Issuing removal orders and exclusion orders and other related activities.

(a)(1) *Consideration of and issuance of exclusion and removal orders*. The Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence shall review the FASC's recommendations and accompanying information and materials provided by the FASC pursuant to § 201.201, together with any information submitted by a source pursuant to § 201.202, and determine whether to issue an order based upon such recommendation.

(2) *Administrative record*. The administrative record for judicial review of an exclusion or removal order issued pursuant to 41 U.S.C. 1323(c)(6) shall, subject to the limitations set forth in 41 U.S.C. 1327(b)(4)(B)(ii)–(v), consist only of:

(i) The recommendation issued pursuant to 41 U.S.C. 1323(c)(2);

(ii) The notice of recommendation and review issued pursuant to 41 U.S.C. 1323(c)(3);

(iii) Any information and argument in opposition to the recommendation submitted by the source pursuant to 41 U.S.C. 1323(c)(3)(C);

(iv) The exclusion or removal order issued pursuant to 41 U.S.C. 1323(c)(5) and any information or materials directly relied upon by the official identified in paragraphs (b) through (d) of this section, as applicable, in issuing the exclusion or removal order; and

(v) The notification to the source issued pursuant to 41 U.S.C. 1323(c)(6)(A).

(3) *Other information.* Other information or material collected by, shared with, or created by the FASC or its member agencies shall not be included in the administrative record unless

the official identified in paragraphs (b) through (d) of this section, as applicable, directly relied on that information or material in issuing the exclusion or removal order.

(b) *Secretary of Homeland Security*. The Secretary of Homeland Security shall issue removal or exclusion orders applicable only to civilian agencies, to the extent not covered by paragraph (c) or (d) of this section.

(c) *Secretary of Defense.* The Secretary of Defense shall issue removal or exclusion orders applicable only to the Department of Defense including national security systems other than sensitive compartmented information systems.

(d) *Director of National Intelligence.* The Director of National Intelligence shall issue removal or exclusion orders applicable only to the Intelligence Community and sensitive compartmented information systems, to the extent not covered by paragraph (c) in this section.

(e) *Applicability of issued orders to Non-Federal entities*. An exclusion order and a removal order may affect non-federal entities, including as follows:

(1) An exclusion order may require the exclusion of sources or covered articles from any executive agency procurement action, including but not limited to source selection and consent for a contractor to subcontract. To the extent required by the exclusion order, agencies shall exclude the source or covered articles, as applicable, from being supplied by any prime contractor and subcontractor at any tier.

(2) A removal order may require removal of the covered article(s) from an executive agency information system owned and operated by an agency; from an information system operated by a contractor on behalf of an agency; and from other contractor information systems to the extent that the removal order applies to contractor equipment or systems within the scope of "information technology," as defined at herein.

(f) *Notification of issued exclusion and removal orders*. The official who issued the exclusion or removal order:

(1) Shall, upon issuance of an exclusion or removal order pursuant to paragraph (a) of this section:

(i) Notify any source named in the order of the exclusion or removal order; and to the extent consistent with national security and law enforcement interests, information that forms the basis for the order;

(ii) Provide classified or unclassified notice of the exclusion or removal order to the appropriate congressional committees and leadership;

(iii) Provide the exclusion or removal order to the ISA;

(iv) Notify the Interagency Suspension and Debarment Committee about the exclusion or removal order.

(2) May provide the exclusion order or removal order to other persons, including public disclosure, as the official deems appropriate and to the extent consistent with national security and law enforcement interests.

(g) *Delegation*. The officials identified in paragraph (a) of this section may not delegate the authority to issue exclusion and removal orders to an official below the level one level below the Deputy Secretary or Principal Deputy Director level, except that the Secretary of Defense may delegate authority for removal orders to the Commander of U.S. Cyber Command, who may not re-delegate such authority to an official below the level of the Deputy Commander.

(h) *Removal from Federal supply contracts*. If the officials identified in paragraphs (b) through (d) of this section, or their delegate, issue orders collectively resulting in a government-wide exclusion, the Administrator for General Services and officials at other executive agencies

responsible for management of the Federal Supply Schedules, government-wide acquisition contracts and multi-agency contracts shall facilitate implementation of such orders by removing the covered articles or sources identified in the orders from such contracts.

(i) *Annual review of issued orders*. The officials identified in paragraphs (b) through (d) of this section shall review all issued exclusion and removal orders not less frequently than annually pursuant to procedures established by the FASC.

(j) *Modification or rescission of issued orders*. The officials identified in paragraphs (b) through (d) of this section may modify or rescind an issued exclusion or removal order, provided that a modified order shall not apply more broadly than the order before the modification.

§ 201.304 Executive agency compliance with exclusion and removal orders.

(a) *Agency compliance.* Executive agencies shall:

(1) Comply with exclusion and removal orders issued pursuant to § 201.303 and applicable to their agency, as required by 41 U.S.C. 1323(d) and 44 U.S.C. 35554(a)(1)(B); and

(2) Not make publicly-available any exclusion order or removal order unless otherwise approved by the FASC prior to such release.

(b) *Exceptions to issued exclusion and removal orders.* An executive agency required to comply with an exclusion order or a removal order may submit to the official that issued the order a request that an issued order not apply to the agency, to specific actions of the agency, to actions of the agency for a period of time before compliance with the order is practicable, and any other request that the requesting agency seeks. The request shall include all necessary information for the issuing official to review and evaluate the request, including alternative mitigations to the risks addressed by the order and the ability of an agency to fulfill its mission critical functions. Other circumstances that may warrant an exception to an issued order include other findings

related to the national interest, including national security reviews, national security investigations, or national security agreements. The request shall be submitted in writing. The FASC may establish and update additional procedures for requesting waivers and criteria for approving or disapproving such requests as appropriate.

[FR Doc. 2020-18939 Filed: 8/31/2020 8:45 am; Publication Date: 9/1/2020]