

Subtitle D—Federal
Acquisition Supply Chain
Security

CHAPTER 201—FEDERAL ACQUISITION SECURITY COUNCIL

| <i>Part</i> | | <i>Page</i> |
|-------------|---------------------------|-------------|
| 201-1 | General regulations | 7 |

PART 201-1—GENERAL REGULATIONS

Subpart A—General

Sec.

201-1.100 Scope.

201-1.101 Definitions.

201-1.102 Federal Acquisition Security
Council (FASC).

Subpart B—Supply Chain Risk Information Sharing

201-1.200 Information sharing agency (ISA).

201-1.201 Submitting information to the
FASC.

Subpart C—Exclusion and Removal Orders

201-1.300 Evaluation of sources and covered
articles.

201-1.301 Recommendation.

201-1.302 Notice of recommendation to
source and opportunity to respond.

201-1.303 Issuance of orders and related ac-
tivities.

201-1.304 Executive agency compliance with
exclusion and removal orders.

AUTHORITY: 41 U.S.C. 1321-1328, 4713.

SOURCE: 86 FR 47587, Aug. 26, 2021, unless
otherwise noted.

Subpart A—General

§ 201-1.100 Scope.

(a) *Applicability.* 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 Federal Government 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) *Clarification of scope.* This part does not require the following:

(1) Mandatory submission of supply chain risk information by non-Federal entities; or

(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.

§ 201-1.101 Definitions.

For the purposes of this part:

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.

Council or FASC means the Federal Acquisition Security Council.

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.

Covered procurement means:

(1) A source selection for a covered article involving either a performance specification, as provided in subsection (a)(3)(B) of 41 U.S.C. 3306, or an evaluation factor, as provided in subsection (b)(1)(A) of 41 U.S.C. 3306, relating to a supply chain risk, or where supply chain risk considerations are included in the executive 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 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 FASC.

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; or

(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.

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 31, United States Code.

Exclusion order means an order issued pursuant to 41 U.S.C. 1323(c)(5) that requires the exclusion of one or more sources or covered articles from executive agency procurement actions.

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).

Information technology has the definition provided in 40 U.S.C. 11101.

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.

National security system has the definition provided in 44 U.S.C. 3552.

Removal order means an order issued pursuant to 41 U.S.C. 1323(c)(5) that requires the removal of one or more covered articles from executive agency information systems.

Responsible source means a responsible prospective contractor and subcontractors, at any tier, as defined in

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 information sharing, analysis, and risk assess-

ment 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.

Fed. Acquisition Security Council

§ 201-1.201

§ 201-1.201 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 pursuant to § 201-1.200. Any information submission to the FASC must comply with information sharing protections described in this subpart 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 in accordance with guidance approved by the FASC pursuant to § 201-1.200 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 that a substantial supply chain risk exists in connection with a source or covered article. 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 in the course of the agency's activities in furtherance of identifying, mitigating, or managing its supply chain risk;

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

(iii) Supply chain risk information regarding any orders issued by the agency under 41 U.S.C. 1323.

(c) *Voluntary information submission.* All Federal and non-Federal entities may voluntarily submit to the FASC information relevant to SCRM, covered articles, sources, or covered procurement actions.

(d) *Information protections—Federal agency submissions.* To the extent that the law requires the protection of information submitted to the FASC, agencies providing such information must ensure that it bears proper markings to indicate applicable handling, dissemination, or use restrictions. Agencies shall also comply with any relevant handling, dissemination, or

use requirements, including but not limited to the following:

(1) For classified information, the transmitting agency 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 and the relevant processes and procedures adopted pursuant to § 201-1.200.

(2) With respect to controlled unclassified or otherwise protected unclassified information, the transmitting agency, the FASC, the ISA, and the Task Force will handle the information in a manner consistent with the markings applied to the information and the relevant processes and procedures adopted pursuant to § 201-1.200.

(e) *Information protections—submissions by non-Federal entities.* Information voluntarily submitted to the FASC by a non-Federal entity shall be subject to the following provisions:

(1) Supply chain risk information not otherwise publicly or commercially available that is voluntarily submitted to the FASC by non-Federal entities and marked "Confidential and Not to Be Publicly Disclosed" will not be released to the public, including pursuant to a request under 5 U.S.C. 552, except to the extent required by law.

(2) Notwithstanding paragraph (e)(1) of this section, the FASC may, to the extent permitted by law, and subject to appropriate handling and confidentiality requirements as determined by the FASC, disclose the supply chain risk information referenced in paragraph (e)(1) in the following circumstances:

(i) Pursuant to any administrative or judicial proceeding;

(ii) Pursuant to a request from any duly authorized committee or subcommittee of Congress;

(iii) Pursuant to a request from any domestic governmental entity or any foreign governmental entity of a United States ally or partner, but only to the extent necessary for national security purposes;

(iv) Where the non-Federal entity that submitted the information has consented to disclosure; or

§ 201–1.300

(v) For any other purpose authorized by law.

(3) This paragraph (e) shall continue to apply to supply chain risk information referenced in paragraph (e)(1) even after the FASC issues a recommendation for exclusion or removal pursuant to 41 U.S.C. 1323.

(f) *Dissemination of information by the FASC.* The FASC may, in its sole discretion, disclose its recommendations and any supply chain risk information relevant to those recommendations to Federal or non-Federal entities if the FASC determines that such sharing may facilitate identification or mitigation of supply chain risk, and disclosure is 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 release such information to impacted entities and appropriate stakeholders. The FASC shall have discretion to determine the circumstances under which information will be released, as well as the timing of any such release, the scope of the information to be released, and the recipients to whom information will be released.

(2) Any release by the FASC of recommendations or supply chain risk information will be in accordance title 41 U.S.C. 1323 and the provisions of this subpart.

(3) The FASC will not release a recommendation to a non-Federal entity, other than a source named in the recommendation, unless an exclusion or removal order has been issued based on that recommendation, and the named source has been notified.

(4) 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:

(i) Controlled Unclassified Information, such as Law Enforcement Sensitive, Proprietary, Privileged, or Personally Identifiable Information, may only be disseminated in compliance with the restrictions applicable to the information and in accordance with the

41 CFR Ch. 201 (7–1–24 Edition)

FASC’s processes and procedures for disseminating controlled unclassified information as required by this part.

(ii) 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—Exclusion and Removal Orders

§ 201–1.300 Evaluation of sources and covered articles.

(a) *Referral procedure.* The FASC may commence an evaluation of a source or covered article 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 a 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) *Relevant factors.* In evaluating sources and covered articles, the FASC will analyze available information and consider, as appropriate, any relevant factors contained in the following non-exclusive list:

(1) Functionality and features of the covered article, including the covered article’s or source’s access to data and information system privileges;

(2) The user environment in which the covered article is used or installed;

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

(4) The ability of the source to produce and deliver covered articles as expected;

(5) 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:

Fed. Acquisition Security Council

§ 201–1.301

(i) Whether a Federal agency 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, testing, packaging, 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.

(6) Implications for government missions or assets, national security, homeland security, or critical functions associated with use of the source or covered article;

(7) Potential or existing threats to or vulnerabilities of Federal systems, programs or facilities, including the potential for exploitability;

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

(9) Credibility of and confidence in available information used for assessment of risk associated with proceeding, with using alternatives, and/or with enacting mitigation efforts;

(10) Any transmission of information or data by a covered article to a country outside of the United States; and

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

(c) *Foreign Ownership.* Nothing in this section shall be construed to authorize the issuance of an exclusion or removal order based solely on the fact of the foreign ownership of a potential procurement source that is otherwise qualified to enter into procurement contracts with the Federal Government.

(d) *Due Diligence.* As part of the analysis performed 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) Reviewing any information the FASC considers appropriate; and

(2) Assessing the reliability of the information considered.

(e) *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.

§ 201–1.301 Recommendation.

(a) *Content of recommendation.* The FASC shall include the following in any recommendation for the issuance of an exclusion or removal order made to the Secretary of Homeland Security, Secretary of Defense, and/or Director of National Intelligence:

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

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

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

(4) 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;

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

(6) 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's rescission of the recommendation.

(b) *Information sharing in the absence of a 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, in accordance with subpart B of this part.

§ 201-1.302 Notice of recommendation to source and opportunity to respond.

(a) *Notice to source.* The FASC shall provide a notice of its 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 and argument in opposition 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) *Submission of response by source and potential rescission of recommendation.* Subject to any applicable procedures or processes developed by the FASC, and in accordance with any instructions provided to the source pursuant to paragraph (b) of this section, a source may submit to the ISA information or argument in opposition to a FASC recommendation. If a source submits information or argument in opposition:

(1) The ISA will convey the source's submission to the FASC and any appropriate constituent bodies and to the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence.

(2) Upon receipt of such information or argument in opposition, the FASC may rescind the recommendation if the FASC, consistent with the sole and unreviewable discretion provided in paragraph (b)(5) of this section:

(i) Determines that the source has undertaken sufficient mitigation to reduce supply chain risk to an acceptable level; or

(ii) Decides that other grounds justify rescission.

(3) In the event that the FASC rescinds its recommendation, the ISA will communicate that decision to the source. The ISA will notify Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence of the rescission, and provide those officials with a summary of the FASC's reasoning.

(d) *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 (a) of this section until an exclusion order or removal order is issued and the source has been notified; 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 (a) of this section if the FASC rescinds the associated recommendation or the Secretary of Homeland Security, Secretary of Defense, and Director of National Intelligence, as applicable, decide not to issue the recommended order.

(e) *Confidentiality of information submitted by source.* Information not otherwise publicly or commercially available that is submitted to the FASC by a source pursuant to paragraph (c) of this section and marked "Confidential and Not to Be Publicly Disclosed" will not be released to the public, including pursuant to a request under 5 U.S.C. 552, except to the extent required by law. That general rule notwithstanding, such information may be released as provided in § 201-1.201(d)(2).

§ 201-1.303 Issuance of orders and related activities.

(a) *Consideration of recommendation and issuance of orders.* The Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence shall each review the FASC's recommendation, any accompanying information and materials provided pursuant to § 201-1.301, and any information submitted by a source pursuant to § 201-1.302, and determine

whether to issue an exclusion or removal order based upon the recommendation.

(b) *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) through (v), consist only of:

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

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

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

(4) The exclusion or removal order issued pursuant to 41 U.S.C. 1323(c)(5), and any information or materials relied upon by the deciding official in issuing the order; and

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

(6) *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 deciding official relied on that information or material in issuing the exclusion or removal order.

(d) *Issuing officials.* Exclusion or removal orders may be issued as follows:

(1) The Secretary of Homeland Security may issue removal or exclusion orders applicable to civilian agencies, to the extent not covered by paragraph (d)(2) or (3) of this section.

(2) The Secretary of Defense may issue removal or exclusion orders applicable to the Department of Defense and national security systems other than sensitive compartmented information systems.

(3) The Director of National Intelligence may issue removal or exclusion orders applicable to the Intelligence Community and sensitive compartmented information systems, to the extent not covered by paragraph (d)(2) of this section.

(4) The officials identified in paragraphs (d)(1) through (3) 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.

(e) *Applicability of issued orders to non-Federal entities.* An exclusion or 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 a covered article 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 in § 201-1.101.

(f) *Notification of order issuance.* The official who issues an 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 order's issuance, and to the extent consistent with national security and law enforcement interests, of the information that forms the basis for the order;

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

(iii) Provide the order to the ISA; and

(iv) Notify the Interagency Suspension and Debarment Committee of the order.

(2) May provide a copy of the order to other persons, including through public disclosure, as the official deems appropriate and to the extent consistent

with national security and law enforcement interests.

(g) *Removal from Federal supply contracts.* If the officials identified in paragraphs (d)(1) through (3) of this section, or their delegates, 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.

(h) *Annual review of issued orders.* The officials identified in paragraphs (d)(1) through (3) of this section shall review all issued exclusion and removal orders not less frequently than annually pursuant to procedures established by the FASC.

(i) *Modification or rescission of issued orders.* The officials identified in paragraphs (d)(1) through (3) 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.

§ 201-1.304 Executive agency compliance with exclusion and removal orders.

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

(1) Comply with exclusion and removal orders issued pursuant to § 201-1.303 and applicable to their agency, as required by 41 U.S.C. 1323(c)(7) and 44 U.S.C. 3554(a)(1)(B); and

(2) Comply with handling and/or dissemination restrictions placed upon the order or its contents by the issuing official.

(b) *Exceptions to issued exclusion and removal orders.* An executive agency required to comply with an exclusion or removal order may submit to the issuing official a request to be excepted from the order's provisions. The requesting agency:

(1) May ask to be excepted from some or all of the order's requirements. The agency may ask, for example, that the order not apply to the agency, to specific actions of the agency, or to actions of the agency for a period of time before compliance with the order is practicable.

(2) Shall submit the request in writing and include in it all necessary information for the issuing official to review and evaluate it, including—

(i) Identification of the applicable exclusion order or removal order;

(ii) A description of the exception sought, including, if limited to only a portion of the order, a description of the order provisions from which an exception is sought;

(iii) The name or a description sufficient to identify the covered article or the product or service provided by a source that is subject to the order from which an exception is sought;

(iv) Compelling justification for why an exception should be granted, such as the impact of the order on the agency's ability to fulfill its mission-critical functions, or considerations related to the national interest, including national security reviews, national security investigations, or national security agreements;

(v) Any alternative mitigations to be undertaken to reduce the risks addressed by the exclusion or removal order; and

(vi) Any other information requested by the issuing official.