



FEDERAL ACQUISITION SECURITY COUNCIL

41 CFR Parts 201 and 201-1

Federal Acquisition Security Council Rule

AGENCY: Federal Acquisition Security Council.

ACTION: Final rule.

SUMMARY: As authorized by the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA), the Federal Acquisition Security Council (FASC) is issuing this 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 the FASC's authorities to recommend issuance of removal and exclusion orders to address supply chain security risks. This rule finalizes the interim final rule and corrects the codification structure of the interim final rule.

DATES: Effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

FOR FURTHER INFORMATION CONTACT: Kosta I. Kalpos, 202-881-9601, Konstandinos.I.Kalpos@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 ad hoc, 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 Government-wide coordination, Congress adopted new legislation in 2018 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. It includes representatives from the General Services Administration; Department of Homeland Security (DHS); Office of the Director of National Intelligence (ODNI); Department of Justice; Department of Defense (DOD); and Department of Commerce. The FASC is authorized to perform a variety of functions, including making recommendations for orders that would require the removal of covered articles from executive agency information systems or the exclusion of sources or covered articles from executive agency procurement actions.

II. Rulemaking

Pursuant to subsection 202(d) of the FASCSA, the FASC is required to prescribe first an interim final rule and then a final rule to implement subchapter III of chapter 13 of title 41, U.S. Code. The FASC published the interim final rule (interim rule) at 85 FR 54263 on September 1, 2020. The interim rule invited interested persons to submit comments on or before November 2, 2020. Six entities submitted comments. The final rule reflects changes made based upon some of those comments, as well as feedback received from internal Federal stakeholders. The final rule also corrects certain structural issues introduced by the interim rule, as explained in more detail in section III. This final rule retains the organization and much of the content of the interim rule. It contains three subparts. Subpart A explains the scope of the rule, 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 standardizes processes and procedures for submission and dissemination of supply chain information and facilitates the operations of a Supply Chain Risk Management (SCRM) Task Force under the FASC. This FASC Task Force consists of of designated technical experts who 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 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.

III. Summary of Changes to Interim Rule

Headings and section numbers for the final rule have been adjusted to match the distinctive structure of CFR title 41. The standard structure of 41 CFR, unlike other titles, is:

- Subtitle [capital letter]
- Chapter [Arabic numeral]
- Part [Arabic numeral hyphen Arabic numeral]
- Subpart [capital letter]
- Section [Arabic numeral hyphen Arabic numeral period Arabic numeral]

The interim rule however, did not align with that structure. It did not add a chapter to title 41 CFR, and its numbering scheme for part and section numbers did not match that of title 41. Because of these structural issues, the interim rule added part 201 to subtitle E

(where the amendments could not be codified) instead of adding chapter 201 to subtitle D. The final rule fixes those structural issues, changing interim part 201 to part 201-1, adjusting the section numbering accordingly, and eliminating the improperly codified interim part 201. Internal cross-references within the rule have been updated accordingly.

In general, numerous minor changes were made to the interim rule's text to clarify or simplify it. Although the substance of the final rule largely matches that of the interim rule, several changes have been made in response to public comments and input from Federal stakeholders. Those changes, as well as numerous more minor, technical changes, are summarized below for each section of the final rule that has been modified from the interim rule.

A. Changes to Subpart A

1. § 201-1.101—Definitions

The final rule incorporates minor technical, clarifying, or simplifying changes to the definitions of “exclusion order,” “national security system,” and “removal order,” and “supply chain risk information.”

2. § 201-1.103—Federal Acquisition Security Council (FASC)

Minor changes were made to paragraph (c) of this section to track the underlying statutory language more closely.

B. Changes to Subpart B

1. § 201-1.200—Information sharing agency (ISA)

Paragraph (a) was modified to clarify that information should be submitted to the FASC by sending it to the ISA.

Paragraph (b) was modified to provide that the ISA, the FASC Task Force, and support personnel will carry out information receipt and dissemination functions on behalf of the FASC.

Paragraph (c) was modified to remove the obligation for the ISA to provide a physical facility to host the FASC Task Force.

Paragraph (d) was modified to clarify the nature of the processes and procedures to be adopted by the FASC.

Paragraph (e) of this section of the interim rule has been deleted from the final rule. That paragraph, which provided for the ISA to identify “resource gaps” to the FASC, was determined to be unnecessary.

2. § 201-1.201—Submitting information to the FASC

Minor technical corrections and clarifying changes were made to paragraphs (a) and (b).

Paragraph (d) was modified to make minor technical and clarifying changes and to make clear that its provisions apply only to submissions by Federal agencies.

The section corresponding to this one in the interim rule erroneously included two provisions labeled as paragraph (d). The second provision labeled paragraph (d) has been labeled paragraph (f) in the final rule. Paragraph (f)(3) of the final rule has been modified from its analogue in the interim rule to clarify that the FASC will not release a recommendation to a non-Federal entity unless an exclusion or removal order has been issued based on that recommendation, and the affected source has been notified.

The provision that appeared in paragraph (e) of this section of the interim rule has been removed from the final rule because it was superfluous and could have been interpreted to imply incorrectly that the FASC must explicitly authorize agencies to rely upon information disseminated to them by the FASC.

Paragraph (e) of this section of the final rule has been added to describe the protection that will be afforded to voluntary submissions by non-Federal entities.

C. Changes to Subpart C

1. § 201-1.300—Evaluation of sources and covered articles

Paragraph (a) was edited for clarity and brevity.

The heading of paragraph (b) was changed to “Relevant factors” from “Criteria.” The list appearing in that paragraph has been modified to clarify or adjust the description of some factors and to include as a factor the user environment in which a covered article is used or installed.

The language in paragraph (c) of the interim rule was shifted to paragraph (d) and replaced with a statement providing that nothing in this section shall be construed to authorize the issuance of a 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.

Paragraph (d)(3) (interim rule paragraph (c)(3)) was removed as duplicative of paragraph (d)(1).

Paragraph (e) of the interim rule was broken into two separate paragraphs and moved into § 201-1.301 to simplify the structure of the final rule.

2. § 201-1.301—Recommendation

Paragraph (e) of interim rule § 201.301 has been moved to this section as paragraphs (a) and (b). Minor clarifying changes were made to the language of those paragraphs.

3. § 201-1.302—Notice of recommendation to source and opportunity to respond

The language included in paragraphs (c) and (d) of interim rule § 201.302 was relocated to paragraphs (d) and (e) in this section of the final rule. A new provision was added as paragraph (c) to clarify how the FASC may rescind a recommendation upon consideration of a source’s response in opposition to a notice of recommendation. Paragraph (d) of the interim rule, now located in paragraph (e) of the final rule, was modified so that the protections afforded under that provision are the same as those afforded with respect to information submitted voluntarily by non-Federal entities.

4. § 201-1.303—*Issuance of orders and related activities*

Various simplifying or clarifying edits were made to the provisions of interim rule § 201.303, and the content of that interim rule section was also reorganized into a more logical paragraph structure for the final rule. The interim rule’s description of the authority of the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence was modified to mirror the underlying statutory language more closely and make clear that the authority to issue exclusion and removal orders is discretionary.

5. § 201-1.304—*Executive agency compliance with exclusion and removal orders*

The final rule includes minor technical corrections and clarifications that were made to the provisions of this section of the interim rule. Paragraph (a)(2) no longer requires agencies to obtain FASC approval before publicly releasing an exclusion or removal order. Instead, the final rule requires that agencies comply with any dissemination or other controls placed upon an exclusion or removal order by the issuing official.

Paragraph (b) of the final rule includes new language specifying certain requirements to be met by agencies requesting to be excepted from the provisions of an exclusion or removal order. Those agencies must submit their request in writing to the official who issued the order and provide specified information, including a compelling justification for the waiver and a description of any forms of risk mitigation to be undertaken if the waiver is granted.

IV. Comments and Responses

The FASC received six sets of comments from the public in response to the publication of the interim rule. Relevant comments from those submissions are addressed below in connection with the rule subpart to which they relate or, if they do not relate to a particular subpart, under the heading “General Comments.” Because no comments

related particularly to subpart A of the interim rule, no heading is provided for that subpart in this section for Comments and Responses.

A. Interim Rule Subpart B

Subpart B establishes the role of the FASC's information sharing agency (ISA), provides for an interagency Task Force to support the FASC, prescribes mandatory information-sharing criteria for Federal agencies, and outlines requirements for marking, handling, and disseminating protected supply chain risk information. Multiple commenters asked for further clarification of the protections that would be afforded to non-Federal entities who voluntarily share information with the FASC. In response to these comments, § 201-1.201(e) was added to the final rule to describe the protection that will be afforded to information that is submitted to the FASC by such non-Federal entities (NFEs) and that is not otherwise publicly or commercially available. If such information is marked by the submitting NFE with the legend, "Confidential and Not to Be Publicly Disclosed," the FASC will not release the marked material to the public, except to the extent required by law. Regardless of any protection offered by that general rule, § 201-1.201(e)(2) makes clear that the FASC retains broad discretion to disclose information submitted by NFEs to appropriate recipients in a range of circumstances.

The FASC recognizes that its retention of such broad discretion may dissuade some NFEs from submitting sensitive information. At this time, however, the FASC has chosen to prioritize greater sharing of information in appropriate circumstances over the possibility of receiving more supply chain risk information from NFEs. If the FASC determines over time that the Federal Government's interests would be better served by a different weighing of priorities, the FASC may revise the rule accordingly.

One commenter asked whether NFEs who shared information with the FASC would receive protection under the Cybersecurity Information Sharing Act of 2015 (CISA 2015), Pub. L. No. 114-113, div. N. The final rule does not address that issue. The

FASC is continuing to coordinate with FASC member agencies to consider any intersections between CISA 2015 and the FASC's authorities and may, as appropriate, provide further guidance to stakeholders at a future date.

Several commenters also suggested that the FASC should afford protections to NFEs whose information might be used to support the issuance of an exclusion or removal order. The final rule provides for no such protections. The FASC lacks authority to obviate, restrict, or otherwise alter the potential legal liability of one private party to another. And other, more indirect forms of protection—such as an automatic guarantee of confidentiality or protection from public disclosure of the identity of providers of information—could decrease the quality of information received from NFEs by removing disincentives that would otherwise deter the submission of inaccurate or misleading information. Shielding the identity of NFEs who submit information might also, depending on the circumstances, unduly interfere with the ability of an affected source to respond substantively to a notice of the FASC's recommendation for the issuance of an exclusion or removal order. In light of these considerations, the final rule includes no additional provisions aimed at protecting NFEs from legal liability. One commenter asked how the ISA will maintain data submitted to the FASC and in what system that data will be stored. The FASC anticipates that the ISA will handle, store, and protect information in accordance with all applicable laws, regulations, and policies. The final rule does not specify the nature of the system in which the ISA will store FASC data or provide detailed requirements for the technical means by which the ISA will maintain that data; such specifications would unduly restrict the ISA.

Another commenter requested more information about the FASC's "influence" on "priorities and taskings" within the intelligence community. No changes to the rule have been made in response to that request. Executive agencies, including those encompassing

components of the intelligence community, will continue to follow their relevant authorities with regard to their own priorities and taskings.

Several comments concerned the possible release of information to the public by the FASC. Some commenters requested more information about the circumstances in which the FASC will share supply chain risk information with the private sector; others suggested that the FASC should maintain a public list of sources and covered articles that have been the subject of exclusion or removal orders. The final rule does not specify circumstances in which the FASC must share information with the public, or require maintenance of a public list of sources and covered articles that have been the subject of exclusion or removal orders. The FASC anticipates that determining whether to release supply chain risk information—including the names of sources and covered articles addressed by exclusion or removal orders—will be a highly fact-specific inquiry. Other applicable law and binding government-wide policies may also limit the information that the FASC may publicly disclose. For instance, national security considerations may require that, in some scenarios, the nature of certain covered articles or sources or the rationale for some FASC recommendations not be made public. Accordingly, the final rule simply states that the FASC will comply with applicable legal requirements in light of the particular circumstances to decide the extent to which supply chain risk information can be released to non-government entities.

B. Interim Rule Subpart C

Subpart C addresses evaluation of sources and covered articles by the FASC. It enumerates the processes by which the FASC may issue a recommendation, obtain a response to a recommendation from named sources, and, when appropriate, rescind a recommendation. Commenters raised several topics in connection with this subpart.

One commenter asked whether protections would be offered for “companies that have been identified to the FASC as a potential risk” but are not the subject of a

recommendation or a removal/exclusion order. The commenter speculated that contracting offices in the Federal Government could create an “informal blacklist” that would prevent companies that had been identified as security risks from contracting with the Federal Government. The FASC has seen no evidence that its activities will result in a blacklist. As a result, the final rule does not include any changes in response to this public comment.

Some commenters suggested that because NFEs may submit information voluntarily to the FASC, the FASC may receive inaccurate or false information from companies attempting to sabotage competitors. Commenters suggested various means to address this contemplated problem: requiring NFEs submitting information to execute a certification of some kind attesting to their good faith; providing affected sources with remedies against NFEs who submit false information; enlisting private-sector entities to “vet” supply chain risk information; or limiting the extent to which information may be requested by the FASC or submitted by NFEs. The FASC does not believe that the rule should include any of these measures at this time. The final rule retains in § 201-1.300(d) the requirement that the FASC perform “appropriate due diligence” in evaluating supply chain risk. The FASC may request and obtain information from a wide range of sources within the Federal Government, including investigative and intelligence-gathering agencies; it has ample means to assess the reliability of information received from the private sector or elsewhere. As a result, the FASC concludes that there is little basis to believe that the submission of inaccurate information by NFEs will subvert the outcome of the FASC’s deliberations.

Commenters also expressed concern that, under § 201-1.300(b), a source’s ties to foreign countries are expressly identified as one factor among many to be considered as part of a supply chain risk analysis. These commenters pointed out that many companies have connections to other nations, and asserted that companies fear that their association

with a certain country or countries will automatically place them under suspicion within the FASC. In response to these comments, the interim rule was modified to include § 201-1.300(c), which echoes 41 U.S.C. § 1323(f)(2)'s text to emphasize that nothing in the rule may be construed to authorize the issuance of an exclusion or removal order based solely on the foreign ownership of an otherwise qualified source. Additionally, the final rule, like the interim rule, lists a source's foreign ties merely as one factor among a non-exclusive list of factors to be considered in the FASC's evaluation; nothing in either rule requires that factor to be given determinative weight.

For that reason, the FASC disagrees with a commenter who suggested that such a factor was inconsistent with treaties intended to encourage international trade. Such treaties form part of the backdrop against which the FASC will make its decisions. Given the international ties of many companies and the extensive participation of the United States in the global economy, the FASC will not be inclined to recommend exclusion of a company simply because it is active in more than one country.

One commenter suggested that the FASC consider foreign ties in its analysis only if those ties concern a country other than an ally of the United States. Another requested that the rule be amended to specify the component of the Federal Government with authority to designate a country as "a country of special concern or a foreign adversary" pursuant to § 201-1.300(b). Neither recommendation has been implemented in the final rule because the FASC is already able to account for the considerations suggested by the commenters. In evaluating the risk posed by a covered article or a source, the FASC may consider not just whether a source has connections to a foreign country, but also the nature of that country's relationship with the United States; it may consider not just whether a Federal agency has designated a country as an adversary, but also which agency or official made that designation and why.

Several comments concerned the process by which exclusion or removal orders may be issued. One, for example, recommended that any source being evaluated by the FASC should be notified “at the outset” of that review and allowed to comment “as early as possible.” The final rule does not implement that recommendation. Depending on the circumstances of a particular case, national security considerations may weigh against informing a source that it has drawn the attention of the FASC at a time when no recommendation has been issued. As a result, the final rule does not mandate either early or ongoing communication with a source prior to the issuance of a recommendation.

Other comments raised the concern that sources named in a recommendation would not receive enough information from the FASC to mount an adequate response. The final rule, like the interim rule, provides that the source named in a recommendation must be notified of the criteria relied upon by the FASC in developing that recommendation. § 201-1.302(b)(2). The source must also be advised of the information upon which the FASC based its recommendation, so long as disclosure of that information is consistent with national security and law enforcement interests. This body of information will allow the source to understand the FASC’s reasoning and so to prepare a response. Contrary to one commenter’s suggestion, the “criteria” to be disclosed to the source are not equivalent to a simple list of the generically described factors identified in § 201-1.300(b) of the final rule. To make that fact clear, the label for that list of factors in the final rule has been changed from “Criteria” to “Relevant Factors.”

The interim final rule provided that the administrative record on judicial review of an exclusion or removal order would include, among other things, “any information or materials directly relied upon by the” official who issued the order. One commenter objected that the use of the word “directly” indicated that the administrative record supporting exclusion or removal orders would not conform to the requirements of the

FASCSA. To prevent any such misinterpretation and mirror the language of the FASCSA more closely, the word “directly” has been removed from paragraphs (b)(4) and (c) of § 201-1.303.

Some commenters made broader or more general suggestions regarding FASC processes. One recommended that the FASC should require what it called “standard due process trappings,” including “hearings, discovery, right to counsel, [and] the ability to appeal [to the] [F]ederal court system.” No change to the interim rule has been made in response to this comment. The final rule, like the interim rule and the FASCSA statutory scheme, provides for due process by ensuring that affected sources will be notified of possible adverse action and given an opportunity to address the Federal Government’s basis for such an action. The rule and the statutory scheme also provide for review by a Federal court of appeals of any exclusion or removal order resulting from a FASC recommendation. Discovery is not contemplated by the FASCSA and is not a “standard due process” element in judicial review based upon an administrative record. There is no due process right to counsel in civil matters. Mandating additional procedures such as a discovery process would make the FASC’s proceedings considerably slower and more expensive, thereby impeding the Federal Government’s ability to protect against serious cyber threats to its systems—a result that is contrary to the purposes of the FASCSA and would significantly undermine important Federal Government interests.

Another commenter requested that the FASC afford the public the opportunity for comment before enacting new rules, and that an opportunity for appeal be given for “measures targeting specific companies.” The FASC has concluded that any applicable requirements of the Administrative Procedure Act are fully sufficient to address the public interests implicated by new rules. In addition, the FASCSA provides sources named in exclusion or removal orders the opportunity to appeal an order to a Federal

court of appeals. 41 U.S.C. 1327(b). Because these requests are addressed by statute, the FASC has not modified the interim rule to address them.

One commenter objected to the statement in the preamble to the interim rule that “the FASC does not intend to publicly disclose communications with the source(s) except to the extent required by law,” suggesting that it conflicted with provisions of the interim rule concerning the treatment of confidential information submitted by a source in response to a notice of a FASC recommendation. For the final rule, the relevant provision of the interim rule has been modified to clarify that confidential information submitted by a source is subject to the same degree of protection provided pursuant to new § 201-1.201(d) for confidential information submitted voluntarily by NFEs.

One commenter inquired about the timing of the FASC recommendation process, suggesting that the rule prescribe “a reasonable timeline regarding when” an exclusion or removal order is issued and “when it will go into effect.” The same commenter asserted that a source named in an exclusion or removal order should be afforded at least 60 days from the effective date of an order “to respond to the FASC.” This comment reflects a misunderstanding of the FASC process. The FASC does not issue exclusion or removal orders, and so a source has no reason to “respond to the FASC” once such an order is issued. The FASC makes recommendations for the issuance of orders. Any sources named in a FASC recommendation will have the opportunity to respond to the FASC before an order may be issued. The FASC may alter or withdraw its recommendation based on a source’s response. If the FASC chooses not to do so, then an appropriate official from DHS, DOD, or ODNI may issue an order based on the recommendation.

Pursuant to 41 U.S.C. 1327, a source may request judicial review of an order within 60 days after being notified of its issuance. The ordering official, not the FASC, is responsible both for deciding the effective date of the order and for providing notification of the order to the source. 41 U.S.C. 1323(c)(5), (6). As a result, the FASC does not in

the interim or the final rule attempt to constrain the ordering official's discretion as to the manner in which the effective date of an order is determined or in which notification of an order is issued to the source.

The same commenter opined that the FASC should prescribe in the final rule "a reasonable timeline" for when a covered procurement action may be announced and when it may go into effect. Fact-specific considerations, such as the imminence of the risk posed by a source and the characteristics of the procurement at issue, will heavily influence the timeline for a covered procurement action. The final rule therefore allows authorized officials to determine an appropriate timeline on a case-by-case basis, rather than prescribing a single approach.

The same commenter also suggested that the FASC should issue a preliminary recommendation, allow submission of a response by the affected source(s), and then issue a final recommendation. The final rule provides for such a process, although it does not label recommendations as "preliminary" or "final." Instead, the final rule includes a new provision at paragraph (c) of § 201-1.302, which makes clear that after the FASC issues a recommendation and the source submits a response, the FASC has the discretion to rescind the recommendation. The final rule thus makes explicit that, if a source demonstrates through its response to the FASC that a removal or exclusion order is unwarranted, the FASC may withdraw its recommendation.

One commenter asked that the FASC clarify whether the FASC may release its recommendation even if no related exclusion or removal order is issued. The final rule addresses that issue in paragraph (f)(3) of § 201-1.201, providing that if a recommendation is rescinded, or the relevant officials determine that no exclusion or removal order will be issued based upon it, the recommendation will be kept confidential and will not be released to entities, other than the source, outside of the Federal Government.

Two commenters suggested that exclusion or removal orders should be narrowly tailored, or should incorporate a finding that the action ordered represents the least intrusive measure reasonably available to address a given supply chain risk. No change to the rule was made in response to these comments. As the interim rule did, the final rule requires the FASC to include in a recommendation for an exclusion or removal order “a discussion of less intrusive measures that were considered and why such measures were not reasonably available to reduce supply chain risk.” § 201-1.301(a)(4). That requirement ensures that the FASC will consider the disruption that may result from a contemplated action, weigh it against the threat to be addressed, and issue a recommendation of appropriate scope.

Several comments requested rule provisions establishing the nature and extent of contractors’ and subcontractors’ obligations under exclusion or removal orders. The FASC anticipates that such obligations will vary widely depending on the nature of the circumstances addressed by an exclusion or removal order. As a result, it is not feasible to attempt to prescribe those obligations categorically through this rulemaking. Instead, those obligations must be ascertained based upon the content of the order in question and any guidance issued by the ordering agency or the agencies implementing that order, as well as any applicable contract terms or procurement regulations.

One commenter recommended that the FASC adopt a rule requiring the notification of prime contractors whenever a subcontractor is the subject of a recommendation. The FASC declines to follow that suggestion. If a FASC recommendation is not implemented through the issuance of one or more exclusion or removal orders, then there may never be a need for prime contractors to react to that recommendation. Furthermore, alerting primes to the issuance of a recommendation that may never yield an order may conflict with national security interests and/or the named source’s interest in confidentiality.

One commenter requested further detail on the manner in which an agency can obtain a waiver relieving it of obligations under an exclusion or removal order. The final rule includes a new paragraph in § 201-1.304 that clarifies the waiver process. An agency seeking an exception to some or all of the requirements of an order must submit a request for that exception to the ordering official. The request must identify the relevant order and the covered article or source affected, describe precisely the exception sought, and provide a compelling justification for the grant of an exception as well as an account of any alternative risk reduction techniques the agency will employ in lieu of complying with the order. The official who issued the order has the authority to decide whether an exception will be granted.

3. Miscellaneous Comments

Some commenters urged the FASC to adopt rule provisions creating a permanent or standardized relationship between the FASC and the private sector. Although the FASC recognizes that the private sector has a great deal of knowledge about and experience with supply chain risk analysis and mitigation, the final rule does not provide for a particular type of formal relationship or engagement with industry. The FASC is still in the early stages of its operations and requires further information—gained from experience—to determine the most effective ways to interact with the private sector. It is premature to prescribe regulations dictating the nature of that engagement at this time.

Some comments suggested that the FASC rely upon an already existing task force housed within the Department of Homeland Security. Although the FASC certainly intends to draw upon the knowledge and experience of that task force to the extent feasible, the final rule does not mandate a role for it. The task force managed by the Department of Homeland Security is not a permanent entity. It would therefore be impractical to mandate a role for that task force in FASC operations.

Other comments emphasized the numerous supply chain risk initiatives within the Federal Government and requested that the FASC make efforts to bring coherence to the standards and activities stemming from those various initiatives. The FASC recognizes that the Federal Government's supply chain risk management activities may benefit from greater consistency and coordination and intends to work toward those goals.

Similarly, one comment urged the FASC to operate through an "inter-agency process" that accounts for "other supply chain-related laws, regulations, and risk mitigation measures." The FASC emphasizes that it is itself an interagency body drawing upon the efforts and resources of its constituent members. The final rule, like the interim rule, provides that the FASC will be supported by a FASC Task Force composed of SCRM experts drawn from across the Federal Government. Because the FASC's activities necessarily constitute an "inter-agency process," no changes have been made to the interim rule in response to this comment.

One commenter protested that exclusion or removal orders could have "disparate impacts" on small businesses. But that commenter did not suggest any specific change that might address that putative problem while ensuring the FASC retained its ability to address supply chain risks. Both the interim and the final rule require the FASC to consider the intrusiveness of its recommendations; the effect of a recommended order on contractors, including small business, may be considered as appropriate as part of that analysis. As a result, no change to the rule has been made based on this comment.

No change to the rule has been made in response to a comment asserting that complying with exclusion and removal orders is likely to be "incredibly expensive" to American companies. The FASC expects to weigh the burden likely to result from a recommended order against the anticipated benefit and would not lightly recommend an order that would be "incredibly expensive" either to the Federal Government or to the private sector. The final rule requires the FASC to include in a recommendation for an

exclusion or removal order “a discussion of less intrusive measures that were considered and why such measures were not reasonably available to reduce supply chain risk.” That requirement will help to ensure that the costs of exclusion and removal orders are not disproportionate to the scale of the risk at issue.

Finally, one commenter asserted that commercial products and commercial-off-the-shelf (COTS) items should be excluded from the reach of the FASC because addressing them through exclusion or removal orders would “deprive government of significant innovation and the latest technologies.” The FASC strongly disagrees with that recommendation. The ubiquity of commercial products and COTS items, not only within the Federal Government, but within the private sector as well, means that they are a frequent target of malicious actors seeking to find and capitalize upon technological vulnerabilities. Excluding those items from oversight by the FASC would undermine the Council’s ability to reduce the Federal Government’s exposure to supply chain risk. No changes have been made in response to this comment.

V. Procedural Requirements

Executive Orders 12866 (Classification): This final rule has been designated non-significant and therefore was not reviewed by the Office of Management and Budget under Executive Order 12866.

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

Congressional Review Act: Pursuant to the Congressional Review Act, (5 U.S.C. § 801 et seq.), the Office of Information and Regulatory Affairs designated this rule as not a “major rule,” as defined by 5 U.S.C. § 804(2).

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 rule 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 201-1

Computer technology, Cybersecurity, Government procurement, Government technology, Information technology, National security, Security measures, Science and technology, Supply chain, Supply chain risk management.

Christopher DeRusha

Chair, Federal Acquisition Security Council

For the reasons set out in the preamble, the FASC amends 41 CFR subtitles D and E as follows:

Subtitle D—FEDERAL ACQUISITION SUPPLY CHAIN SECURITY

1. Revise the heading to subtitle D to read as set forth above.
2. Add chapter 201, consisting of part 201-1, to subtitle D to read as follows:

Chapter 201—FEDERAL ACQUISITION SECURITY COUNCIL

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 activities.

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

Authority: 41 U.S.C. 1321–1328, 4713.

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

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

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

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

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

(4) Processes and procedures describing how the ISA facilitates the sharing of

information to support supply chain risk analyses under 41 U.S.C. 1326, recommendations issued by the FASC, and covered procurement actions under 41 U.S.C. 4713;

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

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

§ 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

(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 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:

(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.

Subtitle E [Removed and reserved]

3. Remove and reserve subtitle E.

[FR Doc. 2021-17532 Filed: 8/25/2021 8:45 am; Publication Date: 8/26/2021]