November 2, 2020

Via OFCIO@omb.eop.gov

Russell Vought
Director
The Office of Management and Budget
725 17th Street NW
Washington, DC 20503

Subject: Federal Acquisition Supply Chain Security Act Interim Final Rule

The U.S. Chamber of Commerce welcomes the opportunity to provide the Office of Management and Budget (OMB) and the Federal Acquisition Security Council (the FASC or the Council) feedback on the interim final rule (the IFR or the rule)[1] to implement the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) (P.L. 115-390).[2]

FASCSA is one of several federal policies, pieces of legislation, and regulations that pertains to policymakers' interests in cyber supply chain security. The law calls for creating a whole-of-government approach to supply chain risk management (SCRM) by establishing the FASC and providing agencies with new authorities to share information and mitigate supply chain risks in the context of procuring information and communications technology (ICT). The FASC is an interagency body headed by OMB and is tasked with several functions related to SCRM, including the development of protocols for assessing risk, a governmentwide strategy, and the authority to recommend orders to (1) remove covered articles from agency information systems and (2) exclude sources or covered articles from future procurements (collectively, removal/exclusion orders).

Further, FASCSA grants the Department of Homeland Security (DHS), the Department of Defense (DoD), and the Director of National Intelligence (ODNI) sweeping authority to issue removal/exclusion orders based on the Council's recommendations. The law also details a limited judicial review process available to an impacted business that wants to challenge the removal/exclusion order made by DHS, DoD, and/or ODNI.

The Chamber offers input on key themes and specific issues that tend to be emphasized by several business groups and welcomes follow-on discussions. Worth stressing, the FASC should coordinate with Congress, agencies, and industry to drive increased coherence to the proliferation of federal SCRM initiatives that are underway.[3]

Key Points

- FASCSA is one of many federal policies, pieces of legislation, and regulations that seeks to address policymakers' interests in cyber supply chain security. The FASC should coordinate with Congress, agencies, and the business community to drive increased coherence to this growing array of federal initiatives.

- Agency officials will need to balance examining the information it receives from third parties for correctness with protecting businesses that voluntarily share risk data.

- The FASC should clarify which agency (or agencies) will maintain the list of private entities and their products/services that are subject to Council recommendations and removal/exclusion orders, including whether the list will be shared with public and private entities.

- Removal/exclusion orders and related mitigation proposals should be narrowly tailored to address discernable supply risks and threats. A source should be given all critical, unclassified information so that it can respond meaningfully to a recommended removal/exclusion order by the FASC.

- A source should be allotted no fewer than 60 days after a removal/exclusion order goes into effect, and not simply noticed, to respond to the FASC. The rule should also feature a reasonable timeline regarding when a removal/exclusion order or a covered procurement action is declared, how long it must be maintained in confidence by a source, and when it will go into effect.

- The FASC has considerable flexibility on agency waiver requests. The waiver process should be swift and efficient for both applicants and the FASC.

SUBPART A—GENERAL

Subpart A describes the scope of the IFR, establishes the membership of the FASC, and provides definitions for relevant terms. Of significance, the definition of "supply chain risk information" includes information that describes or identifies "[f]oreign control of, or influence over, the source (e.g., foreign ownership, personal and professional ties between the source and any foreign entity, legal regime of any foreign country in which the source is headquartered or conducts operations)."[4]

Given today's challenging geopolitical environment and the global reach of U.S. supply chains, American companies are concerned that sources and covered articles connected with certain countries will suffer an almost de facto disadvantage under FASCSA and the IFR. The Chamber anticipates that this foreign country issue will be a recurring point of discussion and possible friction as the FASC and the business community implement the rule.

SUBPART B—SUPPLY CHAIN RISK INFORMATION SHARING

Subpart B of the IFR establishes the FASC Information Sharing Agency (ISA). DHS, acting through the Cybersecurity and Infrastructure Security Agency (CISA), will essentially operate as the ISA. Accordingly, CISA is charged with standardizing the "processes and procedures for submission and dissemination of supply chain information" and facilitating the operations of a SCRM Task Force under the FASC (the FASC Task Force). The FASC Task Force will be composed of technical experts who will assist the Council in implementing its information sharing and risk assessment mandates. In addition, Subpart B prescribes "mandatory and voluntary information sharing criteria" and related information protection requirements.

Selecting an existing group to engage the private sector. Under FASCSA, the FASC is required to engage the private sector to fulfill two principal functions—

> (1) Identifying and recommending that the National Institute of Standards and Technology develop SCRM standards, guidelines, and practices for agencies to use when assessing and establishing mitigation strategies regarding supply chain risks, particularly in the acquisition and use of covered articles.
>
> (2) Identifying or developing criteria for sharing information with agencies, other federal entities, and nonfederal entities with respect to supply chain risks.[5]

Notwithstanding the establishment of the FASC Task Force, whose purpose is to interact with the business community, the IFR does not explain how the Council will engage the private sector. It should be noted that several public-private cybersecurity information sharing efforts already in existence. The FASC Task Force should leverage an available group, particularly the DHS-led ICT SCRM Task Force (the ICT Task Force), rather than stand up a new body. What's more, ICT Task Force participants include approximately 20 federal agencies and 40 of the leading private entities representing the ICT community, and it is well-suited to interact professionally with the FASC.[6] The Chamber assumes that the FASC has the ICT Task Force already in mind and is relying, in part, on public input before finalizing its decision making.

Vetting supply chain risk information. Supply chain risk information that is submitted to the FASC by the private sector about potential sources or covered articles should to be subject to quality control. Submitters may need to be required to certify that the information being provided to the government is truthful and not being shared for an improper purpose (e.g., to disadvantage or harm a competitor). The Chamber thinks that the FASC should develop a means of addressing potentially inaccurate or improper allegations against a contractor made by a business competitor(s). The FASC should consider using a panel of private sector experts to jointly vet information and provide feedback on supply chain risk information that originates from industry.

Protecting information sharing. The FASC will have to balance examining the information it receives from third parties for correctness with protecting businesses that share risk and threat data. Some organizations may want to report potentially risky suppliers but are concerned about litigation and confidentiality protections for the information they provide. The

Chamber urges the FASC to provide industry with details on legal liability and confidentiality protections that are afforded to private parties that voluntarily share supply chain risk data with the FASC. As the FASC likely anticipates, many businesses will seek guidance on how they can confidentially report supply chain risks posed by suppliers, articles, and services to the FASC Task Force without exposing themselves to lawsuits. The ICT Task Force has reportedly created a framework that companies can follow to safely share warnings, as well as an analysis of ways for policymakers to reduce legal uncertainty. In sum, the Chamber requests that the FASC clarify what safeguards private entities have when voluntarily sharing information with the SCRM Task Force.

Addressing additional process and organizational issues. The FASC should address a number of key procedural and organizational issues that affect the private sector and are linked to supply chain risk information sharing.

- The FASC has been granted considerable discretion to collect and disseminate supply chain risk information. However, aside from the contours of the removal/exclusion order processes, it's not clear whether and when such information will be shared across the government and with the private sector. Under what circumstances and how will the FASC share supply chain risk information with industry? What specific data will be shared?

- What protections will be in place for businesses that have been identified to the FASC as a potential risk but have not been subjected to a recommendation or a removal/exclusion order? What protections will be in place for companies that have been informally blacklisted? If a business source or a covered article is banned by the FASC from contracting with an agency, will other agencies be alerted and required to follow suit?

- The IFR does not specify whether the FASC or another federal body will maintain a list of the sources or covered articles that have been subject to a recommendation or a removal/exclusion order. Does the FASC or another federal body plan to develop and maintain such a list? Will nonfederal entities have access to it?

- How will the FASC influence intelligence community (IC) priorities and taskings? What are the IC's responsibilities under § 201.202(b), which involve mandatory information submission requirements vis-à-vis the FASC? Further, will the FBI be expected to notify the FASC each time it opens a counterintelligence investigation that implicates a company or product/service that could end up in the federal government's supply chain? If so, what protections will be put in place to ensure that the FASC is conducting its work consistent with the limitations of U.S. intelligence law?

- How will the data submitted to the FASC Task Force be maintained within CISA? Will the data be part of the National Cybersecurity and Communications Integration Center, including being comingled with cyber threat indicators in the Automated Indicator Sharing program? Or will the data be separated into a different repository or system?

- Contractors welcome consistent, flexible guidance regarding information sharing scenarios. If businesses, for example, share cyber threat data with the government, will the protections authorized under the Cybersecurity Information Sharing Act of 2015 apply?[7]

- Companies want insights on certain scenarios, such as the FASC alerting Company A that it is banned because Company Z brought supply chain risk information forward to the government. How will Company Z be shielded from possible litigation if Company A sues the government?

SUBPART C—REMOVAL/EXCLUSION ORDERS

Subpart C of the IFR provides the criteria and procedures by which the FASC will evaluate supply chain risk from sources and covered articles and recommend issuance of removal/exclusion orders. Subpart C also provides the process for issuance of removal/exclusion orders and, to a lesser extent, agency requests for waivers from these orders.

Recommending removal/exclusion orders (41 CFR § 201.301). According to the IFR, the FASC will evaluate sources and covered articles in line with a common set of (nonexclusive) "factors" that are listed in the rule. The IFR also says that the government is allowed to evaluate "additional information" (not defined) that is provided to the FASC, which gives the Council the needed flexibility to evaluate sources on a case-by-case basis.[8] But the factors listed in § 201.301(b) do not seem to match the "criteria" that are required by § 1323(c) of FASCSA. By using the term criteria, Congress called on the FASC to specify commonly accepted benchmarks through which the risk profiles of covered articles and sources will be evaluated. The Chamber believes that the factors listed in the IFR seem to lack sufficient detail to inform contractors' understanding of the FASC's decision making and expectations.[9]

The Chamber believes that both the criteria and the factors should be disclosed to a source named in a recommended removal/exclusion order. If only the factors are provided, as suggested in the IFR, the source will have minimal awareness regarding what regulators determine to be the key risk(s). Similarly, § 201.301(e) of the rule calls for the FASC to include a summary of the supply chain risk assessment in its recommendation to DHS, DoD, and/or ODNI. The data underpinning the summary, including the severity of a risk(s) and the likelihood of it being realized, should be articulated to the source so that a risk mitigation plan can be developed.

The rule should ensure that materials important to a source (e.g., the criteria, the factors, and/or the supply chain risk assessment that could lead to a rescinded order), which is called for in § 201.301(e), are included in the administrative record for judicial review of a removal/exclusion order. The IFR is not clear on this point, which seems to proscribe a limited collection of information in the administrative record, which could disadvantage a contractor's case.[10]

Noticing a source and an opportunity to respond (41 CFR § 201.302). It is constructive that FASCSA and the IFR give sources time to respond to a FASC

removal/exclusion order. However, the 30-day response window that both measures authorize is very short. Add this to FASCSA's requirement (§ 1327) that parties requesting a judicial review of an order file a petition within 60 days of being notified, and the opportunity for sources to respond to the government is increasingly truncated. A source should be allotted no fewer than 60 days after a removal/exclusion order *goes into effect*, and not simply noticed, to respond to the FASC. Both FASCSA and the IFR are silent on the effective date of such orders.

The rule should feature a reasonable timeline regarding when a removal/exclusion order or a covered procurement action is declared, how long it must be maintained in confidence by a source, and when it will go into effect. It would be useful for the FASC to make a preliminary recommendation, which is simultaneously shared with the source so that it is given an opportunity to respond. Following the source's reply, the FASC could make a final recommendation to DHS, DOD, and/or ODNI with a copy provided to the affected party. Only severe risks should have an immediate effect; confidentiality should be maintained only as long as an affected party needs to petition for a judicial review of a removal/exclusion order or a covered procurement action.

Also, the Chamber contends that a source should be given all pertinent, unclassified information under § 201.302 so that it can respond meaningfully to a recommended order by the FASC. Businesses should be provided the recommendation, including what it applied to (e.g., a source, a product, and/or a service), which agencies received it, and the specific risks associated with such article or source. Contractors have legitimate concerns that the information that they will receive from the FASC will be too sparse. Businesses want to respond substantively to a removal/exclusion recommendation, but the recommendation's context and risk data need to be shared in a full and clear manner.

Issuing removal/exclusion orders and related activities 41 CFR 201.303. The Chamber believes that removal/exclusion orders and related mitigation proposals should be narrowly tailored to address real risks. The FASC's due diligence process should include contractor safeguards to ensure a fair, transparent, and thorough evaluation process governing the removal/exclusion of a source or a covered article. Any business that is subject to scrutiny should receive notice at the *outset* of a review and be given an opportunity to comment as early as possible in the evaluation process.

The administrative record described in § 201.303(a)(2) is apparently less exhaustive in relation to what the legislation requires at § 1327(b)(4)(B). The record should be substantial enough to justify the decision that has been made by agency officials and consistent with administrative law principles. Put another way, § 201.303(a)(2)(iv) calls for including information on a removal/exclusion order that consists of "information or materials *directly* relied upon" [italics added] by national security officials, which strikes the Chamber as somewhat limiting compared with the underlying law.[11] The IFR should feature more specifics about how and when businesses must comply with the rule and whether they can seek exceptions to a removal/exclusion order. An order can affect any source (e.g., cloud service provider) regardless of whether the party is a prime agency contractor or a subcontractor.

Also, the timing for several critical actions that would affect contractors is unclear. For example, § 201.303(e) notes that contractors may need to act on agencies' removal/exclusion orders. But this provision of the rule does not describe the process they should follow (e.g., to remove covered articles from an agency information system or exclude sources from contracts), including how quickly the relevant parties will be notified of an order and the timeline to take action. This part of the rule, like many others, creates much industry uncertainty. Presumably the FASC will set time frames on a case-by-case basis or empower agencies with discretion on how quickly businesses remove/exclude sources or covered articles from their government contract-related activities. The Chamber believes that these contractor responsibilities should be clarified in close partnership with industry.

The FASC has much flexibility on agency waiver requests. The IFR says, "The regulation provides procedures for agencies to submit requests to the issuing official for an exception to an issued order. An agency may request an exception to an issued order for various reasons, … or for a complete waiver based on issues of national security." The FASC notes that it will establish procedures for requesting waivers and criteria for (dis)approving such requests.[12] Yet the *how* and *under what conditions* an agency may obtain a waiver of a removal/exclusion order is not fleshed out in the IFR. Agency exceptions/waivers are often appreciated by industry, but they can paper over substantial difficulties with the underlying law and the regulation. The Chamber contends that the waiver process should be swift and efficient for both applicants and the FASC.

***

The Chamber appreciates the opportunity to provide OMB and the FASC comments on the IFR. If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

Endnotes

[1] Office of Management and Budget (OMB) interim final rule (IFR), Federal Acquisition Supply Chain Security Act, *Federal Register* (FR), September 1, 2020. https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act

[2] https://www.congress.gov/bill/115th-congress/house-bill/7327

https://www.dni.gov/files/NCSC/documents/supplychain/20190424-UpdatedFASC-Overview.pdf

[3] Cyberspace Solarium Commission, *Building a Trusted ICT Supply Chain*, October 19, 2020, pp. ii, 7. https://www.solarium.gov/public-communications/supply-chain-white-paper

[4] FR 5427.

[5] 41 U.S.C. § 1323.

[6] What is more, the ICT SCRM Task Force (the ICT Task Force) assembled an inventory of existing supply chain risk management efforts across the federal government and industry and launched four main workstreams. The ICT Task Force is expected to issue reports in November 2020.

- Developing a common framework for the bidirectional sharing of supply chain risk information between government and industry.
- Identifying processes and criteria for threat-based evaluation of ICT supplies, products, and services.
- Identifying market segment(s) and evaluation criteria for a qualified bidder and manufacturer list(s).
- Producing policy recommendations to incentivize the purchase of ICT from original manufacturers and/or authorized resellers.

https://www.cisa.gov/ict-scrm-task-force
https://subscriber.politicopro.com/newsletter/2020/10/a-look-at-the-two-parties-cyber-platforms-791179

[7] https://us-cert.cisa.gov/ais

[8] FR 54264.

[9] FR 54269.

[10] FR 54269–54270.

[11] The Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) (P.L. 115-390), 132 STAT. 5186.

[12] FR 54265.