ITI Promoting Innovation Worldwide

Information Technology Industry Council

Comments on U.S. Office of Management and Budget 41 CFR Part 201, Federal Acquisition Supply Chain Security Act

The Information Technology Industry Council (ITI) appreciates the opportunity to provide input into the implementation of the Federal Acquisition Supply Chain Security Act and the establishment of the Federal Acquisition Security Council (FASC). ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader around the globe. ITI's membership comprises top innovation companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment and other internet and technology-enabled companies that rely on ICT to evolve their businesses. Many of ITI's members are longstanding partners with the Federal government, providing innovative products and services intended to help the United States deliver on mission and build up its technological advantage against its adversaries.

ITI's members, who have considerable first-hand knowledge of the challenging and evolving nature of cyber threats, wholeheartedly support efforts to secure the Federal ICT supply chain. However, considering the far-reaching nature of both the Federal Acquisition Supply Chain Security Act and the authorities the law grants agency heads and the FASC, the U.S. Office of Management and Budget (OMB) must provide clear instruction in terms of how the FASC will ensure due process for contractors in conducting its work, how it will safely and appropriately share risk information and how it will fulfill its statutory obligation to confer with industry in setting policy.

Our recommendations for amending the interim final rule are as follows:

1. **Provide Additional Detail on Information Sharing Requirements**

The interim final rule establishes within the FASC a supply chain risk management and information sharing Task Force, with the U.S. Department of Homeland Security serving as the Executive Agency for information sharing. This new Task Force will create procedures that direct, in part, how Federal and non-Federal entities will submit supply chain risk information to the FASC and how to share information to support the required federal supply chain risk analyses, recommendations from the FASC and exclusion and removal orders. However, the nature and scope of the risk information being shared, including which non-Federal entities are encouraged to participate, is unclear. To ensure consistency with other provisions in the Federal Acquisition Supply Chain Security Act, we recommend that that the focus of the new information sharing requirements limit itself to sources within the Federal IT supply chain (*i.e.,* prime contractors and subordinate contractors) and exclude companies that have no formal business relationship with the Federal government. Moreover, the information sharing requirements for contractors should be limited to products sold to the government and should not cover commercial supply chains unrelated to the government contract.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Considering the sensitivity of the information being shared and the adverse consequences for impacted companies if this information were to be leaked or otherwise exfiltrated, OMB should develop supplemental guidance detailing the specific protections it will take to safeguard information submitted to the FASC. OMB should also use stronger language when ensuring it will protect companies that engage in the rule's supply chain risk management procedures. The rule currently states "The FASC does not intend to publicly disclose communications with the source(s) except to the extent required by law"—we recommend replacing "does not intend to" with "shall not."

Additionally, OMB should consider and clarify the specific relationship between this new Task Force's information sharing activities, the existing Vulnerabilities Equities Process, which establishes procedures for communicating vulnerability information to a source with the expectation that it will be patched, and, where applicable, the information sharing requirements stipulated in the Department of Energy's Bulk Power Systems Executive Order. Wherever possible, we encourage coordination between all Federal government entities and the streamlining of procedures to avoid duplicative efforts. Finally, we suggest that this Task Force adopt consensus products released by the ICT Supply Chain Risk Management Task Force's Working Group One, which has a similar focus on sharing supply chain risk information between governmental and non-governmental entities. Having a clear understanding of the law's information sharing requirements will ensure optimal coordination and communication between the government and industry.

2. **Formally Establish a Mechanism for Industry Collaboration with the FASC**

The Federal Acquisition Supply Chain Security Act tasks the FASC with "Engaging with the private sector and other nongovernmental stakeholders in [setting supply chain risk management policy and guidance and developing criteria for sharing information] and on issues relating to the management of supply chain risks posed by the acquisition of covered articles." Despite this explicit directive, the rule does not create procedures or a mechanism for the FASC's coordination with industry.

The final rule should establish a permanent partnership between the FASC and industry representatives focusing on supply chain risk management policy and guidance. Over the last two years, the ICT Supply Chain Risk Management Task Force has filled the role of a collaboration vehicle by bringing together subject matter experts in industry and throughout the government (including many agencies that are represented on the FASC) to develop substantial SCRM-related recommendations and best practices. To best leverage the substantial progress that has been made in this space, we suggest that OMB permanently formalize the current ICT Supply Chain Risk Management Task Force, which was originally chartered on a temporary basis, as this collaborative mechanism. Doing so would enable the FASC to receive continuous feedback from industry that could inform updates to processes and improve the FASC's overall effectiveness.

In February 2020, the National Institute of Standards and Technology (NIST) released a pre-draft call for comments on the first revision of NIST Special Publication 800-161, Supply Chain Risk Management for Federal Information Systems. Given the substantial public and industry contributions that will be imputed into this document, we also urge OMB to direct the FASC to confer closely with NIST when developing supply chain risk management guidance, or contemplating updates to such guidance.

3. **Protect the Integrity of the FASC Process Against Bad Faith Claims**

The process for issuing an exclusion or removal order, as outlined in the interim final rule, begins with the FASC's determination that relevant information received is credible. This information could come from any governmental or non-governmental source. The rule must provide further detail on what constitutes "credible" information to eliminate the potential for abuse of the FASC process by a source's competitors. To address principles of both due process and fairness, the FASC should consider requiring any information submitted to be corroborated by multiple sources prior to initiating an investigation based on that information. To ensure the integrity of Federal supply chain risk management processes, OMB should work closely with the FASC to establish remedies or safeguards in the event of false claims against a company, using the suspension and debarment procedures outlined in the Federal Acquisition Regulation (FAR) Subpart 9.4 as a model.

4. **Provide Further Detail on Risk Criteria Within the FASC Process**

ITI is concerned that the factors listed in 201.301(b) don't qualify as "criteria" as required by Section 1323(c). By using the term "criteria," Congress required the FASC to specify standards by which covered articles and sources would be evaluated. What the FASC specifies instead are "factors" devoid of any standard or meaning. These "criteria" must be disclosed to any source named in a recommended exclusion or removal order. If only the factors are provided, as currently specified in the rule, such a party will have no indication as to what the FASC determined to be the risk. We recommend that future iterations of the rule clearly define the specific risk criteria that will be used in the evaluation of covered articles.

5. **Clarify the Extent to Which Foreign Control or Influence Will Be Considered a Risk Factor in Line with Standards Adopted by Other Agencies**

In its analysis of the risk posed by a source, the FASC must consider, in part, "foreign control of, or influence over, the source (e.g., foreign ownership, personal and professional ties between the source and any foreign entity, legal regime of any foreign country in which the source is headquartered or conducts operations). " Too often, the interim final rule makes no distinction between potential adversaries and allies, such as when it considers as a criteria "(iii) Personal and professional ties between the source—including its officers, directors or similar officials, employees, consultants or contractors—and any foreign government." Subpart C should clearly indicate that not all countries are the same. As it relates to connections with foreign governments, the rule should more clearly indicate that the specific country and its relationship with the United States should be considered, as well as the risk mitigation laws and regulations in place in the foreign country.

In addition, this definition, specifically the inclusion of whether a source merely conducts operations overseas, is extremely broad and could potentially apply to every major U.S. company, regardless of the actual risks present. While certain business relationships may raise valid security concerns, this is not the case across the board. The risks presented by a particular U.S./foreign business relationship must be analyzed based on the specific facts and circumstances, with strong consideration of any risk mitigation options already in place. Finally, the need to address underlying security concerns must not cripple American business' global competitiveness, which often depends upon relationships with foreign entities.

To ensure consistency with other Federal initiatives and processes aimed at reducing economic security risks, we recommend adopting the definition of "control" promulgated by the regulations implementing FIRRMA reforms to the Committee on Foreign Investment in the United States (CFIUS). These regulations precisely define "control," explain how to analyze "control" when multiple owners have interests, identify standard minority rights that do not result in control, and provide detailed examples[1]. We also suggest that the FASC consider in its risk evaluation whether a source has entered into a CFIUS National Security Agreement, can provide documented compliance with the recently-released Cybersecurity Maturity Model Certification (CMMC) interim rule or the NIST SP 800-161 supply chain risk management guidance, or has Department of Homeland Security (DHS) Customs Trade Partnership Against Terrorism (CTPAT) certification. Nevertheless, we suggest that the FASC coordinate closely with CFIUS in conducting risk analyses and submitting an exclusion or removal order after the recommendation has been made. Subject companies should have an opportunity to respond and provide information prior to a recommendation for removal or exclusion being sent to agencies.

6. **Provide Additional Elaboration on the Due Process Options Available to Impacted Companies**

We appreciate that the Federal Acquisition Supply Chain Security Act lays out a process by which an impacted source may appeal an exclusion or removal order. However, the rule could greatly benefit from additional clarification and consideration of how this process will work. For instance, the statute requires the FASC to provide affected companies with 30 days' notice of an exclusion or removal recommendation and to give companies a chance to respond to the recommendation. OMB should assert that all FASC recommendations are reviewable on appeal and that the FASC must consider factual corrections it receives from a source during this process. Upon receiving a notice of an exclusion or removal recommendation from the FASC, the impacted source has 30 days to present a mitigation plan. We recommend that OMB provide additional guidance as to what should be included in such a mitigation plan to help sources overcome an exclusion or removal recommendation.

Moreover, an affected source should be provided all pertinent, unclassified information under 201.302(b) for providing a meaningful response, including what the recommendation was, to what it applied (one specific article or the whole company), to whom it was made, and the

[1] *For more information, see https://www.govinfo.gov/content/pkg/FR-2019-09-24/pdf/2019-20099.pdf*

specific risks associated with said article or source. What's provided for in the rule is too vague, and on receiving such a vague notice, no company could provide a meaningful response.

Additionally, the timing of the exclusion or removal order decision and the opportunity for a source to respond could benefit from further consideration. We suggest that OMB require the FASC to make an initial recommendation, which is shared with the affected party, and provide an opportunity to respond. Following that response, the FASC could make a final recommendation to the Secretary of Homeland Security, the Secretary of Defense, or the Director of National Intelligence with a copy provided to the affected party. The administrative record of 201.303(a)(2) is inadequate in its view of what the legislation requires at Section 1327(b)(4)(B). The record should be substantial enough to justify the decision that has been made consistent with administrative law principles. As currently written, the interim rule makes providing information supporting an exclusion or removal order only if it was "directly relied," which we believe is too narrow.

7. **Clarify the Nature and Extent of Exclusion and Removal Orders**

More consideration is needed on both the timeline for and the implications of an exclusion or removal order issued by either the Secretary of Homeland Security, the Secretary of Defense or the Director of National Intelligence. In order to efficiently remove problematic equipment while minimizing negative commercial impacts, all exclusion and removal orders resulting from the process laid out in the interim final rule should be narrowly tailored to address an articulable security risk. To achieve this goal, all exclusion and removal orders should be tied to particular products that present the highest levels of risk and should be time-limited and subject to a periodic reassessment in order to maintain the exclusion. Only severe risks should have an immediate effect, and confidentiality should be maintained for at least long enough for an affected party to file for judicial review and obtain a protective order. The limited timeline at 201.302(c)(1) is not long enough. We recommend that the timeline should be at least 60 days after the order goes into effect given the 60-day time period for judicial review. The rule is silent on effective dates, but some criteria should be specified as part of 201.301(e) of when an order should go into effect in view of the specific risk identified by the FASC.

OMB must also clarify how the exclusion and removal recommendation and order process will interact with other elements of the Federal acquisition process. For instance, it is unclear whether an exclusion or removal order will place an impacted source on the Excluded Parties List, and whether such an order will trigger the suspension and debarment process. The final rule must also clarify whether an exclusion or removal order will have any bearing on responsibility determinations for a future procurement.

8. **Offer Contractors Using an Impacted Source Fair Mitigation Options**

In the event that either the Secretary of Homeland Security, the Secretary of Defense or the Director of National Intelligence issues an exclusion or removal order, the interim final rule stipulates the removal of the covered source in all affected mission areas. Additionally, a determination from all three officials that a source presents a national security risk will trigger a government-wide exclusion or removal order; in such cases, the U.S. General Services Administration and other agency officials responsible for managing the Federal Supply

Schedule, government-wide acquisition contracts, and multi-agency contracts would remove the impacted articles or sources from such contracts. The rule states that non-Federal entities would be impacted "to the extent that an exclusion order or a removal order applies to a prime contractor or subcontractor of a Federal agency."

The rule should clarify the extent to which contractors must make efforts to determine if such ordered items are found within their existing systems and whether they will have to provide a formal representation of compliance with an exclusion or removal order in the System for Award Management (SAM). We recommend that OMB consider using the same standard employed in FAR Case 2019-009, *Prohibition on Contracting with Entities Using Certain Telecommunications or Video Surveillance Equipment or Services*, which requires contractors to conduct a "reasonable inquiry" of information in the entity's possession as to whether they use the impacted equipment. We also urge OMB to articulate what specifically is required of contractors who are themselves operating Federal networks in the event of an exclusion or removal order. This concern applies not just to prime contractors, since an order could affect any source regardless of whether that party has a prime contract (*e.g.,* a cloud service provider to a prime contractor). Relatedly, exclusion and removal orders cannot be shared with only the agencies given their impact on non-federal entities. The rule does not describe how non-federal entities will be informed or may learn of these orders.

The interim final rule allows government agencies to seek either delayed implementation of an exclusion or removal order or a complete waiver based on issues of national security. We recommend that the FASC allow prime contractors using a source impacted by such an order to apply for delayed implementation or a waiver if they are unable to immediately remove the covered equipment for any reason (for instance, if breaking a contract with the impacted source will result in substantial financial damages). Alternatively, any implementation costs should be considered "allowable" for the purposes of an impacted prime's government contracts, or as a "change" subject to an equitable adjustment under a Firm Fixed-Price (FFP) contract.

9. **Provide Centralized Guidance for the Agency Exclusion and Removal Recommendations and Orders Process**

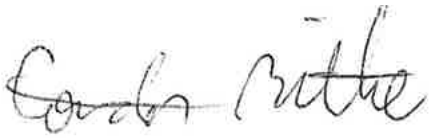
The Federal Acquisition Supply Chain Security Act provides individual agency heads similar authority to exclude and remove problematic IT equipment within their own mission areas. While we understand that OMB likely wishes to provide maximum flexibility to government agencies in addressing supply chain risks, we recommend that the FASC create centralized guidance intended to assist agencies in making risk determinations, ensuring due process to impacted sources, and carrying out exclusion and removal recommendations and orders. We also recommend that OMB establish a process by which an impacted source that disagrees with an agency head's risk determination can appeal to the FASC for additional adjudication options.

--

In closing, we appreciate your attention to these comments and hope they prove useful. We urge OMB to work with industry to create a centralized process for Federal supply chain risk management in a manner that prioritizes IT procurements that create the most risk, offers

appropriate mitigation options for contractors, and allows innovative companies to continue to serve government customers while remaining competitive in the global market. A recently-released white paper authored by the Cyberspace Solarium Commission*, Building a Trusted ICT Supply Chain*[2]*,* recommends consolidating the myriad of government supply chain risk management-focused efforts into one single vision, and ITI's members stand ready to assist OMB and other stakeholders in this work.

Sincerely,



Gordon Bitko

Senior Vice President of Policy, Public Sector

Information Technology Industry Council (ITI)

[2] *For more information, see* https://www.solarium.gov/public-communications/supply-chain-white-paper