wiley

ALERT

# FASC Issues Final Rule on Securing Information and Communications Technology Supply Chains in Federal Systems

August 31, 2021

**WHAT**: On August 26, 2021, the Federal Acquisition Security Council (FASC) issued its final rule to implement the 2018 Federal Acquisition Supply Chain Security Act. *See* 86 Fed. Reg. 47582 (Aug. 26, 2021). The FASC made minor modifications and clarifications to its interim rule, published at 85 Fed. Reg. 54263 (Sept. 1, 2020), but declined to address many of the recommendations of commenting parties, either rejecting them or asserting that the interim rule or existing laws already provide adequate processes.

**WHEN**: The final rule takes effect 30 days after its August 26, 2021 publication in the Federal Register.

**WHAT DOES IT MEAN FOR INDUSTRY**: As cybersecurity and surveillance threats become more prevalent, the U.S. government will continue to ramp up efforts to address the threats through a range of legal authorities. As a result, federal contractors should expect to see increased action by government agencies to address supply chain security risks, including the issuance of removal and exclusion orders pursuant to this final rule. The final rule makes modest revisions to the FASC's interim rule. It reorganizes the rule to conform to the structure and numbering of 41 C.F.R., clarifies a handful of terms, and adds general protections for the submission of information by non-federal entities (NFEs).

**BACKGROUND**

## Authors


Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law


## Practice Areas

Cybersecurity
Government Contracts
International Trade
National Security
Strategic Competition & Supply Chain
Telecom, Media & Technology

The Federal Acquisition Supply Chain Security Act of 2018 (FASCSA or Act), Title II of Pub. L. No. 115-390, is designed to coordinate government efforts to protect the information and communications technology (ICT) supply chain, including by improving information sharing and coordinating actions to protect the supply chain. FASCSA created the FASC, an executive branch interagency council, chaired by a senior-level official from the Office of Management and Budget and including representatives from the General Services Administration, U.S. Department of Homeland Security (DHS), Office of the Director of National Intelligence, and the U.S. Departments of Justice, Defense, and Commerce. The FASC is authorized to perform a variety of functions, including making recommendations for orders that would require the removal of covered ICT articles from executive agency information systems or the exclusion of sources or covered articles from executive agency procurement actions. The FASC's recommendations for exclusion and removal are sent to the Secretaries of Homeland Security and Defense and the Director of National Intelligence, who may then issue an order for removal or exclusion for the information systems under their authority.

The interim rule contained three core parts. Subpart A discussed the administration of the FASC and its membership. Subpart B established DHS, acting through the Cybersecurity and Infrastructure Security Agency (CISA), as the information sharing agency (ISA) or the agency that will conduct day-to-day activities of the FASC. Finally, Subpart C discussed the procedures the FASC will follow when issuing removal or exclusion recommendations and described the process for agency requests for waivers from removal or exclusion orders.

**SUMMARY**

**Confidentiality of Information Provided to the FASC**

The FASC made modest revisions to the interim rule to address concerns with the treatment of information submitted to the FASC. Specifically, the final rule added § 201-1.201(e) to describe the protection that will be afforded to information submitted by NFEs that is not otherwise publicly or commercially available. According to the FASC, 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. Nonetheless, § 201-1.201(e)(2) also makes clear that the FASC retains broad discretion to disclose information submitted by NFEs "to appropriate recipients in a range of circumstances." Although the FASC recognized that this reservation "may dissuade some NFEs from submitting sensitive information," the FASC chose at this time "to prioritize greater sharing of information in appropriate circumstances over the possibility of receiving more supply chain risk information from NFEs." The FASC also stated that it modified the interim rule to clarify that confidential information that an ICT source submits is subject to the same degree of protection provided pursuant to new § 201-1.201(d) for confidential information NFEs submit voluntarily.

The FASC also declined to provide NFEs the same protections as available under the Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, Div. N (CISA 2015) because the FASC is coordinating with FASC member agencies to consider any intersections between CISA 2015 and the FASC's authorities and thus reserved providing any additional guidance until a later date. In addition, the FASC declined to add protections for NFEs that submit information that is used to support a removal or exclusion order. The FASC

reasoned that it "lacks authority to obviate, restrict, or otherwise alter the potential legal liability of one private party to another" and expressed concerns that forms of protection, such as guarantees of confidentiality, could "decrease the quality of information received" by "removing disincentives that would otherwise deter the submission of inaccurate or misleading information."

**Storage and Public Release of Information Held by the FASC**

The final rule declined to address how data submitted to the FASC will be maintained and the system to be used to store such data, stating that the FASC does not want to "unduly restrict" the ISA. The FASC also did not revise the interim rule to address more specifically the release of information to the public. For example, the FASC declined to specify circumstances for sharing supply chain risk information with the private sector or to establish a list of sources and covered articles subject to a removal or exclusion order. According to the FASC, the determination 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." The FASC further explained that other laws and policies, such as national security concerns, also could restrict disclosure of information.

**Accuracy of Information Submitted to the FASC**

The FASC declined to adopt measures to ensure that information submitted to the FASC is accurate and truthful so as to disincentivize companies from submitting information to "sabotage" their competitors. The FASC pointed to § 201-1.300(d), which requires the FASC to perform "appropriate due diligence" in evaluating supply chain risk. The FASC is also authorized to receive information from other government sources, including investigative and intelligence-gathering agencies. Thus, the FASC concluded that it already has "ample means to assess the reliability of information received from the private sector or elsewhere."

**Limitations on Trade and Transactions with Foreign Suppliers**

Section 201-1.300(b) provides that the ties of a source or covered article to foreign countries are a factor to be considered as part of a supply chain risk analysis. As commenters pointed out, many companies have connections to ICT sources around the world, and companies could be chilled in dealing with certain suppliers if their association with a certain country will place them automatically under suspicion by the FASC. To address such concerns, the FASC modified the interim rule to include § 201-1.300(c), which consistent with 41 U.S.C. § 1323(f)(2), emphasizes 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. The FASC declined to go any further, however, to address relationships with global ICT sources, including those in countries that are allies of the United States. The FASC reasoned that these additional protections are not required because, in evaluating the risk of a covered article or 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."

**Process For Issuance of Removal or Exclusion Recommendations and Judicial Review of Removal or Exclusion Orders**

The FASC made minor clarifications in response to recommendations regarding the process for removal or exclusion recommendations and orders but rejected broader recommendations for revision. For example, the FASC declined additional provisions directed at ensuring an ICT source has sufficient information to respond to a removal or exclusion recommendation on grounds that existing provisions of the interim rule provide adequate assurances. The FASC pointed to § 201-1.302(b)(2), which provides that the source named in a recommendation must be notified of the criteria the FASC relied upon for its recommendation. In addition, the source is entitled to know 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." The FASC also declined to require early notifications and early opportunities to respond to FASC recommendations, reasoning that national security concerns could weigh against informing a source that it is under review before a recommendation is made. Further, the FASC declined to augment the due process elements of the rule, including to allow for discovery. According to the FASC, the rule and statute already provide for judicial review by a federal appellate court of any exclusion or removal order resulting from a FASC recommendation. The FASC also reasoned that the FASCSA did not provide for discovery; discovery is not a standard practice in judicial review based on an administrative record; and additional procedures such as discovery would slow FASC proceedings, make them more expensive, and impede the government's ability to protect against cyber threats to its systems. And, the FASC declined to revise the interim rule to provide (i) additional measures for parties to comment on future proposed rules or (ii) additional appeal opportunities for companies that may be specifically targeted, concluding that the Administrative Procedure Act provides adequate opportunities for public participation, and the FASCSA already provides for judicial review of a removal or exclusion order.

The FASC made a small number of clarifications. First, the FASC modified § 201-1.300(b) of the final rule to change the label for the list of factors in the final rule from "Criteria" to "Relevant Factors," modified § 201-1.303(b)(4) and (c) to remove the word "directly" so that the provisions mirror the language of FASCSA, and included a new provision at paragraph (c) of § 201-1.302 to clarify that once the FASC issues a recommendation and the source submits a response, the FASC has the discretion to withdraw the recommendation if a source demonstrates that a removal or exclusion order is unwarranted.

**Practical and Legal Impacts From Exclusion Orders Affecting Contractors' Supply Chains**

Commenting parties raised a variety of concerns regarding the impact of removal or exclusion orders. In general, the FASC made no revisions in response. For example, the FASC declined to identify "a reasonable timeline" for when a covered procurement action is announced and when it may go into effect, explaining that such a determination would be fact-specific and risk-based. The FASC also declined to define the nature and extent of contractors' and subcontractors' obligations under exclusion or removal orders because the FASC posited that contractors' obligations will vary based on specific circumstances. Thus, the FASC deferred to "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."

Regarding the impact of removal or exclusion orders on small businesses or U.S. industry generally, the FASC noted that the final rule requires FASC to include in its recommendations "a discussion of less intrusive measures that were considered and why such measures were not reasonably available to reduce supply chain risk." The FASC also stated that it expects to weigh the burden of compliance against the anticipated benefit of a removal or exclusion order.

The FASC also rejected a request to exempt commercial-off-the-shelf (COTS) items from its rules, a request made on grounds that making such sources subject to the rules could deprive the government of innovation and new technology. The FASC stated that the ubiquity of COTS across the government and private sector make COTS a target of malicious actors, and exclusion of COTS would undermine the ability of the FASC to successfully carry out its mission of reducing the government's exposure to supply chain risk.

**Agency Waivers**

The FASC identified a new paragraph in the final rule, § 201-1.304, that provides clarification on the waiver process for government agencies. Specifically, the agency must request a waiver from the ordering official that (i) identifies the relevant order; (ii) describes the exception sought by the agency; (iii) provides compelling justifications for the grant of the exception; and (iv) provides any alternative risk reduction methods the agency will employ in lieu of complying with the order. The ordering official has the authority to decide whether to grant the exception.

**Harmonization of Various Government and Private Sector Supply Chain Efforts**

The final rule does not provide for a particular type of formal relationship or engagement between the FASC and industry. The FASC explained that, although the private sector has a strong base of experience with supply chain risk and mitigation, it was premature to formalize any relationship with the private sector. The FASC also declined to specify reliance on the ICT Supply Chain Risk Management (SCRM) Task Force within DHS for knowledge and experience in supply chain risk management because the task force is not permanent. In general, the FASC declined to revise the interim rule to augment interagency coordination, reasoning that the FASC itself is an interagency body.

***

Now that the FASC has issued its final rule, companies should prepare for the potential that certain ICT sources may be removed or excluded from federal systems and the supply chain for such systems. Wiley's Supply Chain and Transactional Support; Telecom, Media & Technology; and Government Contracts professionals are closely tracking implementation of the FASCSA by the FASC and stand ready to advise affected contractors and non-contractors of their obligations under FASC rules.