Government Contracts

# OMB Seeks Comments on How Future National Security Risks Will Be Removed from the Government Contracts Marketplace

By: Matthew L. Haws, David B. Robbins, and Cynthia J. Robertson

On September 1, 2020, the Office of Management and Budget (OMB) released an immediately effective interim rule outlining the creation of an interagency council to determine whether new bans of technology are needed to protect federal acquisition from national security risks. 85 Fed. Reg. 54263. The rule invites public comments through October 31, 2020. Given the sweeping impacts of bans on products from, among other companies, Kaspersky Labs and certain providers of telecommunications and video surveillance equipment from China, government contractors should take note.

As authorized by the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA), OMB's rule outlines the framework for the Federal Acquisition Security Council (Council or the FASC). The purpose of the FASC is to evaluate threats and vulnerabilities in federal information, and communications technology and services. The FASC is intended to provide structure and a standardized process to decisions like those that led to the ban of Kaspersky in December 2017, followed in 2019 by a ban of Chinese telecommunications companies, Huawei and ZTE, among others. Historically, individual or small groups of agencies addressed specific supply chain security risks. Awareness of the need for better coordination among a broader group of agencies led Congress to pass legislation to create the FASC in 2018, in an effort to improve executive branch coordination, enhance supply chain information sharing, and authorize exclusion orders/bans.

OMB's rule is divided into three Subparts (A, B, and C), which together comprise a newly codified regulation at 41 CFR part 201, entitled "Federal Acquisition Supply Chain Security." Subpart A sets out the scope of the new rules, definitions, and the framework for the FASC membership. Subpart B describes the role of the FASC's Information Sharing Agency (ISA). Subpart C provides the criteria and procedures by which the FASC will evaluate supply chain risk and recommend future bans.

**Subpart A: Scope/Definitions/FASC Membership:**

Scope: From the lens of a government contractor, only the need to remove or exclude a technology is mandatory – the new rule makes clear it does not require "mandatory submission of supply chain risk information by non-federal entities." § 201.101(b)(1).

Definitions: The rule includes a substantial number of definitions that outline relevant agency and congressional committees as well as key terms for evaluating national security risks over the covered technology. "Covered article" includes information technology, including cloud computing services of all types, as well as telecommunications equipment or telecommunications service. A key term, "supply chain risk" is defined to mean "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." § 201.102(q). "Supply chain risk information" includes a non-exclusive, detailed list of over 14 factors, regarding both foreign ownership or influence, and functionality that assess threat and vulnerability from a level 1 (low) to 5 (high).

FASC Membership: A senior level OMB official will chair the FASC, with representatives from an extensive array of agencies, including the: (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. OMB's Office of the Federal Chief Information Officer will provide day-to-day leadership. § 201.103(a). The FASC is also authorized to consult with other councils, including the FAR Council and the Committee of Foreign Investment in the United States (CFIUS) with respect to supply chain risks posed by the acquisition and use of covered articles.

The rule authorizes FASC to create "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 work. § 201.103(d).

**Subpart B: Information Sharing Agency (ISA):** The rule designates the Cybersecurity and Infrastructure Security Agency (CISA) as the appropriate executive agency to serve as the FASC's Information Sharing Agency (ISA). The ISA will facilitate and provide the administrative support to a FASC supply chain and risk management Task Force; and serve as the liaison to the FASC to communicate the Task Force efforts, as the Task Force develops the required FASC processes.

The Task Force is central to the FASC and will include technical experts in supply chain risk management and related interdisciplinary experts. As the rule makes clear, "all references . . . 'to the submission of information to the FASC' mean the submission of information to the ISA and the Task Force, on behalf of the FASC, pursuant to the FASC-approved processes and procedures described." § 201.201 (a). The Task Force will assist the FASC with implementing its information sharing, risk analysis, and risk assessment functions. 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.

**Subpart C: Removal Orders and Exclusion Orders (Product Bans):** This Subpart sets out the criteria and procedures by which the FASC will evaluate supply chain risk that may lead to a ban from federal systems. The FASC is authorized to issue 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). Agencies may request waivers from such orders.

Referral Process: The FASC may commence an evaluation: (1) upon the referral of the FASC or any member of the FASC; (2) upon written request by the head of an executive agency or designee; or (3) based on "credible" information submitted to the FASC by essentially anyone ("any federal or non-federal entity").

Decision Process: Decisions to exclude are governed by nine specific, non-exclusive evaluation criteria and an additional "catch all" that allows consideration of "any other information that would factor into an assessment of supply chain risk, including any impact to agency mission critical functions, and other information as the FASC deems appropriate." § 201.301(b)(10). Legitimate reasons for exclusion may include ownership or control or influence over the manufacturer or covered item by a foreign government; the functionality of the covered articles; and the security, authenticity, and integrity of covered articles and the supply chain tied to those articles. Vulnerability of federal systems, programs, or facilities are also factors to be considered. The FASC is required to conduct appropriate due diligence, including weighing the level of confidence in the information.

Evaluating Foreign Influence: When considering foreign influence, the FASC has broad powers to consider both official and non-official ties to not only foreign adversaries, but any foreign country. Whether the US government has identified the country as a foreign adversary or country of special

concern is listed as the first factor. § 201.301(b)(4)(i). Yet the FASC may also consider whether the manufacturer or its component suppliers have research, development, manufacturing, test, distribution, or service facilities or other operations in *any* foreign country, not just those identified as being a foreign adversary or "of special concern." § 201.301(b)(ii). Additionally, the FASC may consider "personal and professional ties between the source – including its officers, directors or similar officials, employees, consultants, or contractors – and *any* foreign government."

Notice & Opportunity to Respond: Perhaps in part responding to the (as of yet unsuccessful) legal challenges advanced by both Kaspersky and Huawei as to the constitutionality of prior bans, the new rule sets out a process by which the manufacturer of a potential banned product is notified of the FASC recommendation for exclusion. Within 30 days after receipt of the notice, the source may submit information in response to the recommendation. Where practicable, and "in the FASC's sole and unreviewable discretion," the FASC can provide mitigation steps to be taken by the source that may result in the FASC rescinding the recommendation. The rule outlines that this process shall remain confidential unless otherwise required by law, until an exclusion order or removal order is issued and the source has been notified.

The FASC submits recommendations to the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence, who will then determine whether to issue bans covering civilian, defense, and intelligence agencies, respectively.

Applicability of Exclusion Orders to Federal Contractors/Subcontractors: Under the rule, an exclusion order may require the ban 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. § 201.303(e)(1). 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. *Id*. Covered article(s) may then need to be removed from agency information systems, other information systems operated by a contractor on behalf of an agency, and also 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 the rule. § 201.303(e)(2).

Exclusion orders, once final, are sent to the source (along with the basis for the order), and are likewise shared with the Interagency Suspension and Debarment Committee, relevant congressional committees, and the ISA. Additionally, public disclosure is permitted as "appropriate and to the extent consistent with national security and law enforcement interests." § 201.303(f)(1).

Final Thoughts: The breadth of factors that the FASC may legitimately consider in evaluating the national security risk in the federal acquisition supply chain will likely garner a great deal of interest by those doing business with the federal government, especially those with facilities or supply chains overseas. Those in the federal marketplace may be especially concerned about ensuring appropriate safeguards in the initial referral process where a FASC review may be triggered if credible evidence of a national security risk is received from "any federal or non-federal entity" (essentially anyone). Companies seeking to gain a competitive advantage might consider using a referral to FASC as an effective means of tangling their competition in a system that once triggered, provides little opportunity to rebut the charges. Especially because the factors permissibly considered by the FASC sweep broadly, and include seemingly innocuous ties to foreign countries (like distribution or service facilities), companies who have been referred to the FASC may find the scales tipped against them and have little recourse once the threat of national security is raised. One example is FASC's authority to consider, among other factors, "personal and professional ties" of the referred company's employees, consultants, or contractors to any foreign government. This factor may be especially concerning for companies with a number of foreign nationals in their workforce. Notable too, is the fact that while the FASC's operating framework is provided by the rule, the ISA Task Force must still submit for FASC approval procedures to implement this framework, leaving much still unknown about FASC inner workings and the timeline for implementation. Comments on the rule will be accepted through October 31, 2020.

## Contact Us

**Matthew L. Haws**
mhaws@jenner.com | Download V-Card

**David B. Robbins**
drobbins@jenner.com | Download V-Card

**Cynthia J. Robertson**
crobertson@jenner.com | Download V-Card

**Meet Our Team**

## Practice Leaders

**Marc A. Van Allen**
Co-chair
mvanallen@jenner.com
Download V-Card

**David B. Robbins**
Co-chair
drobbins@jenner.com
Download V-Card

**D. Joe Smith**
Co-chair
jsmith@jenner.com
Download V-Card