COVINGTON

# New Interim Rule Permits the Exclusion of Companies and Products that Represent a National Security Risk to the U.S. Government

September 9, 2020

Government Contracts

On September 1, 2020, the Office of Management and Budget issued a highly-anticipated interim final rule ("Rule") implementing the Federal Acquisition Supply Chain Security Act. Consistent with the U.S. Government's increasingly sharp focus on supply chain security, the Rule authorizes the Executive Branch to exclude indefinitely "covered articles" (products and services) and "sources" (contractors and suppliers) from procurements and to require removal of covered articles from federal information systems if the covered articles or sources represent a national security risk. An exclusion order may prohibit sources from participating in a procurement (at any level of the Government supply chain) and a covered article from being supplied by a source at any level. A removal order may require the removal of covered articles from federal information systems, including those operated by contractors on behalf of the Government. And either type of order would result in an automatic referral to the Interagency Suspension & Debarment Committee, raising the specter of further collateral consequences.

The "scale of supply chain risks faced by government agencies, and the need for better coordination among a broader group of agencies," prompted increased efforts by the Executive Branch and Congress to improve supply chain information sharing and to provide tools for addressing supply chain risks. These efforts ultimately led to the enactment of the Act, which was one of a trio of bills signed by President Trump in December 2018 aimed at hardening the Government's supply chain.

The Rule outlines the process that agencies and the new Federal Acquisition Security Council ("FASC") must follow to determine whether a covered article or source should be removed or excluded from U.S. Government procurements or information systems. The Rule also requires agencies to follow any exclusion or removal orders once they have been issued. The statutory authorities that allow for the Rule are currently set to expire within five years.

The Rule is divided into three subparts. Subpart A provides key definitions and addresses the operation of the FASC, which is charged with evaluating supply chain risks and recommending exclusion and removal orders. Subpart B identifies the Department of Homeland Security ("DHS") as the agency charged with information sharing and addresses the creation of a supply chain risk management ("SCRM") and information sharing Task Force under the FASC. Subpart C describes the process that will be used to evaluate and issue exclusion and removal orders.

Below we describe each subpart in greater detail and offer our observations about the implications of the Rule.

**SUBPART A – The FASC and Key Definitions**

Overview of the FASC

The FASC is an interagency body whose members currently include representatives from OMB (which also chairs the FASC), the General Services Administration ("GSA"), DHS, the Cybersecurity and Infrastructure Security Agency, the Office of the Director of National Intelligence ("ODNI"), the National Counterintelligence and Security Center, the Department of Justice, the Federal Bureau of Investigation, the Department of Defense ("DoD"), the National Security Agency, the National Institute of Standards and Technology, and the Department of Commerce.[1]

The FASC has two primary obligations. The first is to develop a Government-wide strategy for addressing supply chain risks from information and communications technology purchases, facilitating information sharing within the Government and with the private sector, and serving as the central, Government-wide authority for supply chain risk mitigation activities.

The FASC's second primary function is to establish procedures for (i) the exclusion of covered articles and/or sources from agency procurements, and (ii) the removal of covered articles from federal information systems when it determines that those sources or products present a supply chain risk. Although the FASC is tasked with recommending exclusion or removal orders, the heads of DHS, DoD, and ODNI (or their delegates) are authorized to ultimately determine whether to issue (or rescind) exclusion or removal orders for the civilian, defense, and intelligence agencies, respectively.

Key Definitions

Part A of the rule sets forth a number of definitions that are important for defining the scope of the new regulations. A brief summary of the key terms and their definitions is below.

- **Covered Article.** Products and services covered by this Rule include information technology (including cloud services); telecommunications equipment and services; the processing of controlled unclassified information ("CUI"); and hardware, systems, services, software, or services that include embedded or incidental information technology. "Incidental information technology" is not further defined in the Rule.
- **Covered Procurement.** In general, the Rule will apply to procurements and orders for a covered article where there is either a performance specification, evaluation factor, and/or contract clause imposing supply chain risk considerations.
- **Exclusion Order.** The Rule uses this term to refer to an order from the Secretary of Homeland Security, the Secretary of Defense, or the Director of National Intelligence ("DNI") requiring the exclusion of sources or covered articles from executive agency procurement actions.

[1] The Chairperson of the FASC is permitted to add any other executive agency or agency component that he or she deems appropriate.

- **Removal Order.** The Rule uses this term to refer to an order from the Secretary of Homeland Security, the Secretary of Defense, or the DNI requiring the removal of covered articles from executive agency information systems (including those being operated by a contractor on behalf of the Government).
- **Source.** A source is defined as a "non-federal supplier, or potential supplier, of products or services, at any tier."
- **Supply Chain Risk.** This is broadly defined as 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.** This term is extraordinarily broad in scope, as it includes almost all information that describes or identifies potential supply chain risks related to covered articles, including the functionality of covered articles; information on the user environment; supply chain assurances; foreign control or influence over the source; impacts on national security, homeland security and/or national critical functions; vulnerabilities of federal systems; market alternatives to the source; impact of loss of source; likelihood of exploitation of a system; security, authenticity, and integrity of covered articles; capacity to mitigate risks; credibility of supply chain risk information; and "any other information that would factor into an analysis of the security, integrity, resilience, quality, trustworthiness, or authenticity of covered articles or sources."

**SUBPART B – Supply Chain Risk Information Sharing**

Subpart B identifies DHS as the information sharing executive agency (the "ISA") and provides for the creation of a SCRM Task Force that operates under the FASC. The Task Force will be charged with developing processes and procedures that address at least the following: (1) how the ISA and the Task Force will operate; (2) how supply chain risk information should be submitted to the FASC; (3) how supply chain risk information should be shared to support risk analyses within the Government; and (4) how information should be submitted to the FASC and to executive agencies with regard to removal orders and covered procurement actions.

The Rule addresses both mandatory and voluntary submissions of information to the FASC. Federal agencies are required to "expeditiously" submit information to the FASC when they determine that "there is a reasonable basis to conclude a substantial supply chain risk associated with a source, covered procurement, or covered article exists." Voluntary submissions can come from either federal agencies or from non-federal entities (including from companies or individuals). It is unclear whether the submissions from private companies can be made anonymously.

The FASC has the "sole discretion" to decide whether to disclose its recommendations and any supply chain risk information relevant to its recommendation within the Government and/or to any private entity. In making this decision, the FASC will consider whether such sharing would facilitate the identification or mitigation of supply chain risk. If the FASC determines that release to non-federal entities is warranted, then that release will not be made until a decision on exclusions or removal has been made by the Secretary of Defense, the Secretary of Homeland Security, and/or the DNI and the affected source has been notified.

**Subpart C – Removal and Exclusion Orders**

Intake and Due Diligence Process

The FASC is charged with evaluating sources and covered articles to determine whether to recommend an exclusion or removal order. As noted above, the evaluation process starts either from a referral of the FASC or any member of the FASC; upon the written request of any U.S. Government body; or based on information submitted to the FASC by any individual or non-federal entity that the FASC determines to be credible. The evaluation process will involve consideration of the full range of supply chain risk information, as defined under Subpart A. This includes, but is not limited to, the functionality of the covered articles; the security, authenticity, and integrity of covered articles; 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; implications to national, homeland security, or critical functions associated with the use of the source(s) or covered article(s); and capacity of the source or the U.S. Government to mitigate risks.

Although the Rule lists a number of factors that the FASC will consider, the Rule expressly states that these factors are "non-exclusive," so as to allow the FASC the flexibility to consider additional information on a case-by-case basis. The Rule does not provide guidance on the types of circumstances that could warrant the consideration of additional information beyond the articulated factors.

In conducting its due diligence, the FASC is required to review the information that was submitted, as well as "relevant publicly available information as necessary and appropriate," though the Rule does not appear to contemplate that the FASC or its members would conduct any independent investigation of non-public information. However, the Rule does provide that the FASC must consult with the National Institute of Standards and Technology before recommending an exclusion or removal order to ensure that the recommended orders do not conflict with existing federal standards and guidelines. Even if the FASC determines that a removal or exclusion order is not warranted, the FASC may share the information it analyzed within the Government.

Issuance of an Order

If the FASC recommends an exclusion or removal order, that recommendation is provided to the Secretary of Homeland Security, the Secretary of Defense, and the DNI. At this time, the FASC or its designee will provide notice of the recommendation to the affected source. The source then has 30 days to provide a "thorough and complete written response." The FASC encourages the source to provide technical information about the covered article(s), details about the relationship between the source(s) and any foreign government, and a detailed mitigation proposal that the source(s) believes would satisfy the concerns identified in the notice. Although much about how these processes will be implemented remains unclear, a mitigation plan, in particular, may help persuade the FASC that a source can address the national security concerns that prompted the inquiry. This information is expected to be submitted before the source requests any meetings with Government decision-makers.

The FASC can choose to rescind its recommendation based on the information from the source or permit the recommendation to stand. After reviewing the information from the FASC and the source's response to the FASC allegations, the relevant Secretary or Director will determine

whether to issue an order.[2] In the event all three agencies issue the same exclusion orders—resulting in a Government-wide exclusion—officials at GSA and other agencies are required to effectuate the order Government-wide by removing any covered articles or sources from the Federal Supply Schedules. Once an order is issued, the official issuing the order must notify the affected source, as well as the Interagency Suspension and Debarment Committee.

Appeal Rights

Under the statute, other than the opportunity to respond to the FASC's recommendation, a source may only challenge an order by seeking relief directly in the U.S. Court of Appeals for the District of Columbia Circuit through what is equivalent to Administrative Procedure Act review. This challenge must be filed within 60 days of being notified of a covered procurement action. Notably, the Rule also allows the Government to limit the information available in the administrative record, providing that "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 that information was "directly relied on" by the official issuing the exclusion or removal order. If a recommendation is not challenged or if a company is unsuccessful in its efforts and if the statutory authority underlying the Rule is made permanent, the exclusion and removal orders could remain in place indefinitely, subject to a review by the FASC at least annually. Procedures for such reviews are to be determined by the FASC.

**Impact on Contractors and Suppliers**

Given the Government's laser-like focus on supply chain security, companies whose ultimate customer is the U.S. Government should familiarize themselves with the Rule and the processes it describes, particularly if they rely on foreign sources or activities with ties to countries such as China or Russia. Among the considerations that contractors and suppliers should be mindful of are the following:

- **Broad discretion of the FASC.** The rule outlines certain factors that the FASC should consider when determining whether to make a recommendation that a covered article or a source should either be excluded from procurements or removed from federal information systems. However, the Rule expressly permits the FASC to make its recommendation based on any other information that it deems appropriate, and the Rule does not describe how any of the considerations that the FASC assesses should be weighed against one another. This flexibility—and potential opacity—highlights the importance of the notice that the FASC must provide to affected sources when it issues a recommendation. But for better or worse, the detail and utility of that notice may vary significantly from case to case. This is because, under the Rule, the notice must identify the information that forms the basis for the FASC's recommendation only "to the extent consistent with national security," and while the notice may also include a "description of

[2] The rule provides that the Secretary of Homeland Security is responsible for determinations relating to civilian agencies, the Secretary of Defense is responsible for determinations relating to Defense agencies, and the DNI is responsible for determinations relating to intelligence agencies. The determinations can be delegated to an official one level below the Deputy Secretary or Principal Deputy Director level, although the Secretary of Defense may delegate authority for removal orders to the Commander of U.S. Cyber Command.

the mitigation steps that could be taken by the source," whether to recommend mitigation measures is left to "the FASC's sole and unreviewable discretion." Thus depending on the discretion of the FASC, the notice provided to a source may provide very useful information about the underlying concern, or almost no information at all.

- **Suspension and debarment considerations.** As noted above, the Rule also provides that once an exclusion or removal order has been issued, the official who made the determination should notify the Interagency Suspension and Debarment Committee ("ISDC"), a cross-agency group composed of officials with suspension and debarment responsibility at each executive agency. Presumably, the rationale for this requirement is for the ISDC to consider whether additional suspension or debarment action may be required under FAR Subpart 9.4. However, the purpose, procedures, and effect of an exclusion order under the Act differ markedly from a debarment under the FAR. To take just one example, an exclusion order under the Act may apply only to a particular article for only a subset of procurements (*e.g.*, Intelligence Community contracts), while a debarment would prevent the entire entity from pursuing new contracts anywhere within the Executive Branch. And while a full exploration of other differences is beyond the scope of this alert, suffice it to say that there are many circumstances in which an exclusion order issued under this authority would *not* warrant or require an additional debarment action under the FAR. Nonetheless, sources who find themselves facing threatened exclusion actions under the Act should be well aware of the debarment risk posed by the Rule's ISDC referral requirement and must take steps to proactively mitigate the risk of a potentially broader FAR debarment.
- **Teaming agreement and contract performance.** The Rule does not provide that a list of exclusion and removal orders will be made publicly available. Further, it is not clear whether procuring agencies will implement any process to ensure that contractors that work together (such as where they partner under a teaming agreement) are notified if an exclusion order has been issued that could affect the relationship or the ability to perform. For this reason, prime contractors should consider including language in their teaming agreements and subcontracts requiring teaming partners and suppliers to promptly notify them and provide information about any existing or threatened exclusion or removal orders that impact the agreement, as well as preserve the right to terminate or modify the agreement if such an order becomes a possibility. As a supplier or subcontractor, companies may want to include language in agreements with prime contractors to address remedies if the prime contractor becomes an excluded source or if one of the subcontractor's suppliers becomes subject to an order.
- **Section 889 certifications.** The definition of a covered article under the Rule includes telecommunications equipment or telecommunications services, which is the focus of recent regulations relating to Section 889 compliance that we have covered in other posts. Although only five Chinese companies are currently listed in Section 889, there is a process for adding more. If the FASC issues exclusion orders that cover additional Chinese telecommunication companies, this could prompt the Government to expand the list of prohibited companies under Section 889.
- **Sourcing and development oversight.** Given the U.S. Government's emphasis on hardening its supply chain and its increasing adversity with China, companies that sell products or services where the U.S. Government is the ultimate customer need to be mindful of where they are sourcing components and developing software. Similarly, contractors are facing increasing pressure to oversee their suppliers and to know where products, components, and services are being sourced, manufactured, and developed.

Indeed, on June 24, 2020, DoD issued a list of twenty companies headquartered in the People's Republic of China that DoD determined are operating directly or indirectly in the United States and are "Communist Chinese military companies." Such a determination may be the type of information that the FASC considers when determining supply chain risk. Among the entities listed are Hangzhou Hikvision Digital Technology Co., and Huawei, which are prohibited sources for telecommunications equipment and services under the current Section 889 regulations. Moreover, even if a product is compliant with sourcing requirements such as the Trade Agreements Act, the FASC could find that sourcing certain components from countries of concern—such as China—represents a national security risk.

- **A new front in corporate warfare?** In recent years, we have seen a rise in the practice of contractors seeking to direct the Government's investigative and enforcement powers against their rivals. From filing *qui tam* suits against a competitor to submitting derogatory information to an Office of Inspector General (often on an anonymous basis), some contractors are willing to use Government channels to prompt scrutiny of their competitors. While these tactics have only varying degrees of success and carry the potential for significant blowback, they nonetheless are now a reality in the highly competitive Government contracting landscape. In the case of the FASC, it remains unclear whether submissions by non-Government entities will remain anonymous—and if not, the potential for litigation in response to such allegations could be a significant risk depending on the facts. (At a minimum, to the extent that the FASC directly relies on such information in issuing an exclusion or removal order, that information may eventually be shared with the excluded source.) The Rule appears to recognize the risk that companies may try to feed information to the FASC in service of their own competitive objectives, and it makes clear that the FASC will carefully consider the credibility of any information submitted by non-federal entities. Still, even an ultimately meritless allegation can prove incredibly disruptive for a company, and it remains to be seen how effective the FASC will be in vetting information from non-federal sources, particularly where those sources may have a vested interest in the FASC taking action.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Government Contracts practice:


| | | |
|---|---|---|
| **Susan Cassidy** | +1 202 662 5348 | scassidy@cov.com |
| **Ashden Fein** | +1 202 662 5116 | afein@cov.com |
| **Michael Wagner** | +1 202 662 5496 | mwagner@cov.com |
| **Samantha Clark** | +1 202 662 5492 | sclark@cov.com |
| **Ryan Burnette** | +1 202 662 5746 | rburnette@cov.com |