FASCSA ORDER PREPARATION FOR THE FCEB

TLP:CLEAR

WHAT (WHO) IS THE FASC?

Established by the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act of 2018, the Federal Acquisition Security Council (FASC) is an interagency council within the executive branch with representation from a dozen departments and agencies.

The FASC is responsible for establishing criteria and procedures for "recommending orders applicable to executive agencies requiring the exclusion of sources or covered articles from executive agency procurement actions" and "recommending orders applicable to executive agencies requiring the removal of covered articles from executive agency information systems[.]" 41 U.S.C. §§ 1323(c)(1)(A)-(B). These orders are termed as Federal Acquisition Supply Chain Security Act (FASCSA) Orders.

INTERAGENCY COUNCIL

- Office of Management and Budget
- General Services Administration
- Department of Homeland Security
- Cybersecurity and Infrastructure Security Agency
- Office of the Director of National Intelligence
- National Counterintelligence and Security Center
- Department of Justice
- Federal Bureau of Investigation
- Department of Defense
- National Security Agency
- Department of Commerce
- National Institute of Standards and Technology

THE FASC MISSION

To provide leadership and coordination for supply chain risk activities critical to improving the security, reliability, and resiliency of federal information and communications technology systems and acquisition programs.

WHAT ARE "EXCLUSION AND REMOVAL ORDERS"?

Based on a FASC recommendation, the Secretary of Homeland Security (as well as the Secretary of Defense and the Director of National Intelligence for their respective areas of responsibility) can issue an exclusion or removal order for an information and communications technology (ICT) vendor, product, or service. Under FASCSA, the Secretary of Homeland Security is responsible for orders applicable to federal civilian executive branch agencies, and compliance with any FASCSA order is mandatory.

ICT named in these orders may include:

HARDWARE **SOFTWARE** **IT SERVICES**

If the Secretary of Homeland Security issues an exclusion or removal order, there are several outcomes that could potentially impact the federal civilian executive branch agencies:

1. Agencies may be required to **remove** covered articles from federal systems and/or **exclude** the source or covered article from procurements.
2. Agencies may incur additional costs to remove and replace functionality of a source or covered article.
3. Agencies will have reporting requirements on the exclusion or removal order through CyberScope.
4. Orders will provide instructions for exception requests if applicable.

IS YOUR AGENCY READY TO EXECUTE A FASCA EXCLUSION & REMOVAL ORDER?

If the Secretary of Homeland Security identifies a significant cyber risk to the federal ICT ecosystem and issues an Exclusion and/or Removal Order based on a FASC recommendation, agencies are required to take swift action to isolate, exclude, and address the risk posed by the affected article (hardware, software, system settings, vendor services, etc.). Below are recommended steps agencies should follow when preparing to implement an order.

1. ASSEMBLE TEAM

To prepare for the implementation of an order, agencies should assemble a cross-functional team of stakeholders with strategic and operational authority. Key stakeholders may include the agency's C-SCRM Program Office, CIO or CISO, the Chief Acquisition Executive, the Agency Risk Officer, and Office of General Counsel. This team can establish communication channels with ICT product and service program managers to ensure a consistent and coordinated agency response.

2. DETERMINE PREVALENCE

Agencies should establish mechanisms to determine the prevalence of ICT products and services covered by the order in their environments. Agencies can utilize CDM capabilities or other internal tools to pull hardware and software system inventories, coordinate with the agency's logistics management team to identify embedded systems not included in CDM, and identify all supporting service contractors and subcontractors by coordinating with the agency's acquisition office.

3. PREPARE FOR REMOVAL

Agencies should review and update its applicable contingency plans to maintain continuity of operations if an ICT product or service is removed from networks or otherwise excluded from the federal supply chain. The plan should include a way for program owners and operators to report impact and risk to the key stakeholders, both in normal operations and the event of a FASCSA order. Program managers should coordinate with acquisition and IT professionals to identify suitable alternatives for critical components or services to maintain operational resiliency.

4. PREPARE FOR EXCLUSION

Agencies should inform contracting officers, source selection teams, and all participants in active or recently awarded acquisitions that an ICT product or service subject to an exclusion order could be excluded from procurements. Regularly check SAM Supply Chain Orders during the selection process. Ensure purchase card holders are aware that FASCSA Exclusion Orders apply to card transactions and that they are responsible for checking SAM.gov as well as following agency policies prior to acquiring any ICT related products or services.

5. EXCEPTIONS

If pursuing an exception to a FASCSA order, agencies should follow the instructions in the FASCSA order as well as the guidance provided in 41 C.F.R. § 201–1.304 (b). The applicable regulations require agencies to submit to the official issuing the FASCSA order a written description of the requested exception, including a name or description of the covered article sought in the exception, a compelling justification for the exception (such as a mission or national security need), and the alternative mitigations undertaken by the agency to reduce the supply chain risk.