Federal Acquisition Security Council Strategic Plan For Addressing and Managing Supply Chain Risks

Contents

Preface

In September 2018 the President approved the National Cyber Strategy with an objective to improve the Federal Government's management of the supply chain and strengthen cyber security. A critical component of this strategy is the integration of supply chain risk management into the procurement and use of information and communications technology (ICT). This integrated risk management approach will be implemented in accordance with federal requirements and leverage industry best practices to ensure that the Federal Government deploys safe, reliable, and resilient technology.

In December 2018 the President signed into law the SECURE Technology Act, which provides a major step toward implementing the supply chain risk management requirements called for in the National Cyber Strategy. This Act establishes the Federal Acquisition Security Council (FASC), empowering it with authority to develop government-wide criteria for federal supply chain risk management (SCRM) programs, criteria for sharing relevant supply chain risk information across the Government, and protecting Federal information technology(IT) by recommending exclusion or removal of dangerous products. This Strategic Plan describes how the FASC will approach its statutory responsibilities to effectively strengthen and better secure the federal supply chain.

Defining Supply Chain Risk

Supply chain risk is "the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles[1] so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles."[2]

The Current Supply Chain Risk Management Landscape

Federal ICT touches every aspect of our nation's key interests. Our national security is vital and depends on the actions we take to protect the integrity of our critical infrastructure and ensure the health and safety of our citizens. Effectively managing supply chain risks to federal ICT is key to securing our nation in an increasingly interconnected world. The SECURE Technology Act requires executive agencies to assess the risks to their ICT supply chains by establishing a supply chain risk management (SCRM) program.[3] Over the years, Congress has given direction to particular agencies to assess cyber espionage or sabotage risks before acquiring ICT systems. Additionally, OMB identified SCRM requirements in Circular A-130 and the National Institute of Standards and Technology (NIST) has issued SCRM guidance applicable across the federal enterprise. The Office of the Director of National Intelligence (ODNI) has also issued an Intelligence Community Directive and supporting standards to require the IC to develop SCRM programs. But to date, until now, there has not been an overarching effort to establish SCRM practices across the federal ICT enterprise. As a result, federal departments and agencies have varying capabilities to assess and address risk in the ICT supply chain.

Prior to the enactment of the SECURE Technology Act, there was no centralized construct for unifying federal SCRM activities. The SECURE Technology Act establishes the FASC and mandates the development of uniform criteria for SCRM programs to increase capabilities to address supply chain risk across all agencies.

[1] For purposes of the FASC a "covered article" is defined as: "(A) information technology, as defined in section 11101 of title 40, including cloud computing services of all types; (B) telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); (C) the processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program; or (D) hardware, systems, devices, software, or services that include embedded or incidental information technology." 41 U.S.C. § 4713 (k)(2).

[2] 41 U.S.C. § 4713 (k) (6).

[3] 41 U.S.C. § 1326 (a) (1).

ICT SCRM is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. Because each federal agency's supply chain is as unique as each agency's mission, no single SCRM program can be universally applied across the federal government. But now, all federal agencies will be able to look to the FASC for guidance, including for addressing supply chain risks in the procurement and use of ICT; for updates on supply chain risk management standards and guidelines based on NIST standards; federal SCRM expertise to support government-wide coordination; and, sharing of applicable risk information to inform agency SCRM programs and ICT acquisition decisions.

The Council's Mission and Strategic Objectives

The FASC was established to address the escalating risk to federal ICT presented by an increasingly global and opaque supply chain infiltrated by hostile actors. The FASC's mission is to provide leadership and coordination for supply chain risk activities critical to improving the security, reliability, and resiliency of federal ICT. To improve SCRM across the federal enterprise and respond to the mandates laid out in the SECURE Technology Act, the FASC identified the following strategic objectives:

- Facilitate the creation of an effective and consistent process for identifying, assessing, and responding to ICT risk, including mitigations and recommendations for exclusion and removal of ICT sources, goods, and services that pose a risk to our nation's supply chain.
- Ensure all federal departments and agencies have access to best practices for their respective SCRM functions.
- Facilitate the creation of an effective information sharing construct to ensure all federal departments and agencies have access to information essential to their SCRM functions.
- Facilitate the use of shared services and common contract solutions to maximize efficiency and minimize resources needed to effectively manage the ICT supply chain across the federal enterprise.
- Improve stakeholder engagement (e.g., non-Executive Branch Federal entities, private sector and non-governmental organizations) to enhance partnerships to reduce supply chain risk.

The Council's Strategic Efforts in Furtherance of Its Mandated Activities

The FASC intends to implement its mission by creating a strategic foundation built on three central pillars: 1) standards, guidelines, and practices for federal SCRM programs; 2) information sharing; and 3) stakeholder engagement. The strategic actions necessary to implement the FASC's missions are described in greater detail immediately below.

Pillar 1: Standards, Guidelines, and Practices for Federal SCRM Programs

As stated above, the SECURE Technology Act requires departments and agencies to establish and maintain a SCRM program. The FASC will identify criteria, standards, guidelines, and practices for federal SCRM programs that will provide an overarching approach to managing risks to the supply chain. Implementing an overarching approach ensures that all federal agencies can identify, assess, and mitigate supply chain risks consistently. Managing supply chain risk requires a coordinated agency approach that includes participation of an inter-disciplinary team (*e.g.*, acquisition, engineers, security policy, IT, logistics and legal personnel). Finally, the FASC will ensure federal agencies have access to the information needed to manage and reduce supply chain risk.

Statutory Mandates:

To meet the SECURE Technology Act requirements, the FASC will:

1. Identify and recommend to NIST the development of SCRM standards, guidelines and practices for use when assessing and developing mitigation strategies to address supply chain risks.
2. Identify, as appropriate, agencies to provide certain shared SCRM services and common contract solutions.
3. Issue guidance on additional steps that may be required to identify, assess, and respond to supply chain risks throughout the acquisition lifecycle for agencies providing shared services, common contract solutions, acquisition vehicles, or assisted acquisitions.
4. Establish criteria and procedures for information sharing and recommending exclusion or removal orders.

Strategic Activities:

In furtherance of the above statutory mandates and the desire to ensure all agency SCRM programs benefit from uniform guidance, the FASC will conduct the following activities:

- *Strengthen agencies' SCRM capabilities.*

  The SECURE Technology Act requires agencies to assess their own supply chain risks in accordance with the standards, guidelines, and practices identified by the FASC. As part of this assessment, agencies must develop an overall supply chain risk management (SCRM) strategy and implementation plan to guide SCRM activities throughout the life cycle of the system, component, service, or asset.

  SCRM capability maturity levels vary widely among departments and agencies including levels of awareness, capability, and effectiveness related to supply chain security. The FASC will assist departments and agencies in strengthening their respective SCRM strategies and implementation plans by identifying common initiatives, standards, guidelines, processes and proven practices implementable by all organizations. NIST, as a member of the FASC, will develop standards and guidelines to address any identified gaps. Central to an effective implementation plan is raising awareness among all executive agencies, especially among those senior leaders, acquisition officials, and program teams who are accountable to implement SCRM across their organizations. Achieving measurable improvements in the capacity of executive agencies to meet their legislatively mandated SCRM responsibilities will depend heavily upon establishing government-wide tools and shared understanding to transform independent activities into a synchronized ecosystem. Common initiatives, standards, best practices, and processes are key to a successful transformation and improved risk management by all stakeholders.

- *Identify existing authorities for addressing risks.*

  The FASC will establish and maintain a knowledge management repository that includes relevant authorities for addressing supply chain risks. This repository will assist executive agencies with understanding their authorities under the Act as well as those which are more agency-specific. The intent is to increase awareness of the existing authorities and reduce duplication in any new or proposed authorities.

- *Identify best practices and procedures.*

  Several departments and agencies have implemented SCRM programs that provide examples of best practices and procedures for other agencies just starting their SCRM program. Regardless of the maturity level, all departments and agencies will benefit from reviewing identified SCRM best practices and procedures. Further, agency program development plans will benefit from referencing existing guidance, including NIST, FBI, DoD, CNSS, ODNI, and other relevant sources. Understanding and examining existing programs allows agencies to understand the responsibilities and resource requirements for implementing SCRM capabilities across the agency enterprise. The FASC will facilitate SCRM program development through making existing and future guidance as well as best practices available to all executive agencies.

  Accordingly, the FASC will conduct data calls and reports to collect, organize, and evaluate (past, current and planned) SCRM policies, initiatives, practices, and processes and associated resources. The primary purpose of these data calls and the resulting inventory and data analysis is to provide the FASC with better understanding of the current landscape of existing activities and practices, and aid the FASC in the identification and selection of those SCRM practices that should be promulgated across the executive branch. The SCRM inventory analysis may also identify gaps in policies, standards, and guidelines.

- *Address Cross-Agency SCRM Services.*

  Category management, used extensively by industry and other governments for years, is an effective approach to increase acquisition efficiency and manage costs. Given the emerging nature of our adversary's tactics in leveraging ICT, coupled with the growing complexity of global supply chains, shared services and common contract solutions may assist agencies in achieving their SCRM requirements in a variety of ways. The FASC will assess the feasibility of establishing such shared services to support agency SCRM activities such as identifying and assessing supply chain risks. Additionally, the FASC will work with the government-wide IT Category Manager to develop the government-wide acquisition approach for addressing supply chain threats and risks both centrally and by individual agencies.

- *Develop Exclusion and Removal Criteria.*

  Although it may be possible to sufficiently mitigate the risks posed by some goods and services or their specific sources, in some cases the national security concerns may be so great that particular goods and services or specific sources for them may need to be excluded from acquisition or, if already procured, removed from the federal enterprise. To address this specific area of concern, the FASC will establish criteria and procedures in furtherance of its authorities under the Act to recommend the issuance of exclusion or removal orders regarding particular sources of covered articles. Such criteria will be consistent with applicable NIST standards and guidelines and FASC-criteria for information sharing.

- *Evaluate the effect of implementing new policies or procedures on existing contracts.*

  As new efforts to improve SCRM practices across executive agencies are implemented, there will be an impact to existing ICT contracts that may require contract modifications to better address supply chain risks. Evaluating these effects will be essential to understanding what actions agencies may take to mitigate risks in the context of existing contractual commitments. The FASC will work with the government-wide IT Category Management to analyze how new SCRM policies and procedures implemented as a result of the SECURE Technology Act will impact the acquisition lifecycle for both contracts and leases.

- *Measuring outcomes.*

  The SECURE Technology Act amends the Federal Information Security Modernization Act of 2014 (FISMA) to incorporate the criteria for SCRM programs into the annual FISMA requirements metrics.[4] The FASC will develop and recommend to OMB appropriate measurable programmatic metrics for FISMA reporting. The existing Annual FISMA reporting will facilitate reporting of agency efforts and progress, which will allow departments and agencies to address any deficiencies including policy updates, process improvements, and resource needs. While FISMA will serve as a primary source of review for measuring SCRM capabilities across the federal enterprise, the FASC will also produce an annual report on the FASC's activities to mitigate supply chain risks and implement SCRM program improvements consistently.

Pillar 2: Information Sharing

Statutory Mandates:

1. Identify or develop criteria for sharing information with executive agencies, other federal entities, and non-federal entities with respect to supply chain risk.
2. Identify an appropriate information sharing agency to accept information submitted by executive agencies, facilitate the sharing of information to support supply chain risk analyses, and provide the FASC with information regarding specified procurement actions.

Strategic Activities:

The FASC's strategic activities in this pillar are driven by the desire to increase information sharing among all stakeholders, including government to government, government to industry, and industry to industry. In furtherance of the above statutory mandates and this collective goal the FASC will conduct the following activities:

- *Develop criteria and processes for information sharing categories.*

  All agencies have information relevant to managing their supply chains and the risks associated with them. However, most agencies are challenged by the disparate nature of how this information is maintained across their enterprise. For example, the chief information officer, the head security office, and the acquisition office may each have information pertinent to SCRM. Moreover, each office has its own policies and procedures that govern how they can access and disseminate information they maintain. Some of these policies prohibit the sharing of information beyond that office, including restricting dissemination to external organizations; in such cases, the policy reasons for such restrictions should be reviewed to determine if they can be met through an alternative approach that also ensures that the information is available to others who need it to support SCRM activities.

  The FASC will develop criteria to delineate the specific categories (mandatory and voluntary) of information to be shared to ensure the security of federal ICT (including sharing with non-Executive Branch federal entities) while ensuring the information sharing process complies with applicable legal and policy requirements. For each category of information identified as relevant to managing supply chain risks, the FASC will develop the criteria for sharing such information, including:

  - Requirements for submission of supply chain risk information (both mandatory and voluntary submissions of information) to the FASC, including any necessary requirements for information handling, protection and classification;
  - When sharing is mandatory or voluntary;

[4] 44 U.S.C. § 3554(a)(1)(B).

- Authorized recipients of information; and
- Information that supports supply chain risk analyses under 41 U.S.C. § 1326 of the Act, recommendations issued by the FASC, and covered procurement actions under 41 U.S.C. § 4713 of the Act.[5]

This criteria will be described in the Interim Final Rule and further refined upon issuance of a final rule.

➢ *Identify an appropriate executive agent to facilitate and manage the information sharing requirements processes specified by the FASC.*

The FASC will identify an appropriate executive agency—the FASC's Information Sharing Agency (ISA) – to perform the administrative information sharing functions on behalf of the FASC, as enumerated in the law, 41 U.S.C. § 1323(a)(3). 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 processes under which the functions in 41 U.S.C. § 1323(a)(3) will be implemented on behalf of the FASC. The Department of Homeland Security (DHS), acting primarily through the Cybersecurity and Infrastructure Security Agency, is named the appropriate executive agency to serve as the FASC's ISA. The ISA's administrative functions are not construed to limit or impair the authority or responsibilities of any other federal agency with respect to information sharing.

Pillar 3: Stakeholder Engagement

Statutory Mandate:

1. Engage with the private sector and other nongovernmental stakeholders on issues relating to the management of supply chain risks when fulfilling other mandates such as developing guidance and promoting information sharing.

Strategic Activities:

In furtherance of the above legislative mandate and the desire to ensure all stakeholders are appropriately integrated, the FASC will conduct the following activities:

➢ *Establish a stakeholder management plan.*

The FASC will develop a stakeholder management plan to coordinate engagement activities with executive agencies, the private sector, and other nongovernmental stakeholders (*i.e.*, private-public partnerships, federally funded research development centers and academic institutions) regarding supply chain risk. It is clear that there are many different types of stakeholders whose interests must be considered when conducting SCRM activities. Their respective interests and the federal SCRM activities needs regarding each type of stakeholder are not homogeneous. Thus, a stakeholder management plan that identifies the relevant stakeholders, their needs and concerns, and the means for engaging with the respective stakeholders will ensure that the FASC's activities are informed by all relevant information as well as meets the needs of a diverse ecosystem of stakeholders. This stakeholder management plan will include plans for increasing both the FASC and stakeholders awareness of supply chain risks and the respective roles that all parties will play in addressing them.

In particular, private sector stakeholder engagement is essential to driving the long term economic change necessary to make a supply chain risk framework that is proactive, rather than reactive. The ability to effectively manage the risks will depend on consistent bi-lateral outreach and collaboration.

[5] 41 U.S.C. § 1323 (a) (2).

This type of engagement is especially important given the current environment where threats dynamically change, and may become systemic, and remediation cannot be singularly affected by the majority of federal SCRM programs.

Recommendations

As part of the development of this strategic plan, the FASC recognizes that some strategic outcomes may require legislative, regulatory, or policy changes to achieve the desired results.

The FASC will review the implementation of the strategic activities outlined above and if necessary make additional recommendations. This will allow the FASC to make targeted legislative, regulatory, or policy recommendations to further improve ICT supply chain risk management. Additional assessment time also provides departments and agencies with the opportunity to assess their resource needs in order to fully implement the FASC-criteria for improved SCRM capabilities. This strategic approach to the recommendations process will ensure that departments and agencies have what they need to sustain their SCRM programs. Additional FASC recommendations will be captured in the annual report on the progress of FASC activities.

Way Forward

As outlined above, the FASC will begin to implement the strategic activities for each pillar. In support of this implementation activity, the FASC has designated a FASC working group with representatives from each department and agency represented on the Council, and will bring in support from other departments and agencies as appropriate. The working group will assess each strategic activity and determine supporting activities and levels of effort required for implementation. The FASC will continue to collaborate across the Government to ensure that each strategic activity is implemented across the federal enterprise.

Each strategic activity outlined above has resource implications for departments and agencies. Because departments and agencies are required to develop their own SCRM programs (strategies and implementation plans), the FASC's efforts to facilitate the development of streamlined standards, best practices, shared services, and common contract solutions not only supports uniformity for SCRM activities, but also provides a resource roadmap to prioritize funding for the most critical SCRM activities. The FASC will assess those critical SCRM activities and determine the resources needed to ensure implementation.

The FASC is committed to strengthening the SCRM capabilities of all federal departments and agencies. The SECURE Technology Act provides the FASC with the responsibility to lead departments and agencies in developing their respective strategies and implementation plans. This strategic plan outlines the FASC's uniform approach to executing SCRM responsibilities, which fosters better protections for the ICT supply chain across the federal enterprise.