Developing Supply Chain Risk Management (SCRM) Initiatives in the Federal Government

Highlights from a recent roundtable, hosted by the Advanced Technology Academic Research Center (ATARC), September 2023

Supply Chain Risk Management (SCRM) plays a crucial role in safeguarding the integrity and security of supply chains within the Federal government. With increasing reliance on technology, there is a growing need to address potential vulnerabilities and risks associated with procuring, using, and securing products and services. Cyber Supply Chain Risk Management (C-SCRM) is a key focus for agencies navigating the rapidly changing technological landscape.

In a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC), federal experts shared the opportunities and challenges they encounter with SCRM.

Current SCRM Practices and Challenges in Federal Government

Participants kicked off the roundtable by sharing the challenges they face with SCRM and their approaches to risk mitigation. While some agencies' primary function is to provide acquisition services to customer agencies, other agencies on the panel are smaller and have fewer resources dedicated to SCRM.

Larger, more resourced agencies are able to explore policy changes related to C-SCRM, whereas smaller agencies are simply seeking access to reliable information to properly address supply chain risk. However, regardless of size, all agencies share challenges with mitigating supply chain risk.

It's become increasingly difficult for agencies to gain a complete view of the supply chain with the rise of third-party vendors and global sourcing of products and services. Understanding product origins and the manufacturing processes of each product and service is critical, yet increasingly difficult. There is a notable shift towards code-based supply chain concerns as the proliferation of SaaS products flood the government market. Agencies emphasized the importance of building relationships with industry partners to better understand product origins, the relationships between parent and child companies, and manufacturing processes.

“It's almost as if some of these companies are purposely dividing, subdividing, and moving things around. It's just incredibly confusing.”

Agencies are working towards addressing the security challenges with SCRM in several ways, including working to integrate supply chain risk management into the acquisition process. Ideally, these types of contract conditions would be standardized and at an enterprise level. However, C-SCRM is a nuanced and complex matter that will differ for each agency based on mission, existing architecture, security posture, and a myriad of other factors.

Roundtable participants emphasized the interconnected relationship between SCRM and cybersecurity practices and the importance of being able to monitor and assess supply chain vulnerabilities in real-time. Panelists concur that SCRM is one component of a larger, more holistic security program.

As part of a bigger security program, agencies are incorporating Zero Trust principles into SCRM practices, while focusing on insider threats and ensuring personnel involved in the purchase process have the necessary training and tools. Agencies are also working on standardizing language and processes to navigate regulatory complexities and enhance responsiveness in an ever-changing tech landscape.

> **“You're never going to have zero risk. Rather, how do we integrate that risk as much as possible in order to make it safe for the environment of the government?”**

Specific SCRM Examples in Federal Government

Standardization of Contract Language

Agencies are working to include general language and requirements related to C-SCRM into contracts with the goal of creating enterprise-wide contract language. Standardization would increase the confidence of smaller agencies with fewer resources dedicated to risk management. Agencies are also working to avoid the need to recertify and renegotiate during contract terms by preloading contracts with supply chain provisions.

While standardizing contract language would help streamline some aspects of acquisition, panelists highlight the importance of addressing unique supply chain risks specific to agency missions and open-source coding practices. One agency is working specifically to comply with regulations such as upcoming FAST exclusion orders. Others are reviewing processes to illuminate supply chains that were successfully 889 compliant with the hopes of implementing best practices.

> **“Good supply chain management is also about good communication between you and the vendors.”**

Software Bill of Materials

Panelists shifted the discussion to debate the merits of software bill of materials (SBOM) in managing supply chain risk. The overwhelming consensus among panelists is that SBOMs are one tool among many to analyze and document the supply chain, but are not a reliable standalone tool to address risk.

As a static document, an SBOM cannot capture all components of a continually changing supply chain. The constantly evolving nature of the cloud also makes it difficult to stay current with any new supply chain components. Developers often introduce new libraries and code, so it’s important for agencies to use other tools in addition to SBOMs to ensure compliance.

Some panelists view SBOM compliance as a checkbox exercise, and not one that adds significant value to risk management. Agencies are more focused on building repeatable processes, maturing capabilities, and developing a shared service to address C-SCRM challenges. There are pressing issues, such as insider threats, that pose a significant risk to organizations that SBOMs cannot address.

> **“An SBOM is nothing more than a dependency tree that we've collected for years. Quite frankly, an SBOM by itself is next to useless, until you apply it to a tool that actually lets you know what's going on within that dependency tree.”**

But the question on every panelists’ mind is: at what point does SCRM stop? Analyzing the risk of a single application is one thing, but if agencies want to be secure they’ll need to start looking at the tools used to compile the software. The rabbit trail of vendors, suppliers, distributors, and contractors is long and often untraceable.

Zero Trust and Supply Chain Risk Management

When asked if Zero Trust principles make sense in SCRM, panelists agree there are common elements between Zero Trust and SCRM, particularly in terms of segmentation, isolation, and identity. Although agencies know that least privilege access across systems is unlikely, they are able to implement least privilege within each piece of software. By isolating software in such a way, agencies can restrict permission sets and mitigate risk if a vulnerability is detected.

Key Takeaways

- **The Role of Software Bill of Materials (SBOMs**) - As a static document, an SBOM cannot capture all components of a continually changing supply chain. If vulnerabilities exist within the supply chain pipeline, agencies must turn to a more robust, holistic approach to supply chain risk management.

- **Share Information Through C-SCRM Questionnaires** - Some agencies are working to create enterprise-wide SCRM best practices that will support future buying decisions within Federal agencies. Although the guidance will not be available for several months, agencies are being asked to participate in C-SCRM questionnaires. The information pulled from the questionnaires will inform future guidance.

- **Master the Basics** - If agencies do not master SCRM basics, they will have no chance of managing higher level risk. Panelists recommend starting with SBOMs, SCRM contract language, and understand where to insert least privilege in the SCRM roadmap.

- **Understand Third Party Risk** - It’s becoming a more frequent occurrance for companies to use third parties to fulfill multiple aspects of the supply chain. Understanding how these third and sometimes fourth parties fit into an agency’s SCRM roadmap is critically important.

- **Know What Level of Risk is Acceptable** - Because the levels of supply chain risk continue to widen and deepen as more vendors, suppliers, contractors, and distributors become involved, agencies must continually determine what level of risk is acceptable for their particular agency.

- **Consider Insider Threat the Biggest Concern** - Regardless where threats originate, identifying and mitigating insider threats to the supply chain should be a primary focus of SCRM endeavors.

- **Leverage Shared Knowledge** - No one agency will be able to address SCRM in its entirety. Agencies should leverage each other’s investments and resources to tackle the most common risks across the enterprise.

> **SCRM by nature is very complex. We have to juggle many different areas and be good at them. Honestly, we cannot do that if we don’t leverage each other’s expertise.”**

LEARN MORE AT

WWW.ATARC.ORG