MeriTalk
Improving the Outcomes of Government IT

Underwritten by:
DLT A TECH DATA COMPANY
RSA
STERLING

Special Report: Secure Supply Chain

CISA, DoD, Commerce Policies Forcing Progress on Securing Federal IT Supply Chain

The Federal government and critical infrastructure owners and operators spend $500 billion annually on information and communications technology (ICT) from thousands of suppliers – small, medium, and large; national and international. Digital transformation and globalization have brought technology advancements and operational efficiencies to Federal agencies. But the increasingly labyrinthine nature of Federal supply chains impacts the security of Federal systems, data, and missions.

Separate, ongoing policy efforts at three of the largest Federal departments – Defense (DoD) and Commerce (DoC), and the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security – are aiming to take some of the confusion – and potential security harms – out of the supply chain equation.

The roots of supply chain complexity

"These supply chains can be long, complex, and globally distributed and can consist of multiple tiers of outsourcing. As a result, agencies may have little visibility into, understanding of, or control over how the technology that they acquire is developed, integrated, and deployed ..." Gregory C. Wilshusen, Director of Information Security Issues at the U.S. Government Accountability Office, noted in July 2018 congressional testimony.

Essentially, supply chain complexity is a threat to Federal agencies because of its extensive and growing interdependencies, which contribute to limited visibility into third-party products and services. Agencies are subject to risk by proxy.

One of the biggest challenges agencies face is incomplete vendor reporting, experts say. Vendors may be managed by multiple organizations in an agency, and reporting may be accomplished using various tools. That can lead to information silos, and ultimately, inaccurate insights into vendor risks.

Another significant area of vulnerability is the reseller ecosystem. Resellers are the "last mile" in the ICT supply chain, connecting original equipment manufacturers (OEMs) to their government customers. As such, they are targets for cyber threats due to the vast amount of government information they manage and have access to. What's more, the reseller channel's approach to cybersecurity is uneven; smaller organizations, in particular, may lack the resources to protect against sophisticated threats, and all it takes is one successful attack to jeopardize an agency by proxy.

> "You have to know your resellers. It starts with more time educating and training contracting officers and buyers to look beyond just the bill of materials and part number."
>
> *- Jeff Moore, senior vice president, Sterling Computers*

Software is a growing area of concern, amid rising awareness that security issues can be introduced at any point in the software supply chain, from production to implementation to operation. "When mitigating risks in software supply chains, one must think holistically and assess the components of an application, the language framework being used to develop it, the third-party dependencies, and any inherent vulnerabilities that can be exploited," said Rick Stewart, Chief Technologist at DLT.

A supply-chain risk management program begins with cataloging the agency's third parties and where they are used throughout the organization. During the contracting stage, the agency needs to assess risk, and then periodically reassess it. Many employ annual questionnaires, which are helpful but don't go far enough, noted Patrick Potter, Digital Risk Strategist at RSA.

Goal: Risk-informed decision-making

Automation can help agencies monitor vendor risk thoroughly, unobtrusively, and regularly. Via third-party security risk monitoring – which employs automated searching of Internet-facing systems – an agency can monitor vendor systems based upon criteria it sets. Those may include vulnerabilities, patches, and utilization of security tools and best practices, at intervals that reflect the risk of the third parties and the criticality of the products or services they provide. Then, the agency can engage with its third parties to address identified cyber risks.

"Gathering information on each risk, evaluating them, and taking action – it's a huge undertaking. Automation takes the busywork away and lets agencies focus on exercising human judgment," Potter said.

In modern software development, automated testing is essential, Stewart noted. "Software is being built, enhanced, and deployed too frequently to rely on manual testing, as humans cannot perform these repetitive tasks at speed, and keep up with the continuous nature of getting changes out to end users," he said. "It is important to employ automated testing that ensures software is not only secure, but also functionally meets or exceeds requirements and operates resiliently."

Bob Kolasky, Director of the National Risk Management Center at CISA, agreed that automation has the potential to take supply chain security efforts to the next level. "I'm really eager to see some of these [technologies] succeed in using machine learning, using big-data analytics to put information together and translate it into an understanding of risk, and then be able to translate that risk understanding to process decisions," he said. "I think technology is going to be a great enabler of more risk-informed decision making."

CISA: "We're in the middle of a transformation"

Agency and industry executives praise the 2018 National Cyber Strategy and the SECURE Technology Act – which was signed into law in December 2018 – for raising awareness of supply chain risks among Federal agencies and driving integration of supply chain risk management into agency processes, as well as better information sharing among agencies.

"We're in the middle of a transformation around building supply chain risk management best practices into procurement and acquisition decisions," Kolasky said. "It starts with putting contractual requirements in place and pushing expectations down to second, third-order suppliers. The way that happens effectively is through establishing standard practices, templates for information, and information-sharing environments … so companies that want to offer their commodity can demonstrate pretty quickly that they're following good security practices."

Kolasky leads an effort at the forefront of the transformation, the CISA Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, which identified more than 190 supplier-related threats to agencies last fall.

The task force's working groups are taking on myriad efforts to improve ICT supply chain security, including:

- Developing a legal framework to underpin information sharing about supply chain risk between government and industry;
- Building a library of threat scenarios that include recommended controls;
- Creating templates for organizations that need to build qualified bidder lists and qualified manufacturer lists;
- Developing a trusted attestation framework, which is intended to provide a standard set of questions about trust factors that organizations should consider when making supplier decisions; and
- Coordinating efforts across the Federal government and the ICT industry to ensure harmonization around supply chain security initiatives, including efforts by DoD and DoC.

In early May, CISA released the Supply Chain Risk Management (SCRM) Essentials, which outlines actionable steps organizations can take toward implementing SCRM practices to improve their overall security posture. It also published the ICT Supply Chain Risk Management fact sheet, a quick reference guide to ICT supply chain risks.

The SCRM Essentials was designed to encapsulate guidance from the National Institute of Standards and Technology, as well as other supply chain best practices and ideas emphasized in the Defense Department's Cybersecurity Maturity Model Certification (CMMC), in a useful format for executives who need to build and oversee a supply chain security program, Kolasky noted.

The Defense Department (DoD) CMMC program aims to apply unified cybersecurity standards to DoD acquisitions and assess contractors based on their cybersecurity maturity.

CMMC requirements taking effect soon

"CMMC is trying to enable a supplier to provide a demonstration that they've got the right security controls in place for the level of risk they're taking," Kolasky said. "As a buyer, I want to know that I can count on the security practices of whom I'm buying from, that they've got a good risk management program in place."

CMMC standards will be required in selected requests for information (RFI) beginning in June 2020, followed by corresponding requests for proposals (RFP) in September 2020. Industry associations have weighed in on the CMMC, expressing concerns about its scope and implementation timeline, for example, and the desire to have reciprocity with other certifications, such as FedRAMP. Despite the concerns, industry executives say CMMC will help to mature supply chain security practices within the DoD, and those practices will ripple across its vendor base.

"Overall, I think CMMC will help identify responsible companies for the DoD and evaluate on key metrics other than price alone," Moore said. "If nothing else, it has raised awareness and codified the requirement for suppliers to practice good cyber and supply chain hygiene. Any factor that raises awareness and helps organizations implement risk mitigation strategies is a good thing."

On the other hand, "the cost associated with CMMC compliance is not trivial," Moore said. "If working with the DoD becomes expensive and difficult, fewer will want to participate. Innovation and competition are good things – so it's a fine line to walk."

Industry groups are also watching for developments regarding the DoC's proposed rule for securing the ICT supply chain. Pursuant to a May 2019 executive order, the rulemaking would permit the department to identify, assess, and address ICT technology transactions on a case-by-case basis to determine if they "pose an undue risk to critical infrastructure or the digital economy in the United States, or an unacceptable risk to U.S. national security or the safety of United States persons." The comment period closed on Jan. 10.

NTIA: Understanding what's in software, for better risk management

Also at DoC, the National Telecommunications and Information Administration (NTIA) is coordinating an international, multi-sector, public-private initiative to improve transparency around third-party software components so that when vulnerabilities are detected, they can be quickly remedied. A model software bill of materials (SBOM) is at the heart of the project. It's essentially a list of components that comprise software, information about those components, and supply chain relationships between them.

An SBOM helps software developers understand the risks they are shipping with products; it helps buyers make risk-based purchasing decisions; and for users, it raises awareness of risks when new vulnerabilities are identified. The reasoning is that if these groups first understand what they have, they are empowered to take appropriate action.

"We learn about new risks every day. Sometimes they come from private researchers; sometimes they come from the government or intelligence services. That's the hard part," said Allan Friedman, director of cybersecurity initiatives at NTIA. "What shouldn't be hard is everyone in the software ecosystem knowing 'Am I affected?' There's such clear value in enabling every organization to quickly and easily understand whether they are potentially affected, and that's the value of SBOM."

Late last year, the Software Component Transparency initiative published guidance on SBOMs, as well as a case study from the healthcare sector. Working groups continue to advance the SBOM effort, most recently issuing a draft FAQ document in April. The Food and Drug Administration this spring signaled publicly that it would incorporate SBOMs into its guidance for submissions of medical devices containing software, drawing on NTIA's published guidance, Friedman said.

"Looking ahead, we anticipate SBOMs will be a common part of all software, from open source through middleware and commercial off-the-shelf software to contract-driven software and down into the embedded devices in the infrastructure all around us," he said.

Recommendations for agency leaders

The Federal government's myriad efforts to raise awareness about supply chain vulnerabilities and establish requirements and processes to improve security are gaining momentum. Here are recommended actions for agency leaders:

1. Increase communication with potential and existing suppliers. When considering potential suppliers, assess the importance of the products or services they provide, as well as the risks they could bring to the agency's supply chain. Broadly, suppliers should be able to answer, "What is your process for building new software or implementing new hardware? Is it a documented, repeatable, measurable process?" "How do you stay current on existing vulnerabilities, and how do you mitigate vulnerabilities in new and existing systems?" and "What physical security measures are in place?" With existing suppliers, take steps to continually identify third-party risk and measure performance.
2. Review CISA's supply chain essentials, and become familiar with the SBOM initiative. Confirm that staff are actively promoting best practices to improve the agency's security posture and obtain greater transparency from suppliers. Continue to promote ICT resilience amid current and potential strains on ICT due to the current pandemic.
3. Prepare for CMMC requirements in select DoD RFIs and RFPs in June and September 2020, respectively.
4. Evaluate the reseller ecosystem. At a minimum, confirm that the reseller is an authorized seller of the OEM's product and verify the company's ownership structure and sourcing methodologies. Also, ask if the reseller has International Organization for Standardization (ISO) certifications and has met the Open Trusted Technology Partner Standard.
5. Look for ways to automate the risk assessment process. Thanks to artificial intelligence and machine learning advancements, automated tools can provide agencies with deeper and faster insight into their supply chains, so they can better understand and quickly respond to potential risks. Automation generates significant time and cost savings, allowing staff to focus on decision-making.

Because awareness and concern about supply chain security are rising, "Federal and state and local agencies are reaching out more often now about third-party risk and supply chain security," Potter said. "They're asking great questions and really looking to become more educated about where supply chain risk comes from and what they can do to mitigate it. They're allocating resources and budget, and the needle seems to be moving."