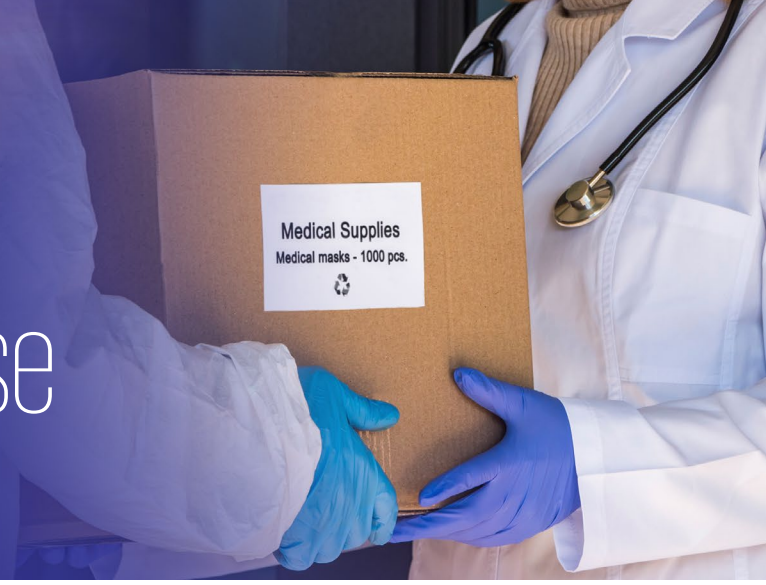


Government supply chain risk is on the rise

Successful methods to cyber secure government supply chains

Supply chain complexity ups the security stakes

Supply chains are the main arteries that keep government organizations operational. Like any life-sustaining function, supply chains must be maintained and protected. The environments in which supply chains operate are complex. They live in cloud and on-premise environments and involve third parties with which governments do business. They involve products and services that governments procure and also deliver to citizens. Threats to these critical supply chains are on the rise and increasing in scope for federal as well as state and local governments. The Department of Homeland Security Cybersecurity & Infrastructure Security Agency reported in September 2019 that federal agencies faced about 180 different information and communications technology supply-chain-related threats.[1]

Growing supply chain complexities and threats are elevating supply chain risk conversations beyond IT, security, risk, and procurement leaders. The topic is on agendas of executive and governance levels—and even among the most powerful private sector corporations and the White House. Discussions that stemmed from the recent White House cybersecurity executive order (EO 14028) resulted in a new partnership between the National Institute of Standards and Technology and tech companies, along with commitments from Apple and Google, to improve IT supply chain security.[2] The executive order also created a rating scale to help consumers know if a software product or service is built securely.

Supply chain threats can bring government operations to a screeching halt whether the hazard is weather, customs delays, fuel shortages, contract issues, a global pandemic, or malicious attacks via software or networks. This article focuses on helping information technology, security, and procurement teams address supply chain cybersecurity risks. It provides practical approaches to manage cybersecurity risks that can impact data, systems, infrastructure, and operations related to state, local, and federal government supply chains.

Why modern government is important

Government agencies in the U.S. must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

[1] "Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks," U.S. Government Accountability Office, December 15, 2020.

[2] Casey Crane, "30 Industry Leaders Meet at White House & Announce Cybersecurity Initiatives," Hashed Out, August 30, 2021.

Third parties pose highest risk

Traditional third-party assurance approaches are no longer effective against new threats, especially since governments are well into digital transformation, cloud adoption, and new ways of working. If they worked, the December 2020 SolarWinds supply chain attack would not have happened. This breach impacted thousands of private sector organizations and government agencies worldwide including U.S. Departments of Treasury, Commerce, and Homeland Security via legitimate third-party software updates.[3] While no system will ever be completely risk-free, when governments understand the security postures of vendors and every stakeholder in their supply chain, they can mitigate risks.

Government teams collaborate with **third-party** vendors such as SolarWinds to create software and applications, and often fourth- or fifth-party vendors considering cloud, and other service providers involved in the supply chain. The result is a development team that is a mix of internal developers, risk, and security professionals with vendor team members who provide cloud, DevSecOps, database services, or other pieces of the development process.

According to recent research, most developer teams pull together existing software libraries or components to create new software rather than developing it from scratch. It is wise for teams who follow this practice to create a **software bill of materials, or SBOM**, to track the application's component inventory similar to ingredient lists on food labels. The application security community identifies vulnerable software components that governments can more easily identify if they have SBOMs for their applications—and reduce cyber risks such as ransomware attacks.

The recent White House executive order on cybersecurity recommends governments use SBOMs to improve software supply chain transparency.[4] The executive order also calls for the Commerce Department and National Telecommunications and Information Administration to "publish minimum elements for an SBOM."[5] Read more about our views on how SBOMs can reduce risk.

Software and services are not the only aspects of supply chain cybersecurity. Counterfeit or gray market hardware, from computer chips to servers, can carry spyware.[6] Agency procurement decision makers have a difficult enough time finding the products they need when they need them. Now they also must make sure the products are secure. Learn more about lowering your third-party risk with AI and automation.

[3] Sophie Bushwick, "Giant U.S. Computer Security Breach Exploited Very Common Software," Scientific American, December 15, 2020.

[4] Matt Howard, "How a software bill of materials can help solve our supply chain woes," FCW, August 19, 2021.

[5] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021.

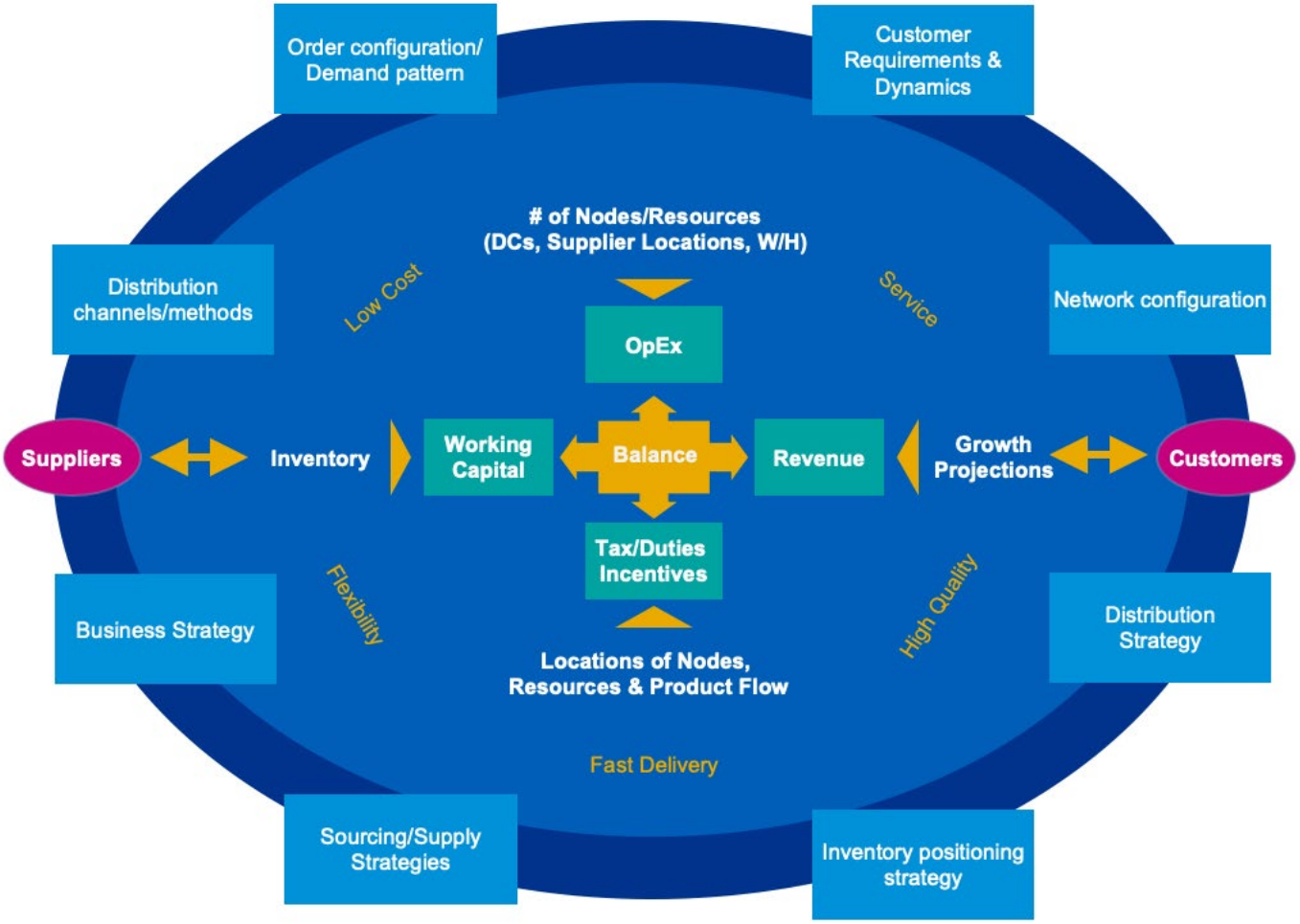
[6] John M. Donnelly, "Pentagon Races to Shore Up Supply Chain Security," Government Technology, April 9, 2021.

Take an integrated, enterprise approach to supply chain risk

The top priority for any government organization is delivering citizens what they need, when and where they need it. Missions might be veterans seeking healthcare from the U.S. Department of Veterans Affairs (VA) or warfighters who need supplies and mission-ready equipment to defend the nation. Citizens count on civilian and health agencies to provide everything from drivers' licenses to cash assistance.

To securely deliver on these missions, governments must **manage supply chain cyber risk from a holistic perspective**—from acquisition, logistics, transportation, and asset management through fulfillment. The perspective also should include reverse logistics when customers have to adjust a service to meet their needs or bring products back in for repairs. They must know where equipment, medications, mail, and any product or service is at any point in time. The strategy must focus on the most critical assets and address **processes, data, technology, and people**. This holistic strategy could look something like the supply chain distribution network in the illustration.

Supply chain distribution network strategy



For example, the **VA** has a complex, global supply chain to secure as the largest healthcare provider in the United States. It also provides benefits services, owns and operates cemeteries, and owns real estate. To cost-effectively manage supply chain risk, the VA must identify its high-value assets and the critical data these assets need. Focusing on high-value assets alone is not sufficient if a connection is made to a lower-valued asset. VA leaders use a risk-based decision matrix to ensure they consider the supply chain from multiple perspectives including cybersecurity, procurement, and sourcing. View a recent panel on this topic here.

Organizations cannot secure ineffective **processes**. Governments do not have the resources to support manual processes, so automating can be more secure. For example, many government warehouse inventory and asset management processes are still manual. Automating basic processes by adding barcoding equipment and handheld readers with voice capabilities is a start. Using a predictive model and completing cybersecurity exercises to test supply chain security can also help organizations find vulnerabilities and get ahead of threats.

It is critical to understand how **data** flows across the supply chain to gauge risk. Real-time visibility into the most critical data is the only way to orchestrate such complex supply chains and avoid blind spots that might disrupt operations or turn into security risks. For example, making a necessary firewall change could block data flow. As a first step to a risk-based approach to protect critical data, organizations must determine their mission-critical information assets, where they are, and how they flow across the supply chain. Next, organizations should understand connectivity, data sharing, data sharing levels, and relationships with every ecosystem partner, including vendors. Migrating applications and data to the cloud forces governments to use new methods to gain assurance or reevaluate risk appetites. Finally, organizations should analyze how types of risks intersect in the ecosystem.

Organizations must also understand their **technology** readiness. Supply chain security management requires modern technologies that can ingest, process, and learn from internal and vendor data and systems. Innovations in continuous controls monitoring, threat intelligence, and machine learning provide ways for governments to address new cyber threats. Many governments make the mistake of purchasing the latest technology before they fully understand the right process to the problem. This strategy is not just about adding controls, but how organizations implement controls into supply chain security.

Most important is for systems to perform well so **people** trust their personal and private information is safe when interacting with government organizations. People do not have a choice when using many government services like they do in the private sector. A framework for understanding how data flows, dependencies on its use, and protecting citizen and employee privacy throughout the supply chain is essential to maintaining trust, especially among growing privacy, security, and regulatory scrutiny.

Managing supply chain cyber risk is **part of each employee's job**, from executives to individual performers. For example, it is critical for purchasing or acquisition professionals to know the right questions to ask to ensure the right terms and metrics are included in contracts. Many government organizations do not have enough people with the skills needed to manage supply chain risk. Regardless of budgets, recruiting and retaining qualified candidates is a challenge in today's competitive employee marketplace. Governments also may lack resources to train current employees in the latest cybersecurity skills. North Carolina has a solution to help fill cybersecurity government jobs. The state partnered with private sector tech companies to create CyberVetsUSA, an on-the-job training program for veterans.[7] While automation and machine learning can fill some gaps, humans must remain involved. People are responsible for solving the most complex problems and also lead and drive supply chain security efforts forward. Learn more about building a workforce to support your digital journey.

[7] "Welcome to CyberVetsUSA," North Carolina Department of Information Technology, November 2018.

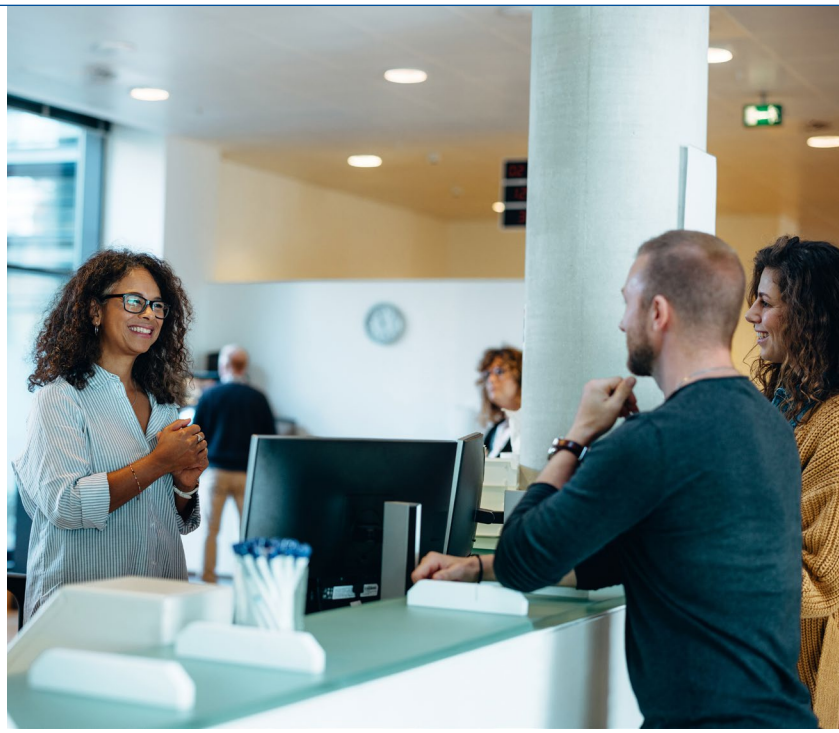
Work smarter together so each agency can succeed

Government organizations are in a unique situation since **they do not compete**. This allows them to collaborate within and across states and intra-agency to **share resources, information, knowledge, and intelligence on cyber threats** so they can make informed decisions to secure their supply chains. Collaboration is especially helpful to state and local governments since resource shortages often put them behind federal. Some states have processes in place to make sure the same threat information and defenses at the state level are also available to local agencies. When people build cross-agency relationships, they know who to contact when they have questions, intelligence, or when an incident occurs.

Mitigating the broad potential cyber threats to supply chains is expensive and complicated, and resources are scarce. Organizations have unique needs since supply chains are dynamic depending on a number of economic and other factors. They vary in size and complexity by organization. We suggest breaking down the task into practical segments that agencies and departments can share. For example, identify core risks for similar types of product and service delivery, and common vendors. Talk with organizations that have similar security, regulatory, or compliance requirements to learn how they deal with these risks. Then collectively document how each organization negates, manages, or mitigates them.

Trust is the cornerstone

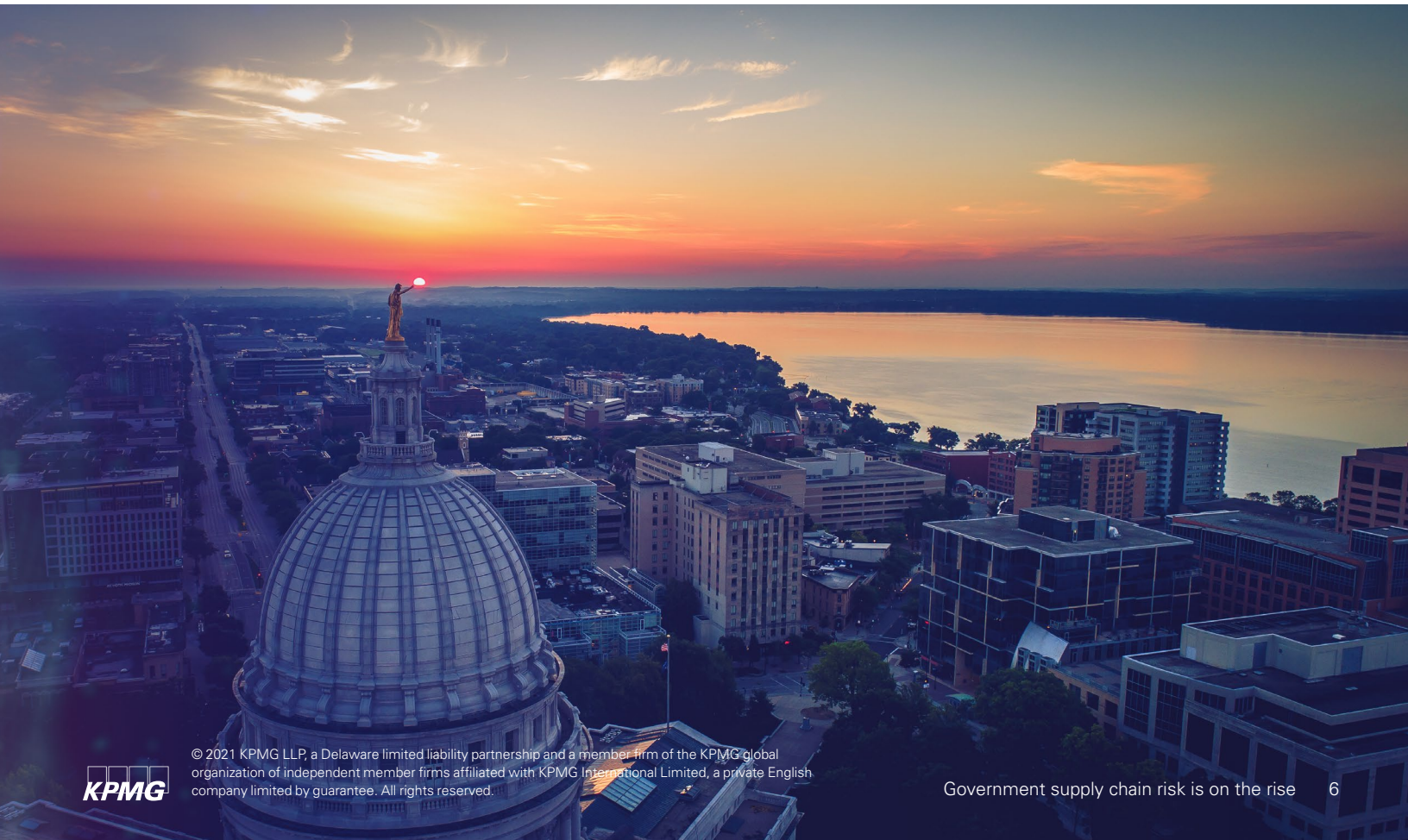
Every government strives to do the most effective job they can for those they serve. With complicated, high-risk issues like supply chain cybersecurity, governments often need assistance. KPMG understands the full scope of supply chain risk, from protecting product and service supply chains against natural disasters and physical breaches to cybersecurity. Our teams combine deep technical experience and government industry knowledge with a broad set of solutions with methodologies, frameworks, and techniques that can address the most complex supply chain challenges. No matter where your organization is in your cybersecurity journey, we can help reduce risk in your supply chain. We can count on a positive effect when governments close supply chain cybersecurity gaps. With watchful cybersecurity eyes on these gaps, federal, state, and local governments can improve product and service delivery and their ability to deliver on the mission.



About KPMG

KPMG has worked with federal, state, and local governments for more than a century, so we know how agencies work. Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.



Contact us

Tony Hubbard
Principal, Government Cyber Security Leader
KPMG LLP
202-486-4945
thubbard@kpmg.com

Viral Chawda
Principal, Advisory
Digital Lighthouse
KPMG LLP
214-840-2000
vchawda@kpmg.com

Joseph Klimavicz
Managing Director, Federal CIO Advisory Leader
KPMG LLP
703-795-8999
jklimavicz@kpmg.com

Chad Jones
Managing Director, Federal Advisory
KPMG LLP
703-343-2226
chadjones@kpmg.com

Kathy Cruz
Director, Government Cyber Security Practice
KPMG LLP
916-792-3976
kathycruz@kpmg.com

---

read.kpmg.us/modgov

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia