



Supply Chain in Government: Enhancing Supplier Networks to Ensure Performance, Resilience, and Security

Supply chain visibility is no longer simply a “nice to have.” It’s essential to government’s reliable, effective, and secure acquisition of mission-critical goods and services. Government decision makers are moving swiftly to gain visibility and protect supply chains from vulnerabilities. In fact, in February, President Biden issued an Executive Order on America’s Supply Chains, which aims at building resilience and strengthening security in American supply chains.

Consider three galvanizing supply chain dynamics that bring into stark relief the critical nature of achieving peerless visibility across all supply chain tiers to better understand and mitigate risks that impact how global supply chains operate.



Great Powers Conflict

China is actively employing traditional and nontraditional means to gain a foothold in the production of the world's higher value goods. Traditional means include investment in technology, artificial intelligence, and robotics. However, in its quest to become a world power, China seeks access to classified and sensitive U.S. intellectual property.

Made in China 2025 is China's national strategic plan to close the innovation gap between their own country and the United States. This plan targets the following key industries:

- Defense applications
- Genomic algorithms
- Autonomous vehicles
- Algorithm factories
- Semiconductor and logic-bearing devices

Similarly, China's 13th five-year plan focuses on obtaining a larger part of the global production chain. While the United States remains the envy of the world in regard to technology and innovation, the Chinese government has committed to doing whatever it takes — including acquiring, appropriating, and stealing from companies in the United States — to advance their own economic and power interests.

National Defense Authorization Act 1999 and 2019 Restricted Entities

Due to the increasing risk to the United States' intellectual property, 21 companies, including Huawei, ZTE, and Hikvision, have been banned from conducting business with U.S. organizations due to their strong connections to the Chinese government. Not only does the ban, which is part of the National Defense Authorization Act of 1999 and 2019 (NDAA), include the parent organization, it also includes all the companies' subsidiaries and affiliates. Consider that subsidiaries are entities in which a restricted entity holds greater than 50 percent interest. Affiliates are entities in which a restricted entity holds a minority (less than 50 percent) financial interest.

COVID-19 Supply Chain Disruptions

The last galvanizing supply chain dynamic is the COVID-19 pandemic. COVID-19 has put U.S. companies and the economy in financial distress. Moving forward, organizations must anticipate predictable and unpredictable risks. Therefore, it is critical businesses examine their supply chains to limit disruptions.

If not addressed, supply chain vulnerabilities due to COVID-19 can endure and pose substantial risk to various industries. Consider that if a significant supply chain disruption is not immediately and

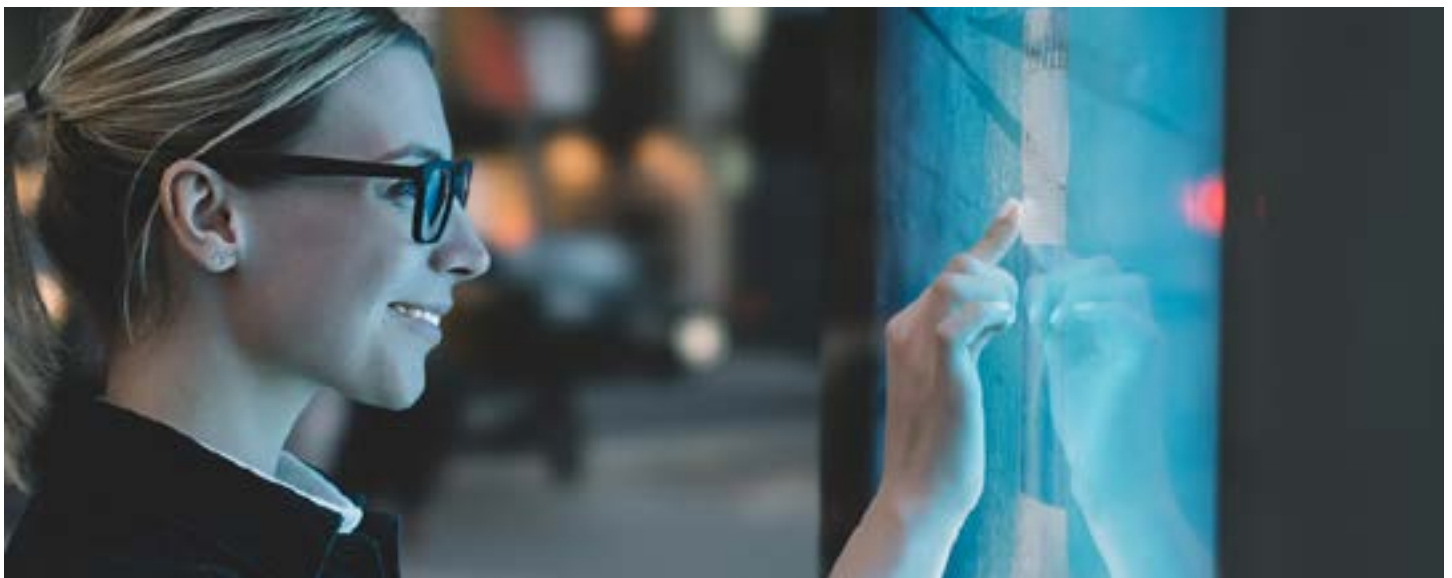
strategically addressed, revenue and, ultimately, share price can decrease.

The government also faces adversity when confronted with supply chain disruption. Remember, during the early days of the pandemic, states' exposed vulnerabilities when they were scrambling to acquire personal protective equipment and ventilators?

Accessing and Mitigating Supply Chain Risk

These days, thanks to media reports, the general population know more about supply chains and how they operate than ever before. However, dealing with the complexities of supply chain risks and vulnerabilities isn't something government entities know how to do as well as they should. Adding to the challenge is that supply chain is uniformly underfunded across government, prohibiting the hiring of enough people with supply chain know-how to identify and mitigate supply chain risk.

Further, many common supply chain risk management practices are inefficient and ineffective. Take supplier surveys, for example. Surveys, typically, are not legally binding nor do they offer timely, actionable information.



The more government organizations can visualize their supply chains, the more and greater risk that can be assessed and mitigated. Experts indicate that agencies often evaluate only their tier one and tier two suppliers. However, starting in the 1990s, industries, such as aerospace, expanded their supplier networks significantly. To be effective in managing supply chain risk, agencies now need to be ready to look at supplier networks of up to 12 tiers.

To bolster supply chain security due to great powers conflict; comply with NDAA; and anticipate supply chain disruptions, such as that caused by COVID-19, government needs supply chain visibility and risk management tools. True visibility means not just knowing the contractors providing your goods and services, but the suppliers providing goods to those contractors, and so on all the

way down to identifying the origins of raw materials, such as individual smelters in China or mines in Australia.

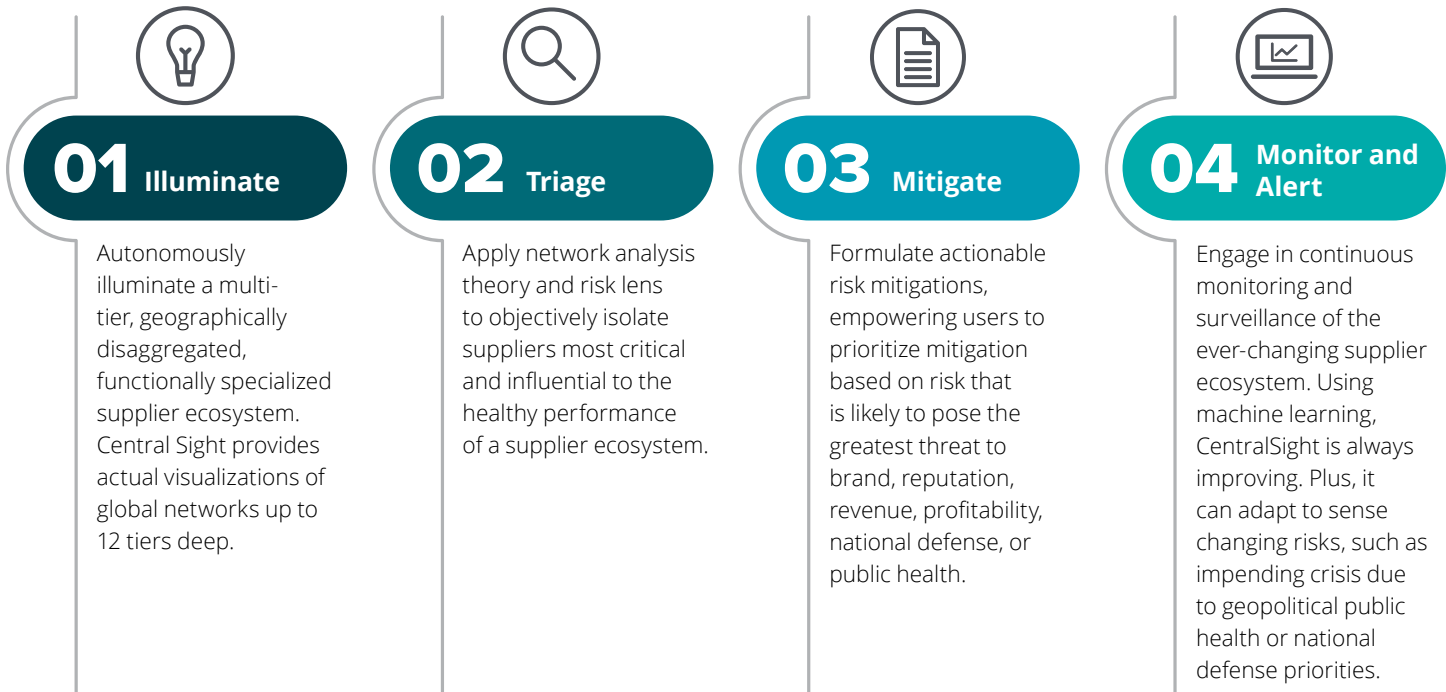
Getting the Right Tools

CentralSight, Deloitte's supply chain risk management platform, unleashes the power of artificial intelligence and machine learning. It enables clients to visualize their complex networks, triage various risks, and prevent supply chain disruptions before they occur — saving money, protecting brand, and radically increasing supply chain integrity and security.

Supply chain visualization is fundamental to effective supply chain risk management. With it, successful agencies can formulate strategies to accommodate, mitigate, or eliminate risk and radically increase supply chain integrity and security.

CentralSight at Work
Deloitte has implemented and supported CentralSight for a variety of clients — from defense and intelligence agencies to civilian and commercial organizations. The supply chains that have been illuminated through CentralSight are as diverse as the clients, and the products and their components are critical. For example, information and communication technology, personal protective equipment, vaccines, and organic food supplies just to name a few.

CentralSight helps organizations, including national, state, and local agencies, using the following four steps:



Supply Chain in Government: Enhancing supplier networks to ensure performance, resilience, and security

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2021 Deloitte Development LLC. All rights reserved.