Guidehouse

guidehouse.com

Supply Chain Risk Management

In the modern global business environment, it is a challenge to keep up with the ever-changing supply chain landscape, rapidly evolving capabilities of adversaries and competitors, strategic changes, the possibility of counterfeit and reused or substandard parts, cyber threats and vulnerabilities, and alternative suppliers.

Government program offices and commercial businesses must be concerned with production, sustainment, maintenance, security, and operations of important platforms and products. Guidehouse has experience helping the United States (U.S.) government, especially those involved in national security operations, and U.S. and companies across the world understand risks and vulnerabilities that could exist in their supply chain and offering strategies for addressing or mitigating those should they be found.

New technologies, teaming partners, vendors, the threat landscape, tactics of adversaries, and more are changing at an increasingly fast pace, due to activities such as mergers and acquisitions, joint ventures, and strategic partnerships.

- There are approximately three-and-a-half to five million changes worldwide in corporations' legal and organizational structures, ownership, and controlling interests every 30-60 days.
- The *National Counterintelligence Strategy of the United States of America 2020-2022* identifies the protection of key U.S. supply chains as one of the five pillars of the U.S. strategy, with a goal to prevent attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of the U.S. government, the defense industrial base, and the private sector.[1]
- The National Counterintelligence and Security Center's *2018 Foreign Economic Espionage in Cyberspace*[2] report stated threat actors are increasingly attempting to inject themselves and their cyber tools into the production stream of important U.S. national security programs.
- U.S. companies, especially those supporting the government, but others as well, have an increasingly high stake in knowing who is in their supply chains — from a risk, legal, efficiency, reputational, operational, financial, and other perspective.

These factors and others mean that the U.S. government (USG) and U.S. corporations need robust supply chain risk management (SCRM) and assessment capabilities to protect our national security and U.S. businesses. Without these risk management mitigation capabilities, our national security, companies, and more are potentially at risk.[3]

1. "The National Counterintelligence Strategy of the United States of America 2020-2022," Office of the Director of National Intelligence (The National Counterintelligence and Security Center). January 7, 2020.
2. "Foreign Economic Espionage in Cyberspace," Office of the Director of National Intelligence (National Counterintelligence and Security Center). 2018.
3. Guidehouse understands the same issues apply governments and companies across the globe.

Threat Actors' Goals

- Obfuscate ownership
- Infiltrate the supply chain
- Enter the design, build, assembly, testing, or maintenance process
- Install counterfeit, reused, or faulty/substandard parts
- Steal sensitive data
- Circumvent cybersecurity measures
- Install malicious cyber payloads or backdoors
- Degrade mission and business readiness
- Economic or industrial espionage
- Undermine national and economic security

The Problem

Notwithstanding this complex landscape, we have repeatedly found that major SCRM-related efforts are narrow in focus and lack the depth to uncover security or operational risks that could negatively impact the mission readiness and business and operational effectiveness of important assets. At the same time, when noteworthy or sometimes even crucial data and other information is obtained, it is rarely shared across the enterprise and acted upon in a strong way. This last point is especially important, as there are frequently other systems or products that have the same parts, components, or vendors that could be adversely impacted if vulnerabilities are identified but not shared. Other key points include:

- The complexities of the global supply chain and increasing shift to digital and automated systems provide bad actors — including unwitting providers of substandard parts — with opportunities for potential cyber, physical, and other entry points into sensitive and important systems and products. Those efforts can be vectored in or have negative impacts many tiers below the prime contractors.
- This is taking place in a changing environment where software-based systems are overtaking hardware-based systems; where departments, their subordinate organizations, and companies are increasingly shifting to the cloud; and where there is increased connectivity, shared services, data lakes, public open source code repositories, crowdsourcing, machine learning, artificial intelligence, and more.

There is frequently a lack of standardized SCRM and cybersecurity performance parameters beyond traditional, often minimal, information assurance standards. Though there are certifications and other quality control measures that companies can voluntarily attain, such as the Cybersecurity Model Maturity Certification (CMMC) being implemented in the U.S[4]., which demonstrates compliance in handling Federal Contract Information and Controlled Unclassified Information, and multiple other global standards on protecting corporate and client data, many program management offices and corporations lack the supply chain awareness, skill sets, experience, resources, and capabilities to adequately manage supply chain risk.

Additionally, companies at lower tiers of production often lack resources, robust insider threat programs, and enhanced data protection controls, potentially causing them to take a minimal check-the-box approach to maintaining compliance.

These types of challenges, furthermore, can apply to sensitive national security weapons platforms, commercial industrial machines, integrated circuits and their component pieces, and nearly everything in between.

The bottom line is that having a vigilant and proactive mindset and leveraging advanced threat detection capabilities to analyze the supply chain to identify potential threats and vulnerabilities across the entire ecosystem — and then applying a risk-based approach to mitigating them — is vital for our public and private sector clients.

4. See https://www.acq.osd.mil/cmmc/ for information on CMMC. All companies doing business with the Department of Defense will have to begin addressing CMMC in June 2020 for requests for information, and in fall 2020 for requests for proposals.

What Can Be Done to Reduce Supply Chain Risks?

Beyond the primary supplier (i.e., Original Equipment Manufacturer) and some major first-level suppliers and integrators, there is often limited, if any, visibility into the rest of the suppliers for a given program or product. For the most critical operational and safety components of a jet fighter, bomber, ship, energy plant, emergency response communications system, microprocessor, or switch or circuit, for example, being able to conduct thorough, independent illumination of the supply chain and then deep due diligence is crucial to identifying and mitigating threats and risks by answering questions such as, "Who are the suppliers? Who owns or controls them? Where did the parts come from? Are the companies financially stable? Do they have sufficient implementation of cybersecurity practices and an insider threat program? Have they had legal issues? Who are the key executives and what are their backgrounds? Where are their production facilities? What are the sources of their raw materials and partners and are they dependable?"

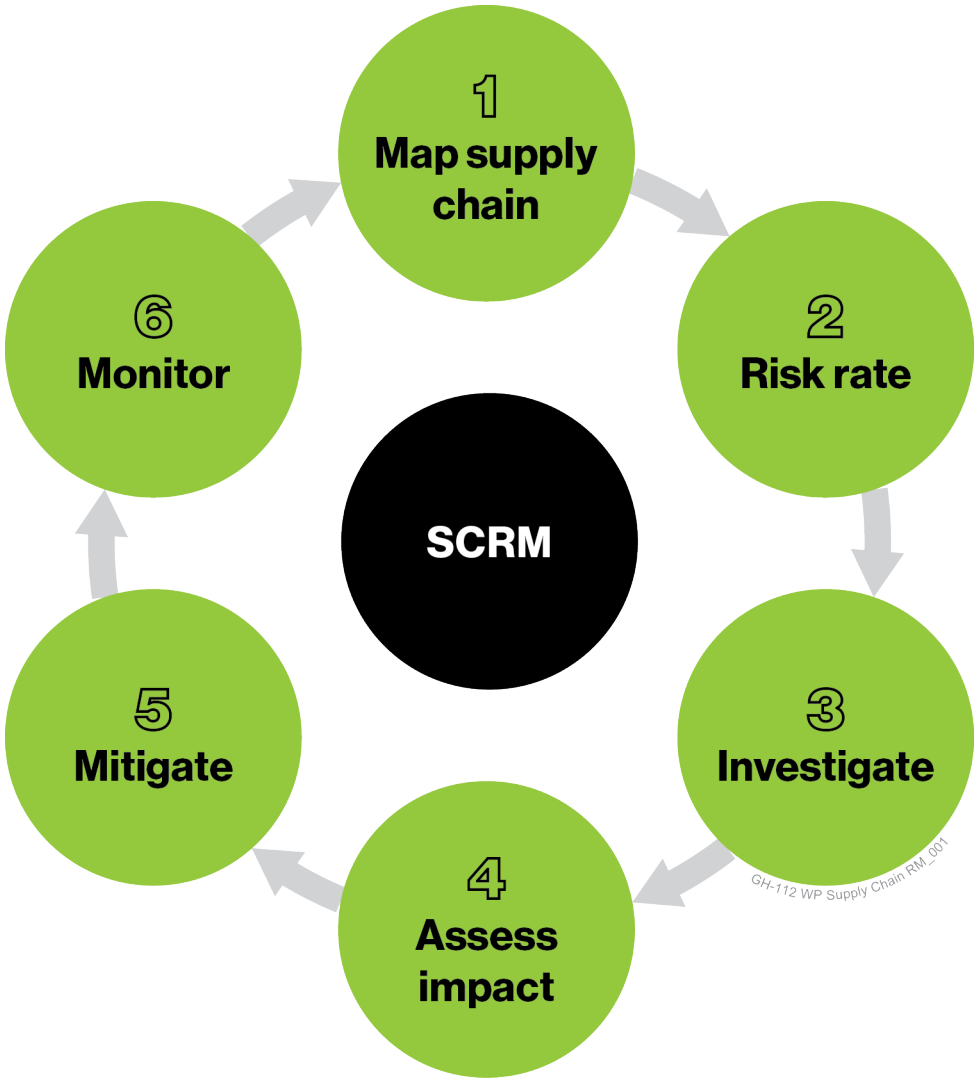
Representative U.S. Government Regulations and Laws

Committee on Foreign Investment in the United States (CFIUS) — as codified and expanded upon in the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) — requires covered transactions (those that could have an impact on national security) to be reviewed. These requirements and other government mandates necessitate that U.S. government officials and agencies enhance their supply chain security, and contractors working with the government to affirm the integrity of their supply chains. The key points are:

- This cannot be approached only as a U.S. government or policy compliance exercise for the public sector or designed to highlight one-off discoveries.
- Identification and analysis of vulnerabilities and threats should be incorporated into a broader strategy driven by requirements for operations, mission and business execution, efficiencies and cost savings, and success.
- This not only increases the security of a particular supply chain, but also translates into an enterprise-wide approach and the sharing of information across the department, agency or company.
- Drive enhanced capabilities and solutions throughout the system's or product's life cycle to detect and respond to supply chain threats, even saving taxpayers and shareholders money.

To help our clients address these vulnerabilities and risks for key systems and products, we apply a comprehensive SCRM analysis capability, illustrated in Figure 1, to include commercial best practices, and scalable and repeatable processes.

Figure 1. Guidehouse's Comprehensive SCRM Analysis Capability



SCRM Analysis Capability Steps:

1. ***Illuminate and map the supply chain*** to identify the parties involved, including suppliers, vendors, manufacturers, brokers, freight forwarders, and other service providers — and, more importantly, the suppliers' suppliers. This creates a "map" showing the entire supply chain for the system, component, or product as detailed as possible, often to the fifth tier or below (as warranted by the risk and available information).

2. ***Tailor risk ratings*** to determine the risk of third parties, those with controlling or influential interests, their location, and the activity they will perform. We work with clients to develop a customized set of risk factors to perform risk assessments on new or existing supply chain providers.

3. ***Conduct open source, commercial due diligence investigations*** to identify potential threats. Using analytical tradecraft and commercial best practices, our due diligence reviews help identify and verify factors such as beneficial ownership, business reputation, financial well-being, commercial practices, related business activities, business partners, disputes or litigation, USG contracts, relationships with foreign governments or individuals, sanctions or watchlist data, and civil or criminal investigations.

4. ***Assess the strategic impact*** and present results in analytical or other types of reports to the client specific to its supply chain. In some cases, there may be nothing of concern; in others, we may find adverse or even high-risk information, such as connections to a hostile foreign head of state, cyber breaches, counterfeiters, substandard parts, or other issues of financial or quality control concern.

5. ***Provide mitigation and remediation*** recommendations to address vulnerabilities or other deficiencies and threats, and work with our clients to implement changes as necessary. For example, we have recommended to some clients that they conduct penetration testing, change suppliers, perform continuous monitoring, enhance common minimum standards, carry out surprise inspections or periodic reassessments, provide referrals to law enforcement or intelligence, and issue warnings about or prohibit certain vendors.

6. ***Continuous monitoring of critical and sensitive components and entities*** is increasingly necessary and should be the standard across the most sensitive parts of national security- and key business-related supply chains. One-time reviews or "snapshots" are no longer adequate. ***Real*** continuous monitoring and evaluation of suppliers is necessary to inform stakeholders of changes to risks that may arise on an almost daily basis.

Serious attention must be given to protect the integrity and security of the supply chain, and not "bolt-on" measures that may not be successful. Instead, SCRM programs should feature concrete and tangible capabilities to help governments, critical infrastructure entities, and corporations secure vital programs, assets, products, lines of production and delivery, systems, and platforms.

Why Guidehouse?

Guidehouse LLP has the supply chain risk management capability, experience, skills, tools, data, and discretion to provide government and industry clients with the ability to develop insights into the business entities and individuals in their vendors' supply chains.

The data, other information, and analysis about those entities enables a holistic, informed understanding of potential risks so that real, effective and informed steps can be taken if problems are discovered.

Further, we are innovative and believe clients should share information across their enterprise to enable an enterprise-wide understanding of risks that may impact more than one part of their business or mission area.

Our work is automated — leveraging online searches, proprietary tools and data, and open source and subscription databases, as well as commercial best practices to refine our research. Our professionals drive and apply analytical tradecraft and automation based on their experience and specialized training to understand and present clear and actionable information to our clients in whatever form they require (e.g., dashboards, text reports, alerts, infographics, spreadsheets, bulk data files).

Our experts come from careers in industry and the government with a range of backgrounds that include supply chain security, corporate espionage prevention, information protection, legal and financial expertise, cybersecurity and technical know-how, research, intelligence, law enforcement, information analysis, insider threat, data analytics and science, and investigations.

Further, we follow strict guidelines and procedures to ensure all information is gathered and analyzed using industry best practices for unclassified, open source reviews. It is maintained and stored using regulatory compliant systems with cloud-encrypted, password, and need-to-know protection, and segregated stand-alone systems as necessary to protect the confidentiality and integrity of the data.

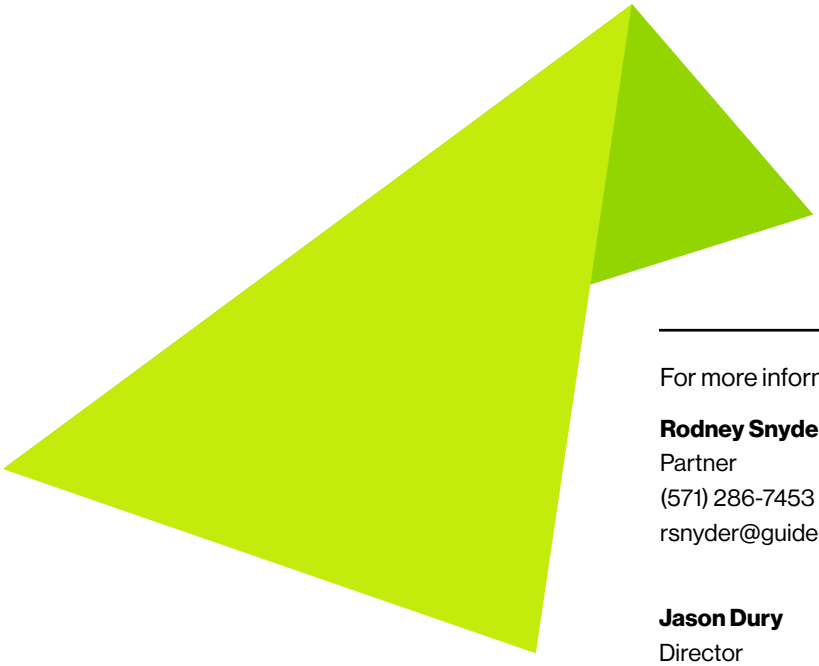
We are successfully delivering this capability right now to multiple, sensitive parts of the U.S. government and the U.S. industrial and technology base.

We've identified important potential risks and provided suggested remedies, as well as provided clients with confidence and the ability to report that they have a powerful and robust SCRM process, safeguards, and capability in place.

Company executives, as well as those on the outside looking in, such as board members, shareholders, or industry analysts, all value and sometimes require seeing these types of independent, powerful mechanisms.

We look forward to a further conversation if you are interested in our assistance to help secure your supply chains.

Guidehouse



For more information, please contact:

Rodney Snyder
Partner
(571) 286-7453
rsnyder@guidehouse.com

Jason Dury
Director
(703) 232-9203
jdury@guidehouse.com