Let's Talk Weapon System Supply Chain Risk Strategy

Logistics as the pacing function requires a Service supply chain risk management strategy

by Maj Julie Aho & Mr. Michael Cirillo

>Maj Aho works with Supply Chain Network Optimization, Headquarters Marine Corps Installations and Logistics.

>>Mr. Cirillo is the Strategic IT Initiatives Lead, Deputy to the Commander for Systems Engineering & Acquisition Logistics/Office of the Chief Engineer Marine Corps Systems Command.

Protecting the defense industrial base's ability to produce secure, capable warfighting capabilities for the Marine Corps is a shared responsibility. Supply Chain Risk Management (SCRM) is a critical force protection requirement not currently owned by any single deputy commandant or commander. Marine Corps weapons systems depend on low-end manufactured components that directly affect the security of our high-end weapon systems and information technology (i.e., hardware, software, and services) on which they rely. The Marine Corps depends on military-unique parts manufactured in a global economy, where the risk of counterfeit, illicit, and fraudulent parts is increasing. Without our knowledge, poorly made microelectronics, potentially exposed to manufacturing conditions vulnerable to malicious intent, can be manufactured into our weapon systems, introducing risk. The Marine Corps lacks the requisite expertise to effectively develop, design, code, test, operate, support, and defend the hardware and software in our weapons systems, which is a major gap in our acquisition process. To help leadership understand the importance of establishing a single SCRM program across the Marine Corps, this article justifies the rationale and describes SCRM best practices.

Protecting the Marine Corps' industrial base of suppliers requires a single point of accountability. While many claim interest, responsibility, or ownership of a component of SCRM, the Marine Corps lacks enterprise acquisition and sustainment oversight. There is no forcing function, acquisition-specific process, or policy to assist in identifying, avoiding, mitigating, or reducing supply-chain risks.

Protecting the Marine Corps' industrial base of suppliers requires a single point of accountability.

Since the 2021 release of Executive Order 14017 on Securing America's Supply Chains, DOD components and agencies have stood up and are taking proactive actions across critical material sectors of defense. In 2022, DOD initiated the development of SCRM policy and guidance to include a common framework and taxonomy, including definitions and a list of 12 risk categories and 124 sub-categories. In November 2022, the Office of the Deputy Assistant Secretary of Defense for Logistics published a record of initial discussions among DOD, industry, and academia, which included three definitions of SCRM. Later in 2023, the Deputy Secretary of Defense, via the Office of Industrial Base Policy, will be releasing a data call to all Services to collect data on all prime contractors and first- and second-tier suppliers for specific weapon systems to guide acquisition and sustainment strategies, policies, and risk mitigation.

A recently published document signed by the Commandant of the Marine Corps that specifies lines of effort across Installations and Logistics priorities through 2030 fails to account for SCRM actions across the Service. This is likely attributed to the fact that not many leaders are familiar with or bear responsibility for SCRM. Under the direction of the Deputy Assistant Secretary of Defense for Logistics, the DOD has proposed the following definitions to inform DOD SCRM Policy.

- *Supply Chain Resilience.* The capability of supply chains to respond quickly to unexpected events, adapt to

changes, and ensure continuity of operations after a disruption. Resilience is the outcome of proactive Supply Chain Risk Management and supply chain security.

- *Supply Chain Risk Management.* A process of proactively identifying supply chain vulnerabilities to potential disruptions and implementing mitigation strategies and actions to ensure the security, integrity, and uninterrupted flow of products as risks are found, or disruptions occur.
- *Supply Chain Security.* The application of policies, procedures, processes, and technologies to ensure the security, integrity, and uninterrupted flow of products while moving through the supply chain. Examples include the ability to protect supply chains from cyber infiltrations and the introduction of counterfeit material.

No formal SCRM program exists in the Marine Corps, as evidenced by our lack of a data repository of all our suppliers and their global sub-contractor base. Analysts cannot quickly quantify risk when foreign ownership, control, or influence is detected in our programs and systems. The Deputy Commandant for Plans, Policies, and Operations currently oversees the Marine Corps program related to the Committee on Foreign Investment in the United States. Today, the Marine Corps is highly dependent on the work of other Services to detect Committee on Foreign Investment in the United States cases that put our programs at risk. One such risk area resides in the defense sector known as the Information and Communications Technology (ICT) industrial base. An ICT product is defined as a commercial end-item that stores, retrieves, manipulates, transmits, or receives information electronically in an analog or digital form. ICT products exist in every acquisition item that contains a microchip. The numbers and types of devices requiring a microchip for a digital network are increasing at an incredible rate—thus, our risk exposure is increasing with force modernization.

Consider the following vignette. The deployment of a newly formed Marine Littoral Regiment depends on the prime vendor of a new acquisition program delivering on time and in full. A major hurricane is approaching an area that manufactures parts of a sub-assembly. The prime vendor notifies the Marine Corps of the expected disruption to assembly and delivery. Because the Marine Corps has proactively stood up and funded an SCRM program, a smart civilian analyst begins running the SCRM model and playbook for the Advanced Reconnaissance Vehicle. Because the Marine Corps prioritizes data initiatives that inform decision making, the analyst is quickly able to perform supply chain impact analysis with optimization/simulation of the prime vendor's multi-tier manufacturing supply chain of the components at risk, thanks to our Service's SCRM policy that requires Program Managers to develop SCRM playbooks in partnership with the vendors and obtain data rights to suppliers. The analyst determines that the hurricane will cost the Marine Corps $400,000 more to have the prime vendor switch to an alternate supplier. The commander of MARCORSYSCOM receives the analysis, which was completed in a matter of hours, and assesses the $400,000 cost to switch suppliers as a worthy course of action to avoid a four-month delay in the fielding of the Advanced Reconnaissance Vehicle.

Today, the Marine Corps is highly dependent on the work of other Services to detect Committee on Foreign Investment in the United States cases that put our programs at risk.

There are three industry-proven digital SCRM concepts applicable to the Marine Corps. They include:

- Artificial Intelligence (AI) mapping of the supplier base.
- Validated multi-tier supply chain mapping of the supplier base.
- Model-based risk profiling by location/node of internal supply chains.

The first best practice of SCRM is AI (or autonomous) mapping of the supplier base. Commercially available AI mapping encompasses years of supplier intelligence harnessed from public domain sources. These technologies use AI to collect information on the most likely suppliers of a weapons system. AI analyzes billions of records and has the power to scan the web for part-level and site-level insights. AI mapping also provides the benefit of being able to automate product teardowns to get the most accurate parts and suppliers used three tiers deep in the supply chain. Industry has already mastered the analytic techniques to find such data, clean, de-duplicate, and normalize noisy data to create usable insights. While AI mapping of our suppliers is a great way to rapidly gain insights and visibility into the supply chains of our weapons systems, it also comes with a surplus of irrelevant data that is not verified. Therefore, it should not be thought of as a single-source solution to SCRM but as an insightful tool in the toolbox. Under the Office of the Under Secretary of Defense for Acquisitions and Sustainment initiative, a software-as-a-service provider is providing illuminations across weapons-system-supplier bases to provide AI mapping to MARCORSYSCOM and other DOD Program Managers. The illuminations have provided invaluable information that includes:

- Identify foreign ownership, control, and influence.
- Quantify environmental, social, and government risks.
- Report reputational, criminal, and regulatory risks.
- Monitor financial health.
- Evaluate cyber risk.
- Quantify operational risk.

Another SCRM best practice is multi-tier supply chain mapping of the supplier base. This approach requires validating suppliers at different levels (or tiers) throughout the supply chain.

Unlike AI mapping, multi-tier mapping involves supplier-validated data—providing a more accurate picture of the supplier base. Multi-tier mapping seeks to improve the reliability of deeper-tier supplier data. Under a well-developed SCRM program, the Marine Corps would be able to align suppliers identified through multi-tier mapping with our internal digital supply chain models to quickly analyze data to determine alternate sources of supply for deployed naval expeditionary forces. Below is a graphic of what multi-tier supply chain mapping looks like.

Visibility is key to supply chain resiliency. Achieving visibility is time-consuming. Does MARCORSYSCOM have the time to reach out to each supplier across joint programs and maintain updated data? Because this task is so daunting, SCRM programs across the DOD have been quick to rule out multi-tier supply chain mapping and opted for AI mapping instead. AI mapping is a good first step, but the goal should be to achieve multi-tier supply chain mapping of the supplier base. Industry is paving the way in developing best practices to digitally map their supply chains, and many of these commercial software vendors are ready to do business with the DOD.

The third best practice of SCRM is model-based risk profiling by location/node of the internal supply chain. This approach uses a deliberate approach through supply chain design concepts to measure and quantify supply chain risk. *Force Design 2030* calls upon the Service to ensure the sustainment of distributed forces in a contested environment. While everyone has been talking about modeling and simulation for contested logistics, few understand the purpose. The ultimate goal and purpose of digitally modeling and simulating contested logistics are to define, measure, analyze, improve, and control the continuity of the supply chain such that sustainment objectives are not inhibited. Once contested logistics scenarios (e.g., loss of a port, loss of a supply node, or loss of transport) are quantified in terms of risk, the information can be used to prioritize real-world risk mitigation actions to

Figure 1. Six dimensions of supply chain supplier risk. *(Source: Exiger, Supply Chain Management Products, GSA Contract for U.S. Government.)*

The ... purpose of digitally modeling and simulating contested logistics are to ... control the continuity of the supply chain such that sustainment objectives are not inhibited.

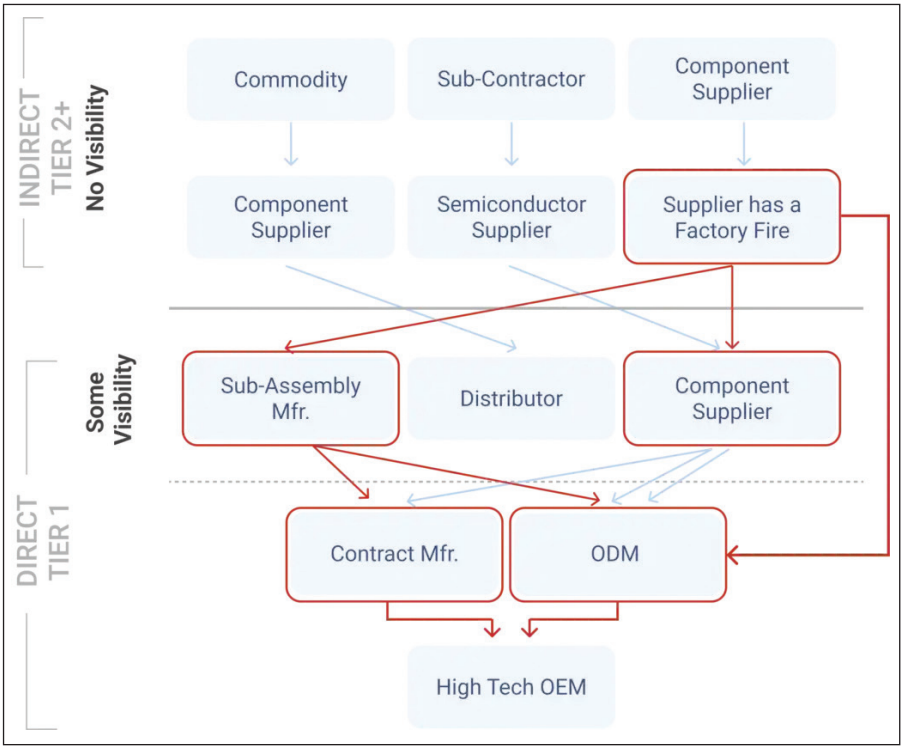

Figure 2. Multi-tier supply chain mapping. *(Source:* **Resilinc**, *"Multi-Tier Mapping vs. AI Mapping: What's the Difference?")*

Figure 3. Measuring risk to build a resilient supply chain. Identifying risky aspects of the Marine Corps supply chain network, understanding potential contested logistics scenarios (disruptions), and using the design process to mitigate and reduce risk is an essential part of creating a resilient supply chain. *(Source:* **Optilogic**, *Take a Proactive Approach to Risk Identification and Mitigation.)*

minimize the impact of disruptions. Instead of spinning our wheels, bleeding money, and trying to develop our own proprietary predictive analytics software for logistics, the supply chain software market is a multi-billion-dollar industry that has reinvented this problem based on lessons learned during unprecedented times of demand and supply variability.

Today, supply chain vulnerabilities across Marine Corps ground weapon systems go unnoticed because it is often unclear who is in charge of managing risk when it comes to relationships with suppliers and third-party vendors. Even if it is known that a supplier may have vulnerabilities, a problem may never be addressed as there is no designated person or team with the responsibility to manage a vendor. This problem is not unique to the DOD. Even the largest corporations have minimal teams for SCRM. However, industry is much better resourced to manage the challenges presented by supply chain failures, while the Marine Corps is not so adept at doing so and does not operate agilely. Relying on program managers to develop, implement, and manage SCRM from the ground level up is sub-optimal. Partnering with our original equipment manufacturers for data rights and supplier information is essential. The Marine Corps must develop and adopt a Service SCRM strategy to manage supply chain risks. Delegating SCRM to tactical or regional commanders does not enable us to take advantage of economies of scale. Logistics modernization is progressing slowly because unilateral and uncoordinated actions across commands remain largely unknown to others. It would be difficult to ensure SCRM is adhered to if not managed through a Service strategy and centrally funded.

Figure 4. Foreign ownership, control or influence (FOCI) indicator chart. The National Counterintelligence Strategy states that China is increasingly asserting itself by stealing our technology and intellectual property in an effort to erode U.S. economic and military superiority and that Russia remains a significant intelligence threat to U.S. interests. *(Figure provided by author.)*

SCRM is a critical force protection requirement that requires attention, prioritization, and resourcing. SCRM is a large problem set that spans all Services and agencies within the federal government, intertwined between departments and the defense industrial base. Given its relevance to achieving global logistics awareness, SCRM funding ideally belongs in the Deputy Commandant for Installations and Logistics' portfolio. The Assistant Secretary of the Navy for Research, Development, and Acquisition is appointed to the Office of Primary Responsibility for four major lines of effort to align the Navy with DOD SCRM initiatives. Given the current DOD emphasis on SCRM across material sectors critical to national defense, particularly ICT products, MARCORSYSCOM (the acquisition authority for Marine Corps for ground weapon systems and information technology) is well positioned to lead SCRM. CMC/ACMC should appoint and effectively resource MARCORSYSCOM to stand up and lead a Marine Corps SCRM Program. MARCORSYSCOM, as Office of Primary Responsibility, would lead the development of an SCRM framework on behalf of DC I&L, aligned to the Navy for Research, Development, and Acquisition's efforts underway.

In summary, protecting the defense industrial base's ability to produce secure, capable warfighting capabilities for the Marine Corps is a shared responsibility. We need a single office or individual accountable for SCRM, to define the roles and responsibilities, and effectively resource goals and objectives. Until such a time when an SCRM strategy manifests, the Marine Corps will remain amateur at best when it comes to SCRM execution. Competing interests no doubt influence near and long-term objectives, but *Force Design 2030* must include a concerted approach to protect our supply chains.

USMC