CENTER FOR SPACE POLICY AND STRATEGY

MAY 2020

MANAGING THE FUTURE STATE OF SUPPLY CHAIN RISK

LORI W. GORDON
THE AEROSPACE CORPORATION

AEROSPACE

LORI W. GORDON

Lori W. Gordon is a technology strategist in national and homeland security, cybersecurity, and infrastructure risk and resilience at The Aerospace Corporation. She is an advisor to ISO, ANSI, and NIST technical working groups and is a visiting fellow at the National Security Institute. She has also served on curriculum advisory boards in the areas of cybersecurity and infrastructure security, law and government, and resilient design. Lori has a bachelor's degree in geography from the University of Maryland, and a master's degree in public administration from the University of Massachusetts, Amherst.

ABOUT THE CENTER FOR SPACE POLICY AND STRATEGY

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

Contact us at www.aerospace.org/policy or policy@aero.org

Summary

Threats from adversaries and natural disasters can disrupt supply chains, challenging organizations to respond effectively. Policies and guidance are important, but they are also piecemeal and almost immediately out of date. To effectively counter modern supply chain threats, organizations must be flexible and have a standing ability to respond. Fundamentally, this requires a culture of collaboration guided by a framework that can highlight the current and targeted states of supply chain risk management (SCRM) governance, information sharing, risk tolerance, process, and technology practices.

When applied to government organizations, the SCRM collaboration framework has illustrated widely varying levels of maturity, not only at the enterprise level, but also among an organization's divisions, and down to the program levels. This is due to a variety of factors: emerging threats (e.g., Huawei and COVID-19) that are differentially affecting a wider array of sectors and organizations; an organization's size, centralization, or geographic distribution; and an organization's involvement in partnerships, such as information sharing and analysis centers (ISACs), and inter-organization agreements.

To get ahead of a constantly shifting threat environment, organizations can mature institutional collaboration to better manage the future state of supply chain risk.

Introduction

Over the last decade, new adversarial as well as naturally occurring threats to global supply chains—from Huawei to COVID-19—have evolved rapidly, destabilizing economies and making long-term geopolitical outlooks less certain. National and organization-level policies have tried to keep pace, requiring organizations to increase scrutiny of their supply chains for critical products, materials, and services. This requires not just significant investment in risk management practices, but also confidence that those investment decisions are informed by valid, actionable data. Access to information about risks requires tapping a range of sources. To facilitate access and exchange of this critical information, organizations can take the significant step of establishing a cross-cutting supply chain risk management (SCRM) function. To do this effectively, an approach to drive functional collaboration *within* the organization and *across* peer organizations can be put into place. A SCRM collaboration framework can provide organizations with a roadmap to build and execute their SCRM function and to more easily and quickly comply with new requirements from Congress and their organizations.

This paper lays out a number of threats that are increasingly affecting organizations' supply chains. It discusses key federal guidance that has been put into place to help manage those threats. Finally, to complement that guidance, this paper provides a framework to help organizations understand where they are in the process of maturing their governance, risk tolerance, processes, technology, and information-sharing through the context of intra- and inter-organizational collaboration. The framework has five different levels of maturity in ascending order: inquiring, exploratory, established, adoptive, and extensible. The higher the level, the greater the organization's collaboration and integration of internal and external resources and capabilities to manage supply chain risk.

Threats to Supply Chains

SCRM has traditionally focused on managing weaknesses in product lifecycles, such as defects introduced through mistakes or negligence that result in deficiencies, vulnerabilities, or degraded lifecycle performance. It also focuses on failure in aging devices, market risk and resiliency issues from sole-sourced suppliers, long lead times, and counterfeit risk from relabeled, recycled, cloned, defective, or out-of-spec devices.

However, supply chains must also brace against well-funded and targeted attacks by malicious actors who exploit highly interconnected networks to gain access to sensitive and proprietary information and intellectual property (IP). The insertion of malicious components and coding could cause mission failure.

Naturally occurring, systemic threats such as hurricanes or pandemics can shut down operations altogether, compromising the stability of the workforce.

These challenges to national security and homeland security operations have far-reaching economic and geopolitical impacts. As we speed toward 5G, and even thinking to 6G, we may be vulnerable to suppliers who work backdoors into the microelectronics that make up our systems of systems—from supervisory control and data acquisition (SCADA) that manage energy grids to constellations of satellites. Suppliers that produce parts and materials for national security operations will increasingly overlap with those that produce parts and materials for commercial space. During the COVID-19 pandemic, shortages in essential supplies such as personal protective equipment have been felt across multiple industries, including the national defense and medical sectors.

Managing our supply chain risk will become more crucial as we evolve the infrastructure that enables our national critical functions such as positioning, navigation, and timing (PNT) services; cargo, material, and passenger transport; and consumer and commercial banking services. Newly integrated technology including space-based solar power, synthetic chemicals, precision medicine and robotic surgery, and 3-D and 4-D printing will incorporate a range of component parts and processes creating an even larger threat plane. Their supporting supply chains will require a more deliberate and dedicated level of risk management than is currently practiced by government and industry.

Policy Response

Over the years, these supply chain threats have energized Congress, the White House, executive agencies, and other international bodies[1] to respond with new policies. These policies have focused primarily on four areas: SCRM roles, threat evaluation, information sharing, and supplier restrictions.

SCRM Roles

Early guidance focused on roles: who had responsibility for what. In 2012, the National Institute for Standards and Technology (NIST) produced NIST Interagency Report (NISTIR) 7622, which recommended establishing diverse SCRM

teams. These teams included staff involved in procurement, production, and distribution for awareness of adversary attack methods, preventative tactics, and legal aspects.[2]

In April 2013, NIST went further. It produced Special Publication (SP) 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which established "baseline" controls for SCRM-related roles and included rules for ensuring legitimate suppliers and security protocols in shipping, warehousing, and operations. Fast-forward to May 2020 and NIST's fifth revision of NIST SP 800-53, which adds SCRM controls to its program management family and establishes a new supply chain risk management family. The fifth version also aligns to NIST SP 800-161 and the Committee on National Security Systems Directive (CNSSD).[3]

Supply Chain Threat Evaluation

As the volume of suppliers entering markets expands, so is the need to scrutinize business relationships and ensure transparency to limit technology or process vulnerabilities in products or services. In April 2015, NIST issued NIST SP 800-161, *SCRM Practices for Federal Information Systems and Organizations*, which sought to standardize SCRM practices to better measure and manage supply chain risk across different organizations. SP 800-161 provides guidance for identifying, assessing, and mitigating risk in supply chains and integrating the SCRM process as part of an organization's overall risk management program. It also describes organizational functions (e.g., legal, procurement, information security, and logistics) that are necessary for conducting holistic supply chain risk management.[4]

In April 2018, NIST updated its *Framework for Improving Critical Infrastructure Cybersecurity*, also known as the Cybersecurity Framework—a voluntary framework for reducing cyber risks to critical infrastructure—to include SCRM-related provisions to help users better understand how to evaluate cyber threats to supply chains and risks associated with commercial off-the-shelf products and services.[5]

Supply Chain Information Sharing

As threats have become more complex, it is more important than ever to share indicators and warnings. In July 2016, the Office of Management and Budget (OMB) revised Circular A-130, "Managing Information as a Strategic Resource" to update governance, acquisitions, records management, open data, workforce, security, and privacy provisions and encourage agencies to shift from a compliance approach to a strategic and continuous risk-based approach to information management.

In July 2018, the Department of Homeland Security (DHS) announced the establishment of the National Risk Management Center (NRMC), which stood up a task force to bridge government and industry and develop processes, policy recommendations, and evaluation criteria to reduce near- and long-term supply chain risk.

Restrictions on Suppliers

Even more recently, policy has focused directly on the suppliers, including banning certain suppliers. Section 889 of the National Defense Authorization Act for Fiscal Year 2019 mandated that no executive agency could procure or obtain any telecommunications and video surveillance equipment and services provided by Huawei—a Chinese-owned firm whose aims impose security and privacy risks to the U.S.—or other named organizations.

In December 2018, NIST updated its Risk Management Framework (RMF 800-37)[6] to address untrustworthy suppliers, insertion of counterfeits or malicious code, tampering, unauthorized production, theft, and poor manufacturing and development practices in system lifecycles.

Also in December of that year, Congress passed the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (the "SECURE Technology Act"), which strengthened the DHS' cyber defense to mitigate supply chain risks in the procurement of information technology by providing some agencies with the authority to issue exclusion and removal orders as to sources and/or covered articles.[7] It required each agency to establish a SCRM program that meets SCRM criteria established by a new Federal Acquisition Security Council (FASC).[8] The SCRM collaboration framework described later in this paper can assist those agencies and the organizations supporting their supply chains to reduce supply chain risk.

In May 2019, the White House went further and issued the *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*, which declared a national emergency from "foreign adversaries" seeking to create and exploit vulnerabilities in U.S. information and communications technology and services. It addresses the use of technologies from certain types of foreign companies in U.S. communications networks and block those transactions and designates DHS to assess components that pose the greatest threats to the national security of the United States.[9]

Around the same time the executive order was issued, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) added Huawei (and Huawei-affiliated entities located in 26 countries) to the Entity List, which is a "list of foreign entities that have engaged in activities that could result in increased national security risk and that are subject to specific license requirements for the export of specified items."[10]

Figure 1 shows the policies and standards described in this section and categorizes them according to the four broad themes: roles, threat evaluation, information sharing, and supplier restrictions.

A Collaborative Approach

While policy responses and guidance are important, they are also piecemeal and almost immediately out of date. To effectively counter modern supply chain threats, organizations must be flexible and have a standing ability to respond.

Agencies are attempting to do this by producing their own policy aligned to federal guidance. For example, the Office of the Director of National Intelligence (ODNI) published Intelligence Community Directive (ICD) 731, "Supply Chain Risk Management," in 2013 and subsequent guidance: "Supply Chain Criticality Assessments," "Supply Chain Threat Assessments," "Supply Chain Information Sharing," and "Supply Chain Vulnerability Assessments,"[11] which generally follow the sequence of themes presented in Figure 1. Department of Defense (DOD) and civil agency guidance include DOD Instruction (DoDI) 5000.02 "Operation of Defense Acquisition System,"[12] and 5200.44, "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks,"[13] and NASA's PR 7120.5.

However, these policies and directives need to be taken a step further to emphasize a collaborative approach to supply chain risk management. An organization must engage its procurement, acquisition, general counsel, counterintelligence, security, and other functions to address supply chain. It must also engage with other sources of knowledge and capabilities (e.g., supplier counterintelligence or open source threat information sharing), which may be found in peer organizations. This level of collaboration is hard to do without a guided approach or framework to help formalize and mature intra-organization and inter-organization collaboration processes.

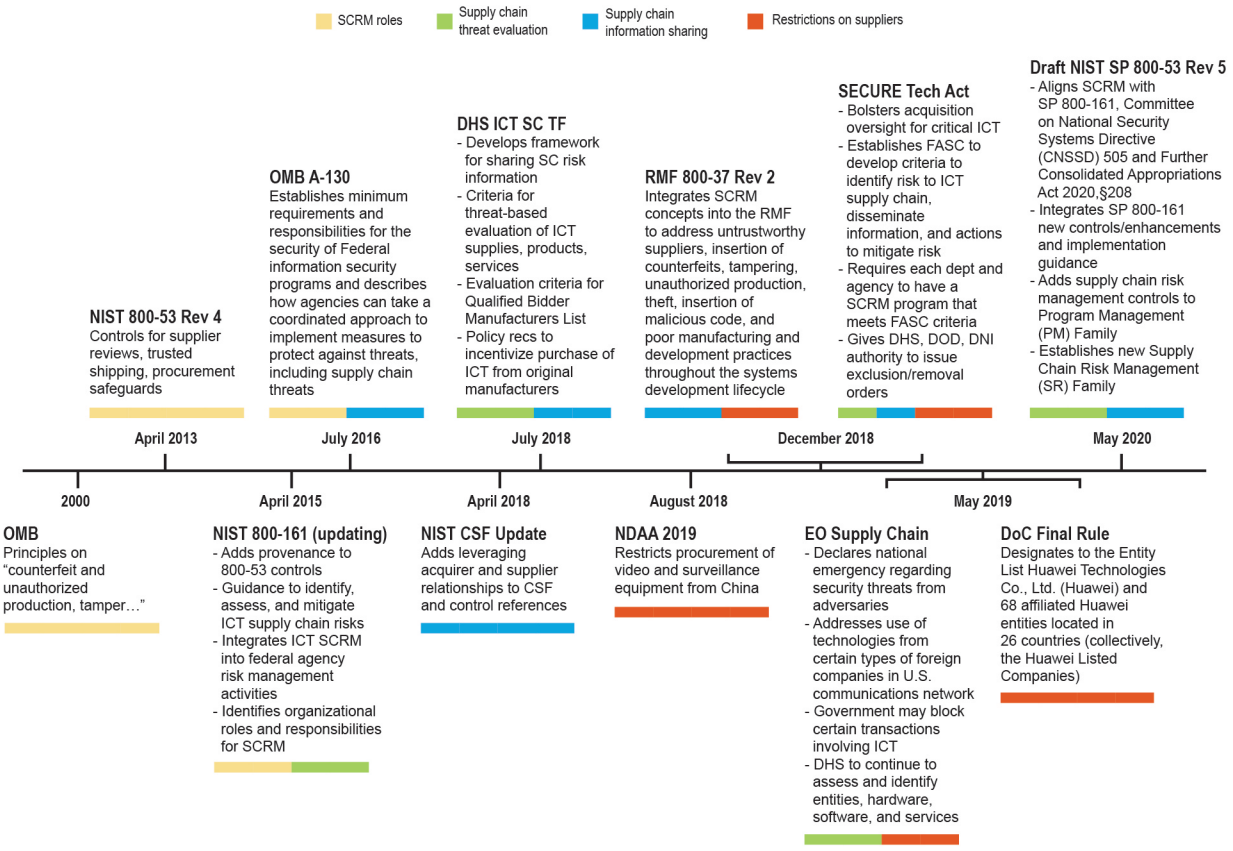

Figure 1: SCRM policy and guidance.

A Collaboration Framework for Supply Chain Risk Management

The evolution of SCRM guidance, practices, and processes over the past decade (i.e., roles, threat evaluation, information sharing, and supplier assessment and restrictions) cannot be accomplished without significant collaboration across the organization (procurement, security, counterintelligence, etc.) and across its peer network. A growth framework can provide a roadmap to achieve the needed collaboration.

One type of growth framework is a maturity model. A maturity model is an assessment tool for evaluating an organization's level of progress toward a goal. It contains criteria that will be evaluated and capabilities that are exhibited by an organization at each level of development. It can be used to provide an organization with an initial benchmark for how close to "fully developed" it is with regard to the criteria being assessed. It is a tool for leading discussions, prioritizing investment, and providing management with a roadmap for the next steps. Maturity models have been developed for other domains to facilitate adoption of improved cybersecurity, product quality, workforce, and risk management practices. Examples of maturity models include the following:

- Carnegie Mellon University (CMU), Software Engineering Institute's (SEI's) Capability Maturity Model Integration (CMMI), which evaluates an organization's ability to develop and refine the software development process.

- CMU and Johns Hopkins University Applied Physics Laboratory's Cybersecurity Maturity Model Certification (CMMC) to assess and enhance an organization's cybersecurity posture; levels range from "Basic Cybersecurity Hygiene" to "Advanced."

- Information Technology Infrastructure Library's (ITIL) model to standardize the selection, planning, delivery, and maintenance of IT services and achieve predictable service delivery; levels range from general lack of knowledge (0) to a working environment in which best practices have been fully integrated and optimized (5).

- An IBM model to define the extent to which automated subprocess components represent a unit of work done as part of a specific business function.

These models can consist of multiple processes and practices that are organized into a set of domains and mapped across maturity levels with specific capabilities within each domain. The models also reference processes and best practices from standards, frameworks, and other guidance.

The collaboration framework presented in this paper is less complex. With five collaboration areas across five levels it provides a benchmark for an organization to evaluate its current level of capability and to set goals and priorities for improvement. It can help an organization understand how mature its practices are and therefore how effectively it is reducing supply chain risk.

The SCRM collaboration framework draws from the SCRM policies and guidance that are referenced in this paper to establish five main areas of collaboration: governance, risk tolerance, processes, technology, and information sharing. The steps needed to mature each of these areas are shown from Level 1 (the Inquiring organization) to Level 5 (the Extensible organization). As an organization improves along each of these collaboration areas, its overall SCRM will improve. However, they will improve in differing ways depending on what collaboration areas they emphasize and how far along each organization is in each area.

These levels are shown in Figure 2 and described in Table 1.

Although it may appear in Figure 2 that the growth of the SCRM function could require additional resources, this cost is in part mitigated due to near- and/or longer-term risk reduction.

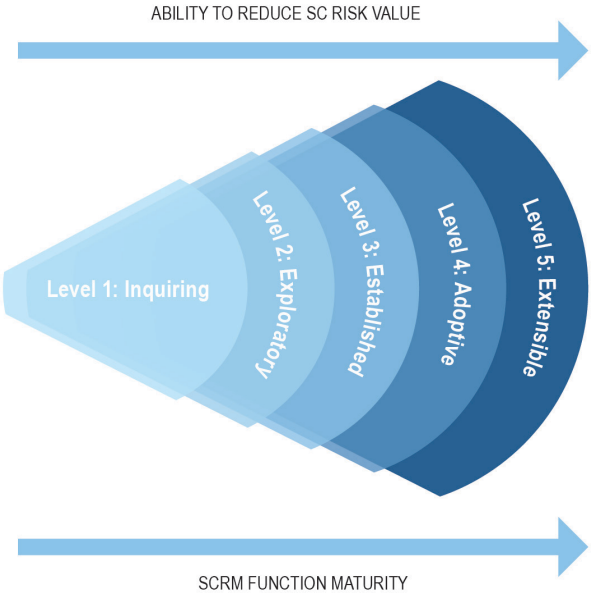

Figure 2: SCRM collaboration framework.

Table 1: Collaboration Framework Phases

Collaboration Areas		SCRM Collaboration Levels				
		Inquiring	Exploratory	Established	Adaptive	Extensible
Governance	Leadership	No SCRM leadership defined	SCRM leadership in place	SCRM leadership engaging with internal collaborators	SCRM leadership engaging externally and building network; collaborator roles communicated	External leadership partnerships in place and leveraging as necessary
	Documentation	No artifacts developed	Enterprise SCRM governance approach in development	SCRM function chartered (see Appendices B and C) and in early implementation	Interagency agreements in place (see Appendix C); governance practices implemented and exceed minimum performance/ compliance requirements	Governance practices recognized by others as the highest standard; roles have grown and evolved, with ability to surge as necessary
Risk Tolerance/Posture	Classification	No risk classifications identified	Risk classification and tolerance criteria identified	Risk tolerance classifications applied	Risk tolerance classifications shared with peer agencies	Risk tolerance classification adapted to enhance broader interagency risk goals
	Action	No response to risk	Respond reactively to risks	Proactively identify risk	Proactively anticipate and prepare for anticipated risk (both enterprise and edge)	Able to protect against risk by taking calculated risks and share/synchronize risk
Process	Action	No process enacted	Informal process	Formal process	Repeatable process with controls established (i.e., SCRM language) is included in the procurement process and attestation processes ensure validity of data based on agreed-upon criteria	Validated data based on legal or authoritative references (e.g., hearings, reports, and engineering journals) are agreed upon and shared across organizations

Table 1: Collaboration Framework Phases (cont.)						
Collaboration Areas		SCRM Collaboration Levels				
		Inquiring	Exploratory	Established	Adaptive	Extensible
Technology	Infrastructure	No technology procured	Threat information sharing platforms identified	Technologies selected	Technology and networks in use	Continuous/improved use to achieve targeted results
	Action	Not able to access platforms	Identifying people/staff needed to operate technology	Able to access restricted and nonrestricted platforms	Able to share/educate/train on platforms	Enhanced sharing/education/ training
Information Sharing	Type	No data types identified	Criteria for data is identified	Data is identified that should be shared with internal organizations	Guidelines for sharing data within and outside the organization are established	Data informs shared decisions among collaborators/partners/ peers
	Action	No information sharing	Looking for a repository to ingest information	Some internal data sharing, data is informing decisions	Organizations are identified for external sharing and arrangements are established for sharing	Data informs shared decisions among collaborators/partners/ peers

The Inquiring Organization

In the Inquiring organization stage, no formal SCRM function has been established yet, and, accordingly, no organizational governance, risk posture, process, technology, or information-sharing platforms or channels have been developed. SCRM-like functions may exist in distributed parts of the organization, but they have not yet coordinated across the organization or have evolved into an enterprise function. Threats may be profuse across hardware and software, requiring a range of detection, assessment, and mitigation technology, processes, and information sharing that does not yet exist.

While organizations at this phase are aware of the legislative mandates placing requirements on them (see Figure 1), they may have less understanding about what resources and capabilities are required to conduct the work. Because of the uncertainty, management may require a somewhat rigorous business case to establish the SCRM function. At this stage, manager resistance may be strongest as resources and capabilities have yet to be established and proven. It is likely that a SCRM lead will be established to conduct this exploratory research.

The Exploratory Organization

In the Exploratory organization stage, the organization has established a formal SCRM lead (see Appendix A) to begin to clearly define the high-level threat landscape and any existing posture and processes for addressing supply chain risk.

The SCRM lead is spending more time understanding where pockets of mature SCRM processes exist across the organization in an informal distributed model (e.g., a regional office may independently conduct SCRM activities). The lead is identifying what capabilities (e.g., intelligence, legal, logistics, and procurement) it must leverage at the enterprise level to define an enterprise SCRM process, governance, risk tolerance, and technology and information sharing needs. It is also assessing external organizations' SCRM functions for best practices and getting a shared understanding of terms, including what *trusted* means in terms of parts or services.

The organization may still be in "response" mode as the SCRM function has not yet formalized these internal or external partnerships or collaborative processes that would enable it to take a proactive approach with managing supply chain risk. However, as the SCRM lead has gained formal executive sponsor support in this phase, change management processes needed to instantiate the function into the organization are being created.

At this stage, the organization may be relying on ad hoc threat and vulnerability data collection while it strives for a systematic and efficient collection capability. To get to the point at which capability is in its minimum useful state, referred to as *initial operating capability* (IOC), the organization must be able to identify needed technologies (e.g., vulnerability identification) and information sources (e.g., open source and classified counterintelligence).

At this phase, the organization is considering goals and objectives for reducing risks and exploring metrics. To move to the Defined stage, the SCRM function must finalize governance principles and a charter (see Appendix B) to set strategic direction and vision. The organization should be able to see where the SCRM function can benefit it as a whole. The value gap for the SCRM function begins to close as its collaborations and partnership engagements rise. SCRM champions are increasing their campaign, and getting others to recognize that achievement of the organization's mission will improve as the SCRM function matures.

The Established Organization

Now at IOC, the SCRM lead is engaging with internal collaborators through information-sharing mechanisms. The formal SCRM function has been chartered and integrated into the organization's routine operations. A general risk tolerance level has been established, and the organization has moved from a response to advanced threat identification mode. This is because the organization is sharing internally, and it is leveraging (and monetizing) systematic and efficient data collection to inform risk assessments. This means that there is a collection team in place that knows how and from where to collect threat data (as opposed to the ad hoc team, which tries to figure it out as the need arises) and has a centralized repository that they continue to update so when a new "customer" asks for data or an existing customer needs a refresh, they have the data available.

In the Established organization stage, while the SCRM function has clearly defined roles and responsibilities, it needs to ensure it is measuring adherence to the strategy. To progress to the Adoptive stage, organizations must communicate their vision and direction for collaboration and start implementing all that was launched in the SCRM function's Established stage. The organization should be realizing the value of collaboration to reduce supply chain risk. The SCRM function has been defined, and the organization is ready to implement it.

The Adoptive Organization

The SCRM lead has now reached out externally to build a network and has had success championing and getting cross-organization buy-in for the SCRM function and working toward interagency agreements in reciprocal information and intelligence sharing (see Appendix C).

Risk tolerance is now better understood and differentiated where it makes sense, such as having different risk tolerances at the enterprise level and at the edge. Risk posture is now focused on anticipating and preparing for threats, rather than just identifying risk. Command media and controls have been established in the procurement process (i.e., through the addition of questions such as: Who are your suppliers? What formal security programs do they employ? Where are their manufacturing and fabrication facilities located? Who are their second- and third-tier suppliers, and where are they located?). An attestation process is in place to evaluate and review the data and information used to answer these questions to ensure validity and alignment to achieve a stated risk management policy or criteria to ensure security, availability, or integrity. The SCRM lead is growing the SCRM function to accommodate the level of supply chain risk assessment demanded by the organization.

The integration of technology and information sharing processes have been instantiated, as the SCRM function and collaborating/contributing capabilities across the organization have access to sensitive compartmented information facilities (SCIFs), information-sharing platforms, etc., on demand. The organization is using data to make decisions.

At the Adoptive organization stage, the organization is in the process of full implementation. The organization construct has been established, the vision has been communicated, measures of success have been established, and strategy has been developed. Staff resistance may be greatest at this stage as they integrate new strategies and technologies. In the collaborative process, staff is able to share data-driven information, and information is easier to find and share as needed functions are working in trusted relationships.

The Extensible Organization

The organization is now a role model for collaboration, with all processes and technology meeting required goals and objectives. SCRM roles have grown and evolved, with expansion as

necessary—even to accommodate needs from other agencies via interagency agreements.

The organization now has a shared risk tolerance with other agencies and is focused on supply chain risk prevention, rather than identification, preparation, or mitigation. It has essentially moved to "left of boom" and the incident management lifecycle. Threat assessments are utilizing counterintelligence as well as open source information, with robust documentation that explains risk-based procurement decisions (documentation references authoritative federal government hearings and reports, engineering journals, and other classified and unclassified information repositories). Organizations are also referencing or conducting impact analyses to inform their risk management decisions, including analyses on critical technologies, products, and services.

The Extensible organization stage is a continuous cycle of improvement and evolution. The organization has engaged headquarters and regions into the operating model and understands that agility and flexibility is paramount for success. This is when IOC has moved to full operating capability (FOC). It is when stated criteria are met, which may include an approved concept of operation, the right mix of "matrixed" personnel, and SCRM training.

This is where the organization sees the greatest value from collaboration as problems are solved and successes are repeated. Inefficiencies begin to be eliminated. The organization is now able to adapt to new changes, behaviors, or feedback. All necessary components for collaboration are integrated, and sharing, finding, and collaborating on information are at their peak. As new use cases emerge, the organization is quickly able to create solutions. Productivity increases and opportunities are identified and implemented regularly and efficiently that result in cost-saving opportunities.

Broad Application of the Framework

With the continuing release of new guidance imposed upon organizations to counter supply chain threats, they need a structure and approach in place that can help them operate better within and across peer organizations to implement the new requirements. Without mature governance, information sharing, or a well-understood risk posture, organizations can be at a loss to mitigate threats. Organizations can remain at the behest of the constantly shifting threat environment, or they can improve their internal and external approaches to collaborate to combat the threat. A growth framework gives us a way to approach the hard challenge of collaboration.

Looking across the interagency and down through their industry supply chains, organizations are at different levels in their SCRM collaboration. For example, since the DOD and Intelligence Community agencies have traditionally been a rich target for adversaries, they have long been monitoring threats to their supply chains and, as a result, are at a higher level of maturity in their internal—and to some extent external—collaboration processes, which puts them at a more advanced phase. Civil agencies and the private sector, however, have more recently become increasingly targeted and as such are in the less mature phases of the collaboration framework. In addition, agencies that are more decentralized or those with a broader geographic or international footprint may still be in the process of instantiating an enterprise SCRM function and may likely be closer to the level of an Inquiring organization (Level 1). Agencies that are involved in coordinated interagency discussions to develop criteria for supply chain risk management, such as those who are members of interagency SCRM working groups (for instance, the DHS Information and Communications Technology [ICT] Supply Chain

Task Force) and who apply their guidance and best practices, may be in more advanced phases of the framework. NASA, for example, is not only part of the DHS ICT Supply Chain Task Force but has also established a "Circle of Trust" that includes federal, commercial, and nonprofit members. Information sharing and analysis centers (ISACs) also provide significant partnership and knowledge-sharing opportunities with industry.

No agency may yet be at the Extensible organization level.

An agency can also exhibit varying levels of maturity for each of its collaboration areas. For example, the same agency or program that exhibits the behavior of an Established organization (Level 3) by including SCRM language in procurement and contracts, may only be at the Exploratory level (Level 2) in its SCRM governance if it has not yet developed interagency agreements.

For agencies that are not, to a large extent, acquisition agencies, the framework is less applicable.

Also note that as programs within an organization may have varying levels of collaboration, assessing SCRM collaboration at the program level may be more appropriate.

Conclusion

Today's SCRM is difficult with change happening on many fronts, and it seems as if there is no one step to success. Instead agencies must respond in various ways; in doing so, however, their response is all over the map. To synchronize an approach, they can utilize a growth framework to understand how far along they are in different areas and where they need to go to improve.

A SCRM collaboration framework can help drive collaboration *within* an organization and *across* its peer organizations to achieve its risk reduction goals. It can assist organizations in moving from a state of less defined SCRM governance, risk posture, process, technology, and information sharing to a state of maturity in which it proactively leverages and exchanges peer knowledge, processes, and best practices internally and externally to achieve the goal of reducing risk to organizational supply chains. It can prompt analysis of future threats and impacts across economic, geopolitical, and technological aspects that can help inform today's decisions.

Government and industry alike can benefit from a collaborative SCRM function. Industry testimony on supply chain practices states: "We need to continue to explore the extent to which we can leverage public sector SCRM solutions in the private sector and vice versa."[14] The SCRM collaboration framework is one such approach.

Acknowledgments

This paper draws from the deep supply chain risk management exploration and subject matter expertise of David Meshel, whose experience across the intelligence community—and translating that into more agile approaches for application in civil agencies—was extremely valuable. Great appreciation to Torrey Radcliffe and Thomas Kashangaki for their big picture SCRM ideas and to Michelle Yohannes, Scott Van dyke, and Tim O'Brien for their invaluable reviews. As external reviewers, the incisive comments of Gregory Schlegel and the Supply Chain Risk Management Consortium are also very much appreciated.

Appendix A. SCRM Governance: *Leadership*

A combination of organizational SCRM lead and SCRM contributors across the organization can provide the collaborative approach to achieve better SCRM outcomes.

Structure	Organizational SCRM Lead (centralized approach)
Process	Planning, directing, coordinating, and communicating goals, objectives, and resources
Benefits	♦ Ability to formalize SCRM and determine priorities interdependent with other organizations ♦ Ability to strategize to promote SCRM's mission/"voice" ♦ Ability to cultivate, develop, or harness targeted expertise ♦ Serves as a central point of connectivity with other agencies' SCRM functions
Costs	Formalizing the role might negate or obfuscate input from other organizations
	These costs are mitigated when combined with cross-cutting SCRM contributors.

Structure	SCRM Contributors (decentralized approach)
Process	Representatives from various functional organizations contribute routinely
Benefits	♦ Contributes multi-domain expertise to the SCRM process ♦ Brings awareness and accessibility to needed intelligence and information ♦ Adds flexibility to spin up highly specialized problem-solving to address short-term tasks or needs
Costs	♦ A contributor may prioritize their "home" needs over the good of the SCRM function ♦ Can run off track if there is no consistent understanding and/or adherence to SCRM governance, process, information sharing, risk tolerance, or common or shared technology ♦ Confusion and conflict over role definition
	These costs are mitigated when combined with an Organizational SCRM lead.

Appendix B. SCRM: *Charter*

A charter that lays out vision, strategic intent, goals, strategic actions, activities to measure progress, and stakeholder requirements is described below.

- **Vision** – Describes what the SCRM function is trying to build for the future to guide its internal decisionmaking
- **Strategic Intent** – Describes how an organization intends to achieve the vision in the environment in which it operates
- **Strategic Actions** – Describes actions to advance the strategic intent
- **Measure Progress** – Describes outcomes to achieve the SCRM function's vision, strategic intent, and strategic actions, and what it is doing now and will do in the future that it can measure against
- **Stakeholder Requirements** – Includes all stakeholders who have SCRM equities and ensures stakeholders:
  - Promulgate roles and responsibilities for desired outcomes
  - Maintain a balanced, proportionate, and stable contribution to SCRM
  - Can surge when issues arise and conditions might dictate
  - Agree on key guidance parameters, such as risk tolerance
  - Understand their role and contribution and accept responsibility
  - Communicate progress throughout execution, to include compliance with national-level policy
  - Disclose their work in a transparent manner

Appendix C. SCRM: *Inter-organization Agreements*

A collaborative SCRM process requires determining whether an organization can develop a capability "in-house" or if it should partner with another organization to obtain the capability. For example, some capabilities such as intelligence gathering may be more mature in some agencies than others, and an inter-organization agreement for information sharing may be appropriate. A decision tree is shown below.

- Identify other entities' resources that may fill the gap (e.g., products or services from information sharing and analysis centers [ISACs], security operations centers, and threat analysis centers)
- Are there factors that would promote or inhibit exchange of that capability between this organization and another organization?
  - Legal and other authorities
    - Is this organization authorized to procure from private sector? Or must the data be inherently governmental?
    - Are the sources legitimate?
    - Are they reliable?
  - Collection
    - Does the means of collection and the collection format meet this organization's requirements?
    - Does the frequency of information exchange meet this organization's requirements?
    - What are the contingencies if this organization fails to receive the information?
  - Cost
    - Would this capability be procured through an agency agreement, reciprocal sharing, etc.?
    - Is it at a cost that this organization can afford?

Answers to these questions will help determine if the organization is better served to develop the capability in-house, procure it from another organization, or find an organization with a similar need with whom the development cost could be shared.

References

[1] International organizations such as the International Organization for Standardization (ISO) have also developed guidance and standards to address supply chain threats.

[2] https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf.

[3] Committee on National Security Systems Directive (CNSSD) 505 provides requirements for the U.S. Government to implement and sustain SCRM capabilities for NSS, and provides guidance for organizations that own, operate, or maintain NSS to address supply chain risk and implement and sustain SCRM capabilities. http://www.cnss.gov/CNSS/openDoc.cfm?zK/Mir7wF+n1YPvLtCm4HQ==.

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

[5] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[6] https://csrc.nist.gov/News/2018/rmf-update-nist-publishes-sp-800-37-rev-2

[7] https://www.congress.gov/bill/115th-congress/house-bill/7327/text

[8] https://www.dni.gov/files/NCSC/documents/supplychain/20190424-UpdatedFASC-Overview.pdf

[9] https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

[10] https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file

[11] https://fas.org/irp/dni/icd/index.html

[12] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2020-01-23-144114-093

[13] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=2019-04-04-095238-053

[14] https://homeland.house.gov/imo/media/doc/Testimony-Miller.pdf