Research Report

ELVIRA N. LOREDO, JEREMY M. ECKHAUSE, ANDREA M. ABLER, SEAN COLBERT-KELLY, AISHA NAJERA, KARLYN D. STANLEY, ANITA SZAFRAN, N. PETER WHITEHEAD

Frameworks for a Common Operating Procedure for Supply Chain Risk Management Over the Acquisition Life Cycle

For more information on this publication, visit **www.rand.org/t/RRA2002-1**.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-1451-9

About This Report

This report documents research and analysis conducted as part of a project entitled *Framework for Supply Chain Situational Awareness*, sponsored by the Assistant Secretary of the Army Acquisition, Logistics, and Technology. The purpose of the project was to develop frameworks to support implementation of an Army common operating procedure for managing supply chain risks. The frameworks incorporate consideration of the cause-and-effect relationships within and among elements of the supply chain and will be designed to support Army senior leaders' and Program Evaluation Offices' decisions.

This research was conducted within RAND Arroyo Center's Forces and Logistics Program. RAND Arroyo Center, part of the RAND Corporation, is a federally funded research and development center (FFRDC) sponsored by the United States Army.

RAND operates under a "Federal-Wide Assurance" (FWA00003425) and complies with the *Code of Federal Regulations for the Protection of Human Subjects Under United States Law* (45 CFR 46), also known as "the Common Rule," as well as with the implementation guidance set forth in DoD Instruction 3216.02. As applicable, this compliance includes reviews and approvals by RAND's Institutional Review Board (the Human Subjects Protection Committee) and by the U.S. Army. The views of sources used in this report are solely their own and do not represent the official policy or position of DoD or the U.S. Government.

Acknowledgments

First, we would like to thank our sponsor, Timothy Goddette, Deputy Assistant Secretary of the Army, Acquisition Policy and Logistics, and our action officer, Glenn Carthron, for their guidance, assistance, and frequent feedback during this study. We were truly privileged to have such an engaged sponsor, without which we believe the usefulness of the recommendations would be far more limited.

We would like to thank the personnel at various Army and DoD offices, who provided important insights and information. Special thanks are due to the experts within the Logistics Modernization Program for being so generous with their time and providing us an extended tutorial on their systems.

We would like to thank our RAND colleagues. We are grateful to James Broyles and Jonathan Welburn for their insights on related supply chain risk management work focused on acquisition and sustainment, which helped provide recommendations relating to how the frameworks might operate. Much appreciation is due to our Arroyo Forces and Logistics Division management colleagues, Wade Markel and Anu Narayanan, for their support, flexibility, helpful recommendations, and encouragement. Finally, we would like to thank our peer reviewers, Elizabeth Hastings Roer at RAND and Tobias Schoenherr of Michigan State University, for their very helpful suggestions to greatly improve the quality of this report.

Summary

The research reported here was completed in February 2023, followed by security review by the sponsor and the Office of the Chief of Public Affairs, with final sign-off in November 2024.

Introduction

This report documents research and analysis conducted as part of a project entitled *Framework for Supply Chain Situational Awareness*, sponsored by the Assistant Secretary of the Army Acquisition, Logistics, and Technology (ASA [ALT]). The purpose of the project is to develop frameworks to support implementation of an Army common operating procedure for identifying and managing supply chain risks during the acquisition life cycle. This objective is consistent with the U.S. Department of Defense (DoD) and Army leadership guidance on the strategic importance of recognizing and managing supply chain risks. This work should also complement other initiatives, including the creation of the DoD Supply Chain Resiliency Working Group, by providing an approach to identify risks within the supply chains for microelectronics, castings and forgings, raw materials, batteries, and chemicals.

Cost margin preferences; reliance on sole source or single-source suppliers; and the increased complexity of the supply chain because of globalization are some of the factors that have gradually increased supply chain fragility. The coronavirus disease 2019 (COVID-19) pandemic stressed the supply chain, in some instances to the breaking point, and made clear the vulnerabilities inherent in the supply chains across multiple sectors, such as automobile manufacturing, pharmaceuticals, petroleum, and electronics. DoD and the Army have long been aware of certain supply chain risks, such as malicious tampering with electronics and software by adversaries or the introduction of counterfeit parts.

Although policy guidance is in place to manage some risks, there is no comprehensive procedure on how to manage the array of risks that can afflict supply chains. During our research, it became clear that the Army did not have an organizational structure dedicated to conducting supply chain risk management (SCRM). As a result, the Army has a limited ability to proactively identify and manage supply chain risk across a weapon system program's life cycle.

With that in mind, ASA (ALT) asked the RAND Arroyo Center to develop frameworks to support implementation of a common operating procedure for managing supply chain risks. The frameworks should incorporate consideration of the cause-and-effect relationships within and among elements of the supply chain across the weapon system's life cycle. The frameworks should be designed to support Army senior leaders and Program Evaluation Offices (PEOs) by creating awareness of supply chain risks and informing decisions on how to manage supply chain risks across the weapon system's life cycle. A key design decision in the development of the life-cycle supply chain risk management (LSCRM) frameworks was to implement its execution within the canonical acquisition life-cycle process described in Department of Defense Instruction (DoDI) 5000.02T, *Operation of the Defense Acquisition System*.

The existing acquisition life-cycle process provides the organizational structure and determines the activities required to transform a warfighting concept into a weapon system or to modernize an existing weapon system. The acquisition life-cycle process determines the conditions for the manufacture, operation, and maintenance of the system from its fielding to its disposal. Incorporating an SCRM process within the acquisition life-cycle process would align the SCRM activities with key decisions affecting supply choices. It would also place the activities required to collect information regarding supply chain risk, assess risk, and initiate

mitigations within established acquisition management processes that are led by acquisition and engineering experts. These experts have deep knowledge of the design and material solutions and how these affect supply chain requirements. These experts also collaborate closely with original equipment manufacturers (OEMs) and are in the position to effect contract changes that will enforce SCRM.

Research Approach

In developing the LSCRM frameworks, we address three key questions that inform the functioning of the framework:

1. What kinds of supply chain risks should be assessed and managed?
2. How should those assessments be integrated into the acquisition process?
3. What organization should have primary responsibility for assessing supply chain risks over each distinct phase of the acquisition life cycle?

To investigate the third research question, we examined the roles of the major Army organizations that share responsibility for the acquisition life cycle: Army Futures Command (AFC); ASA (ALT), mostly through its PEOs and program managers (PMs); and Army Materiel Command (AMC). We aligned primary organizational LSCRM responsibilities using three considerations with the understanding that all Army organizations and contractors have a shared responsibility to manage supply chain risk. The main considerations for assigning primary responsibility are

- the organization that has primary responsibility for the acquisition process activities during that phase of the life cycle
- the organization that has the most knowledge about the acquisition activity or life-cycle process being supported (e.g., research, development, test, and evaluation (RDT&E); manufacturing; or sustainment).
- the organization with access to the relevant information and the ability to request information from the suppliers.

In most instances, the same Army organization meets all three considerations and is responsible for all SCRM aspects during an acquisition life-cycle phase. However, there will always be a need to coordinate SCRM activities and share information among Army organizations and between Army organizations and outside vendors. For example, the PM clearly has the responsibility for acquisition decisions, but the vendors know their own supply chains best and can provide information about sub-tier supplier risk. We based our alignment of primary organizational responsibilities on information obtained through consultation with stakeholders and reviews of Army policy documents.

To answer the first research question, we surveyed the literature to develop risk categories to guide risk assessment. We reviewed academic, industry, and previous RAND research on SCRM. We cataloged and defined 10 supply chain risk categories and 31 supply chain risk drivers across the categories provided later in Table S.1. This list of risks is not intended to be exhaustive, but it provides comprehensive coverage to the types of risks that might arise during the weapon system's life cycle. Although not every risk can be anticipated, we contend that preparing for risks creates resilience, which in turn makes unanticipated risks easier to manage. We also document lessons learned from three supply chain risk case studies. The analysis also included a review of the nascent SCRM process within the Army and interviews with a company that special-

izes in developing data required to identify and manage supply chain risk. We conducted an extensive review of Army data systems, specifically through the assistance of PEO LMP, the Army's logistics modernization program, to understand the type of information that is gathered and stored by the Army's logistics systems.

Finally, to answer the second research question, we identified the appropriate insertion points for supply chain risk assessments. We relied on an extensive review of the process steps and documents described in DoDI 5000.02T, *Operation of the Defense Acquisition System*, to identify opportunities to integrate supply chain risk assessments. We also interviewed representatives from the acquisition and sustainment communities to understand how they currently approach SCRM; insights from these interviews were used to shape the recommendations in this report. These included representatives from U.S. Army Tank and Automotive Command (USTACOM), U.S. Army Communications and Electronics Command (CECOM), the Army Program Executive Office for Aviation (PEO Aviation), Defense Logistics Agency (DLA) Headquarters, DLA Land and Maritime, DLA Aviation, and the Office of the Secretary of Defense (OSD). We developed an understanding of the roles of the main organizations involved in the process, how the organizations interact, and how their roles change across the weapon system's life cycle. Having reviewed the existing process and organizations, we identified the steps along the process where SCRM activities might take place.

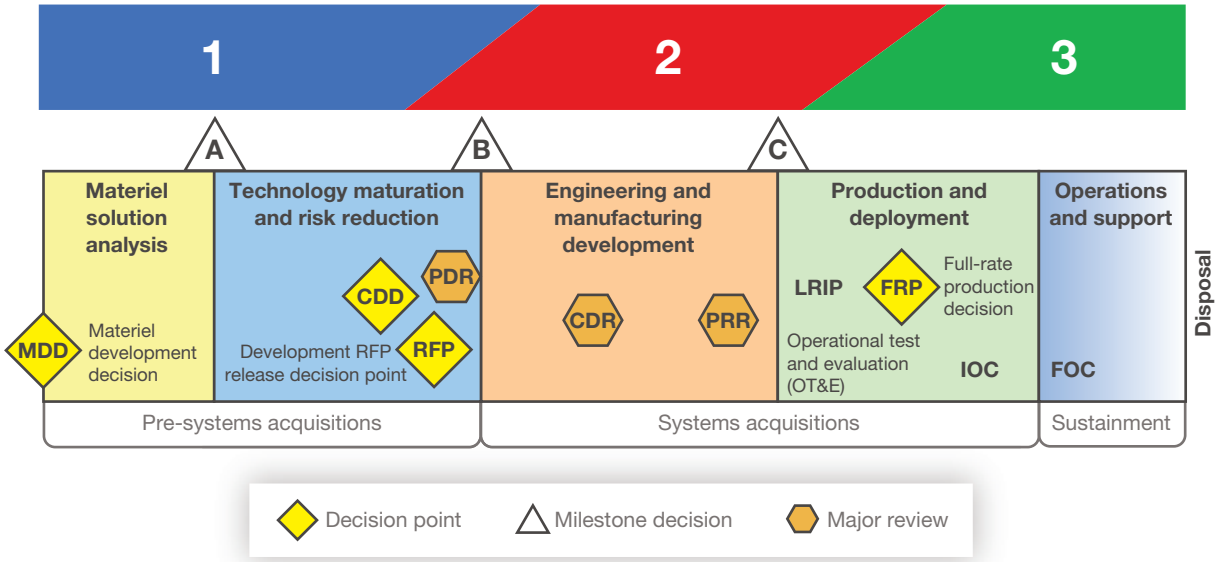
Proposed Frameworks for Integrating Supply Chain Risk Management into the Acquisition Process

A key factor in Army SCRM is the information asymmetry inherent in the acquisition process. This asymmetry between the supplier and the Army includes decisions by the contractor that affect supply chains; these decisions can be made for a variety of reasons, including system design considerations or financial benefits.

In this report, we recommend the Army adopt an SCRM process that is integrated into the existing DoD acquisition life-cycle model. Although not all Army acquisition programs are subjected to the oversight and rigor detailed in the life-cycle model, by establishing standards and practices for supply chain management for the major DoD programs, the Army can accomplish two objectives. First, they can establish the foundation for SCRM that can be built upon as the system enters long-term sustainment (i.e., gather initial data, map the supply chain, identify potential long-term risks). Second, the Army can establish practical tasks and processes (application of SCRM theory) that can be adopted by smaller acquisition programs.

The process would consist of three related frameworks, with transitions between frameworks taking place at two naturally occurring points in the acquisition life cycle: (1) between the initial development of new concepts (or modernization of existing concepts) and engineering and manufacturing leading to low-rate and full-rate production (FRP) and (2) between FRP and full-scale operational deployment; maintenance and sustainment; and retirement of the system, as shown in Figure S.1.

FIGURE S.1
Proposed LSCRM Frameworks Overlap with the Acquisition Life Cycle



SOURCE: Adapted from DoDI 5000.02T, *Operation of the Defense Acquisition System*, Office of the Under Secretary of Defense for Acquisition and Sustainment, January 7, 2015, change 3, August 10, 2017.

NOTE: CDD = capabilities development document; CDR = critical design review; FOC = full operational capability; IOC = initial operational capability; LRIP = low-rate initial production; PDR = preliminary design review; PRR = production readiness review; RFP = request for proposal.

By managing across three frameworks, the Army can focus SCRM activities within the organizations that have the most knowledge and information about the weapon system at that point in the life cycle. The interrelated nature of the frameworks promotes sharing knowledge and acknowledging the changing nature of risks across the life cycle (e.g., how decisions in design could affect risks during production and sustainment).

A description of each framework is presented next along with an illustration of the processes and documents produced during Framework 2 and the transition to Framework 3: These two frameworks account for the majority of a system's life cycle and are where the system is most vulnerable to supply chain risk.

- **Framework 1:** Under this framework, the capability developer assesses the supply chain risk implied by different sets of potential requirements. Framework 1 incorporates SCRM considerations at program conception, during the development process, and as a part of the Army's modernization strategy. This framework systemically considers SCRM in the earliest phases of the materiel solution analysis (pre-Milestone A). SCRM documents are added to the existing processes to explore tradeoffs in early design concepts (each with a different potential set of supply chain risks) that could lead to more sustainable supply chains in later phases. SCRM in development programs would be documented from the initial capabilities document (ICD) through Milestone B, as shown in Figure S.1.

  Proposed Lead Organization: Because AFC has primary responsibility for capabilities and requirements development, it would be a natural choice for leading the LSCRM in this framework. Because the decisions made during this framework set the risk environment during manufacture and sustainment, both the program office and Life Cycle Management Commands (LCMC) should be represented in this phase of the SCRM process.

- **Framework 2:** This framework covers the transition from the initial engineering and manufacturing development (EMD) phase after Milestone B until the system enters FRP. OEMs would be primar-

ily responsible for assessing and managing supply chain risk under Framework 2 under the supervision and with the assistance of Army PMs. The OEM would gather information and promote supply chain mitigations as a system begins FRP. The OEM would also capture SCRM data that can be used to manage risk once the system enters sustainment. PMs would validate potential vendors' risk assessments or conduct their own assessment for some risk categories. By the end of Framework 2, the system has entered FRP. At that point, supply chain risk shifts from developmental to operational. If a system is transitioning from Framework 1, then information on initial system design and supply chain structure is known at a moderate level. For systems entering the acquisition process at this phase, retroactive actions supporting SCRM will be required, as determined by the nature of the specific program. During low-rate initial production (LRIP), more information about the supply chain can be gathered and the supply chain risk assessment refined as components and materials are being procured. The refinement of SCRM information and mitigation decisions begin to eliminate uncertainties as the system enters FRP. As these uncertainties resolve, the definitive SCRM process for the system comes into more focus, establishing the foundation for the operations and sustainment of the system. Framework 2 prescribes cooperation, guidance, and contract data requirements list (CDRL) deliverables from the OEM in support of the PEOs, PMs, and chief systems engineers in conducting SCRM activities.

Proposed Lead Organization: Because of their existing roles, ASA (ALT) PEOs or PMs are in the best position to prepare the CDRL and manage the supply chain risk information that is being gathered by the OEM. The PM's role in the initial manufacturing engineering design allows them to work closely with the OEM and validate the supply chain risk assessment produced by the OEM. The PM has the most visibility and inherent responsibility in this phase of the acquisition life cycle. They would receive support from AFC to understand the tradeoffs made during system development and their effects on the supply chain. The PM would also include AMC to consider such impacts in sustainment.

- **Framework 3:** The SCRM roles in Framework 3 manage and maintain supply chain resilience and security through the duration of the life cycle from production through operations, sustainment, updates, reconditioning, rebuilding, life extension, and any other considerations until disposal. Responsibilities might include SCRM in performance-based life-cycle product support.

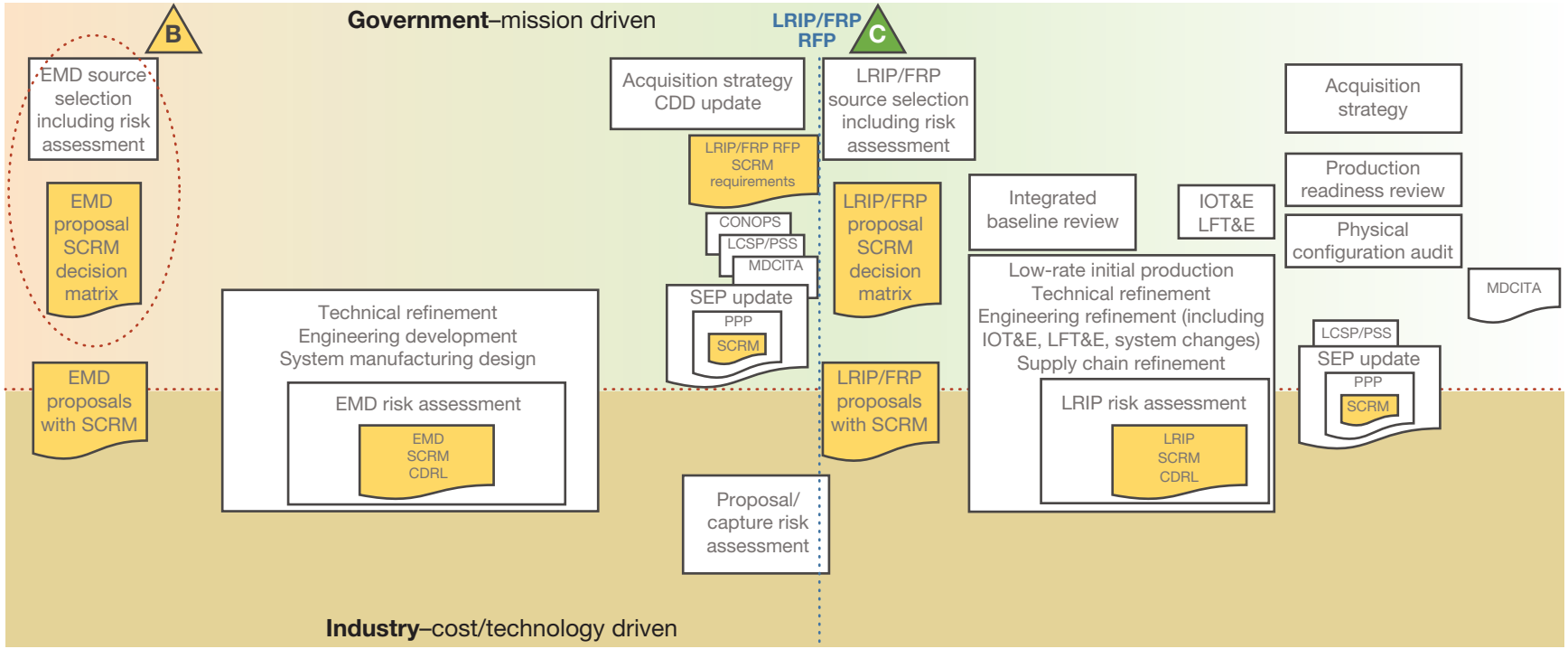
  Proposed Lead Organization: AMC's LCMCs have the inherent responsibility to maintain weapons systems once they are fielded and until they are retired. Logistics programs, managed under the LCMCs, establish and manage sustainment supply chains, which might differ significantly from the original production supply chains. AMC would receive support from ASA (ALT) during the early phases of weapon fielding and from DLA during sustainment.

As an illustration of how LSCRM can be integrated into existing acquisition processes, Figure S.2 shows in orange where additional steps could be taken to augment the existing acquisition processes with SCRM-specific actions during Framework 2. Not all life-cycle processes would contain a proposed SCRM activity: Only those processes and decisions in the acquisition life cycle related to (1) materiel solutions, (2) sources of supply, or (3) engineering design would include SCRM. Taken together, these changes will reduce the supply chain information asymmetry and improve system SCRM.

For instance, the dashed red oval in Figure S.2 shows that, in addition to producing an EMD source selection document, the framework calls for a supply chain risk assessment of the proposed source selection. The two documents create an augmented document, the EMD source with supply chain risk, that will be used as an input into the next acquisition process step. The supply chain risk assessment is captured and integrated into the existing acquisition process.

FIGURE S.2

Critical LSCRM Aspects Within Framework 2, Leading into Framework 3



SOURCE: Adapted from DoDI 5000.02T, 2017.
NOTE: Documents in orange represent proposed SCRM processes. Actions in white are existing acquisition functions that are enhanced for SCRM practice. CONOPS = concept of operations; IOT&E = initial operational test and evaluation; LCSP = life-cycle sustainment plan; LFT&E = live fire test and evaluation; MDCITA = multidisciplinary counterintelligence threat assessment; PPP = program protection plan; PSS = product support strategy; SEP = systems engineering plan.

Supply Chain Risk Categories

Each weapon system program will be subject to a different variety of risks at each stage of the process. Approaches to identifying, assessing, and managing risk will differ depending on the technical and materiel nature of the program and the specific supply chains relevant to each program. Assessing risk for different programs will require a variety of methods and data. The risk categories and their drivers, as shown in Table S.1, are derived through analysis, including prior RAND research, original research for this project, academic literature, industry practices, and discussions with stakeholders.

A risk category will encompass several related risks. We provide definitions for the associated risks and discuss their underlying drivers, their potential impacts, and how to mitigate their effects as a first step in informing the Army generally and the PMs specifically on what information to request, analyze, and evaluate to determine a system's supply chain risks. Although each category might not apply to a given weapon system, this list provides a comprehensive list of potential risks and a starting point for populating the proposed SCRM-related sections within the existing life-cycle documents and processes.

TABLE S.1
Proposed Supply Chain Risk Categories and Drivers

Risk Category	Drivers of Risk
Climate and environmental	• Natural disasters • Man-made disasters • Pandemics, disease, public health
Corporate and finance	• Contracting issues • Financial health • Funding uncertainty • Regulatory or judicial • Cost uncertainty
Supplier	• Sole source • Single source • Diminishing source of supply • Underdeveloped product pipeline • Supplier quality • Supplier collaboration • Counterfeit parts • Provenance
Cybersecurity	• Components' software or hardware vulnerabilities • Network vulnerabilities
Intellectual property and data rights	• Access to data and technical specifications
Demand	• Fluctuations and uncertainty
Geopolitical	• Country risk • Currency and exchange rate fluctuations • Nation-state or terrorist adversarial activity • War or armed conflict
People and skills	• Labor disruptions • Skill obsolescence
Strategic materials	• Raw material access
Transportation and inventory	• Aging infrastructure • Long lead times • Product obsolescence • Product characteristics

SCRM Implementation Challenges

Understanding SCRM through industry examples (e.g., automotive, airlines, electronics) can help the Army be more aware of the risks in the supply chain. By analyzing industries with some similarities to the Army, insights into methods and processes that predict and ideally mitigate supply chain disruptions might be applicable. Specifically, activities that improve vendor trust and supply chain visibility are highlighted as highly critical. It was beyond the scope of this effort to recommend a larger set of SCRM implementation activities across the Army (e.g., legacy weapon systems that are currently in long-term sustainment would not have had the opportunity to begin SCRM during acquisition); a separate SCRM effort will be needed to assess supply chain risks associated with legacy systems. However, the highlighted challenges and recommended mitigation approaches based on the literature for implementing SCRM processes across an organization apply to both new and legacy systems.

Conclusions and Next Steps

SCRM is not done systematically throughout the acquisition life cycle for an Army weapon system. To mitigate the risks inherent in supply chains from a variety of risk categories, we recommend the adoption of three interconnected LSCRM frameworks that span the acquisition life cycle. By managing across three frameworks, the Army can focus SCRM activities within the organizations that have the most knowledge and information about the weapon system at that point in the life cycle. The interrelated nature of the frameworks promotes sharing knowledge and acknowledging the changing nature of risks across the life cycle (e.g., how decisions in design could affect risks during production and sustainment). We recommend that the Army evaluate each weapon system for its potential supply chain risks by considering relevant categories and definitions. Once the relevant categories are determined for that system, those evaluations are then performed throughout the life cycle by the key Army stakeholders, with supporting input from OEMs and relevant vendors, where appropriate.

For next steps, we suggest that ASA (ALT) consider a cost or impact analysis of LSCRM processes in the context of both system risks and operational risks because employing these risk management processes will not be without costs to the Army. Additional work will be required to understand how to integrate the limited existing SCRM activities (e.g., counterintelligence) into OEM-led analysis. Work will also be needed to provide the PEOs and PMs with guidance on implementing these frameworks, including how to evaluate the completeness of the OEM's supply chain risk assessments and any additional Army-led supply chain risk assessments, such as providing guidance on what information and details PEOs should request in contractual deliverables. Further refinement of how SCRM should be conducted once a system enters sustainment would need to be considered as part of an AMC-led initiative to consider SCRM across the entire life cycle of the weapon system. One approach to refine and validate the recommendations might be through analyzing selected Army acquisition case studies followed by effectiveness testing through a pilot project. Finally, if the adoption of these frameworks goes forward, mapping out a timeline for implementation must be established.

Caveats and Limitations

The LSCRM frameworks presented in this report are not comprehensive with respect to the SCRM issues facing the Army. For example, the frameworks address the transition of new acquisitions into sustainment, but they do not address supply chain risk faced by legacy systems (i.e., weapon systems that have long passed active acquisition and are now in sustainment). The frameworks also do not address supply chain risk associ-

ated with less expensive or less complex acquisitions programs that do not follow the strict Joint Capabilities Integration and Development System (JCIDs) process. However, supply chains associated with legacy systems and with non-JCIDS acquisition programs are likely to share common suppliers and similar risks. Additional research on the organizational design and operational requirements of a more comprehensive SCRM system is needed to address remaining gaps in the Army's SCRM approach.

Contents

APPENDIXES

Figures

Tables

CHAPTER 1

Introducing Supply Chain Risk Management

This report documents research and analysis conducted as part of a project entitled *Framework for Supply Chain Situational Awareness*, sponsored by Assistant Secretary of the Army Acquisition, Logistics, and Technology (ASA [ALT]). The purpose of the project is to develop frameworks to support implementation of an Army common operating procedure for identifying and managing supply chain risks during the acquisition life cycle. This objective is consistent with the U.S. Department of Defense (DoD) and Army leadership guidance on the strategic importance of recognizing and managing supply chain risks. This work should also complement other initiatives, such as the DoD Supply Chain Resiliency Working Group, by providing an approach to identify risks within high-value supply chains for microelectronics; castings and forgings; raw materials; batteries; and chemicals.[1]

Cost margin preferences; reliance on sole source or single-source suppliers; and the increased complexity of the supply chain because of globalization are some of the factors that have gradually increased supply chain fragility. The coronavirus disease 2019 (COVID-19) pandemic stressed the supply chain, in some instances, to the breaking point and made clear the vulnerabilities inherent in the supply chains across multiple sectors, such as automobile manufacturing, pharmaceuticals, petroleum, and electronics. DoD and the Army have long been aware of certain supply chain risks, such as malicious tampering with electronics and software by adversaries or the introduction of counterfeit parts. Although policy guidance is in place to manage some risks, there is no comprehensive procedure on how to manage the array of risks that can afflict supply chains. As a result, the Army has a limited ability to identify and manage supply chain risk across a weapon system program's life cycle.

This report provides the Army with frameworks to identify and manage supply chain risk across the life cycle of a weapon system. It was beyond the scope of this effort to recommend a larger set of supply chain risk management (SCRM) implementation activities across the Army (e.g., legacy weapon systems that are currently in long term sustainment would not have had the opportunity to begin SCRM during acquisition); a separate SCRM effort will be needed to assess supply chain risks associated with legacy systems. However, the highlighted challenges and recommended mitigation approaches based on the literature for implementing SCRM processes across an organization apply to both new and legacy systems.

In this chapter, we present basic definitions needed to set conditions for SCRM and introduce aspects of the proposed frameworks that will be discussed in detail in subsequent chapters.

[1] As directed in Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," Executive Office of the President, July 21, 2017; Executive Order 14017, "Securing America's Defense Critical Supply Chains," Executive Office of the President, February 24, 2021; and Department of the Army, Draft SCRM Directive, provided to the authors for this project, November 17, 2021.

Defining Supply Chain Risk and Supply Chain Risk Management

There are multiple definitions of risk, supply chain risk, and SCRM in the literature. The following are three definitions we propose (including two that have already been adopted by the Army).[2]

- *Risk* is defined by the International Organization for Standardization as the "effect of uncertainty on objectives."[3]
- *Supply Chain Management* is the process of planning, managing, executing, and improving the key business processes that ensure effective delivery of products and services from suppliers through the end customer.[4] For DoD, supply chain management is defined as

> [m]eeting customer-driven materiel requirements through the acquisition, maintenance, transportation, storage, and delivery of materiel to customers, and managing materiel returns, movement of reparable materiel to and from maintenance facilities, and ensuring the exchange of information among customers, maintainers, supply chain managers, and suppliers.[5]

- *Supply Chain Risk Management (SCRM)* is defined as

> [t]he process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DoD supply chain from beginning to end, to ensure mission effectiveness. Successful SCRM maintains the integrity of products, services, people, and technologies, and ensures the undisrupted flow of product, materiel, information, and finances across the life-cycle of a weapon or support system. DoD SCRM encompasses all sub-sets of SCRM, such as cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, and other categories of risk that affect the supply chain.[6]

Strategic Management of Army Supply Chain Risk

DoD and the Army have long been aware of risks affecting its supply chains, such as risks from counterfeit parts, cyber intrusion, and limited or diminishing sources of supply. Several DoD policies and instructions have been introduced to manage these risks.[7] However, the existence of these documents alone does not constitute an SCRM strategy.

---

[2] Department of Defense Instruction (DoDI) 4140.01, *DoD Supply Chain Material Management Policy*, Office of the Under Secretary of Defense for Acquisition and Sustainment, March 6, 2019; Nancy Y. Moore, Elvira N. Loredo, Amy G. Cox, and Clifford A. Grammich, *Identifying and Managing Acquisition and Sustainment Supply Chain Risks*, RAND Corporation, RR-549-AF, 2015.

[3] International Organization for Standardization, "ISO 31000:2018, Risk Management—Guidelines," 2018.

[4] Department of Defense Manual (DoDM) 4140.01, Volume 1, *DoD Supply Chain Materiel Management Procedures: Operational Requirements*, December 13, 2018.

[5] DoDM 4140.01, 2018, p. 17.

[6] DoDM 4140.01, 2018, p. 17.

[7] DoDI 4140.01, 2019; DoDI 4140.67, *DoD Counterfeit Prevention Policy*, Office of the Under Secretary of Defense for Acquisition and Sustainment, April 26, 2013, change 3, March 6, 2020; DoDI 4245.15, *Diminishing Manufacturing Sources and Material Shortages Management*, Office of the Under Secretary of Defense for Acquisition and Sustainment, November 5, 2020; DoDI 5010.44, *Intellectual Property (IP) Acquisition and Licensing*, Office of the Under Secretary of Defense for Acquisition and Sustainment, October 16, 2019; DoDI 8500.01, *Cybersecurity*, March 14, 2014, change 1, October 7, 2019.

Managing supply chain risk should be part of an overall supply chain management strategy. For commercial entities, a supply chain management strategy might include the markets that the company will operate in; which suppliers and supply chains the company prefers; and how it plans to identify and prevent risks in the upstream and downstream supply chain.[8]

For the Army, the challenge of developing a supply chain management strategy is magnified because the decisions for the design and production of a weapon system and its supporting supply chains are not entirely under the Army's control. For instance, program managers (PMs) might not be aware of the decision analysis used by the prime contractor to select sub-tier suppliers. Unlike many—but not all—examples presented in the supply chain management literature, the Army's span of control over the supply chain is limited by its business environment. The lack of consistent operational control and visibility over the decisions made in the upstream supply chain heightens the importance of managing the risk to operational readiness, technical performance, or costs due to unforeseen disruptions of the supply chain.

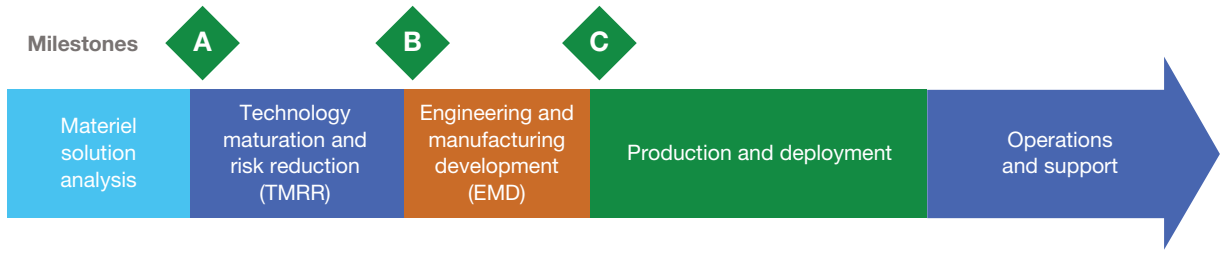
Supply Chain Risk Management Should Start with Army Acquisition

To better manage supply chain risk, we propose that the Army develop an SCRM strategy that (1) leverages the existing DoD acquisitions life-cycle process; (2) broadens the scope of supply chain risks considered; and (3) develops policies and practices that support an SCRM strategy.

Figure 1.1 depicts DoD's acquisition life-cycle process. This process provides the Army with an opportunity to ask questions about supply chain risk. Throughout each of the major steps of the process, the Army is exchanging information and collaborating on decisions made by its commercial partners. We use this framework to propose a life-cycle supply chain risk management (LSCRM) process.

One key aspect of the Army's operating environment distinguishes its supply chain management challenges from those commonly described in the academic literature: the longevity of the systems acquired and the Army's role in sustaining those systems well into the future. Thus, the Army must endeavor to anticipate not only how decisions related to supply chains affect the immediate cost, performance, and schedule during acquisition, but it must project how those decisions will affect the long-term sustainability and cost of the system. There are a handful of industries that have these characteristics (e.g., airlines), and methods surrounding SCRM for them are discussed in Appendix A.

FIGURE 1.1
DoD Acquisition Life Cycle Model



SOURCE: Adapted from Department of Defense Instruction (DoDI) 5000.02T, *Operation of the Defense Acquisition System*, Office of the Under Secretary of Defense for Acquisition and Sustainment, January 7, 2015, change 3, August 10, 2017.

[8] Marc Helmold, Ayşe Küçük Yılmaz, Tracy Dathe, and Triant G. Flouris, "SCRM Strategy," in *Supply Chain Risk Management: Cases and Industry Insights*, Springer International Publishing, 2022, p. 14.

In addition to the proposed LSCRM process, this report provides a series of risk categories that should be considered for most systems that go through the acquisition life cycle. These risk categories derive from our analysis of the SCRM literature. In addition to the risk categories and their definitions, we provide examples of how each category of risk can cause disruption, how the respective risk is measured (if applicable), and what mitigation strategies might be employed. We also distinguish certain categories of supply chain risk in which the burden of the risk assessment might lie at least partially with the Army rather than the original equipment manufacturer (OEM). In those cases, specific Army or DoD vulnerabilities and access to controlled information make the Army engagement critical. Although the list of risk categories is not intended to be comprehensive or necessary for all Army systems going through the acquisition life cycle, this collection represents a suggested roadmap for PMs to analyze during acquisition to identify key supply chain risks and, if necessary, put in steps for mitigation.

Finally, we present some ideas for managing the LSCRM system, including the roles and responsibilities of different organizations within the LSCRM process. Although we believe the proposed LSCRM process creates a disciplined approach to SCRM, we acknowledge that the process should be nested within an Army supply chain risk strategy. Although it was beyond the scope of this research to fully develop an SCRM strategy for the Army, we present several important concepts that would support its development.

Research Approach

In developing the LSCRM frameworks, we address three key questions that inform the functioning of the framework:

1. What kinds of supply chain risks should be assessed and managed?
2. How should those assessments be integrated into the acquisition process?
3. What organization should have primary responsibility for assessing supply chain risks over each distinct phase of the acquisition life cycle?

In pursuing the objective of developing an SCRM process that is embedded within an existing life-cycle acquisition process, we relied on an extensive review of the process steps and documents reflected in the DoDI 5000.02T Joint Capabilities Integration and Development System (JCIDS) acquisition life cycle.[9] We also interviewed representatives from the acquisition and sustainment communities to understand how they currently approach SCRM. We developed an understanding of the roles of the main organizations involved in the process, how the organizations interact, and how their roles change across the weapon system's life cycle. Having reviewed the existing process and organizations, we identified the steps along the process where SCRM activities might take place.

To inform possible approaches, we reviewed academic, industry, and previous RAND Corporation research on SCRM. We cataloged and defined supply chain risks and documented three supply chain risk case studies. The analysis also included a review of the nascent SCRM process within the Army and interviews with a company that specializes in developing data required to identify and manage supply chain risk.

[9] The JCIDS process is implemented by the Joint Requirements Oversight Council (JROC). Although not all system acquisition activities will necessitate approval and management through the JROC, the JCIDS process is a recognized best practice for managing complex system acquisition programs, and we adapt it as a framework for managing supply chain risk across the entirety of a system's life cycle (from concept development to retirement).

Caveats and Limitations

The LSCRM frameworks presented in this report are not comprehensive with respect to the SCRM issues facing the Army. For example, the frameworks address the transition of new acquisitions into sustainment, but they do not address supply chain risk faced by legacy systems (i.e., weapon systems that have long passed active acquisition and are now in sustainment). The frameworks also do not address supply chain risk associated with less expensive or less complex acquisitions programs that do not follow the strict JCIDS process. However, supply chains associated with legacy systems and with non-JCIDS acquisition programs are likely to share common suppliers and similar risks. Additional research on the organizational design and operational requirements of a more comprehensive SCRM system is needed to address remaining gaps in the Army's SCRM approach.

Organization of the Report

In Chapter 2, we address research question 1 and provide a detailed list of supply chain risk categories and their underlying drivers. For each driver, we provide a suggested definition, how it might manifest in terms of disruptions, and suggested mitigation strategies. We frame the discussion of risk within the production and deployment acquisition phase.

In Chapter 3, we describe recent Army and DoD responses to supply chain risks, including new guidance and initiatives. We then propose a life-cycle process of three dovetailing frameworks that map to various phases of the acquisition life cycle, including a description of the respective supply chain risk assessment activities and how they manifest within existing acquisition documents and decisions. We provide suggestions for how these mitigations might occur through contracting documents, including how this process can include software and cyber-physical acquisitions. We then propose SCRM roles and responsibilities for key organizations that map to these frameworks. Finally, we propose some ideas on how to operationalize the evaluation of supply chain risk assessments. We also address research questions 2 and 3 in Chapter 3.

In Chapter 4, we examine the challenges of SCRM through several examples and process steps that can be followed to effectively implement an SCRM process.

In Chapter 5, we provide a set of conclusions and suggested next steps, followed by four appendixes.

In Appendix A, we discuss SCRM case studies from various industries. In Appendix B, we provide an analysis on data rights in terms of mitigating supply chain risk. In Appendix C, we reference the relevant regulations and guidance related to SCRM topics discussed in Chapter 3. Finally, in Appendix D, we discuss some proposed LSCRM activities that relate to software.

CHAPTER 2

Categories and Drivers of Supply Chain Risk Within the DoD Acquisition Life Cycle

Figure 1.1 presented the five distinct phases of the DoD acquisition life cycle:

1. Materiel solution analysis
2. Technology maturation and risk reduction (TMRR)
3. Engineering and manufacturing development (EMD)
4. Production and deployment
5. Operations and support.

The categories and drivers of supply chain risk; the roles and responsibilities for managing those risks; and the types of available mitigation strategies differ across phases of this acquisition life cycle. In Chapter 3, we will cover each of these phases in detail and expand on how SCRM can be developed within and across each phase. The importance of specific categories of supply chain risks varies throughout the acquisition life cycle. However, the portions of the Army responsible for each phase of the life cycle should be aware of all life-cycle risks even if they manifest in a different phase: Decisions in one phase might have supply chain implications elsewhere. For example, during the materiel solution analysis phase, decisions regarding the material properties (e.g., stealth) or performance characteristics (e.g., ability to operate in extreme temperature conditions) establish some of the fundamental properties of a weapon system that in turn limit the supply choices going forward.

Thus, in this chapter, we present an array of supply chain risks that can appear throughout the acquisition life cycle. In addition, we provide these risk categories to guide the SCRM process during the production and deployment phase. We emphasize this phase because it is one in which the primarily responsibility for managing the supply chains lies outside the Army. Therefore, understanding what risk categories an OEM might face, as well as what additional risk categories the Army might wish to consider or augment, provides a component for managing supply chain risks.

Developing Risk Categories

During the production and deployment phase, ASA (ALT) is concerned mainly with supply chain risks associated with how the OEM is performing relative to three measures of program success: cost, system performance, and schedule. More specifically, the PMs and Program Evaluation Offices (PEOs) are relying on the OEM, as the prime contractor, to identify, mitigate, and manage potential supply chain disruptions that might delay the production schedule, increase costs, or affect performance.

Accordingly, for many of the risk drivers discussed in this section, the onus is on the OEM to demonstrate to the Army—first during source selection and then throughout the production and deployment process—that they are sufficiently resilient and robust to disruptions in the supply chain. They can do this by provid-

ing the Army with OEM-conducted assessments of supply chain risk. These OEM-led assessments might include such risk drivers as natural disasters and pandemics; corporate financial health; funding or cost uncertainty; decisions to source materials from single or sole providers; vulnerability to cyberattacks; labor disruptions; and long lead times, among others.

There are, however, some areas of risk where the OEMs might not have complete information or their incentives might be poorly aligned to those of the Army. In these cases, there is a role for ASA (ALT), with support from Army subject matter experts (SMEs), to either lead their own supply chain risk assessment or supplement analyses provided by the OEM. Joint OEM–ASA (ALT) assessments might include such risk factors as product provenance, fluctuations in Army demand, and geopolitical factors, such as nation-state or terrorist adversarial activity, in which DoD's and Army's counterintelligence capabilities are best suited to assess the risk.

The Army might take on a dual role, sometimes functioning as risk identifiers and other times as risk mitigators. One risk area where ASA (ALT) should consider leading their own risk assessment concerns intellectual property (IP) and data rights. For some systems and subsystems, it can be critical for the Army to access OEM data and technical specifications to produce, support, maintain, or operate the system or subsystem. In these cases, the Army's need to access OEM IP might directly conflict with the OEM's desire to retain strict control of data rights. These are considerations that should be covered in contracting language. Appendix B presents an analysis of IP and data rights in relation to supply chain risk.

In Table 2.1, we present a list of categories derived from a review of 37 academic studies from 2015 to 2021 on SCRM. The categories were also informed by previous RAND research on SCRM, interviews with representatives from Exiger and Govini on SCRM, and discussions with ASA (ALT). In Table 2.2, we describe each potential risk category and its drivers. Based on their relevance for each study, we identified the type of risk addressed and grouped the studies by risk type. Understanding what risk categories are most common among the case studies provides some intuition on where the key risks might be for the Army's suppliers and, thus, can help shape the focus of SCRM.[1]

Risk Categories and Drivers of Risk

For developing drivers of risk for each risk category, we expanded upon the literature to ensure robust definitions within each category. The references aim to justify the drivers within each category and provide indirect, but relevant, justifications for our definitions. Table 2.2 describes potential risk categories and drivers of risk and identifies where there might be a role for the Army to lead or supplement risk assessment efforts, or when it might be led by the OEM. This section is not proposed as a rigid, prescriptive list of risks; rather, the intent is to illustrate the variety of risks that might be considered as part of the Army's SCRM strategy. Although this list of risks is not intended to be exhaustive, it provides a comprehensive coverage to the types of risks that might arise. Not every risk can be anticipated, but we contend that preparing for risks creates resilience, which in turn makes unanticipated risks easier to manage.

Each Army program will have its own distinct and complex requirements and supply chain, so each program will have its own unique risk assessment. However, the general risk types shown in Table 2.2 will be applicable to most programs. Determining which risks should be assessed should be part of the LSCRM strategy for each program.

[1] Corporate and finance; supplier; and transportation and inventory are the most frequently mentioned supply chain risk categories in the literature review.

TABLE 2.1

Mapping of Recent Business Case Studies on Supply Chain Risk by Risk Category

Risk Category	Sources	Count
Corporate and finance	• Sheridan Titman, "Risk Transmission Across Supply Chains," *Production and Operations Management*, Vol. 30, No. 12, December 2021 • Jon Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Electronics Company*, National Institute of Standards and Technology (NIST), February 2020a • Jon Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Consumer Goods Company*, NIST, February 2020b • Jon Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Anonymous Renewable Energy Company*, February 2020c • Jon Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic*, NIST, February 2020d • Jon Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Palo Alto Networks, Inc.*, NIST, February 2020e • Jon Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Seagate Technology*, NIST, February 2020f	7
Supplier	• Xishu Li, Rommert Dekker, Christiaan Heij, and Mustafa Hekimoğlu, "Assessing End-Of-Supply Risk of Spare Parts Using the Proportional Hazard Model," *Decision Sciences*, Vol. 47, No. 2. April 2016 • Patrick Bains, Kyle Ferris, Justin Gregoire, James Kim, Jacob Kozloski, Jonathan Lazenby, Dimitri Ofiesh, Evan Shank, Kevin Wu, Peter Beling, and Cody Fleming, "Risk Analysis of Globalized Airline Supply Chains," *IEEE Systems and Information Engineering Design Symposium*, June 13, 2016 • Giselle C. Rampersad, Ann-Louise Hordacre, and John Spoehr, "Driving Innovation in Supply Chains: An Examination of Advanced Manufacturing and Food Industries," *Journal of Business and Industrial Marketing*, Vol. 35, No. 5, April 23, 2020 • Michael Hoeksema, "Understanding and Managing Future Risk: Case Study on Managing Supply Chain Data," *Journal of Supply Chain Management, Logistics and Procurement*, Vol. 2, No. 2, Winter 2019–2020 • Titman, 2021 • Boyens et al., 2020a • Boyens et al., 2020b	7
Transportation and inventory	• Bains et al., 2016 • Hoeksema, 2019–2020 • Tobias Sund, Claes Lööf, Simin Nadjm-Tehrani, and Mikael Asplund, "Blockchain-Based Event Processing in Supply Chains—A Case Study at IKEA," *Robotics and Computer-Integrated Manufacturing*, Vol. 65, October 2020 • "Strategies to Build a Resilient Supply Chain and How to Manage the People to Keep It Operational," *Supply Chain Management Review*, Vol. 25, No. 4, May/June 2021 • Scott DuHadway, Steven Carnovale, and Benjamin Hazen, "Understanding Risk Management For Intentional Supply Chain Disruptions: Risk Detection, Risk Mitigation, And Risk Recovery," *Annals of Operations Research*, Vol. 283, No. 1–2, 2019 • Boyens et al., 2020a • Boyens et al., 2020b	7
Geopolitical	• Bains et al., 2016 • Sarah Gregson, Ian Hampson, Anne Junor, Doug Fraser, Michael Quinlan, and Ann Williamson, "Supply Chains, Maintenance and Safety in the Australian Airline Industry," *Journal of Industrial Relations*, Vol. 57, No. 4, September 2015 • Archie Lockamy III, "An Examination of External Risk Factors in Apple Inc.'s Supply Chain," *Supply Chain Forum: An International Journal*, Vol. 18, No. 3, May 16, 2017 • L. Douglas Smith, Anthony Vatterott, and Wesley Boyce, "Assessing Performance and Risk in Complex Supply Chains and Tying Performance Measures to Strategic Concepts," *Supply Chain Forum: An International Journal*, Vol. 23, No. 1, 2022 • DuHadway, Carnovale, and Hazen, 2019	5

Table 2.1—Continued

Risk Category	Sources	Count
Cybersecurity	• Niyazudeen Kamarudeen and Balan Sundarakani, "Business and Supply Chain Strategy of Flying Above the Dessert: A Case Study of Emirates Airlines," *9th International Conference on Operations and Supply Chain Management, Vietnam*, 2019 • Jennifer Bisceglie and Mark Weatherford, "New Technologies Bring New Risks to the Supply Chain," *Journal of Supply Chain Management, Logistics and Procurement*, Vol. 2, No. 2, Winter 2019–2020 • Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, NIST, February 2021 • Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, Case Studies in Cyber Supply Chain Risk Management: *Summary of Findings and Recommendations*, NIST, 2020g	4
Climate and environmental	• Kamarudeen and Sundarakani, 2019 • Veronica H. Villena, Andrew M. Novakovic, Mark Stephenson, and Charles Nicholson, "Management Lessons from the U.S. Dairy Sector's Pandemic Response," *Supply Chain Management Review*, Vol. 25, No. 5, September/October 2021	2
People and skills	• "Strategies to Build a Resilient Supply Chain and How to Manage the People to Keep It Operational," 2021 • Villena et al., 2021	2
IP and data rights	• Boyens et al., 2020b	1
Demand	• Villena et al., 2021	1
Strategic materials	• James R. J. Goddin, "Identifying Supply Chain Risks for Critical and Strategic Materials," in S. Erik Offerman, ed., *Critical Materials: Underlying Causes and Sustainable Mitigation Strategies*, World Scientific, 2019	1

NOTE: Column 3 represents the number of sources mentioning the risk category in the first column.

TABLE 2.2

Proposed Risk Categories and Drivers of Risk

Risk Category	Drivers of Risk	Description of Risk and How It Might Be Explained	Role for Assessment	Sources
Climate and environmental	Natural disasters	The extent to which the OEM and sub-tier suppliers are resilient to the effects of floods, tornadoes, hurricanes, earthquakes, etc.	OEM led, Army informed	• Elvira N. Loredo, John F. Raffensperger, and Nancy Y. Moore, *Measuring and Managing Army Supply Chain Risk: A Quantitative Approach by Item Number and Commercial Entity Code*, RAND Corporation, RR-902-A, 2015 • Timothy J. Pettit, Joseph Fiksel, and Keely L. Croxton, "Ensuring Supply Chain Resilience: Development of a Conceptual Framework," *Journal of Business Logistics*, Vol. 31, No. 1, Spring 2010 • Mark Hillman and Heather Keltz, *Managing Risk in the Supply Chain—A Quantitative Study*, AMR Research, Inc., January 2007 • Sunil Chopra and Manmohan S. Sodhi, "Managing Risk to Avoid Supply-Chain Breakdown," *MIT Sloan Management Review*, Vol. 46, No. 1, Fall 2004
	Man-made disasters	The extent to which the OEM and sub-tier suppliers are resilient to the effects of toxins, hazards, or dangerous environmental conditions	OEM led, Army informed	• Léa A. Deleris, Debra Elkins, and M. Elisabeth Paté-Cornell, "Analyzing Losses from Hazard Exposure: A Conservative Probabilistic Estimate Using Supply Chain Risk Simulation," in Ricki G. Ingalls, Manuel D. Rossetti, Jeffrey S. Smith, and Brett A. Peters, eds., *Proceedings of the 2004 Winter Simulation Conference*, Institute of Electrical and Electronics Engineers, December 2004 • Christopher S. Tang, "Robust Strategies for Mitigating Supply Chain Disruptions," *International Journal of Logistics Research and Applications*, Vol. 9, No. 1, 2006
	Pandemics, disease, public health	The extent to which the OEM and sub-tier suppliers are resilient to the effects from pandemics, disease, and other public health issues	OEM led, Army informed	• Jeff Luckstead, Rodolfo M. Nayga, Jr., and Heather A. Snell, "Labor Issues in the Food Supply Chain Amid the COVID-19 Pandemic," *Applied Economic Perspectives and Policy*, Vol. 43, No. 1, March 2021 • Kazi Safowan Shahed, Abdullahil Azeem, Syed Mithun Ali, and Md. Abdul Moktadir, "A Supply Chain Disruption Risk Mitigation Model to Manage COVID-19 Pandemic Risk," *Environmental Science and Pollution Research*, January 2021
Corporate and finance	Contracting issues	The extent to which an OEM and sub-tier suppliers are robust to potential contracting issues with their suppliers	OEM led, Army informed	• Loredo, Raffensperger, and Moore, 2015 • Chopra and Sodhi, 2004
	Financial health	The financial health of the OEM and sub-tier suppliers (e.g., revenue and changes in revenue; risk of bankruptcy; financial performance compared with competitors; small firms going out of business)	OEM led, Army informed	• Loredo, Raffensperger, and Moore, 2015 • Chopra and Sodhi, 2004
	Funding uncertainty	The extent to which the OEM is resilient to funding uncertainty, delayed funding, etc., on the part of the Army	OEM led, Army informed	• Loredo, Raffensperger, and Moore, 2015 • Chopra and Sodhi, 2004

Table 2.2—Continued

Risk Category	Drivers of Risk	Description of Risk and How It Might Be Explained	Role for Assessment	Sources
	Regulatory or judicial	The risk of the OEM and sub-tier suppliers being unable to deliver to a contract because of regulatory or judicial issues	OEM led, Army informed	• Pettit, Fiksel, and Croxton, 2010 • Marta Wincewicz-Bosy, Adam Sadowski, Katarzyna Wąsowska, Zbigniew Galar, and Małgorzata Dymyt, "Military Food Supply Chain During the COVID-19 Pandemic," *Sustainability*, Vol. 14, No. 4, February 2022 • Hillman and Keltz, 2007
	Cost uncertainty	The extent to which the OEM and sub-tier suppliers can deliver on contracts if production or component costs rise	OEM led, Army informed	• Pettit, Fiksel, and Croxton, 2010 • Tang, 2006 • Chopra and Sodhi, 2004
Supplier	Sole source	The extent to which the OEM is required to source a product or component from a sole critical sub-supplier (whose inability to deliver will have a significant impact) because no other suppliers are available	OEM led, Army informed	• Paul D. Larson and Jack D. Kulchitsky, "Single Sourcing and Supplier Certification: Performance and Relationship Implications," *Industrial Marketing Management*, Vol. 27, No. 1, January 1998 • Nicola Costantino and Roberta Pellegrino, "Choosing Between Single and Multiple Sourcing Based on Supplier Default Risk: A Real Options Approach," *Journal of Purchasing and Supply Management*, Vol. 16, No. 1, March 2010 • Chopra and Sodhi, 2004 • Moore et al., 2015
	Single source	The extent to which the OEM chooses to source a product or component from a single critical supplier (whose inability to deliver will have a significant impact) even though other suppliers are available	OEM led, Army informed	• Larson and Kulchitsky, 1998 • Costantino and Pellegrino, 2010 • Chopra and Sodhi, 2004 • Moore et al., 2015
	Diminishing source of supply	The extent to which the OEM or the Army's supply chain is resilient to the loss, or impending loss, of approved sub-tier suppliers of items or software	OEM led, Army informed	• DoDI 4245.15, 2020
	Underdeveloped product pipeline	The extent to which the OEM is resilient to delays in supply chain capacity and development needed to meet extant and nascent manufacturing requirements	OEM led, Army informed	• Anita Patel, Maryann M. D'Alessandro, Karen J. Ireland, W. Greg Burel, Elaine B. Wencil, and Sonja A. Rasmussen, "Personal Protective Equipment Supply Chain: Lessons Learned from Recent Public Health Emergency Responses," *Health Security*, Vol. 15, No. 3, May/June 2017 • Tinglong Dai, Ge Bai, and Gerard F. Anderson, "PPE Supply Chain Needs Data Transparency and Stress Testing," *Journal of General Internal Medicine*, Vol. 35, No. 9, September 2020
	Supplier quality	The ability of the OEM and sub-tier suppliers to provide on-time delivery and quality parts and be resilient to supply chain disruption	OEM led, Army informed	• Loredo, Raffensperger, and Moore, 2015 • Pettit, Fiksel, and Croxton, 2010 • Hillman and Keltz, 2007

Table 2.2—Continued

Risk Category	Drivers of Risk	Description of Risk and How It Might Be Explained	Role for Assessment	Sources
	Supplier collaboration	The level of collaboration and information exchange between the OEM and its suppliers	OEM led, Army informed	• Mary Siegfried, *Critical Issue Report: Third Party Risk Management*, CAPS Research, September 2019 • DuHadway, Carnovale, and Hazen, 2019
	Counterfeit parts	The ability of the OEM to identify and eliminate components whose identity or characteristics have been deliberately misrepresented, falsified, or altered without legal right to do so (e.g., parts that are not military-grade sold as if they are)	OEM led, Army informed	• DoDI 4140.01, 2019 • Loredo, Raffensperger, and Moore, 2015
	Provenance	The extent to which the OEM and sub-tier suppliers rely on parts that are manufactured, sold, or distributed by companies that have part or whole foreign ownership	Joint with OEM	• Caolionn O'Connell, Elizabeth Hastings Roer, Rick Eden, Spencer Pfeifer, Yuliya Shokh, Lauren A. Mayer, Jake McKeon, Jared Mondschein, Phillip Carter, Victoria A. Greenfield, and Mark Ashby, *Managing Risk in Globalized Supply Chains, RAND Corporation*, RR-A425-1, 2021
Cybersecurity	Components' software/ hardware vulnerabilities	The risk to the OEM and sub-tier suppliers of components whose function can be manipulated by an external entity to degrade, deny, or destroy the functionality of that component	OEM led, Army informed	• Bisceglie and Weatherford, 2019–2020
	Network vulnerabilities	The risks to the OEM and sub-tier suppliers that arise from the loss of confidentiality, integrity, or availability of information or information systems	OEM led, Army informed	• Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, and Matthew Fallon, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, NIST, Special Publication (SP) 800-161r1, May 2022 • Sandor Boyson, "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems," *Technovation*, Vol. 34, No. 7, July 2014
IP and data rights	Access to data and technical specifications	The degree to which lack of access to the OEM's recorded information and technical data (e.g., research and engineering data, specifications, process sheets, manuals, technical reports, software, etc.) could impede the ability to produce, support, maintain, or operate a system or subsystem	Army led	• DoDI 4245.15, 2020

Table 2.2—Continued

Risk Category	Drivers of Risk	Description of Risk and How It Might Be Explained	Role for Assessment	Sources
Demand	Fluctuations and uncertainty	The degree to which the OEM and sub-tier suppliers are resilient to fluctuations and uncertainty in Army procurement quantities, especially during transitions between wartime and peacetime when demand can decrease; smaller suppliers that provide specialized items or rely predominantly on revenues from the DoD might be particularly susceptible to reductions in orders.	Joint with OEM	• Loredo, Raffensperger, and Moore, 2015 • Pettit, Fiksel, and Croxton, 2010 • Chopra and Sodhi, 2004
Geopolitical	Country risk	The quality of governance in OEM and sub-supplier nations, including such factors as accountability, political instability, government effectiveness, regulatory quality, rule of law, control of corruption, business climate indicators, and trade regulations	Joint with OEM	• Richard Silberglitt, James T. Bartis, Brian G. Chow, David L. An, and Kyle Brady, *Critical Materials: Present Danger to U.S. Manufacturing*, RAND Corporation, RR-133-NIC, 2013 • Lockamy, 2017
	Currency and exchange rate fluctuations	The extent to which the availability of OEM and sub-supplier products and components is impacted by currency and exchange rate fluctuations	OEM led, Army informed	• Pettit, Fiksel, and Croxton, 2010 • Chopra and Sodhi, 2004
	Nation-state or terrorist adversarial activity	The extent to which the OEM and sub-tier suppliers are resilient to disruptions caused by the malicious activity of nation-state actors or terrorist organizations	Joint with OEM	• O'Connell et al., 2021 • Hillman and Keltz, 2007
	War or armed conflict	The extent to which the OEM and sub-tier suppliers are resilient to disruptions caused by war or armed conflict in the OEM or sub-supplier nations	Joint with OEM	• Chopra and Sodhi, 2004

Table 2.2—Continued

Risk Category	Drivers of Risk	Description of Risk and How It Might Be Explained	Role for Assessment	Sources
People and skills	Labor disruptions	The extent to which the OEM and sub-tier suppliers are resilient to disruptions incurred by labor disputes, organizational realignments, or other labor shortages	OEM led, Army informed	• Loredo, Raffensperger, and Moore, 2015 • Luckstead, Nayga, and Snell, 2021 • Chopra and Sodhi, 2004
	Skill obsolescence	The extent to which the OEM or sub-supplier rely on skills that are increasingly difficult to find among new generations of personnel	OEM led, Army informed	• Peter Sandborn, Varun J. Prabhakar, and Abisola Kusimo, "Modeling the Obsolescence of Critical Human Skills Necessary for Supporting Legacy Systems," *Proceedings of the ASME 2012 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, American Society of Mechanical Engineers, August 12–15, 2012 • Loredo, Raffensperger, and Moore, 2015
Strategic materials	Raw material access	The ability of the OEM and sub-supplier to access raw and semi-finished materials that are required to make products and components	OEM led, Army informed	• James S. Thomason, Robert J. Atwell, Ylli Bajraktari, James P. Bell, D. Sean Barnett, Nicholas S. J. Karvonides, Michael F. Niles, and Eleanor L. Schwartz, *From National Defense Stockpile (NDS) to Strategic Materials Security Program (SMSP): Evidence and Analytic Support*, Institute for Defense Analyses, P-4593, May 2010 • Silberglitt et al., 2013
Transportation and inventory	Aging infrastructure	The extent to which the OEM and sub-tier suppliers are robust to disruptions caused by aging infrastructure	OEM led, Army informed	• Loredo, Raffensperger, and Moore, 2015
	Long lead times	The extent to which long lead times (periods between when the orders are placed to when the orders are received) result in backorder and supply disruption for the OEM and sub-tier suppliers	OEM led, Army informed	• Timothy McClean, "How Do You Reduce Lead Time in Your Supply Chain?" TXM Lean Solutions blog, 2017
	Product obsolescence	The extent to which the OEM and sub-tier suppliers rely on obsolete parts, thereby requiring stockpiling or other mitigation strategies	OEM led, Army informed	• Michael J. Gravier and Stephen M. Swartz, "The Dark Side of Innovation: Exploring Obsolescence and Supply Chain Evolution for Sustainment-Dominated Systems," *Journal of High Technology Management Research*, Vol. 20, No. 2, 2009 • Chopra and Sodhi, 2004
	Product characteristics	The degree to which the characteristics of product components (e.g., inventory holding cost, interchangeability, substitutability, critical component to weapon system) affect the OEM's procurement ability	OEM led, Army informed	• Loredo, Raffensperger, and Moore, 2015 • Chopra and Sodhi, 2004

The remainder of this chapter details the potential risk drivers and discusses their characteristics; assessment and mitigation strategies; and historical examples as identified and described in relevant SCRM literature.

Climate and Environmental

Natural Disasters

Natural disasters, such as floods, tornadoes, hurricanes, and earthquakes, are some of the most cited drivers of risk in SCRM studies.[2] Indeed, there are numerous historical examples of significant international supply chain disruptions from natural disasters, from the 1999 Taiwanese earthquake that disrupted computer components supply chains,[3] to the March 2011 earthquake and tsunami in Japan that majorly affected the global automotive and electronics industry,[4] to the flooding in November 2011 in Thailand that disrupted Western Digital's production of disk drives.[5]

Risks associated with natural disasters are important to consider during production and deployment.[6] OEM contracts often include a force majeure clause, which absolves the supplier from responsibility to meet the terms of the contract after a natural disaster. Force majeure clauses provide a necessary safety net for the supplier but fail to provide an incentive to mitigate risks and essentially pass risk on to the Army without any recourse to recover costs from the supplier. One way the Army can account for this is to require that OEMs meet certain standards around regulations, preemptive mitigation, or resiliency measures.[7] An important measure of resiliency is time to recovery (TTR). TTR is the time it takes to resume operations after a supply chain disruption. The likelihood of supply chain disruption from natural disasters can also be part of a calculation to ascertain overall supplier risk.[8] Sources such as the U.S. Geological Survey's natural hazard dataset, which includes earthquake, hurricane, tornado, and flood data by zip code for locations in the contiguous United States, can be used during risk assessment to highlight places of performance that are located in natural disaster risk zones.

Suppliers can mitigate natural disaster risk in several ways, such as by designing their products to allow parts from several different sub-tier suppliers (in case one supplier is affected) or managing the demand of

---

[2] Yossi Sheffi, James B. Rice, Jr., Jonathan M. Fleck, and Federico Caniato, "Supply Chain Response to Global Terrorism: A Situation Scan," *Proceedings from the EurOMA POMS Joint International Conference, Cernobbio*, June 17, 2003; Chopra and Sodhi, 2004; Chris I. Enyinda, Chris H. Mbah, and Alphonso Ogbuehi, "An Empirical Analysis of Risk Mitigation in the Pharmaceutical Industry Supply Chain: A Developing-Country Perspective," *Thunderbird International Business Review*, Vol. 52, No. 1, January/February 2010; Faisal Aqlan and Sarah S. Lam, "Supply Chain Risk Modelling and Mitigation," *International Journal of Production Research*, Vol. 53, No. 18, 2015; Loredo, Raffensperger, and Moore, 2015; O'Connell et al., 2021.

[3] Tang, 2006.

[4] Xiaojun Wang, Puneet Tiwari, and Xu Chen, "Communicating Supply Chain Risks and Mitigation Strategies: A Comprehensive Framework," *Production Planning and Control*, Vol. 28, No. 13, May 22, 2017.

[5] O'Connell et al., 2021.

[6] In a 2015 study of Air Force supply chain risk, United States Air Force (USAF) acquisition personnel, risk managers, sustainment personnel, and sustainment managers were interviewed to explore which supply chain risks they consider in their decisionmaking process. Acquisition personnel considered natural disasters "half the time," and 40 percent of risk managers cited natural disasters as a concern. On the sustainment side, natural disaster risk was considered less often: sustainment personnel reported considering the risk less than half of the time and only 15 percent of sustainment managers cited natural disasters as a concern. See Moore et al., 2015, pp. xvii, 12.

[7] O'Connell et al., 2021, p. 16.

[8] Nancy Y. Moore, Clifford A. Grammich, and Judith D. Mele, *Findings From Existing Data on the Department Of Defense Industrial Base*, RAND Corporation, RR-614-OSD, 2014.; Loredo, Raffensperger, and Moore, 2015.

an affected product by changing price points to make unaffected products more desirable while waiting for a disrupted supply chain to stabilize.[9]

Man-Made Disasters

Man-made disasters, such as toxins, oil spills, nuclear incidents, and industrial fires, are also important supply chain risks to consider. Although similar in character to natural disasters, man-made disasters are not covered under force majeure clauses, and suppliers often retain liability for these risks. Because the likelihood of these events is difficult to predict, risk assessment is challenging; however, modeling methods can be used to predict losses from supply chain disruption without requiring any estimation of likelihood.[10]

Regulations exist to minimize or prevent many man-made disasters, so ensuring OEMs and sub-tier suppliers are compliant is an important factor for mitigation. As with other types of risk, suppliers can also mitigate the risk from man-made disasters by managing their product design or the demand for products to weather supply chain disruptions.[11]

Pandemic, Disease, and Public Health

As experiences around the COVID-19 pandemic have made clear, major health events have a significant impact on supply chains across sectors. Beginning in early 2020, global transportation and manufacturing came to a halt, and consumer demand shifted rapidly in response to widespread quarantine conditions (e.g., from buying food at restaurants to making food at home).[12] Numerous country lockdowns slowed or even temporarily stopped the movement of raw materials and finished goods, resulting in the interruption of businesses ranging from electronics and furniture to civilian and military food supply chains.[13] The extreme supply chain disruptions from the COVID-19 pandemic have prompted a slew of research into SCRM models with scenarios involving unavailability of suppliers, management of perishable products, social life-cycle assessments, multitier supply chains, and other contexts specific to COVID-19.[14]

The COVID-19 pandemic's impact on the global supply chain is unprecedented in its breadth and severity; however, other more limited—though still serious—public health events have driven supply chain risk. For example, livestock disease can majorly affect supply chains; for example, the United Kingdom's 2001 outbreak of foot-and-mouth disease cost the country an estimated £7 billion loss,[15] and the 2003 Canadian outbreak of mad cow disease caused major disruptions for several years to the North American agricultural supply chain.[16]

Mitigation strategies vary widely based on the extent and severity of a disease or public health issue. During incidents that are relatively geographically contained, buyers might have the option to simply work with unaffected suppliers. However, in a global pandemic, in which all suppliers are affected, broader solu-

---

[9] Tang, 2006, p. 37.

[10] Deleris, Elkins, and Paté-Cornell, 2004.

[11] Tang, 2006, p. 37.

[12] Luckstead, Nayga, and Snell, 2021.

[13] For raw materials and goods, see Sean Harapko, "How COVID-19 Impacted Supply Chains and What Comes Next," webpage, Ernst & Young, 2021. For electronics and furniture, see Villena et al., 2021. For civilian and military food supply chains, see Luckstead, Nayga, and Snell, 2021; Wincewicz-Bosy et al., 2022.

[14] Shahed et al., 2021, p. 3.

[15] Michael Bourlakis and Johanne Allinson, "The Aftermath of the Foot and Crisis in Agricultural Logistics: The Case of the UK Fat Lamb Supply Chain," *International Journal of Logistics Research and Applications*, Vol. 6, No. 4, 2003.

[16] Ellen Kline, "Canadian BSE Continues to Disrupt the Supply Chain for Beef," *Law and Business Review of the Americas*, Vol. 13, No. 3, 2007.

tions must be introduced. In response to the COVID-19 pandemic, such mitigation strategies as inventory management,[17] product change,[18] and improved disruption modeling and forecasting have been proposed.[19]

Corporate and Finance

Contracting Issues

Although not commonly cited in SCRM literature, contracting issues have been identified by Army SMEs as a source of supply chain risk. In a 2013 workshop, Army Materiel Command (AMC)'s Strategic Sourcing Working Group (SSWG) described long administrative lead times, delays in contracting awards, and length of contract among the supply chain risks faced by AMC.[20] Contract length is also an example of how risk drivers are deeply interconnected and how mitigation requires balancing of conflicting priorities. Long-term contracts can mitigate the risk of rising production cost by locking the customer in at a fixed price; however, a long-term contract becomes a liability itself by reducing a customer's options for suppliers if something unforeseen happens.[21]

Financial Health

The financial health of the OEM and sub-tier suppliers is an important component in the determination of supplier risk during acquisition.[22] Deeper into the sub-tier of suppliers, the financial health of a supplier might be unknown, especially if they are privately held. A supplier of a critical component several tiers down in the supply chain might file for bankruptcy without the knowledge of companies that depend on that component two or three tiers later. Production is then delayed while a new supplier is found.[23] For example, in 2016, the ocean transport company Hanjin filed for bankruptcy protection, stranding cargo outside ports for months. Because the cargo industry shares cargo space across carriers, many customers did not realize their cargo was booked for transport on a vessel managed by Hanjin.[24]

Although more analysis is needed to establish financial health metrics, potential indicators might include revenue and changes in revenue; risk of bankruptcy; and financial performance compared with competitors. Altman proposes modeling several factors that might indicate a risk of bankruptcy and suggests a Z-score based on the weighted sum of factors, such as working capital/total assets, retained earnings/total assets, earnings before interest and taxes/total assets, market value equity/book value of total liabilities, and sales/total assets.[25] Several databases are useful in financial health assessment for federal contractors and U.S.

---

[17] Shahed et al., 2021; Jarrah F. Al-Mansour and Sanad A. Al-Ajmi, "Coronavirus 'COVID-19'—Supply Chain Disruption and Implications for Strategy, Economy, and Management," *Journal of Asian Finance, Economics and Business*, Vol. 7, No. 9, 2020, p. 669.

[18] Jingzhe Chen, Hongfeng Wang, and Ray Y. Zhong, "A Supply Chain Disruption Recovery Strategy Considering Product Change Under COVID-19," *Journal of Manufacturing Systems*, Vol. 60, July 2021.

[19] Seyedmohsen Hosseini and Dmitry Ivanov, "A Multi-Layer Bayesian Network Method for Supply Chain Disruption Modelling in the Wake of the COVID-19 Pandemic," *International Journal of Production Research*, Vol. 60, No. 17, 2022.

[20] Loredo, Raffensperger, and Moore, 2015, pp. 51–52.

[21] Chopra and Sodhi, 2004, p. 58.

[22] Chopra and Sodhi, 2004, p. 54; Moore et al., 2015, p. xvi.

[23] Loredo, Raffensperger, and Moore, 2015, p. 50.

[24] Caleb Kwon, *Supply Chain Disruptions: Evidence from the Bankruptcy of Hanjin Shipping*, Social Science Research Network, July 17, 2021, p. 3.

[25] Edward I. Altman, "Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy," *Journal of Finance*, Vol. 23, No. 4, September 1968.

companies: three years of supplier annual revenue data for federal contractors are available from the System for Award Management (SAM); the U.S. Census Bureau Economic Census provides employee and revenue data by industry; and the U.S. Census Bureau Statistics of U.S. Business database captures firm births, deaths, expansions, and contractions by industry.[26]

Funding Uncertainty

Related to—but distinct from—financial health is the impact of funding uncertainty on an OEM or sub-tier supplier's ability and willingness to provide a product. From the supplier's perspective, this risk can be conceptualized as the "financial strength of customers."[27] In particular, small companies that provide a specialized product (e.g., weapon systems and components) exclusively to DoD might find it difficult to stay in business if DoD funding is reduced or uncertain because of unanticipated changes in demand.[28] The risk is a salient one: the AMC SSWG identified funding uncertainty as one of the top three supplier risks.[29]

Although it is challenging to predict funding uncertainty, risk assessment can include an evaluation of how vulnerable a supplier is to disruptions in funding.[30] Metrics include whether there has been a sharp decrease in revenue from a customer, what percentage of total revenue the critical component makes up, and the change in revenue compared with other suppliers.[31] Like financial health metrics, relevant data for federal contractors and U.S. companies can be found in the SAM and in U.S. Census Bureau databases. From the customer side, this risk can be mitigated by minimizing internal administrative lead times and investing in methods to improve demand forecasting.[32]

Regulatory or Judicial

Abrupt changes in regulation can lead to delayed production and supply chain disruption for an OEM or sub-tier supplier. For example, in 2010, the availability of rare earth elements plunged when China restricted its exports by 40 percent.[33] Domestic import regulations—such as increased tariffs—can also alter the structure of supply chains.[34] These risks are identified as consequential to supply chain management in both civilian and military literature.[35] During supplier selection, an OEM should be able to demonstrate that it meets federal contracting requirements, such as those outlined in the Federal Acquisition Regulations (FAR), and that it has the organizational flexibility to respond to potential abrupt regulatory shifts. As with other types of risk, this becomes more difficult to assess as visibility into the chain of sub-tier suppliers becomes increasingly obscure.

[26] Loredo, Raffensperger, and Moore, 2015, pp. 18–19.

[27] Chopra and Sodhi, 2004, p. 54; Loredo, Raffensperger, and Moore, 2015, p. 14.

[28] O'Connell et al., 2021, p. 9.

[29] Loredo, Raffensperger, and Moore, 2015, pp. 14, 50.

[30] Loredo, Raffensperger, and Moore, 2015, p. 14.

[31] Loredo, Raffensperger, and Moore, 2015, pp. 18–19.

[32] Loredo, Raffensperger, and Moore, 2015, p. 44.

[33] Shardul Phadnis and Nitin Joglekar, "Configuring Supply Chain Dyads for Regulatory Disruptions: A Behavioral Study of Scenarios," *Production and Operations Management*, Vol. 30 No. 4, April 2021, p. 1014.

[34] Phadnis and Joglekar, 2021, p. 1014.

[35] Enyinda, Mbah, and Ogbuehi, 2010; Moore et al., 2015.

Cost Uncertainty

Cost uncertainty is another fundamental driver of supply chain risk. When the cost for a critical component or source material rises, manufacturing costs might become too high for some suppliers to continue production.[36] This is another area that highlights trade-offs in mitigation strategies. To mitigate the risk of rising cost, an OEM might sign long-term contracts with suppliers, locking in the current rate. However, this comes with its own risks, such as the risk that the cost of the item might decrease, keeping the OEM locked in a contract in which they end up paying much more than market share for a critical component.[37]

Supplier

Sole Source and Single Source

In sole source supply, the OEM is required to source a product or component from a sole supplier because no other suppliers are available. In single source supply, the OEM chooses to source a product or component from a single supplier even though more than one supplier is available.[38] The outcome of risks associated with single and sole source is similar: When the single or sole supplier's production is disrupted, the OEM is unable to acquire its product. However, the distinction between sole source and single source is important when seeking to mitigate this risk. For example, in single source supply, the OEM has the option to use another supplier (either preemptively or reactively) if the first supplier fails to meet distribution requirements. This option is, by definition, unavailable when a product or component is provided through sole source supply.[39] The Federal Procurement Database System provides contract-level data that records which contracts are sole source; this metric is sometimes included in risk assessment calculations.[40] Appendix A also highlights some of these issues for specific case studies.

Diminishing Sources of Supply

Diminishing sources of supply refers to the risk that suppliers of critical items leave the market, the number of approved sub-tier suppliers substantially declines, or suppliers consolidate. This can affect supply chains by reducing availability of the product and restricting mitigation options (e.g., diversifying supply is no longer an option) for the Army and OEMs.

Risk management for diminishing sources of supply is addressed directly in DoD policy. Published in 2020 by the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S), Department of Defense Instruction (DoDI) 4245.15 "establishes policy, assigns responsibilities, and prescribes procedures for diminishing manufacturing sources and material shortages (DMSMS) management" and "implements risk-based, proactive management for all DoD materiel, parts, equipment, assemblies, components, material, and software."[41] DoDI 4245.15 prescribes that DMSMS risk management processes be integrated into acquisitions; contracts; sustainment; research and engineering; military departments; and the industrial base.[42]

[36] Loredo, Raffensperger, and Moore, 2015, p. 4; Tang, 2006.

[37] Chopra and Sondhi, 2004, p. 58.

[38] Larson and Kulchitsky, 1998; Costantino and Pellegrino, 2010.

[39] Chopra and Sodhi, 2004.

[40] Loredo, Raffensperger, and Moore, 2015, p. 20.

[41] DoDI 4245.15, 2020, p. 1.

[42] DoDI 4245.15, 2020, pp. 4–7.

Underdeveloped Product Pipeline

The risk associated with underdeveloped product pipelines is a mirror image of the risk from diminishing sources of supply. In the latter, approved suppliers are disappearing from a market that currently exists. Conversely, in an underdeveloped product pipeline, a new market is emerging and the supply chain—including the number of suppliers—has not yet developed to sufficiently support demand. For example, in the early stages of the COVID-19 pandemic, such personal protective equipment (PPE) as N95 filtering masks became a household necessity almost overnight, and the existing supply chain could not keep pace with the rapidly rising demand.[43] In the United States, N95 masks were particularly difficult to come by because almost 90 percent of the product is foreign-supplied, and those companies prioritized their own domestic needs above exports.[44] Mitigation strategies for this type of risk include adapting processes and production to allow for wider substitutability of products; preemptively publishing guidelines prescribing how much product would be needed in scenarios that require a sudden demand surge; eliminating inefficiencies in product use and distribution; increasing visibility on product orders; and developing a capability for emergency domestic production during a demand surge.[45]

Supplier Quality

Supplier quality refers to the OEM or sub-tier supplier's ability to deliver quality products on time and within cost while remaining resilient to disruption. This risk driver is fundamentally correlated with many of the other risk drivers we describe in this section: Such factors as financial health or long lead times can affect supplier performance and resilience. SCRM studies often include characteristics that speak to supplier quality, such as whether the supplier has sufficient mitigation strategies in place;[46] supplier failure or vendor fail risk;[47] and poor quality or defective parts.[48] Supplier resilience is particularly important because many mitigation strategies depend on an organization's response to disruption.[49]

Part 9 of FAR "prescribes policies, standards, and procedures for determining whether prospective contractors and subcontractors are responsible."[50] Among other provisions, Part 9 stipulates that responsible suppliers must have adequate financial, organizational, construction, and technical resources and facilities; the ability to adhere to delivery schedule; and a record of integrity and ethical business practices.[51]

---

[43] Interestingly, the underdeveloped PPE supply chain was a known issue even before the COVID-19 pandemic. A 2017 study on PPE supply chains stated, "The US PPE supply chain has minimal ability to rapidly surge production, resulting in challenges to meeting large, unexpected increases in demand that might occur during a public health emergency" (Patel et al., 2017, p. 244).

[44] Dai, Bai, and Anderson, 2020.

[45] Patel et al., 2017, pp. 248–250.

[46] Loredo, Raffensperger, and Moore, 2015, p. xii.

[47] Enyinda, Mbah, and Ogbuehi, 2010, p. 47; Loredo, Raffensperger, and Moore, 2015, p. 18.

[48] Chopra and Sodhi, 2004, p. 54; Aqlan and Lam, 2015, p. 5647.

[49] Srinivas Talluri, Thomas J. Kull, Hakan Yildiz, and Jiho Yoon, "Assessing the Efficiency of Risk Mitigation Strategies in Supply Chains," *Journal of Business Logistics*, Vol. 34, No. 4, 2013, p. 262.

[50] Federal Acquisition Regulations, Part 9, Contractor Qualifications; Subpart 9.1, Responsible Prospective Contractors; Section 9.100, Scope of Subpart.

[51] Federal Acquisition Regulations, Part 9, Contractor Qualifications.

Supplier Collaboration

Strong relationships and collaboration between suppliers, such as open sharing of information, can be effective in preventing or diminishing the effects of supply chain disruption.[52] Similarly, effective supplier relationship management (SRM)—which can include supplier portfolio management, relationship management frameworks, and distinguishing *key* relationships from *transactional* relationships—is found to bolster supply chain health.[53] Thus, the absence of strong supplier collaboration and SRM can be a key supply chain risk indicator. OEMs who have long standing relationships with sub-tier suppliers and the Army and have information-sharing and collaboration tools in place help manage supply chain risk. The effects of supplier collaboration and the importance of supplier relationships are detailed in several examples in Appendix A.

Counterfeit Parts

During source selection, the OEM might be asked to demonstrate its ability to identify and eliminate counterfeit parts (i.e., components whose identity or characteristics have been deliberately misrepresented, falsified, or altered without legal right to do so). In the military sector, counterfeit parts pose a particularly grave risk. If, for example, a low-quality counterfeit part is sold as military-grade it could directly affect critical weapon systems and operations.

Because of the critical nature of this risk, mitigation strategies tend to focus on risk avoidance; that is, they seek to identify and remove counterfeit components from the market before they are fielded rather than to minimize the impact after a breach occurs.[54] A 2021 study for USAF recommended creating a centralized database within USAF to collect reports of suspected counterfeits to improve the processes around counterfeit identification and removal.[55]

Relevant policies for counterfeit prevention are provided in DoDI 4140.01 and DoDI 4140.67.

Provenance

The matter of provenance—the extent to which the OEM and sub-tier suppliers rely on parts that are manufactured, sold, or distributed by companies that have part or whole foreign ownership—is a crucial one in the military supply chain. Elements of the supply chain that exist outside domestic production increase U.S. vulnerabilities to espionage, sabotage, and exploitation.[56] Restricting all military sourcing to domestic suppliers would be the most effective way to mitigate this risk; however, this is not a practical approach. Not only is redomiciled production economically infeasible, it also reduces resilience to domestic supply chain disruptions by eliminating the use of foreign sources as an alternative.[57]

The Committee on Foreign Investment in the United States (CFIUS) is one conduit through which the United States reviews foreign investment. The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), legislation that bolsters CFIUS authorizations and activities, reflects a growing concern in Congress about the role of foreign investors on national security.[58]

---

[52] Siegfried, 2019; DuHadway, Carnovale, and Hazen, 2019.

[53] Dario Miocevic and Biljana Crnjak-Karanovic, "The Mediating Role of Key Supplier Relationship Management Practices on Supply Chain Orientation—The Organizational Buying Effectiveness Link," *Industrial Marketing Management*, Vol. 41, No. 1, January 2012.

[54] Enyinda, Mbah, and Ogbuehi, 2010, p. 49.

[55] O'Connell et al., 2021, p. 40.

[56] O'Connell et al., 2021, p. 34.

[57] O'Connell et al., 2021, p. 1.

[58] O'Connell et al., 2021, p. 1; Public Law 115-232, Title XVII—Review of Foreign Investment and Export Controls, The Foreign Investment Risk Modernization Act of 2018, August 13, 2018.

Although the OEM should provide its own assessment of provenance during source selection, this is one area where the OEM does not have the same level of information that is available to DoD through counterintelligence operations and classified resources.[59] For this reason, there is a role for ASA (ALT) to supplement OEM reports with their own analyses.

Cybersecurity

In recent times, supply chains have evolved from purely physical to include digital components, such as the internet of things (IoT), 3D printing, and blockchain applications.[60] Companies can gain new efficiencies through the implementation of new technologies and software distribution channels. These new technologies also can allow access to data by applications and automated tools. This comes with risks that need to be managed and mitigated so that the supply chain can continue to operate. Digital supply chains help to increase the performance of a company's supply chain, but they also introduce cyber risks. Cyber supply chain risk management (C-SCRM) combines elements of cybersecurity, supply chain management, and enterprise risk management to assess and mitigate risk across end-to-end processes.[61] C-SCRM looks at the increased risk of supply chain vulnerabilities in connection with cybersecurity, both intentional and unintentional. DoD has issued DoDI 8500.01 to state responsibilities and procedures on cybersecurity implementation.[62] In addition, in 2022, NIST released revised guidance on how to identify, assess, select, and implement processes for C-SCRM.[63]

Components' Software and Hardware Vulnerabilities

New devices and technologies, such as IoT devices, 5G, 3D printing, and software used in the supply chain, increase attackers' accessibility to a company's valuable assets.[64] Some mitigation strategies include creating a separate network for IoT devices; using technology to identify unknown companies in the sub-tiers of the supply chain and highlighting their risks; and securing the 3D printing. Software supply chain attacks conceal malicious code in authentic commercial software. It has been stated by the U.S. National Counterintelligence and Security Center that "software supply chain infiltration is one of the key threats that corporations need to pay attention to."[65] This type of attack can expand rapidly through the supply chain, exploits the use of open-source code, and violates the trust among software makers, distributors, and consumers. Some mitigation strategies include consistent scanning and assessment of all third-party components for risk; using only pre-vetted components on a local repository server; and running vulnerability scans on all software builds that use internet-based component repositories.[66]

[59] For a discussion of the limitations of counterintelligence operations in the military supply chain, see O'Connell et al., 2021, p. 36.

[60] Bisceglie and Weatherford, 2019–2020, p. 148.

[61] Boyson, 2014, p. 342.

[62] DoDI 8500.01, 2014.

[63] Boyens et al., 2022.

[64] Bisceglie and Weatherford, 2019–2020.

[65] Bisceglie and Weatherford, 2019–2020, p. 152.

[66] Bisceglie and Weatherford, 2019–2020.

Network Vulnerabilities

C-SCRM involves an organization's approach to assess and mitigate risks across the "end-to-end processes" that establishes the supply chain for hardware, software systems, and information technology (IT) networks.[67] Organizations use hardware and software systems and components sourced from sources that might not be well known and have critical functions that are "hosted, exposed, and accessed" on possibly corrupted network environments.[68] These components and technologies allow access to the network within these organizations. This vulnerability has resulted in a need to manage the design, build, and deployment of these systems in an effective and efficient manner and has led to the need for C-SCRM. Gabriel Davis, risk operation federal lead in the Cybersecurity Division at the Cybersecurity and Infrastructure Security Agency, stated that privileged access is one way that supply chain risk is introduced inadvertently.[69] This type of risk involves giving elevated privileges to run third-party software, even the "highest level of privileges that are allowed on the system." Another risk is introduced by devices with constant communication to and from a vendor through software updates and patches.[70] There are policies and practices that can be used to help mitigate these and other risks factors (e.g., NIST SP 800-161r1).

Intellectual Property and Data Rights

Access to Data and Technical Specifications

One risk area where ASA (ALT) should consider leading their own risk assessment concerns IP and data rights. For some systems and subsystems, it can be critical for the Army to access OEM data and technical specifications to produce, support, maintain, or operate the system or subsystem. In these cases, the Army's need to access OEM IP might directly conflict with the OEM's desire to retain strict control of data rights. Some IP and data rights considerations are prescribed in doctrine; for example, Army Directive 2018-26 provides that short- and long-term needs for data rights should be developed and updated before the issuance of a contract solicitation.[71]

There are several potential options to reduce supply chain risk linked to data rights and IP. These include the use of a technology escrow account,[72] the use of "specially negotiated" data rights early in an Army contract,[73] and an easily accessible central database that records the data rights that have been licensed or purchased by the Army.[74] Finally, lawyers in the DoD IP Cadre or other Army IP lawyers could assist PMs in identifying supply chain risks early in the IP strategy development process.[75]

We provide more details on IP and data rights as they relate to supply chain risks, along with mitigation strategies, in Appendix B.

---

[67] Boyson, 2014, p. 342.

[68] Boyson, 2014, p. 342.

[69] Samantha Schwartz, "Cyber Needs to Be a Part of Supply Chain Risk Management, Federal Agency Says," *Supply Chain Dive*, October 6, 2021.

[70] Schwartz, 2021.

[71] Army Directive 2018-26*, Enabling Modernization Through the Management of Intellectual Property*, Secretary of the Army, December 7, 2018.

[72] Julie Antonelli, "Protecting Emerging and Existing Technology Investments with Escrow," *Defense One*, August 14, 2020.

[73] DoDI 5010.44, 2019.

[74] U.S. Government Accountability Office (GAO), *Defense Acquisitions: DoD Should Take Additional Actions to Improve How It Approaches Intellectual Property*, GAO-22-104752, November 2021.

[75] GAO, 2021.

Demand

Demand Fluctuation and Uncertainty

Demand fluctuation and uncertainty is a fundamental supply chain risk studied in SCRM literature. Demand uncertainty can take the form of, for example, order cancellations, rush orders, or poor demand forecasting.[76] In the military supply chain, demand can be difficult to predict and can change dramatically during periods of transition between peacetime and wartime operations.[77] Demand fluctuation can also be driven by funding uncertainty: in most cases, if the demand is not there, the funding will not follow. However, in some cases, the demand is valid but funding shortfalls limit the amount that can be procured. Demand fluctuation can also mean that OEMs and sub-tier suppliers encounter sudden increases in demand that they might not be prepared to meet.

Mitigation options for demand fluctuation include investing in improved demand forecasting methods,[78] increasing the substitutability of products, and modifying inventory management strategies and distribution inefficiencies to increase supply chain agility and responsiveness surges in demand.[79]

Geopolitical

Country Risk

Country risk examines the quality of governance in OEM and sub-supplier nations. One important metric for this are the Worldwide Governance Indicators, which evaluate governance based on accountability, political instability, government effectiveness, regulatory quality, rule of law, and control of corruption.[80] Such business climate indicators as economic, financial, and political factors are another important component of country risk.[81]

Like provenance, country risk is another dimension where military counterintelligence and classified sources offer ASA (ALT) an additional layer of information beyond what can be provided by the OEM. For example, DoD regularly conducts validated online life cycle threat (VOLT) assessments that assess the threat presented by adversaries to current and future capabilities. These assessments uniquely assess risks in ways that are not provided by the OEM. For this reason, additional Army analyses can complement OEM country risk assessments.

Currency and Exchange Rate Fluctuations

Another driver of geopolitical supply chain risk regularly cited in SCRM literature is the fluctuation of currency and exchange rates.[82] In a global supply chain, there is a persistent risk that exchange rates between supplier nations will drastically change to the point that a supplier can no longer afford component parts. This was the case in 2007, when the Indonesian rupiah fell dramatically, and Indonesian companies could no longer afford imported critical components. The supply chain of customers who relied solely on Indonesian

[76] Aqlan and Lam, 2015; Loredo, Raffensperger, and Moore, 2015; O'Connell et al., 2021; Chopra and Sondhi, 2004; Sheffi et al., 2003.

[77] O'Connell et al., 2021, pp. 1, 9, 13.

[78] Loredo, Raffensperger, and Moore, 2015, p. 44.

[79] Patel et al., 2017, pp. 248–250.

[80] Silberglitt et al., 2013, p. 4.

[81] Lockamy, 2017, p. 179.

[82] Enyinda, Mbah, and Ogbuehi, 2010; Chopra and Sodhi, 2004; Pettit, Fiksel, and Croxton, 2010.

suppliers was severely disrupted. However, companies that diversified their sourcing were largely unaffected: These companies were able to procure their products from sources outside of Indonesia and provide financial assistance to their Indonesian suppliers.[83]

Nation-State or Terrorist Adversarial Activity

Military supply chains, especially when they are global, are vulnerable to espionage, sabotage, strategic manipulation of trade policies, and exploitation by nation-states or terrorist organizations. This is related to provenance; although domestic supply chains are still susceptible to attack, it is much easier for malicious actors to work within their own nations. Thus, one mitigation method is to restrict the countries and companies the United States does business with.[84]

The force majeure clause in OEM contracts generally covers risks associated with nation-state or terrorist adversarial activity: As with the risk from natural disasters, the supplier is absolved from liability and the risk is passed on to the buyer. One way ASA (ALT) can account for this is to require contracting OEMs to meet certain standards around regulations, preemptive mitigation, or resiliency measures.[85] Because ASA (ALT) has greater visibility on these issues than the OEM, there is a role for Army analysis to supplement any OEM assessments.

War or Armed Conflict

The Russian invasion of Ukraine in 2022 has highlighted the impact of war or armed conflict on supply chains, such as those related to energy. This risk driver is distinct from nation-state adversarial activity in that although war might be the activity of nation-states, the purpose of war has other aims besides disrupting the supply chain. Supply chain disruption is a consequence of war, but (often) not the main objective.

In addition to the obvious decline in production capacity while a country is embroiled in war, the supply chain can also be affected by sudden changes in trading between the warring nations and nations who are outside the physical conflict but become involved in other ways. Economic sanctions are a common tool in times of war, and they affect both the target nation and the originating nation. Here too, military counterintelligence and classified resources give ASA (ALT) information on risks that can complement those available from the OEM.

People and Skills

Labor Disruptions

SCRM literature identifies labor disruptions in the form of labor disputes (strikes),[86] organizational restructuring,[87] and other reasons for labor unavailability.[88] Labor strikes contribute to supply chain disruption in a very visible way, including strikes that occur outside of the OEM and sub-tier suppliers. For example, a 2002 dockworker strike in California shut down major ports for ten days, essentially stopping

[83] Tang, 2006, p. 37.

[84] O'Connell et al., 2021.

[85] O'Connell et al., 2021, p. 16.

[86] Chopra and Sodhi, 2004, p. 55; Loredo, Raffensperger, and Moore, 2015, p. 13.

[87] Loredo, Raffensperger, and Moore, 2015, p. 13.

[88] Moore et al., 2015, p. 66; Luckstead, Nayga, and Snell, 2021.

supply chain flow through the West Coast.[89] However, strikes are not the only source of labor disruption; throughout 2020, the COVID-19 outbreak caused labor shortages in a different way. In the food industry, to give one example, supply chains that were already strained from a rapid shift in consumer spending from the food service industry to food retailers were stressed even further as large numbers of workers were required to quarantine.[90]

Mitigation of labor disruption is baked into some acquisition regulations. Section 22.101-2(b) of FAR, for example, stipulates that the risk of a labor disruption itself is not the supplier's responsibility, but the delays do become the supplier's responsibility if the supplier does not act within their capabilities to resolve the labor disruption.[91] Thus, it is important during source selection to consider an OEM's resilience to disruption due to labor issues.

Skill Obsolescence

Skills obsolescence is not often studied in SCRM literature, but in the military and aerospace sectors, where products have decades of field lifetime, it is a real risk. As the labor force ages and individuals leave the workforce, essential knowledge and skills vital to legacy systems become increasingly difficult to obtain.[92] Modeling can demonstrate the cost of skill obsolescence and motivate appropriate hiring and training practices to mitigate this risk.[93]

Strategic Materials

Raw Material Access

The United States is dependent on imports of many critical materials that are used in manufacturing and that support both commercial and military applications.[94] U.S. companies rely on imports for many critical materials used in manufacturing, including "semiconductors, such as indium, gallium, and germanium; metals used in high-temperature alloys, such as vanadium and rhenium; antimony . . . and tungsten, a critical component in materials for drilling, cutting, and machining."[95] This introduces an element of risk: If export restrictions begin limiting access to these materials, the ability of OEMs and sub-tier suppliers to provide products could be severely hampered.[96] The risk is not insignificant; a 2010 study examined the availability of 51 critical materials under several conflict scenarios and determined that there would be a shortage of 21 of these materials.[97]

---

[89] Chopra and Sodhi, 2004, p. 55; Castellan, *Supply Chain Continuity: The Impact of Global Labor—How COVID-19 Exposed Risk for Disruption*, White Paper, 2020.

[90] Luckstead, Nayga, and Snell, 2021, pp. 383–384.

[91] Federal Acquisition Regulation, Part 22, Application of Labor Laws to Government Acquisitions; Section 22.101-2, Contract Pricing and Administration.

[92] Loredo, Raffensperger, and Moore, 2015, p. 51; Moore et al., 2015, p. 66.

[93] Sandborn, Prabhakar, and Kusimo, 2012.

[94] Silberglitt et al., 2013.

[95] Richard Silberglitt, *Critical Materials and U.S. Import Reliance: Recent Developments and Recommended Actions*, RAND Corporation, CT-485, 2017, p. 2.

[96] Silberglitt et al., 2013.

[97] Thomason et al., 2010.

To assess this risk, a criticality assessment framework was developed by the National Research Council Committee on Critical Mineral Impacts on the U.S. Economy.[98] This framework assesses material risk by examining both the likelihood and estimated severity of a restriction of that material.

At the OEM and sub-tier supplier levels, importing critical materials from multiple nations is one way to reduce this risk. However, many mitigation measures require coordination at higher levels, including internationally. For example, if a nation has a controlling market share in a material, it takes an international effort to prevent that share from increasing by, for example, that nation obtaining control of material sources in additional nations. Long-term mitigation methods include increasing the efficient use of critical materials, increasing secondary production of critical materials, and reducing demand of critical materials through alternate product design.[99]

Transportation and Inventory

Aging Infrastructure

Aging infrastructure can delay extraction, transportation, or production of critical components and strategic materials. The obvious risk here is when infrastructure suffers a catastrophic failure, materiel shortages can lead to massive disruptions at the OEM and sub-tier supplier levels.[100] Even without a catastrophic failure, at some point aging infrastructure needs to be upgraded or replaced. Depending on the scale and criticality of the infrastructure, this process can be extremely resource and time consuming. A well-planned replacement strategy will minimize supply chain disruption, but it might be impossible to guarantee complete business as usual.

Ensuring suppliers are up-to-date on relevant regulations and plan sufficiently for upgrades can help mitigate the risk from aging corporate infrastructure. However, some major components of supply chain infrastructure, such as roads, seaports, and airports, are outside the purview of any supplier. For these components, infrastructure risk could be incorporated as an element of country risk.

Long Production Lead Times

A long production lead time—the period between when an order is placed and when the order is received—is a compounding factor in supply chain risk. Long lead times hamper a supplier's ability to react to market changes and can result in backorder and supply disruption for the OEM and sub-tier suppliers, which in turn can cause a financial burden along the supply chain participants.[101] The risk is an important one for the Army to consider: AMC's SSWG identified long lead times as one of their top three supplier risks.[102]

Long lead times are often an artifact of international supply chains; however, international shipping is not the only factor that contributes to long lead times. Delays in order processing, suppliers with no on-hand inventory, and suppliers with long internal lead times, for example, can all contribute to lengthy production processes. Some factors contributing to long lead times are inherent in a supply chain and cannot be reduced,

[98] Committee on Critical Mineral Impacts of the U.S. Economy, National Research Council of the National Academies, *Minerals, Critical Minerals, and the U.S. Economy*, National Academies Press, 2008.

[99] Silberglitt et al., 2013.

[100] Loredo, Raffensperger, and Moore, 2015.

[101] McClean, 2017.

[102] Loredo, Raffensperger, and Moore, 2015, p. 14.

but lean supply chain management practices, such as value stream mapping, can be used to remove inefficiencies in the process.[103]

Product Obsolescence

Product obsolescence occurs when technological innovation outpaces product life cycles and critical components for the product can no longer be obtained.[104] The risk during a product's sustainment phase is obvious: Weapon systems are intended to be sustained for decades, increasing the likelihood that electronics and other technological components are no longer produced by suppliers in favor of the newest, state-of-the-art versions.[105] However, this risk is also present in the acquisition phase, where long administrative lead times can lead to products whose designs are obsolete before they are even produced or fielded.[106]

Product obsolescence also affects mitigation strategies that suppliers might use in response to other risks. For example, suppliers might stockpile products to protect themselves against disruption; however, if that product has a high rate of obsolescence, in a few years, the supplier might find itself with a warehouse full of goods it cannot sell. To avoid stockpiles of obsolete goods, supply chain experts recommend that suppliers bolster supply chains against disruption by increasing their pool of suppliers rather than stockpiling.[107] However, this strategy could increase the Army's risk from obsolescence down the road because there will be fewer worldwide stocks of parts and components that are no longer actively produced.

Product Characteristics

Finally, characteristics of the products themselves can affect supply chain risk. One product or component might carry more risk than another simply because of its inherent properties. These might include inventory holding cost, which might be larger if the item is bulky or requires special storage procedures; whether the item is interchangeable with others; whether a different part can be substituted for the item; or whether the item is a critical component to the weapon system. These characteristics can affect the OEM's procurement ability and introduce risk into the supply chain.[108]

Summary

In this chapter, we proposed a list of supply chain risk categories that should be considered by the Army for assessment (either by the Army or through the OEM, or jointly) during the acquisition life cycle. We provided proposed definitions, examples of their effects on supply chains, and—where applicable—appropriate mitigation strategies. The supply chain risks provided in this chapter are intended to be the most-likely risks for the majority of major acquisition systems—although, for any given system, many risks might be insignificant or not apply at all. In addition, some of these risks have overlapping challenges, resulting in some mitigations that affect multiple risks. The priority assigned to each risk will change based on many factors, such as perceived cost and severity of a disruption and the interactions among any potential mitigation.

In the next chapter, we describe recent Army and DoD responses to supply chain risks, including new guidance. We propose three frameworks that correspond to phases of the acquisition life cycle with a descrip-

[103] McClean, 2017.

[104] Gravier and Swartz, 2009.

[105] O'Connell et al., 2021, p. 9.

[106] Gravier and Swartz, 2009, p. 87.

[107] Chopra and Sodhi, 2004, p. 56.

[108] Loredo, Raffensperger, and Moore, 2015; Chopra and Sodhi, 2004.

tion of what supply chain risk assessment activities should occur and how they manifest within existing documents provided during the key acquisition milestones. We then provide suggestions for how these mitigations might occur through contracting documents.

CHAPTER 3

Proposed Common Operating Procedure for Life-Cycle Supply Chain Risk

This chapter addresses two of the sponsor's three key questions: how to integrate supply chain risk assessments into acquisition decisions and who should be primarily responsible for assessing and managing those supply chain risks during each phase of the acquisition life cycle. The chapter describes the initial DoD and Army responses to the emergence of supply chain risk as an issue of concern; describes proposed risk assessment frameworks and relates them to acquisition milestones; and recommends how the Army should align SCRM responsibilities.

The Army and DoD Response to Supply Chain Risk

Over the past several years, DoD and the Army have recognized and refined their approach to supply chain management and SCRM. In a draft SCRM directive from the Secretary of the Army in 2021, the Army recognized a need to change how it views SCRM. See Appendix C for a review of relevant SCRM policies and guidelines.

Department of the Army Draft SCRM Directive Objective

The 2021 Army draft SCRM directive states that

> SCRM will change how the Army identifies, assesses, mitigates, and monitors supply chain risk. SCRM will become an integral part of Army's acquisition and sustainment business processes as a risk-based approach to enable supply chain resiliency and security. SCRM will be implemented in a phased approach to support scalability and evolve processes.[1]

The draft directive goes on to state that SCRM will be conducted on "all systems throughout their *lifecycle* [emphasis added] beginning at pre-milestone B or earliest acquisition entry point suitable and reviewed periodically throughout the operations and sustainment phase until disposal."[2] Although this draft policy is still under review, it is a clear articulation of the Army's intent to establish an SCRM capability. The draft policy also describes the roles and responsibilities of ASA (ALT), the Deputy Assistant Secretary of the Army for Sustainment (DASA-S), Army Futures Command (AFC), and Army Materiel Command (AMC). Table 3.1 summarizes the responsibilities outlined in the draft policy.

[1] Department of the Army, 2021, p. 2.

[2] Department of the Army, 2021, p. 2.

TABLE 3.1
Organizations and Responsibilities for Army SCRM

Organization	Responsibility
ASA (ALT)	• Develop SCRM policy and delegate oversight responsibilities to DASA-S
DASA-S	• Establish a single SCRM policy, set of procedures, and guidebook • Forge relationships with other DoD organizations and federal agencies to adopt best-of-breed SCRM practices within Army's SCRM capabilities • Develop and promulgate recommended contract language to support SCRM activities within the acquisition and sustainment communities • Provide SCRM policy and procedures execution responsibilities to the PEO
PEO	• Conduct SCRM activities within the framework of identify, assess, mitigate, and monitor on systems for which they oversee development • Conduct SCRM assessments on systems for which they oversee development and document the results, identifying the highest risk to the system with potential mitigating actions • Develop funding requirements to support SCRM activities across systems for which they oversee development within the following priorities (as applicable): 1. Army's (31 plus 4)[a] systems 2. systems identified on the critical programs and technologies list 3. national security systems 4. all other new systems 5. legacy systems
AFC	• Integrate SCRM into the Army's modernization strategy to ensure supply chain resiliency enablers are included in system sustainment requirements • Identify critical program technologies requiring greater levels of protection
AMC	• Integrate SCRM activities into Army's sustainment enterprise management process to identify organic industrial base sector risk and mitigating actions • Synchronize with the Defense Logistics Agency (DLA) (provisioning) and OSD Industrial Policy (ammunition-chemicals) to ensure there is proper alignment with Army SCRM efforts and risk mitigation • Integrate the Army Contracting Command (ACC) into Army SCRM approach to ensure contracts contain appropriate language to support SCRM activities • Through the Life Cycle Management Commands (LCMC), partner with materiel developers • During SCRM assessments, formulate an understanding of the system's supply chain risk, mitigating actions, and monitoring requirements to effectively execute supply chain management at provision and throughout the system's life cycle until disposal.

SOURCE: Department of the Army, 2021.

[a] 31 plus 4 are the signature weapon systems necessary to achieve the Army's Multi-Domain Operations Concept.

Following the roles and responsibility guidance provided by the draft SCRM Directive shown in Table 3.1, we developed an LSCRM approach using the JCIDS Major Acquisition, Acquisition and Procurement Milestones, Phases and Decision Points, also known as the Defense Acquisition University (DAU) Defense Acquisition Life Cycle (see DoDI 5000.02T). The Defense Acquisition Life Cycle is a doctrinally defined process that covers multiple programs and can be adapted to suit the details of each program, as shown later in Figures 3.2 through 3.4.[3]

The proposed approach consists of three frameworks, nested within the Defense Acquisition Life Cycle, that together provide LSCRM. This chapter describes each framework in detail and provides guidance for their implementation. The intent is twofold: to provide the Army with a step-by-step process that can systematically identify supply chain risk and to identify SCRM information requirements.

[3] Where appropriate, references are also made to DoDI 4140.01; DoDM 4140.01, 2018; Department of the Army Pamphlet 70-3, *Army Acquisition Procedures*, Department of the Army, September 17, 2018; Army Regulation (AR) 25-1, *Army Information Technology*, Department of the Army, July 15, 2019; AR 70-1, *Army Acquisition Policy*, Department of the Army, August 10, 2018; and AR 702-19, *Reliability, Availability, and Maintainability*, Department of the Army, February 12, 2020.

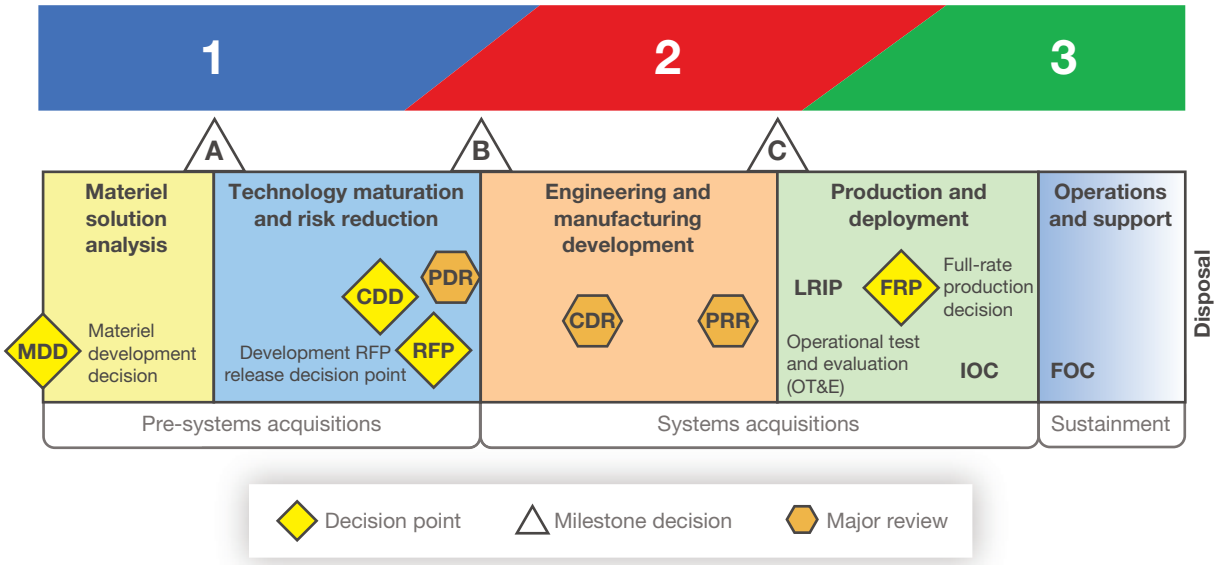
The three frameworks are aligned with naturally occurring transitions in the acquisition life-cycle flow: (1) between the initial development of new concepts and transformational approaches to Army mission objectives into low-rate and full-rate production (FRP) levels and (2) the transition to the full-scale operational deployment; maintenance and sustainment; and retirement of the system. Figure 3.1 illustrates how these frameworks align over the acquisition life cycle.

Several Army entities cooperate to direct and advance programs and manage supply chain risk. The key organizations include AFC, ASA (ALT), and AMC. The proposed assignment of lead organization to frameworks is based on the level of expertise, decisionmaking authority, and visibility these organizations currently hold during each phase of the acquisition life cycle. The proposed assignment of lead responsibility is also reflected in the draft Army SCRM Directive summarized in Table 3.1.

An Approach for Lifecyle SCRM over the Course of the JCIDS Acquisition Life Cycle

In this section, we review the processes described in the JCIDS acquisition life cycle, focusing on how SCRM might play a role in a system's life cycle. We highlight and provide a description of the key processes and documents in the acquisition process, including how SCRM might be incorporated into existing process steps. These recommendations rest on our review of acquisition policy and practice to identify activities and decisions that would benefit from assessments of supply chain risk.

FIGURE 3.1
Proposed LSCRM Frameworks Overlap with the Acquisition Life Cycle



SOURCE: Adapted from DoDI 5000.02T, 2017.

NOTE: CDD = capabilities development document; CDR = critical design review; FOC = full operational capability; IOC = initial operational capability; LRIP = low-rate initial production; PDR = preliminary design review; PRR = production readiness review; RFP = request for proposal.

We emphasize that coordination across all acquisition activities will be critical for LSCRM, though some activities, such as the multidisciplinary counterintelligence threat assessment (MDCITA) and the critical intelligence parameters (CIP) should necessarily be government-centric, requiring special clearance and access. The processes described in this section are systemic and cumulative, relying on all the preceding actions; where the LSCRM for an acquisition might be implemented or enhanced mid-stream, some foundational actions and decisions will be required retroactively.

Framework 1: Initial Capabilities Development to Engineering and Manufacturing Development and Milestone B

Figure 3.2 illustrates the JCIDS actions, decisions, and documents produced in the portion of the life cycle covered by Framework 1. These are the steps between the initial capabilities document (ICD) decision and engineering and manufacturing development (EMD), leading to the milestone B decision point. Box 3.1 details the proposed LSCRM activities integrated within the existing JCIDS process.

At the conclusion of the phase covered by Framework 1, design decisions, engineering, and planning result in a gradually improving understanding of the program supply chain and supply chain risk. Correspondingly, approaches to managing supply chain risks should begin to be codified during this phase.

Framework 2: From Milestone B to Full-Rate Production

Figure 3.3 illustrates the time phasing of the key process steps and documents produced and executed in Framework 2. These are the steps between the EMD step, after Milestone B, and entering FRP of the system. At this point in the process, a prime contractor is selected, and they have already provided information regarding supply chain risk. For systems entering the acquisition process at this phase, retroactive actions supporting SCRM will be required, as determined by the nature of the specific program.

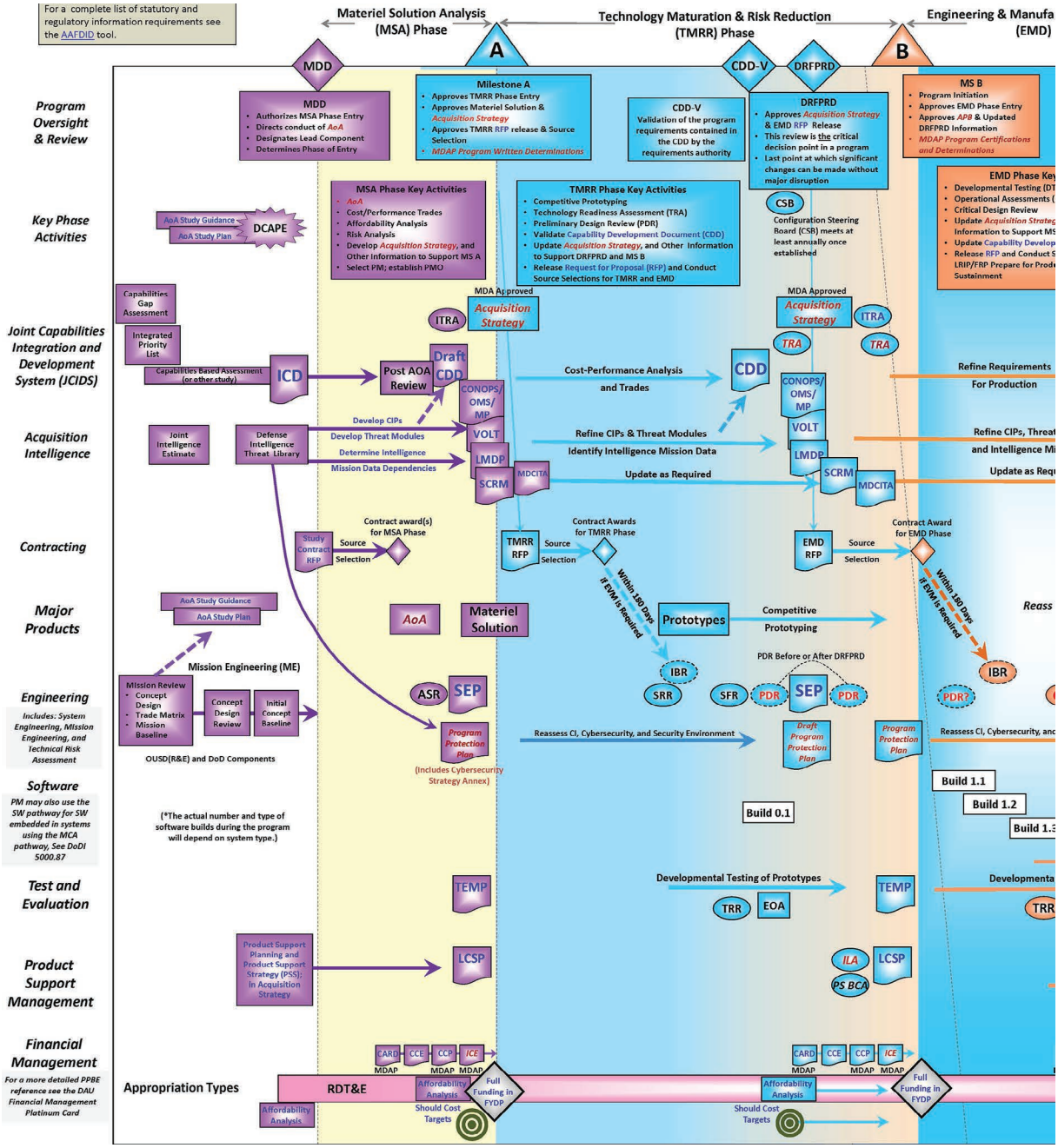
Box 3.2 details the proposed LSCRM activities integrated within the existing JCIDS process covering Framework 2. At the conclusion of the steps covered by Framework 2, the system has entered FRP. At that point, supply chain risk shifts from developmental to operational, meaning that some supply chain risks that were identified in earlier phases might become apparent, while others will be identified.

Framework 3: From Full Rate-Production to End-of-Life

Figure 3.4 illustrates the time phasing of the key process steps and documents produced and executed in Framework 3. These are the steps after entering FRP and continuing into sustainment and end-of-life phases. Box 3.3 details the proposed LSCRM activities integrated within the existing JCIDS process covering Framework 3.

FIGURE 3.2

Portion of the DAU Life Cycle Chart Corresponding to Framework 1



SOURCE: Reproduced from DAU, "Major Capabilities Acquisition (Pre-Tailoring): Acquisition & Procurement Milestones, Phases and Decision Points," chart, Ver. 2.1, October 21, 2022b.
NOTE: Abbreviations used in this figure that are relevant to this report are defined in Boxes 3.1 through 3.3 or can be found in the Abbreviations list.

BOX 3.1

Proposed Life-Cycle Supply Chain Risk Management Touchpoints in Framework 1, from Program Concept to Milestone B, based on JCIDS Major Capabilities Acquisition Chart

1. Initiation of LSCRM process: The initial capabilities document (ICD) provides the initial system concept upon which the program protection plan and concept of operations (CONOPS) will be developed. It is also the entry document for the material development decision (MDD). This initiation establishes the basic description of the system under development and begins to define the key elements of the supply chain and supply chain risk.
2. Analysis of alternatives (AoA): Comparison of possible solutions for the ICD, a trade study that should include respective supply chains. This step provides an opportunity to begin to anticipate potential supply chain risks and risk mitigation methodologies for each alternative. The AoA could include a comparison of supply chain risk factors for each alternative. This formation is obtained through the initial request for proposal (RFP) to industry shown in Figure 3.2 (in the contracting lane).
3. Major defense acquisition program (MDAP) and major automated information system (MAIS): Congressional mandate for accounting in major programs requires independent technology risk assessment (ITRA) and foreign involvement assessment, including risk-sharing. Currently, this is the only supply chain risk assessment required by policy.
4. Program protection plan (PPP): Includes annexes or links to the validated online life cycle threat (VOLT); the life cycle mission data plan (LMDP), which documents the critical intelligence parameters (CIP); and the SCRM requirements.[a] It is an annex of and linked to the systems engineering plan (SEP). This document is a natural collection point for risk mitigation strategies once risks have been identified.
5. Product support strategy (PSS)/life-cycle sustainment plan (LCSP) ties in with the SEP and includes plans for supply chains in sustainment. In the frameworks, we prescribe a series of contractual deliverables in the form of contract data requirements lists (CDRLs) to provide the Army with the contractor's concise supply chain risk analysis and mitigation efforts.
6. The LCSP informs the concept of operations/operational mode summary/mission profile (CONOPS/OMS/MP), which should include system plans for delivery and sustainment supply chains.
7. The CONOPS informs the draft capabilities development document (CDD), which informs the acquisition strategy and the TMRR RFP. Note that the RFP will require new language delineating SCRM information requirements, which DAU indicates is an area for new research.[b] The material solution is the statement of work (SOW) and not the system design because the system design is determined after the contract award. At this phase, early technology and material decisions might affect the resulting product supply chain and supply chain risk.
   a. After receipt of the proposals from interested prime contractors, the source selection reflects the decisions of a panel of experts—including users, risk, costing, and the technology relevant to the program—culminating in the selection of one proposal to be awarded a contract with the government. Including supply chain experts in the source selection panels and providing them with the respective preliminary bills of materials (PBOMs) and the respective SCRM plans will facilitate elevating SCRM to a selection score criterion.
   b. Contract award transforms the proposal that was selected into a contract with the government, generally with some minor adjustments.
      i. TMRR contract award is the point at which the government has the path for technical development and all the contract obligations of the awardee. Any LSCRM effort to be performed by the awardee in TMRR must be delineated in this contract.
      ii. Discussions with DAU reveal there are no standard approaches for this documentation of LSCRM in the RFP or in the contract.

Box 3.1—Continued

8. System requirements review (SRR) (The draft system requirements document [SRD] is the input document for the decision gate of the SRR. The output is the approved version of the SRD): In most development efforts, the system requirements will be a refinement of the deliverable parameters (technical, operational, functional) worked out between the awardee and the government and will include (in section 2.2.1 of the SRD) a listing of all relevant DoD and Army standards, including for SCRM. It feeds into the integrated baseline review (IBR) and the system functional review (SFR).
9. SFR is held to validate whether the functional baseline satisfies the end-user requirements and capability needs (including support, logistics, and supply chain) and whether functional requirements and verification methods support achievement of performance requirements. This includes validation of the system supply chain and SCRM. At completion of the SFR, the functional baseline is normally taken under configuration control—an important step for documenting the supply chains.
10. Capabilities development document (CDD) (developed from the draft CDD, building on engagement and refinements with prime contractor) specifies capability requirements in terms of developmental key performance parameters (KPPs), key system attributes (KSAs), additional performance attributes (APAs), and other related information necessary to support development of one or more increments of a materiel capability solution. CDD validation precedes the development RFP release decision point.
11. Prototypes in SCRM: The bill of materials (BOM/PBOM) that is refined during a prototype development provides foundational information for the LSCRM process. Also, the Build 0.1 of the software establishes the software supply chain foundation. LSCRM will need to establish sources for all materials and origins of all code (including open-source software) used.
12. The program progression toward Milestone B and the engineering and manufacturing development phase includes revisiting the acquisition strategy and the continuous revision and iteration of several documents related to SCRM, including the VOLT, LMDP, SCRM (PM and systems engineer working with the awardee) and the MDCITA (the latter by the Army Intelligence and Security Command [INSCOM] and the Defense Intelligence Agency [DIA]). The SEP and the PPP are updated by the government and contractor systems engineers and the PSS is updated and cleared through the independent logistics assessment (ILA).
13. The engineering and manufacturing development (EMD) phase RFP will contain the LSCRM criteria and prescriptive processes developed in the many respective documents and decision gates up to this point in the program, including the draft SEP and the draft PPP.

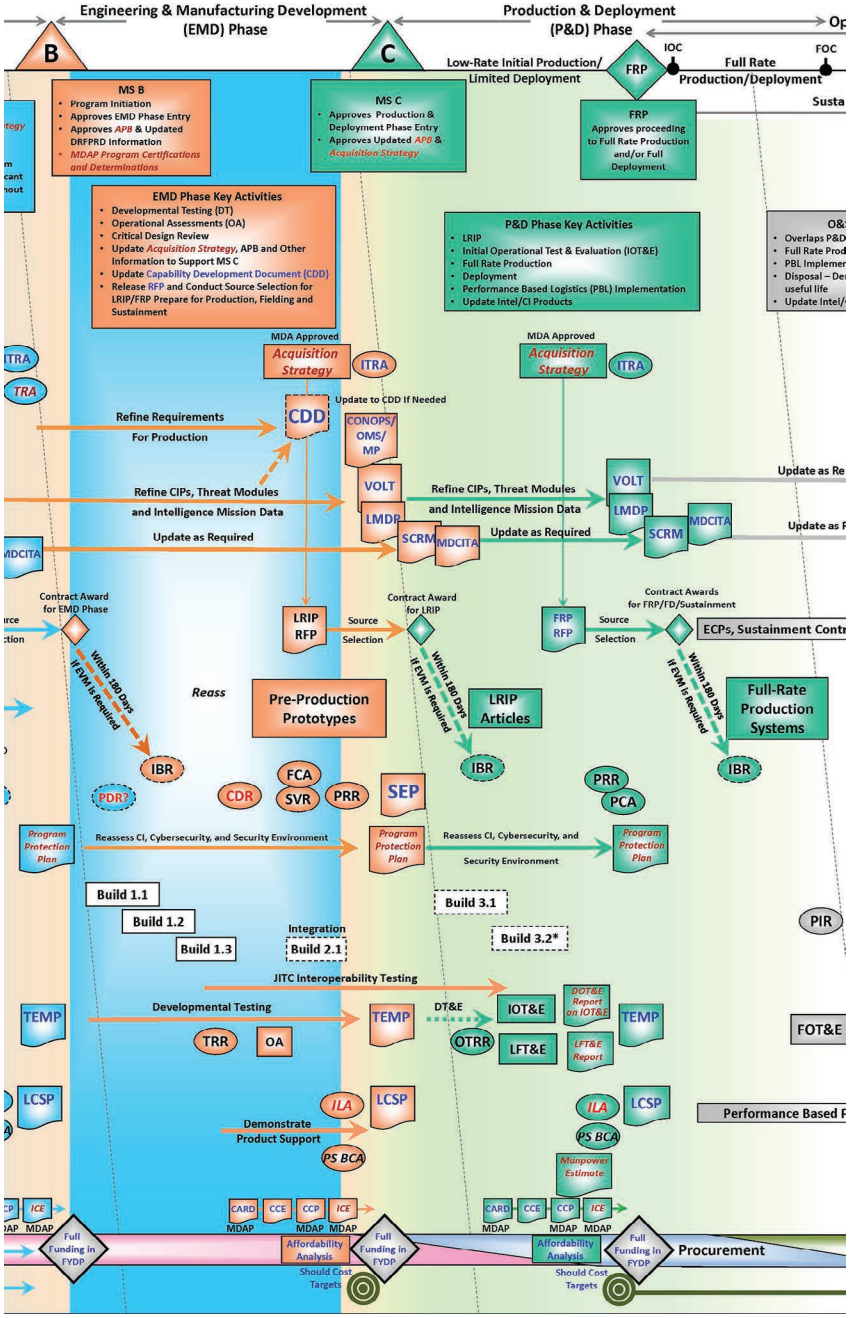
SOURCES: Authors' analysis of DoDI 5000.02T, 2017; AcqNotes, "Capability Production Document (CPD)," webpage, February 12, 2020; AcqNotes, "Critical Design Review (CDR)," webpage, June 1, 2021a; AcqNotes, "Statement of Work (SOW)," webpage, June 6, 2021b; AcqNotes, "Performance Measurement Baseline (PMB)," webpage, June 24, 2021c; AcqNotes, "Integrated Baseline Review (IBR), webpage," June 26, 2021d; AcqNotes, "Functional Configuration Audit (FCA)," webpage, June 29, 2021e; AcqNotes, "Low-Rate Initial Production (LRIP)," webpage, June 30, 2021f; AcqNotes, "Life-Cycle Sustainment Plan (LCSP)," webpage, July 2, 2021g; AcqNotes, "Initial Operational Test & Evaluation (IOT&E)," webpage, July 8, 2021h; AcqNotes, "Product Support Strategy (PSS)," webpage, July 14, 2021i; AcqNotes, "Live-Fire Test and Evaluation (LFT&E)," webpage, July 17, 2021j; AcqNotes, "System Verification Review (SVR)," webpage, July 26, 2021k; DAU, "Engineering and Manufacturing Development (EMD) Phase," webpage, undated-b; DAU, "Systems Engineering Plan (SEP)," webpage, undated-c; DAU, *Product Support Strategy Development Tool*, 2022a; DAU, 2022b.

[a] The multidisciplinary counterintelligence threat assessment (MDCITA) is a classified annex to the SCRM that involves Army INSCOM, 902nd Military Intelligence Group, and likely DIA.

[b] DAU communication to the authors via DAU's "Ask a Professor" webpage, February 14, 2022.

FIGURE 3.3

Portion of the DAU Life Cycle Chart Corresponding to Framework 2



SOURCE: Reproduced from DAU, 2022a.
NOTE: Abbreviations used in this figure that are relevant to this report are defined in Boxes 3.1 through 3.3 or can be found in the Abbreviations list.

BOX 3.2

Proposed Life-Cycle Supply Chain Risk Management Touchpoints in Framework 2, from Milestone B to Full-Rate Production

14. The EMD phase source selection process, in addition to assessing and comparing the respective offerors' systems solutions to the RFP and their capability to progress to a manufacturable/deployable system, will be a critical assessment point of the LSCRM knowledge and methods of the potential awardee. Additions to the source selection process, including clear SCRM requirements in the RFP and the inclusion of supply chain experts in the source selection panel, will help the Army address this. The integrated LSCRM plan should be a part of the EMD SEP and EMD PPP, developed cooperatively by the Army program systems engineer and the awardee at the start of the EMD phase. During EMD, the capability production document (CPD) is prepared and should include supply chain risk factors.
15. The PM and systems engineer will finalize system designs for product support elements and integrate them into a comprehensive support package that is documented in a PSS. The PSS is detailed in the LCSP, which documents the plan for formulating, integrating, and executing the PSS (including any support contracts) to meet the warfighters' mission requirements and the sustainment requirements within the milestone decision authority (MDA)-approved program goals established at Milestone A. The PSS and the LCSP in the EMD phase set the baseline for program support logistics and the associated supply chains. The risks associated with the respective, proposed supply chain choices should be weighed and managed at this phase, along with setting early criteria for logistics/sustainment SCRM over the duration of the life cycle.
16. The EMD contract award codifies everything to this point in the life cycle, including LSCRM requirements, in a contract with the EMD phase awardee. If something was not asked for in the RFP, it will not be in the proposal, and if it is not in the proposal, it will not be in the contract. The requirements and the indices of performance are codified in the SOW and the performance measurement baseline (PMB) (*not shown in Figure 3.3*). Getting to this point with an LSCRM plan requires a well-worded RFP.
17. The integrated baseline review (IBR) is a joint assessment conducted by the PM and the contractor to establish a mutual understanding of the PMB. This understanding provides for an agreement on a plan of action to evaluate the risks inherent in the PMB and the management processes that operate during program execution. The approach for assessing performance measurement should include metrics on the completeness of the developing SCRM approach as a function of the certainty of the supply chain.
18. During the EMD phase, system requirements are continuously refined for production and deployment; these refinements are reflected in the updated CDD. The LMDP, CIP, MDCITA, and PPP are continuously updated; the SCRM requirements should also evolve with the technical requirements, and all are a part of the SEP *living document*. LSCRM evolves while keeping pace with the needs of the EMD phase.
19. The critical design reviews (CDR) are decision gates to ensure that a system can meet the refined CDD requirements and proceed into production and deployment within cost, schedule, and risk—including supply chain risk—parameters. In complex systems, there are usually multiple CDRs, so at least one should include LSCRM. The decision results are validated at the functional configuration audit (FCA), which is the decision gate to proceed to low-rate initial production (LRIP). Supply chain risks should be reviewed and mitigation plans discussed as part of the FCA.

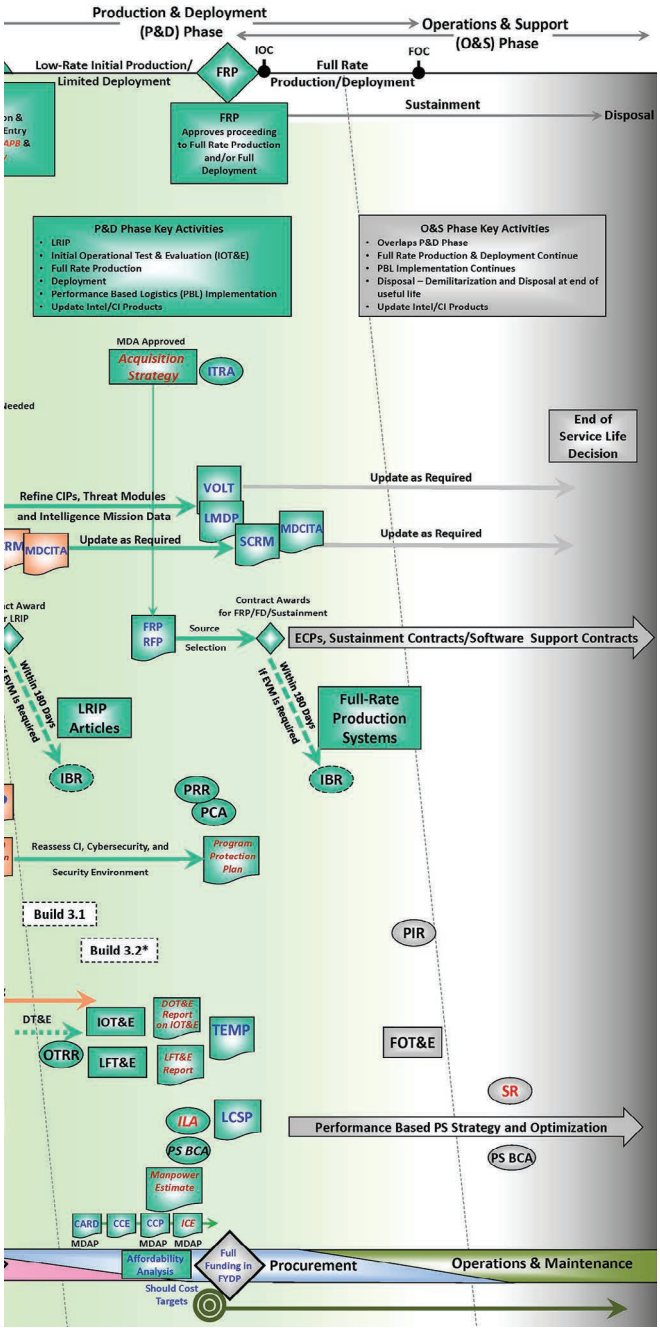
Box 3.2—Continued

20. The actions preceding LRIP include revisiting the acquisition strategy to ensure it is correct for the program entering LRIP; updating the CDD; finalizing the CONOPS for the program; and drafting the LRIP RFP based on the FCA and the system verification review (SVR). The LSCRM processes and metrics should be assessed and included in the verbiage for the LRIP RFP.
21. Note that the award of LRIP marks the transition period from research, development, test and evaluation (RDT&E) funding to procurement funding.
22. Contract award for LRIP (generally combined with award for full-rate production [FRP]) means a full revisiting (with the awardee) of the VOLT, LMDR, SCRM requirements, and MDCITA appropriate revisions made to the SEP and PPP with respect to changes in the supply chain for low-rate production. It also requires revised LCSP/PSS for LRIP/FRP (including a demonstration of the product support plan) and a plan to manage supply chain risk associated with all the supply chain changes. FRP should include an end-of-life LSCRM plan/CDRL.
23. Per Department of the Army Pamphlet 70-3, Chapter 10, the type classification process takes place during the transition from RDT&E funds to procurement funds.

SOURCES: Authors' analysis of DoDI 5000.02T, 2017; AcqNotes, 2020; AcqNotes, 2021a; AcqNotes, 2021b; AcqNotes, 2021c; AcqNotes, 2021d; AcqNotes, 2021e; AcqNotes, 2021f; AcqNotes, 2021g; AcqNotes, 2021h; AcqNotes, 2021i; AcqNotes, 2021j; AcqNotes, 2021k; DAU, undated-b; DAU, undated-c; DAU, 2022a; DAU, 2022b.

FIGURE 3.4

Portion of the DAU Life Cycle Chart Corresponding to Framework 3



SOURCE: Reproduced from DAU, 2022a.
NOTE: Abbreviations used in this figure that are relevant to this report are defined in Boxes 3.1 through 3.3 or can be found in the Abbreviations list.

BOX 3.3

Proposed Life-Cycle Supply Chain Risk Management Touchpoints in Framework 3, Full-Rate Production to Retirement

24. The transition from Framework 2 to Framework 3 requires extensive coordination and hand-off between program offices, presumably ASA (ALT) and AMC. It aligns with the transition from procurement funding to operations and maintenance funding and associated requirements for supply management and supply chain capacity under DoD 7000.14-R.[a]
25. Initial operational test and evaluation (IOT&E) and live fire test and evaluation (LFT&E) (preceded by the CPD certification at Milestone C [*not shown in Figure 3.4*]) frequently lead to changes in production materials and system design, with impacts on supply chain and LSCRM. Accommodation for these changes should be accounted for in the CDRL and data item description instructions in the RFP and a review of LSCRM before FRP decision review. By the start of FRP/Framework 3, the production supply chain should be codified and documented. The SCRM plan in the SEP, the PPP, and the PSS should be in final form.
26. FRP, sustainment, and support contracts should have an LSCRM plan and an LSCRM CDRL that was defined during source selection.
27. The FRP contract should also include an end-of-life LSCRM CDRL developed during LRIP.
28. LSCRM plans and deliverables codified during Framework 2 as we have proposed will be included in Framework 3 system maintenance and sustainment contracts; performance-based life-cycle product support; and performance-based logistics programs.

SOURCES: Authors' analysis of DoDI 5000.02T, 2017; AcqNotes, 2020; AcqNotes, 2021a; AcqNotes, 2021b; AcqNotes, 2021c; AcqNotes, 2021d; AcqNotes, 2021e; AcqNotes, 2021f; AcqNotes, 2021g; AcqNotes, 2021h; AcqNotes, 2021i; AcqNotes, 2021j; AcqNotes, 2021k; DAU, undated-b; DAU, undated-c; DAU, 2022a; DAU, 2022b.

[a] DoD 7000.14-R, *Financial Management Regulation*, Volume 2A, "Budget Formulation and Presentation (Chapters 1–3)," Office of the Under Secretary of Defense (Comptroller), June 2017.

The preceding boxes are intended to provide an overview of the LSCRM touchpoints for each of the respective actions in the DoD 5000.02T process. They might be useful for a PEO, PM, chief systems engineer, or other acquisition stakeholder addressing the supply chain aspects of a specific gate or document in the acquisition life cycle, including how that action might fit in the systemic SCRM process. The next section addresses proposed SCRM improvements and changes to the existing acquisition process and the cooperation of the awardee (i.e., the OEM) with the government in achieving better supply chain awareness and risk management.

Proposed Critical LSCRM Activities Across the Acquisition Lifecyle

The figures presented later in this section correspond to those sections of the JCIDS major capabilities acquisition chart provided in Figures 3.2 through 3.4 and the LSCRM-related activities described in Boxes 3.1 through 3.3, with the addition of the documents that will directly capture information related to LSCRM.

This section also proposes an alignment of responsibilities for SCRM across the different phases of the acquisition life cycle. We made those recommendations based on three considerations:

- the organization that has primary responsibility for the acquisition process activities during that phase of the life cycle
- the nature of the acquisition activity or life-cycle process being supported
- the organization that has the best access to the relevant information.

Proposed Framework 1 Activities

This subsection outlines the proposed LSRCM activities that would occur during the early phases of acquisition. Specifically, we map the proposed activities from Box 3.1 to those portions of the JCIDS major capabilities acquisition chart shown in Figure 3.2.

For instance, the dashed red oval in Figure 3.5 shows that, in addition to producing an AoA trade study, Framework 1 calls for the creation of an AoA supply chain risk assessment matrix. This AoA matrix uses the information gathered on supply chain risk during the request for information (RFI) phase of the system development process. It augments the information provided in the AoA and forces a consideration of supply chain risk as part of the AoA decision process.

We propose that AFC—working closely with the PEO under which the program falls and with ASA (ALT) with respect to its legal acquisition milestone decision authorities—would be the natural lead for the SCRM activities described in Framework 1. This recommendation is based on AFC's authorities to develop the Army's future warfighting capabilities and the alignment of the Army's research and development laboratories under AFC. As the proposed systems are being developed through AFC's innovation and prototyping processes, questions about how the material and design choices will be supported by supply chains should be raised and addressed. AFC has the greatest control and visibility over the decisions that will affect supply chain risk. This recommendation is also supported by the language in the Army's draft SCRM directive.

Addressing Life-Cycle Supply Chain Risk Management from Program Conception

The top half of Figure 3.5 shows the processes and documents that fall within the responsibility of the U.S. government. The boxes shown in the bottom half of Figure 3.5 are the points during the acquisition process where information about supply chain risk should be requested from the commercial entities, such as the prospective prime contractor or OEM, as part of the initial RFI offering. The boxes that overlap industry and government lanes represent points in the process of very close coordination between the government and the commercial vendors, for example, during prototype development and evaluation.

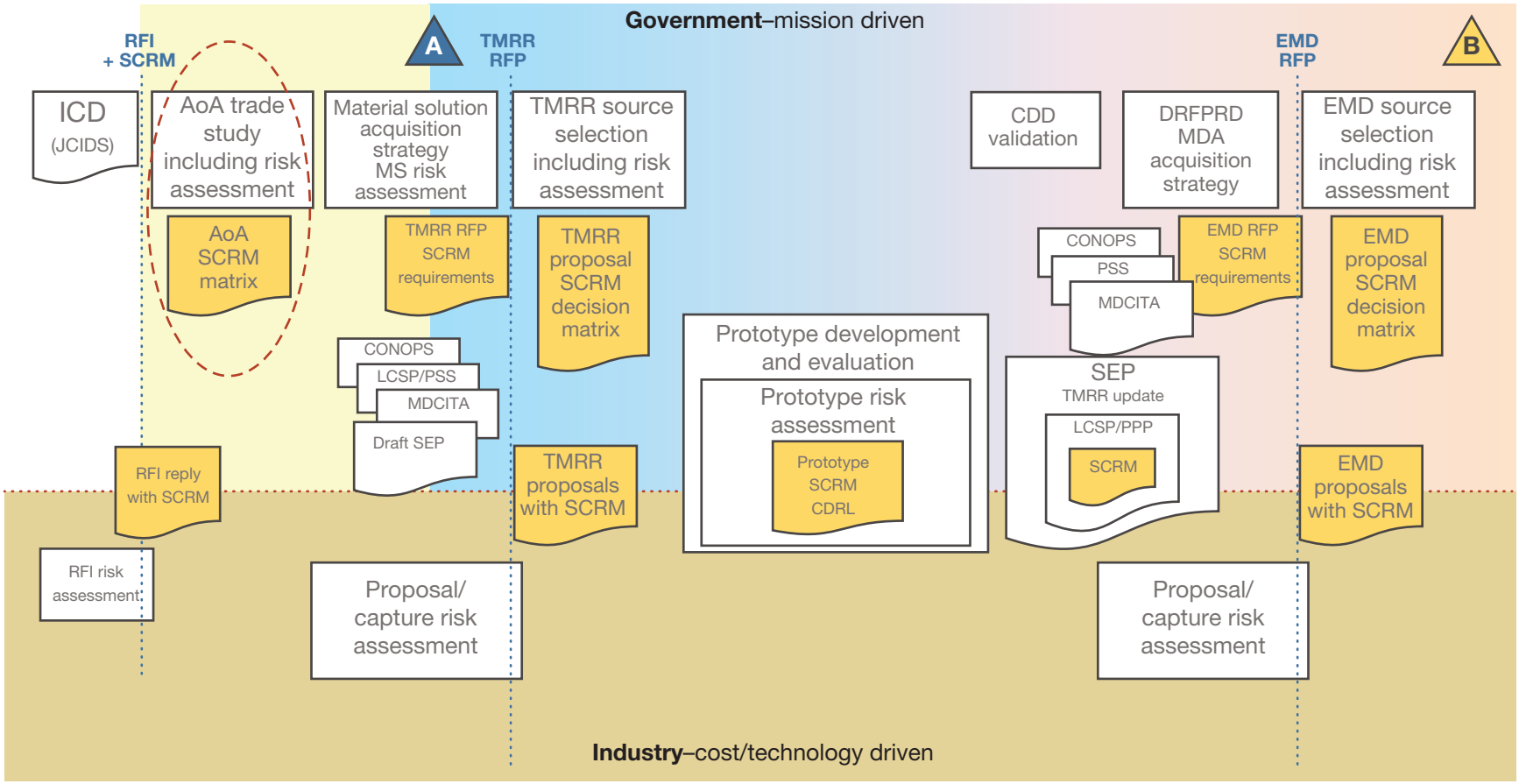
In the proposed LSCRM process, issues related to supply chain risk during the prototype development phase should be identified and mitigated. Therefore, an important consideration in establishing a foundation for LSCRM is determining what information is required from the prime contractor and how it should be translated into the government process to inform decisionmaking.

When Army capabilities managers supported by engineers and scientists first start working to develop the ICD and CONOPS and to improve the technology readiness level (TRL) of the concept, their design decisions and tradeoffs should include considerations of supply chain and supply chain risk. For example, choosing a material that works equally well as another material but that might be more readily accessible and less likely to cause supply chain problems is a tradeoff; cost versus long-term availability of such a material might also be a factor. Following Figure 3.5 from left to right: a published RFI should also include queries about the supply chain aspects of a solution, to be included in responses. The AoA should include a trade study of supply chain aspects of a solution, to be evaluated by supply chain risk experts and systems engineers.[4]

[4] Note that NIST SP 800-161r1 provides detailed guidance on SCRM questions to be asked in an RFI and requirements to include in an RFP.

FIGURE 3.5

Framework 1 Critical LSCRM Aspects



SOURCE: Adapted from DoDI 5000.02T, 2017.
NOTE: Includes steps that might not apply to all acquisitions. White-colored actions are existing actions with SCRM improvements; those in orange are new, additional actions or contract deliverables. DRFPRD = development request for proposals release decision; MS = milestone.

Contractual Requirements in the RFP for LSCRM

A key to successful sharing of SCRM responsibility with the prime contractor will be the correct wording in the RFP that will lead to succinct clauses in the proposals and the contract. As much as possible during source selection, the criteria for what will be required and what will be acceptable need to be codified. Naturally, different technical solutions will present different LSCRM issues and require different approaches to achieve secure, resilient, and robust supply chains, so the clarification question and answer section of the source selection should drill down on any uncertainties identified by the selection panel.[5]

The RFPs for all acquisition phases should describe in detail the obligations of the awardee to provide not only supply chain awareness, but also assessment and plans for mitigation of supply chain risks.

Source selection panels reviewing LSCRM RFP responses should quantitatively assess their comprehensiveness and capability to accomplish the required risk management. A trade study of the respective approaches should be conducted using the SCRM decision matrices that occur at Milestone A (TMRR), Milestone B (EMD), and Milestone C (LRIP), as shown in Figures 3.5 and 3.6. Any RFP should also include a description of specific LSCRM CDRL to accompany the PBOM in the proposal and address supply chain risks. Note the CDRL SCRM deliverable related to the prototype development illustrated in Figure 3.5.

Building a prototype or developing a software package revision 0.1 provides exceptional insight to the supply chain for production—by no means the final supply chain, but a good, early approximation. Using this, critical first estimation of supply chain risks across the life cycle and system boundaries might be derived. For example, in the case of software, an estimate of how much open-source material will be leveraged in the code is an early indicator of supply chain risk.

This SCRM CDRL will then be incorporated into the SEP as part of the LCSP and the program protection plan (PPP), in cooperation with the prime contractor. It is recommended that these CDRLs align with the recent ASA (ALT) regulations (e.g., AR 770-2, AR 770-3)[6] for consistency across programs.

Proposed Early Framework 2 Critical Activities: EMD Phase Milestone B to Milestone C

We recommend that ASA (ALT) should lead the LSCRM activities under Framework 2 through its PEOs and PMs. This recommendation is in line with the transition that takes place between AFC and ASA (ALT) as the system goes from the initial concept design and prototyping phase to a program of record. The acquisition milestone authorities, direct engagement with the prime contractors, and expertise needed to assess and manage supply chain risk reside within the PEO and PM structure. During this phase of the acquisition process, the TRL develops from the prototype to the EMD phase. This proposal envisions an LSCRM process that builds on the previous work and discovery about the supply chain (led by AFC) in Framework 1.

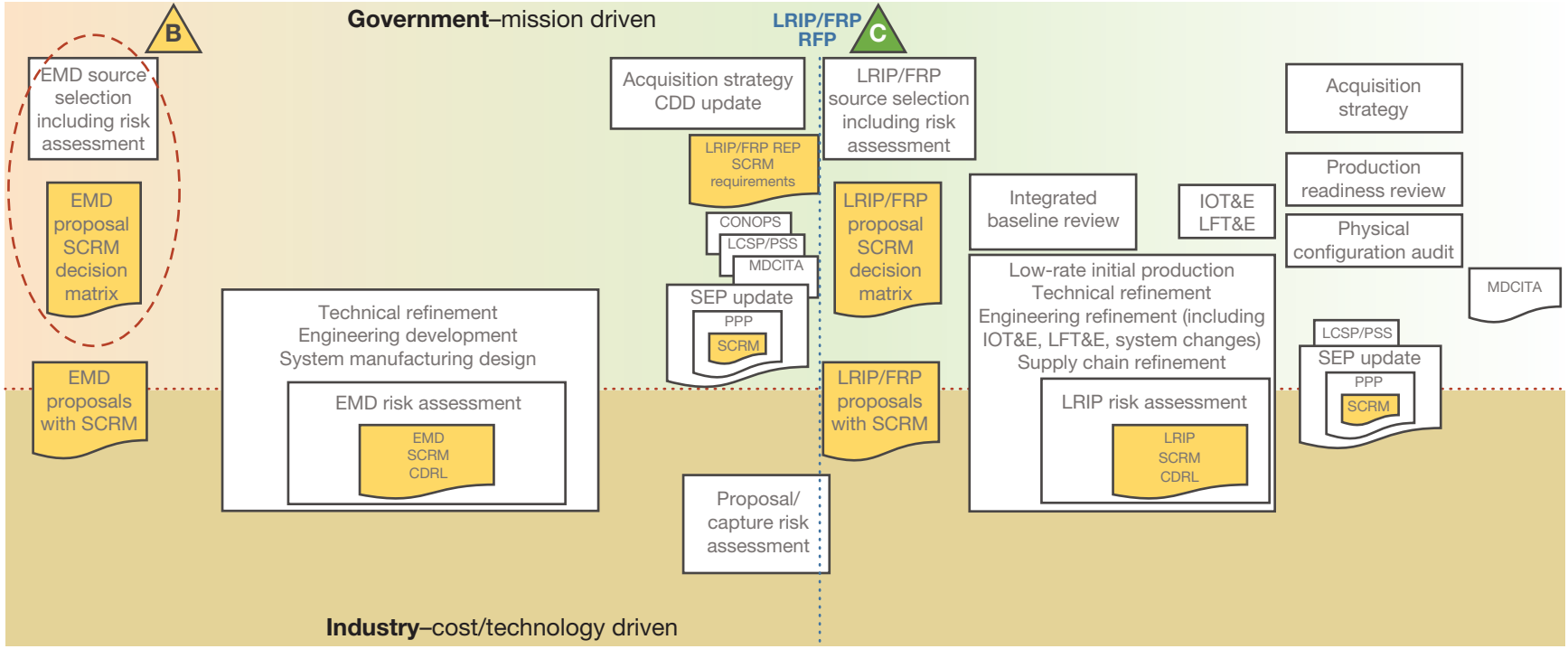
The confidence level of the design engineering and the provenance of materials and suppliers for the system during this phase progresses from approximately 50–60 percent known before Milestone B to closer to 80–90 percent known at Milestone C. The manufacturing processes, system manufacturing design, and manufacturing machinery refinement progress to low-rate production levels and the initial issues with the supply chains should be analyzed and resolved. It is not unusual for design changes and modifications of requirements to take place during EMD as issues are resolved and new approaches and better solutions are

[5] The correct DoD contract clauses and requirements for SCRM remain nebulous and highly program dependent. In communication with the authors via DAU's "Ask a Professor" webpage on February 14, 2022, a DAU representative stated that "[f]rom a literature review and interviews with Supply Chain and Contracting leaders and POCs, [DAU] was unable to find an established, widely used, standardized baseline/benchmark for RFP verbiage specifically related to SCRM." They continued, "The question of what a Supply Chain Resiliency Plan would look like is fodder for further research."

[6] AR 770-2, *Materiel Fielding*, July 16, 2021; AR 770-3, *Type Classification and Materiel Release*, July 16, 2021.

FIGURE 3.6

Proposed Framework 2 and the Transition to Framework 3 Critical LSCRM Aspects



SOURCE: Adapted from DoDI 5000.02T, 2017.
NOTE: Includes steps that might not apply to all acquisitions. White-colored actions are existing actions with SCRM improvements; those in orange are new, additional actions or contract deliverables.

developed. These engineering changes affect supply chains, which now expand to include the machinery and infrastructure for increased-rate manufacturing. The number of personnel engaged in engineering and production increases, and the ability of suppliers down the chain to provide secure, resilient supplies becomes more of a factor. Climate and environmental impacts based on where and how manufacture will take place need to be studied and managed and the operational sustainment aspects of the supply chain refined.

As the acquisition process approaches the LRIP point, the requirements for the LRIP/FRP SCRM CDRL will be refined as a part of the SEP, the acquisition strategy, and the RFP. If there is an LRIP/FRP source selection process, LSCRM approaches for these phases should be codified in the CDRL issued to the contract awardee.

Proposed Late Framework 2 Transition to Framework 3 Critical Activities: Milestone C, Low-Rate Initial Production to the Start of Full-Rate Production

Developing knowledge and refinement of the supply chain—including the supply chain aspects for manufacturing equipment, personnel, and infrastructure—provide increased fidelity for the management of supply chain risks in the second part of Framework 2. Resolving and refining the required data in AR 770-2, AR 770-3, and other ASA (ALT) requirements during this part of the life cycle improves the ability to manage supply chain resiliency and security.

Engineering and manufacturing changes resulting from LRIP, IOT&E, and other manufacturing and system testing will affect the supply chain. These supply chain changes should be incorporated in the LSCRM process before FRP. The need to make engineering changes quickly under a testing and retesting schedule makes the LSCRM process fluid as the final FRP design is codified. As with the original ICD and AoA processes, SCRM tradeoffs might come into play as part of critical design decisions during this phase. Final dispositions of the supply chain and the risk management will be documented in the LRIP SCRM CDRL after the conclusion of IOT&E and LFT&E, to be included in the production readiness review and the SEP update, LCSP, and PPP, as shown in Figure 3.6. The LRIP SCRM CDRL will form the baseline of the FRP SCRM plan.

Transitioning from Framework 2 to Framework 3

The updated SEP for FRP—including the PPP, FRP SCRM plan, LCSP, and the output of the production readiness review—will provide the LSCRM baseline during the cooperative and coordinated transition from Framework 2 to Framework 3. As the SCRM CDRL will be aligned with the ASA (ALT) regulations for life-cycle logistics and support, the transition documentation for LSCRM should share common formats across Army programs. At this point, the lead responsibility for the LSCRM process would transition from ASA (ALT) to the AMC LCMC overseeing the sustainment of the weapon system. As the system enters long-term sustainment, new supply chain solutions will need to be developed as new risks become apparent. For example, risks related to diminishing sources of supply and IP rights might now become more salient. The LCMC's sustainment management function and close integration with the AMC organic industrial base provide it with both the expertise and the visibility over the sustainment supply chain needed to make it an ideal candidate to assume the leadership role over SCRM at this point in life cycle.

End-of-Service Life

The disposal aspect of the supply chain presents specific risks, such as compromise of technology and improper parts recycling. Equipment will be tested to failure and require disposal during LRIP, so the end-of–service life SCRM CDRL should be delivered by the start of the FRP phase. The end-of-service life review should also plan for recycling and reuse, where possible, of critical materials and any reusable mate-

rials and equipment under controlled conditions and for any special supply chain issues that come with the mass retirement of a system.

Defining Roles and Responsibilities for LSCRM Within the Army

In the prior section, we propose the lead organization for each of the three frameworks. However, the lead organizations have a set of responsibilities that often span into frameworks beyond the one for which they are the lead. In this section, we define the critical responsibilities for the organizations involved in each of the three frameworks. Table 3.2 outlines the major proposed LSCRM roles and responsibilities for AFC.

TABLE 3.2
Proposed AFC Roles and Responsibilities During Framework 1 or Framework 2, Depending on System's Acquisition Life Cycle

Role/Responsibility	Comment
Create an initial SCRM plan. The plan will inform the SCRM RFI activities within Framework 1.	In collaboration with the program lead, Army capabilities manager, chief systems engineer, and ASA (ALT) experts, establish the requirements for SCRM based on the weapon system. The requirements for SCRM and the risks that need to be emphasized will vary depending on the material properties, technical requirements, and novelty of the system considered.
Conduct initial SCRM assessments on systems for which they oversee development. Document the results, identifying the highest risks to the system with potential mitigating actions.	This is the initial assessment based on the SCRM plan developed above. This would take place after the development of the ICD and inform the SCRM RFI and RFP language that will be shared with prospective prime contractors.
Develop funding requirements to support SCRM activities across systems for which they oversee development within the following priorities, as applicable: 1. Army's (31 plus 4) systems 2. Systems identified on the critical programs and technologies list 3. National security systems 4. All other new systems 5. Legacy systems.	Working with industry partners and ASA financial management and comptroller, prepare estimates for the costs of SCRM activities. SCRM CDRL costs will be proposal/contract line items.
Integrate SCRM into Army's modernization strategy to ensure supply chain resiliency enablers are included in system development and sustainment requirements for all proposed *initial* SCRM documents (e.g., LCSP/PSS, MDCITA, TMRR SCRM, SEP SCRM).[a]	In collaboration with the PM and chief systems engineer, lead assessments of SCRM information gathered during Framework 1. Leverage engineering expertise to inform tradeoffs between managing supply chain risks and system performance, cost, and schedule over the system's life cycle.
Identify critical program technologies requiring greater levels of supply chain risk protection.	Provide analysis for capability protection and IP protection.

[a] See Figure 3.4.

Proposed LSCRM Role of ASA (ALT) and Supporting Organizations Throughout the Acquisition Life Cycle

The Department of the Army draft directive on SCRM introduced earlier in this chapter proposes roles for ASA (ALT), DASA-S, PEOs, and PMs. Table 3.3 expands on the roles and responsibilities proposed in the draft directive to support the LSCRM activities described in this chapter.

The role of ASA (ALT)—either as a lead or a supporting organization—and its subordinate organizations will change depending on the point of entry of the weapon system into the acquisition life cycle; the role would also be different if the system has already entered operations and sustainment. In Table 3.3, we propose several roles and responsibilities for ASA (ALT).

TABLE 3.3

Proposed Roles and Responsibilities of ASA (ALT) and Supporting Organizations Across the LSCRM Frameworks

Organization	Role/Responsibility	Sources
ASA (ALT)	• Develop SCRM policy and delegate oversight responsibilities to the Deputy Assistant Secretary of the Army for Sustainment (DASA-S)	Army draft directive
	• Serve as the lead organization during the life-cycle acquisition phase defined by Framework 2 (Milestone B to FRP) • Serve as the supporting organization for Framework 1 and Framework 3 • Support analysis of value adjusted total evaluated price (VATEP)	LSCRM proposal
DASA-S	• Establish a single set of SCRM policy, procedures, and guidebook across all LSCRM frameworks with emphasis on Framework 2	Army draft directive, LSCRM proposal
	• Establish management processes to guide the execution of SCRM activities at the PEO and PM level to provide standardize guidance across PEOs	LSCRM proposal
	• Forge relationships with other DoD organizations and federal agencies to adopt best-of-breed SCRM practices within Army's SCRM capability • Coordinate with AMC on SCRM data requirements for transition from FRP to operations and sustainment • Support AMC's LCMCs in the transition of SCRM to sustainment	Army draft directive, LSCRM proposal
	• Develop and promulgate recommended contract and CDRL language to support SCRM activities within the acquisition and sustainment communities • Coordinate with ACC, PEOs/PMs, and DIA to identify contract requirements for SCRM	Army draft directive, LSCRM proposal
	• Provide SCRM policy and procedures execution responsibilities to the PEO	Army draft directive
	• With chief systems engineer(s), create and conduct SCRM assessments, as delineated in Framework 2, on systems for which they oversee development • Document the results, identifying the largest risk to the system • In coordination with the OEM, develop potential mitigating actions	Army draft directive, LSCRM proposal
	In collaboration with AFCs and OEM: • Prepare to conduct SCRM activities within all frameworks to identify risks and prioritize risks based on the weapon system • Provide guidance to the OEMs on the SCRM information requirements • Support the drafting of contract language and CDRLS to ensure contractors at all tiers have information requirements clearly delineated	Army draft directive, LSCRM proposal

Table 3.3—Continued

Organization	Role/Responsibility	Sources
PMs and PEOs	• Develop funding requirements to support SCRM activities across systems for which they oversee development within the following priorities, as applicable: – Army's (31 plus 4) systems – Systems identified on the critical programs and technologies list – National security systems – All other new systems – Legacy systems	Army draft directive
	• Oversee SCRM at the weapon system level with chief systems engineer • Use SCRM guidance to create supply chain risk evaluations • Based on information provided by OEM, identify gaps in SCR knowledge • Collaborate with the OEM to clarify and follow up on knowledge gaps in SCR assessments • Collaborate with the OEMs to develop SCRM mitigation strategies and monitors the execution of those strategies • For legacy systems that are in the process of life extension or modernization, coordinate with AMC LCMCs and DLA to identify known supply chain risks.[a]	LSCRM proposal
	• With contracting officer's representative, shape contract requirements defined in the SOW for areas of risk assessment	LSCRM proposal
	• Manage the transitions between frameworks to assure continuity of SCRM strategies and execution and monitoring of SCR mitigation strategies.	LSCRM proposal

SOURCE: Authors' analysis of Department of the Army, 2021.

[a] See Figure 3.5.

Proposed LSCRM Role of AMC and LCMCs During Framework 2 and 3

AMC and the LCMCs have direct responsibility over the sustainment of Army weapon systems once they are fielded. This includes managing all aspects of support that ensure the operational readiness of weapon systems, such as determining stock levels for spare parts; coordinating with depot operations to overhaul major end items; planning and executing strategic sourcing for spare parts; maintaining technical specifications and approving modifications to technical drawings; and managing contractor support to the field, among many other functions.

In this section, we limit the scope of SCRM to the activities described in Framework 3 of the proposed LSCRM scheme. Table 3.4 describes proposed roles for AMC and the LCMCs within Frameworks 2 and 3. We recognize the importance of a close collaboration among the PEOs, PMs, and the LCMCs in maintaining continuity of SCRM initiatives as systems transition from FRP decision review to operations and sustainment. Furthermore, we recognize the additional role of the LCMCs in developing SCRM processes for legacy systems and in providing information on suppliers and supply chain risk that can inform Framework 1 and Framework 2 decisions.

Operationalizing the Management of Supply Chain Risk Through Risk Models

Operationalizing SCRM, involving multiple stakeholders in an Army system acquisition, depends upon accurate and clear communication to reduce Army-Awardee information asymmetry and asymmetry among Army elements. The literature discusses the many and varied media and models for assessing, organizing, and communicating the supply chain risk data.

For illustrative purposes, the risk reporting matrix, known by some companies as a *risk cube*, is presented here. The risk reporting matrix allows an easily understood cross-reference of the likelihood that an issue

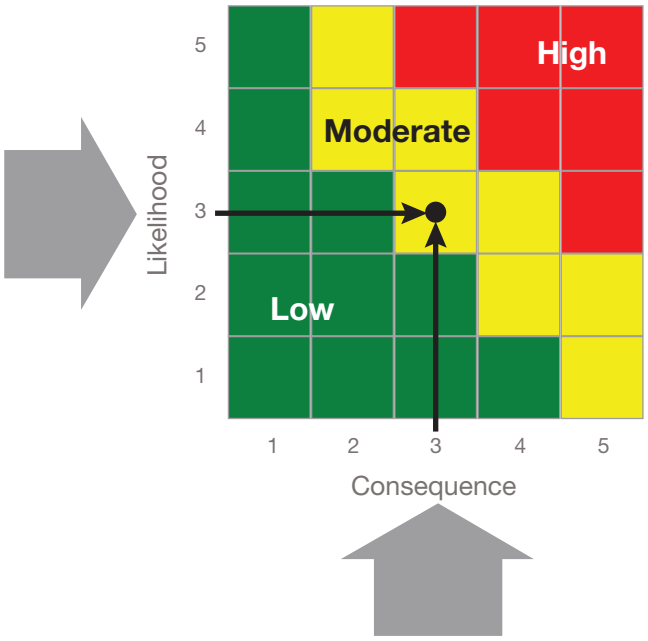
TABLE 3.4
Proposed Additional Roles and Responsibilities for AMC and LCMCs Across LSCRM Frameworks

Organization	Role/Responsibility	Sources
AMC / Supply Chain Integration Lead	• Develop SCRM policy and establish procedures in alignment with Framework 3 and supporting Framework 2.	LSCRM proposal
	• Act as lead for the operations and sustainment portion of LSCRM (Framework 3) • Manage supply chain risk during operations and sustainment.	LSCRM proposal
LCMCs	• Provide skills and expertise to train functional experts and provide matrix support. • Support analysis of OEM SCRM assessments to validate and identify knowledge gaps during Framework 2. • Use sustainment data systems (G-Army, logistics modernization program [LMP]), product deficiency reports, and other internal reports to support SCRM data requirements during Framework 2. • Maintain continuity of documents and information on LSCRM as systems transition into operations and sustainment.	LSCRM proposal

will occur with the consequence (severity and duration) of that issue on cost, performance, and schedule. Figure 3.7 shows a visual representation of the risk on a five-by-five, color-coded grid that allows multiple risks to be plotted on the same grid for comparison.

It is important to note that this risk cube requires an in-depth analysis for each of the identified supply chain risk categories (presumably some subset of those outlined in Chapter 2) for both likelihood and consequence. For the earlier frameworks, business intelligence tools (e.g., Govini, Exiger) combined with other

FIGURE 3.7
Risk Reporting Matrix and Criteria



SOURCE: Adapted from Office of the Deputy Assistant Secretary of Defense for Systems Engineering, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, January 2017, p. 28.

sources of information might be useful in providing some of these inputs. Fortunately, for the operations and sustainment activities phase tied to Framework 3, existing, mature tools, such as LMP, can be used to provide insights into these risk cubes. Ideally, these existing Army tools would inform the earlier frameworks about the potential supply chain risks in time to inform material solution and sourcing decisions.

Although the risk reporting matrix approach has been employed for decades (and assuming the appropriate inputs described above), it has limits that ASA (ALT) should consider. It is constrained by its simplicity: The matrix does not map interdependencies of risks nor conditional risks. Ideally, the subjective risk perspectives of multiple experts should be leveraged to improve accuracy, requiring time and cost, and those experts might change over a program life cycle, changing risk perspectives. Where risk models are a key to operationalizing an SCRM, the limitations and assumptions need to be well understood, especially by the decisionmakers to include the Army PM and chief systems engineer.

Summary

This chapter has presented an analysis of the DoD acquisition process and recommended LSCRM actions throughout the JCIDS acquisition life cycle and certain leverage points where the Army might be able to improve the practice of life-cycle SCRM efficiently and effectively. Highlights of those leverage points include:

- Improving supplier-Army communications on SCRM by refining and delineating SCRM requirements in RFPs, ranking responses through the source selection process, and codifying the resulting risk management process in acquisition contracts and contract deliverables (e.g., CDRLs)
- Defining CDRL deliverables to include program-specific supply chain awareness, risks, data, and management actions
- Emphasizing C-SCRM in all procurements with care to understand risks associated with open-source and Agile software development (see Appendix D)
- Leveraging NIST standards, such as SP 800-171 and the new SP 800-161r1 from 2022, to include risk exposure evaluations[7]
- Including draft end-of-service-life SCRM requirements and plans as decision gates at low-rate initial production and finalized by the FRP decision.

In addition to describing the three frameworks, we outline a set of proposed roles and responsibilities that build upon the existing Army draft directive for SCRM. The proposed roles outline both the leads for each of the frameworks and how those organizations would interact with the other portions of Army responsible for SCRM. We outline responsibilities that help guide supply chain risk information both upstream and downstream from the decision points along the acquisition life cycle.

Finally, we present initial thoughts on how to operationalize the evaluation of supply chain risk assessments. Although more work would need to be done if the proposed frameworks are adopted, the evaluation of risks should consider the benefits of the simpler systems (e.g., risk cubes) with more complicated analyses (e.g., Bayesian networks) that consider increased complexities, such as risk interdependencies.

[7] Ron Ross, Victoria Pillitteri, Kelley Dempsey, Mark Riddle, Gary Guissanie, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, National Institute of Standards and Technology, Special Publication 800-171, Revision 2, February 2020.

CHAPTER 4

Overview of Approaches for Supply Chain Risk Management Implementation

In Chapter 3, we presented three frameworks that span the acquisition life cycle to enable LSCRM. The frameworks integrate SCRM activities with the existing acquisition processes. However, the execution of the LSCRM activities proposed in the frameworks will rely heavily on collaboration between lead organizations within the Army and the OEM. The frameworks represent a process; this chapter presents information on challenges to implementing an SCRM process and some strategies to overcome them.

Summary of SCRM Industry Examples

OEMs play a vital role in identifying, assessing, managing, and mitigating supply chain risk to meet their customers' needs. Because OEMs are a critical component during Army acquisition, we are interested in understanding how OEMs perform supply chain risk assessments and what mitigation strategies they employ.

The literature is replete with examples of severe financial consequences to companies resulting from disruptions to their supply chain. During the COVID-19 pandemic, the major automotive manufacturing companies failed to recognize their lack of leverage with semiconductor chip manufacturers compared with such companies as Apple and Samsung. So, when the demand for new automobiles began to surge, automakers were not able to surge supply of the chips needed to build their vehicles.[1]

The challenge faced by the car manufacturers stemmed, in part, from a lack of information about their supplier's future manufacturing commitments. It can be argued that this lack of information obscured a risk and left the car manufacturers vulnerable. The car manufacturers were operating under a false assumption regarding supplier capacity and the importance of the auto industry to the overall semiconductor marketplace.[2]

On occasion, significant supply chain disruptions have revealed the consequences of unforeseen vulnerabilities in the supply chain. Lessons learned provide additional motivation for making the changes needed to implement SCRM. Our goal is not only to understand the consensus among OEMs about their SCRM practices but also to highlight commercial organizations that have supply chain management challenges of interest to the Army.

[1] See Appendix A for details.

[2] Boston, William, Asa Fitch, Mike Colias, Ben Foldy, "How Car Makers Collided with a Global Chip Shortage," *Wall Street Journal*, February 12, 2021.

OEM SCRM Mitigation Strategies: Literature Review

We conducted a literature review of supply chain risk mitigation strategies used by industries with some supply challenges similar to those of the Army.[3]

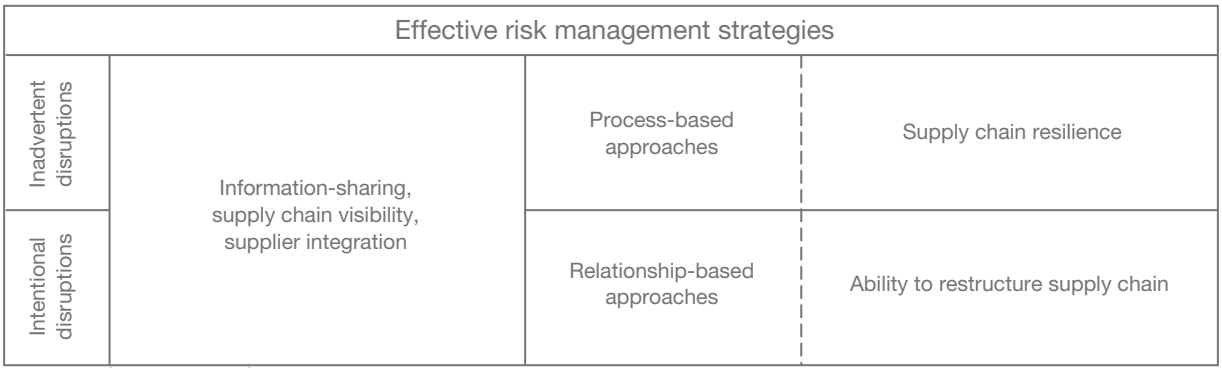
One strategy that was emphasized in the literature is the importance of fostering and maintaining strong supplier relationships.[4] A key aspect of a strong relationship is to establish practices that allow for good information-sharing. Through frequent information-sharing of disruptions and abnormalities by all the actors, supply chains can effectively overcome their vulnerabilities.[5] In addition to information-sharing, supply chain visibility and supplier integration are effective deterrents of both intentional and inadvertent disruptions.[6]

A common mechanism used to establish details on the types and modes of information-sharing is contractual agreements. Contracts stipulate data privacy regulations and cyber hygiene best practices and are often used as the main mechanism to enforce processes. Tailored contractual clauses are common practice in cybersecurity risk management. Examples of things that can be found in contracts include obligation to disclose component vulnerabilities, data loss, and security incidents.

The literature also points to the need to understand the type of disruption; as shown in Figure 4.1, the type of disruption shapes the risk management strategy.[7] When the disruption is inadvertent, the strategy is to work on process-based approaches; for intentional disruptions, it is important to focus on relationship-based approaches.

As shown in Figure 4.1, DuHadway, Carnovale, and Hazen proposed two parallel strategies to SCRM depending on whether the underlying cause of the disruption is intentional or inadvertent. For both strategies, information-sharing, supply chain visibility, and supplier integration activities are key to detecting and understanding the risk of both intentional and inadvertent supply chain disruptions. However, the authors propose that different mitigation strategies should be pursued when dealing with inadvertent disruptions

FIGURE 4.1
Effective Risk Management Strategies



SOURCE: Adapted from DuHadway, Carnovale, and Hazen, 2019, p. 194.

[3] See Appendix A for examples from the airline, automotive, and electronic industries.

[4] Supplier collaboration and related risk categories are provided in Chapter 2.

[5] M. J. Hermoso-Orzáez, and J. Garzón-Moreno, "Risk Management Methodology in the Supply Chain: A Case Study Applied," *Annals of Operations Research*, Vol. 13, No. 2, June 2022.

[6] DuHadway, Carnovale, and Hazen, 2019.

[7] DuHadway, Carnovale, and Hazen, 2019, p. 185.

(quality problems, supplier bankruptcy, and natural disaster) versus intentional disruptions (opportunistic behavior, legal action, terrorism, or other pre-meditated causes). Inadvertent disruptions can be mitigated more effectively through process-based controls and a focus on improving supply chain resilience. However, intentional disruptions are best mitigated through relationship-based approaches, such as contracts, government relations, and procurement strategies that might allow a restructuring of the supply chain if needed.

Determining where third-party risk management should reside, how to measure it, and what to measure are common struggles in a variety of industries.[8] Yet, there is consensus that working with vendors improves the overall security posture. Specific recommendations include:

- investing in unified secure platforms for information exchanges,[9] adding confidentiality and authentication
- establishing a central risk management team responsible for the entire organization with clearly defined governance, operational structure, policies, and procedures[10]
- end-to-end risk frameworks that cover every stage of the life cycle and use continuous improvement.

OEM Supply Chain Risk Identification Approaches

In Chapter 2, we provided an extensive list of potential supply chain risks. Given the complexity of large supply chains and the number of risks that can befall them, managing supply chain risk is challenging, and the practices are still under development. Often, the dedicated resources are limited; thus, a common practice we found in the literature is the development of a risk profile for the suppliers. Some companies have proprietary processes that allow them to categorize suppliers as critical with a combination of qualitative and quantitative inputs.[11] Companies can purchase products and services from tens of thousands of suppliers every year, but just under 100 are considered *critical*. The concept of criticality is often introduced as a metric to reflect how certain suppliers would have a higher impact on the business if they were to fail or be compromised.[12] Business impacts are often expressed in terms of product delivery, quality, availability, and the cost of alternative sourcing. Categorizing suppliers according to their criticality allows for better allocation of resources and can help define different management strategies.

Other companies measure the suppliers' level of access to the company's network and facilities and the supplier's business stability; if a critical supplier might not be viable in the future, they find replacements.[13] Some firms depend on commercial SCRM products, such as intelligence and news mining subscriptions, to identify suppliers at risk.[14] For example, companies such as Dun and Bradstreet, Exiger, and Govini provide data analytic services and decision analysis tools that attempt to quantify supply chain risk, map supply chains, and tailor solutions to specific service and manufacturing supply chains based on client need.

[8] Siegfried, 2019.

[9] Boyens et al., 2020a.

[10] Boyens et al., 2020d.

[11] Boyens et al., 2020d.

[12] Boyens et al., 2020f; Boyens et al., 2020c; Boyens et al., 2020b; Boyens et al., 2020a.

[13] Boyens et al., 2020c; Boyens et al., 2020f.

[14] Boyens et al., 2020e.

Processes for Instituting Supply Chain Risk Management

It is understood that implementing an SCRM process is a complex endeavor. A study by McKinsey and Company cites three reasons why establishing an SCRM process has eluded many companies:[15]

1. Complexity: Identifying all elements of the supply chain can be a resource intensive process, and one that must be continuously updated. Companies might view this as an unmanageable process.
2. Uncertainty: The scope and scale of the risk might be difficult, if not impossible, to predict and quantify. Determining the nature of the risk might seem beyond the control of the risk managers.
3. Information deficit: Information, such as place of performance and sub-tier suppliers, is sometimes well-guarded and not accessible to risk managers.

The McKinsey and Company study proposes a structured approach to supply chain management, including by first differentiating between known and unknown risks. Known risks can be managed directly through a process mitigation; unknown risks are managed indirectly by building a resilient manufacturing process. The process for managing known risks is shown in Box 4.1.

A 2015 RAND study commissioned by the U.S. Air Force constructed a composite process for managing supply chain risk.[16] Key elements of the process are shown in Figure 4.2 and Box 4.2.

BOX 4.1

McKinsey and Company SCRM Process for Known Risks

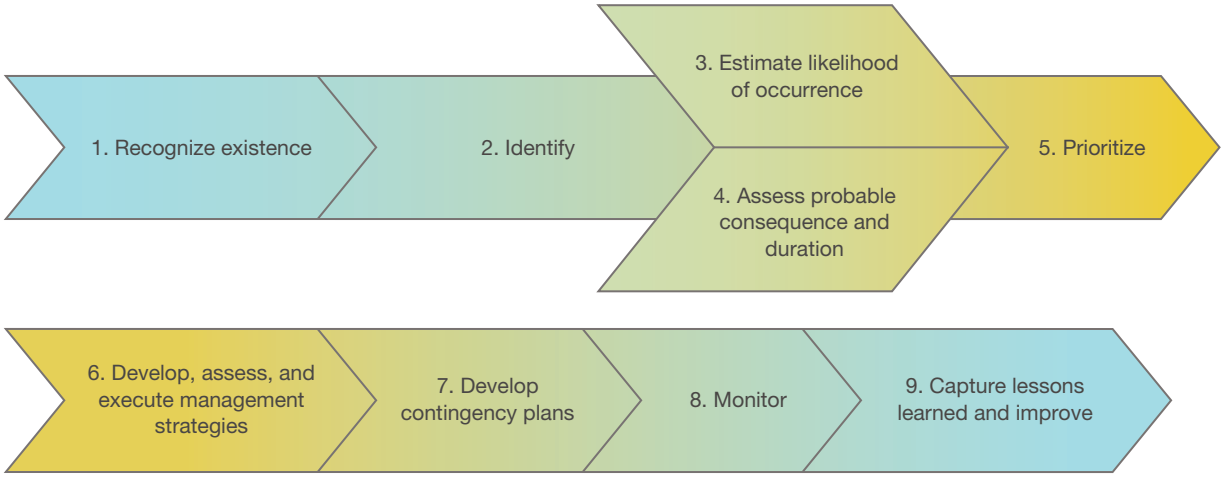
1. Identify and document risks. A typical approach for risk identification is to map out and assess the value chains of all major products. Each node of the supply chain—suppliers, plants, warehouses, and transport routes—is then assessed in detail. Risks are entered on a risk register and tracked rigorously on an ongoing basis. In this step, parts of the supply chain where no data exist and where further investigation is required should also be recorded.
2. Build an SCRM framework. Every risk in the register should be scored based on three dimensions to build an integrated risk-management framework: impact on the organization if the risk materializes, the likelihood of the risk materializing, and the organization's preparedness to deal with that specific risk. Tolerance thresholds are applied on the risk scores, reflecting the organization's risk appetite.
3. Monitor risk. Once a risk-management framework is established, persistent monitoring is one of the critical success factors in identifying risks that might damage an organization. The recent emergence of digital tools has made this possible for even the most complex supply chains, by identifying and tracking the leading indicators of risk.
4. Institute governance and regular review. The final critical step is to set up a robust governance mechanism to periodically review supply chain risks and define mitigating actions, improving the resilience and agility of the supply chain.

SOURCE: The descriptions in this box are drawn verbatim from Bailey et al., 2019, with minor omissions and adjustments.

[15] Tucker Bailey, Edward Barriball, Arnav Dey, and Ali Sankur, "A Practical Approach to Supply-Chain Risk Management," McKinsey and Company, March 8, 2019.

[16] Moore et al., 2015, pp. xiv–xv.

FIGURE 4.2
Composite SCRM Process



SOURCE: Adapted from Moore et al., 2015, p. 22.

BOX 4.2
Steps in a Composite Supply Chain Risk Process

1. Recognize the existence of risk. Before an enterprise can address supply risks, it must be aware of its supply vulnerabilities and the possibility that its actions, or inaction, can create supply chain risks.
2. Identify risks. Enterprises must identify the possible risks associated with a supply strategy. Natural disasters, for example, can pose supply chain risks, which enterprises can map. Supplier participation is also necessary to identify and mitigate risks.
3. Estimate the likelihood of occurrence. Enterprises can do this by assigning a relative weight to the probability of occurrence or classifying the probability of occurrence into categories, such as low, medium, or high.
4. Assess the probable consequences and duration of a risk if one is realized. In this step, concurrent with step 3, enterprises assess the relative total consequence or significance of the prospective loss to calibrate the exposure of the business. The total consequences of a risk are a function of its scale, scope, duration, recovery time, and total cost.
5. Prioritize risks. Few, if any, organizations have the resources to eliminate all risks. Consequently, rather than addressing all vulnerable areas at once, enterprises might focus their SCRM efforts on those events where their efforts are likely to provide the greatest relief. One way the Air Force does this is by plotting risks by categories of likelihood and consequence and then classifying these as level A-risk (highest risk), B-risk (medium risk), or C-risk (lowest risk).
6. Develop, assess, and execute a risk management strategy. The strategies an enterprise develops will depend on the phase of the weapon system's life cycle and the risks it seeks to address. An enterprise might choose to ignore or accept low-priority risks while trying to avoid or reduce the likelihood of a high-priority one.

Box 4.2—Continued

7. Develop contingency plans. This step focuses on developing contingency plans for disruptions because not all risks can be effectively avoided, adequately mitigated, or even identified. Such plans should focus not on every possible source of disruption but rather on outcomes and how to restore operations in event of a disruption, independent of the source. Contingency plans can help enterprises quickly respond to unforeseen disruptions and, thus, reduce their total consequences.
8. Monitor continuously. After establishing a supply strategy and risk management plan, organizations should continuously monitor the environment for any change in prospective supply chain risks that warrant modification of the supply strategy or risk management plan.
9. Capture lessons learned and improve. This step focuses on continuous learning and knowledge management. When a supply disruption occurs, an enterprise should conduct post-incident audits to determine the cause of the disruption and to document any lessons learned for better managing future events.

SOURCE: The steps presented in this box are drawn verbatim from a previous RAND research report (Moore et al., 2015, pp. xiv–xv), with minor omissions and adjustments.

The two processes described above have common elements. Another process described by Tummala and Schoenherr also covers most of the same steps.[17] The key challenge comes in implementing the process steps.

A 2019 study on measuring and managing risks in supply chains interviewed 17 senior executives across 12 different corporations. The study included interviews with chief procurement officers, SCRM consultants, and senior risk managers serving in corporations in the technology, banking, oil exploration, logistics, and manufacturing industries, among others.[18] The study documents a four-step SCRM process, very similar to those described in other research. In addition, the research provides several insights from the supply chain professionals interviewed, including the following that are particularly relevant to our study:

- A critical element in effective risk measurement and management is the presence of a formalized risk management process.
- Communicating risks and risk metrics, as well as lessons learned is critical to successfully mitigating risks.
- Effective risk measurement and management demands a risk management culture that understands the organization's exposure to risk and is able to confidently manage risk.
- A major challenge expressed by companies is how to make use of the wealth of data that is available and how to identify relevant metrics for risk management.[19]

[17] Rao Tummala and Tobias Schoenherr, "Assessing and Managing Risks Using the Supply Chain Risk Management Process (SCRMP)," *Supply Chain Management*, Vol. 16, No. 6, September 27, 2011.

[18] Tobias Schoenherr, Carlos Mena, and Thomas Choi, "Measuring and Managing Risks in the Supply Chain," CAPS Research, April 2019, p. 17.

[19] Schoenherr, Mena, and Choi, 2019, p. 9.

Summary

In this chapter, we examined the academic literature to understand the challenges and approaches commercial firms have found when implementing SCRM. The frameworks in the previous chapter describe a process; this chapter highlights challenges and some potential mitigations for implementing SCRM. Multiple studies reference the complexity of the global supply chain as a contributing factor to the increased challenges that companies face managing supply chain risk. Some commonalities among the proposed SCRM processes emerge, which form the recommendations that should be considered as the Army develops its SCRM approach. These recommendations include:

- Building strong relationships with suppliers is a key element to anticipating and managing supply chain risk.
- Good information-sharing practices enable the building of strong relationships. Through frequent information-sharing of disruptions and abnormalities by all actors, supply chains can effectively overcome their vulnerabilities.
- Understanding the type of possible disruptions shapes the risk management strategy. When the disruption is inadvertent, the strategy is to work on process-based approaches. For intentional disruptions, it is important to focus on relationship-based approaches; in the case of the Army, gathering intelligence about malicious actors is critical.
- A common mechanism used to establish details on the types and modes of information-sharing is contractual agreements. SCRM requirements should be spelled out in contracts with vendors. We provide methods for doing so in the frameworks provided in Chapter 3.
- Determining where third-party risk management should reside, how to measure it, and what to measure are common struggles in a variety of industries. Yet, there is consensus that working with vendors improves the overall security posture. Specific recommendations include:
  - Investing in unified secure platforms for information exchanges, adding confidentiality and authentication
  - Establishing a central risk management team responsible for the entire organization with clearly defined governance, operational structure, policies, and procedures
  - Developing end-to-end risk frameworks that cover every stage of the life cycle and use continuous improvement.
- Most companies seek to focus their risk management activities on the *critical few* suppliers.
- The final critical step is to set up a robust governance mechanism to periodically review supply chain risks and define mitigating actions, improving the resilience and agility of the supply chain.

CHAPTER 5

Summary and Next Steps

ASA (ALT) asked the RAND Arroyo Center to develop a set of frameworks to support implementation of a common operating procedure for managing supply chain risks. The frameworks should incorporate consideration of the cause-and-effect relationships within and among elements of the supply chain and will be designed to support Army senior leaders' and PEO decisions. The key decision was to develop frameworks to guide the Army's implementation of a process within the canonical acquisition life cycle. The acquisition life-cycle process provides the organizational structure for those frameworks and determines the activities required to transform a warfighting concept into a weapon system or to modernize an existing weapon system. It determines the conditions for the manufacture, operation, and maintenance of the system from its fielding to its disposal. Incorporating an SCRM process within the acquisition life-cycle process would align the SCRM activities with key decisions affecting supply choices and with the experts best able to evaluate risk.

Key Findings

DoD and the Army have long been aware of certain supply chain risks, such as malicious tampering with electronics and software by adversaries or the introduction of counterfeit parts.

Although policy guidance is in place to manage some risks, Army risk management initiatives are mostly reactive in nature; that is, the Army is often mitigating the effects of risks that have materialized rather than reducing the risk or the vulnerability of the weapon system to that risk. The reactive nature of risk management is due in part to a lack of a comprehensive SCRM system. As a result, the Army has a limited ability to identify and manage supply chain risk across a weapon system program's life cycle.

In addition, the complexity of the supply chain management is magnified because Army PMs are not in direct control of all the design decisions and production processes that support the production of their weapons systems. For instance, the PMs and Army chief systems engineers are not privy to the information and tradeoff analysis employed by the prime contractors. This creates information asymmetry about supply chain risks and system vulnerabilities that promulgate throughout the system's life cycle.

To address the lack of a comprehensive SCRM process, the RAND Arroyo Center developed integrated LSCRM frameworks to support implementation of a common operating procedure for managing supply chain risks. The LSCRM frameworks integrate existing acquisition processes with SCRM activities and are operationalized through the implementation of the following recommendations.

Principal Recommendations

Our recommendations stem from the three key questions identified in this study:

1. What kinds of supply chain risks should be assessed and managed?
2. How should those assessments be integrated into the acquisition process?
3. What organization should have primary responsibility for assessing those risks over each distinct phase of that life cycle?

We provide recommendations relating to supply chain risk categories, adopting frameworks within the acquisition life cycle to manage supply chain risks and by whom. In addition, we extend beyond these three questions to provide considerations on how to adopt SCRM more broadly within the Army.

Categorizing and Prioritizing Supply Chain Risks

The academic and business literature on supply chain management consistently identifies a variety of risks that have befallen the global supply chains and severely affected the operations of leading firms. In this report, we provide an extensive list of supply chain risks and discuss ways to measure and mitigate them.

As the Army considers how to manage supply chain risks, it is important to acknowledge that risk is not static. Risks and vulnerabilities vary over time and depend on circumstances. In the case of the Army, the risk to a weapon system's supply chain will evolve as the system goes from initial capability development to LRIP, to FRP, and then into fielding and sustainment (i.e., across the entire acquisition life cycle). The Army organizations with lead responsibility for each phase of the life cycle should be aware of all life-cycle risks even if they manifest in a different phase: Decisions in one phase might have supply chain risk implications in later phases.

Chapter 2 presents a list of supply chain risks and their drivers (summarized in Table 5.1) that can appear throughout the acquisition life cycle. Some risks will be more relevant during certain phases of the life cycle; for example, IP and data rights are important to consider during early acquisition phases, whereas product obsolescence might manifest later during sustainment. Although the list is not intended to be comprehensive, it provides the Army with a set of risks that it should consider for each major weapon system. We recommend that the Army consider which risks are most relevant rather than attempt to measure all of them for all systems.

The risk categories can be used as a guide for the proposed LSCRM process. For instance, during the production and deployment phase, much of the supply chain is controlled by the OEM. Therefore, understanding what risk categories an OEM might face and how the OEM is incentivized to address risk will provide the Army's PMs with a clearer understanding of the OEM's likely decisionmaking with regard to risk. This will allow the Army to understand if risk is being passed on to it and how the Army might wish to manage those risks.

Adopting Life-Cycle SCRM Frameworks

As of this writing, the Army does not have a process in place to identify and manage supply chain risk across a weapon system's acquisition life cycle. To mitigate the risks inherent in supply chains from a variety of risk categories, we recommend the adoption of three interconnected LSCRM frameworks that span the acquisition life cycle. By managing across three frameworks, the Army can focus SCRM activities within the organizations that have the most knowledge and information about the weapon system at that point in the life cycle. The inter-

TABLE 5.1
Proposed Supply Chain Risk Categories and Drivers

Risk Category	Drivers of Risk
Climate and environmental	• Natural disasters • Man-made disasters • Pandemics, disease, public health
Corporate and finance	• Contracting issues • Financial health • Funding uncertainty • Regulatory or judicial • Cost uncertainty
Supplier	• Sole source • Single source • Diminishing source of supply • Underdeveloped product pipeline • Supplier quality • Supplier collaboration • Counterfeit parts • Provenance
Cybersecurity	• Components' software or hardware vulnerabilities • Network vulnerabilities
IP and data rights	• Access to data and technical specifications
Demand	• Fluctuations and uncertainty
Geopolitical	• Country risk • Currency and exchange rate fluctuations • Nation-state or terrorist adversarial activity • War or armed conflict
People and skills	• Labor disruptions • Skill obsolescence
Strategic materials	• Raw material access
Transportation and inventory	• Aging infrastructure • Long lead times • Product obsolescence • Product characteristics

related nature of the frameworks promotes sharing knowledge and acknowledging the changing nature of risks across the life cycle (e.g., how decisions in design could affect risks during production and sustainment).

In this report, we recommend the Army adopt an SCRM process aligned with the DoD acquisition life-cycle model. The process would consist of three frameworks, with transitions between frameworks taking place at two naturally occurring points in the life cycle: (1) between the initial development of new concepts (or transformational approaches) and entry into low-rate and full-rate production and (2) the transition from full-rate production to operational deployment, sustainment, and retirement of the system. The proposed frameworks take advantage of process and documents that are already well known and exercised by the Army's acquisition community and expands them to include SCRM.

- **Framework 1:** Under this framework, the capability developer assesses the supply chain risk implied by different sets of potential requirements. Framework 1 incorporates SCRM considerations at program conception, during the development process, and as a part of the Army's modernization strategy. This framework systemically considers SCRM in the earliest phases of the material solution analysis. SCRM in development programs would be documented from the ICD through Milestone B.

  Proposed Lead Organization: AFC would be a natural choice for leading the LSCRM in this framework because it has primary responsibility for capabilities and requirements development.

- **Framework 2:** This framework covers the transition from the EMD after Milestone B until the system enters FRP. OEMs would be primarily responsible for assessing and managing supply chain risk under Framework 2 under the supervision and with the assistance of Army PMs. The OEM would gather information and promote supply chain mitigations as a system begins FRP. The OEM would also capture SCRM data that can be used to manage risk once the system enters sustainment. PMs would validate potential vendors' risk assessments or conduct their own assessment for some risk categories.

  Proposed Lead Organization: Because of their existing roles, ASA (ALT) PEOs or PMs are in the best position to prepare the CDRL and manage the supply chain risk information that is being gathered by the OEM. The PM's role in the initial manufacturing engineering design allows them to work closely with the OEM and validate the supply chain risk assessment produced by the OEM. The PM would also include AMC to consider such impacts in sustainment.

- **Framework 3:** The SCRM roles in Framework 3 manage and maintain supply chain resilience and security through the duration of the life cycle from production through operations, sustainment, updates, reconditioning, rebuilding, life extension, and any other considerations until disposal. Responsibilities might include SCRM in performance-based life-cycle product support.

  Proposed Lead Organization: AMC's LCMCs have the inherent responsibility to maintain weapons systems once they are fielded and until they are retired. AMC would receive support from ASA (ALT) during the early phases of weapon fielding and from DLA during sustainment.

Developing Effective Processes to Formalize SCRM

Understanding SCRM through industry examples can help the Army be more aware of the risks in their supply chains. By analyzing industries with some similarities to the Army, insights into methods and processes that predict and (ideally) mitigate supply chain disruptions might be applicable. Specifically, activities that improve vendor trust and supply chain visibility are highlighted as highly critical. Although it was beyond the scope of this effort to recommend a larger set of SCRM implementation activities across the Army, Chapter 4 highlights some challenges and recommended approaches based on the literature for implementing SCRM processes across an organization.

Next Steps

The establishment of these frameworks is an important first step in performing SCRM throughout the entire acquisition life cycle. However, if adopted, many additional activities remain before the SCRM management process would be fully mature.

For next steps, we suggest that ASA (ALT) consider a cost or impact analysis of LSCRM processes in the context of both system risks and operational risks because employing these risk management processes will not be without costs to the Army. Therefore, we recommend ASA (ALT) consider developing a repeatable

costing analysis approach for SCRM processes. Developing a repeatable process could help improve SCRM budgeting in acquisitions.

Analysis of counterintelligence is one of the few existing SCRM activities that occurs early in the life cycle. Integrating this into the proposed SCRM process and determining the responsibilities of the respective stakeholders requires some effort. In addition, methods for integrating OEM-provided risk assessments with those done at least partly by the Army (e.g., data rights, counterintelligence) will need to be identified.

Work will be needed to provide the PEOs, PMs, and chief systems engineers guidance on implementing the LSCRM frameworks, including how to evaluate the completeness of the OEM's supply chain risk assessments and any additional Army-led supply chain risk assessments, such as providing guidance on what information and details PEOs should request in contractual deliverables. One approach might be through analyzing selected Army acquisition case studies followed by effectiveness testing through a pilot project.

Although the risk categories we provide are ideally close to exhaustive, further analysis of the interdependencies of supply chain risks in the Army's integrated, cyber-physical acquisitions—and as a part of the larger Army and DoD enterprise—is needed. Understanding how to model and assess conditional and interdependent risks will improve the performance of SCRM across the system and the enterprise while making the Army better prepared for war, pandemics, and other nonlinearities in supply chain management.

Finally, if the adoption of these frameworks and their associated roles and responsibilities goes forward, mapping out a timeline for implementation—perhaps in stages through test cases or new weapons systems—must be established. Identifying a central manager of this implementation process will likely be necessary to ensure it progresses as intended.

APPENDIX A

SCRM Industry Examples

In this appendix, we highlight SCRM practices of three industries: airlines, automotive, and electronics. These three industries are important for our analysis because their business practices and supply chain risks have some overlaps with those of the Army.

Airline Industry Case Studies

Like the Army, the airline industry has high acquisition costs, long time horizons for product development, and long system life.[1] Another similarity is that parts designed for aviation often have special material properties, and these parts can be subject to counterfeiting schemes in which identical parts without the required material properties are sold in their place. As a result, studying the relationships between the airlines and their suppliers—where such studies exist—can provide a useful guide for the Army SCRM activities, including during the production of new systems.

The airline industry and the production of commercial aircraft have been increasingly globalized.[2] This globalization has had positive effects, such as compressing aircraft programs, reducing costs, and increasing productivity and global competitiveness.[3] On the other hand, globalization increases the vulnerability of supply chains. New aircraft, such as the Airbus A350X and the Boeing 787 Dreamliner, required significant mitigation strategies to deal with this dispersed supply chain network. Nevertheless, the global grounding due to the 787's faulty batteries caused millions of dollars in disruptions.[4] A variety of mitigation strategies are necessary to avoid the near certainty of disruptions otherwise.

Key Aspects of Managing Relationships—American Airlines

American Airlines (AA) places a strong emphasis on supplier relationship management. In part, AA leadership recognized that the success of its operations depends heavily on their supplier's ability to stock the right parts and provide them quickly. To accomplish this, AA developed close working relationships with and communicated its priorities and performance expectations to their suppliers.[5] When AA plans changes to its scheduled maintenance program, it brings the suppliers in to discuss how those changes will affect demand and turn time requirements. The suppliers in turn share information about supply availability and

[1] Li et al., 2016.

[2] Bains et al., 2016.

[3] Daniela Mocenco, "Supply Chain Features of the Aerospace Industry Particular Case Airbus and Boeing," *Scientific Bulletin – Economic Sciences*, University of Pitesti, Vol. 14, No. 2, 2015.

[4] Tao Song, Yan Li, Jiashan Song, Zhao Zhang, "Airworthiness Considerations of Supply Chain Management from Boeing 787 Dreamliner Battery Issue," *Procedia Engineering*, Vol. 80, 2014.

[5] "American Airlines' Approach to Examining Supplier Performance," *Aviation Week & Space Technology*, Vol. 176, No. 35, October 6, 2014.

lead times. Acknowledging the importance of supplier relationship management, the airline claims that productive supplier relationships hold the customer accountable as well. Communication of expectations to suppliers are vital according to the analysis.

How To Measure Risk

Several risk factors are considered in the airline industry related to their supply chains. A 2019 case study on Emirates Airlines provides a list of supply chain risks the airline manages, some of which are relevant for the Army: disruptions (natural or man-made), procurement risk (ability of parts or aircraft to be delivered on time), and cyber or IT systems risk.[6] In AA's case, they maintain customer service scorecards based on metrics measuring turn time, parts availability, quality of work, and customer service to help measure a supplier's performance and, by extension, its associated risk. The airline industry, like the Army and other defense organizations, is concerned with end-of-supply or diminishing source of supply risk. Several methods for predicting this risk at the airline part level exist.[7] Finally, because of the global nature of airplane production, country and other geopolitical risks can greatly affect the supply chain for airplane production.[8] Methods that weigh those risks with the part criticality and ubiquity (i.e., sources of supply) is one way that is proposed to measure supply chain risk.

Automotive Industry Case Study

The automobile industry introduced many of the innovations in supply chain management that are common practice today, such as lean manufacturing, total quality management, and Six Sigma. It is undeniable that the Toyota Corporation has had a profound effect on supplier management and was, in many cases, the exemplar to be emulated by other companies. However, even Toyota has faced serious challenges related to SCRM. In *The Toyota Way*, the authors describe several instances that highlight Toyota's challenges with supply chain risk but also point to how Toyota's management principles have allowed it to be resilient to those risks.[9] We highlight three instances of SCRM issues at Toyota that are applicable to the wider automotive industry:

1. Toyota vehicle sudden and unintended acceleration:[10] Beginning in 1999, "at least 2,262 Toyota and Lexus owners have reported to the National Highway Traffic Safety Administration [NHTSA], the media, the courts and to Safety Research & Strategies, that their vehicles have accelerated suddenly and unexpectedly . . . result[ing] in 815 crashes, 341 injuries and 19 deaths."[11] The literature on this incident is varied and complex. In the end, several factors, including driver error, faulty floor mats, faulty accelerator pedals, and the introduction of an electronic throttle control, have all been cited as potential causes. Some reports faulted Toyota's culture of secrecy for mishandling the initial reports of sudden and unintended acceleration and that the increased computerization of the automobile has

[6] Kamarudeen and Sundarakani, 2019.

[7] Li et al., 2016.

[8] Bains et al., 2016.

[9] Jeffrey K. Liker and Gary L. Convis, *The Toyota Way to Lean Leadership: Achieving and Sustaining Excellence Through Leadership Development*, McGraw-Hill, 2011.

[10] National Highway Traffic Safety Administration, "U.S. Department of Transportation Releases Results From NHTSA-NASA Study of Unintended Acceleration in Toyota Vehicles," press release, February 8, 2011.

[11] Sean Kane, Ellen Liberman, Tony DiViesti, and Felix Click, *Toyota Sudden Unintended Acceleration*, Safety Research & Strategies, February 5, 2010.

made it very difficult to identify faults that can lead to severe failures.[12] Toyota's internal assessment of this incident concluded that the management team took too long to recognize and react to mounting reports from its customers. The internal assessment also concluded that key decisions were being made at the levels of the company too far removed from the manufacturing floor, lacking the first-hand knowledge needed.[13] Finally, U.S. government oversight provided by NHTSA was also faulted for a failure to act and for relying too strongly on Toyota's version of the facts.[14]

2. Fire at a key supplier:[15] In 1997, a severe fire at Aisin, a single source supplier of a component (p-valve) used in all Toyota vehicles, threatened to halt production of the p-valve for weeks. Because of Toyota's principal of just-in-time production, the manufacturing assembly lines only carried three days of inventory on hand. The fire took place just as Toyota was maximizing production output to hit elevated sales forecasts. A production stoppage of several weeks would have created severe financial consequences for Toyota and its dealers. However, in a classic example of resilience and robustness, Toyota was able to leverage its supplier relationship networks and its relationship with senior management at Aisin to limit the shortage to a few days. Toyota identified other companies in its supply chain with the capability of manufacturing the p-valves and shifted production accordingly. The new valves were then sent to Aisin for quality inspection. This example illustrated how Toyota's investment in supplier relationship management allowed it to respond quickly to the manifestation of a supply chain risk. In addition, the incident changed Toyota's SCRM policy. After the fire, Toyota required "at least two suppliers of a critical part in at least two geographic areas."[16]
3. The 2011 Tohoku earthquake and tsunami: At approximately 2:00 p.m. local time on March 11, 2011, a magnitude 9.1 earthquake, with an epicenter approximately 70 kilometers from the coast of Japan, occurred, creating a tsunami that stuck the Tohoku region of Japan. This event was the greatest natural disaster to strike Japan in the modern era, forcing many industrial shutdowns. Many manufacturing operations in the region were forced to close for extended periods of time. Some of the Japanese factories that closed provide a variety of products to the automobile industry, including paint and electronic chips not easily available elsewhere.[17] In the aftermath of this event, Toyota discovered that they had limited knowledge about the affected companies in their supply chain. While the fire in 1997 had exposed one key supplier vulnerability, in fact, many other vulnerabilities existed in the sub-tiers. The Tohoku earthquake had a global effect on almost every automaker. However, Toyota, who manufactured almost 45 percent of its vehicles in Japan, was among the hardest hit. The report on the aftereffects of the earthquake noted that "[i]nventory shortages of its Lexus line mean that the car will not be available in quantities large enough to meet demand and that it is likely to end its decade-long record as the top-selling U.S. luxury brand."[18]

[12] Joel Finch, "Toyota Sudden Acceleration: Case Study of the National Highway Traffic Safety Administration—Recalls for Change," *Loyola Consumer Law Review*, Vol. 22, No. 4, 2010, pp. 474, 481.

[13] Liker and Convis, 2011, p. xxii.

[14] Finch, 2010, pp. 487–490.

[15] Toshihiro Nishiguchi and Alexandre Beaudet, "The Toyota Group and the Aisin Fire," *MIT Sloan Management Review*, Vol. 40, No. 1, Fall 1998.

[16] Liker and Convis, 2011, p. xiv.

[17] Bill Canis, *The Motor Vehicle Supply Chain: Effects of the Japanese Earthquake and Tsunami*, Congressional Research Service, R41831, May 23, 2011.

[18] Canis, 2011, p. 11.

A review of the literature indicates that the automotive industry's SCRM is limited and points to the need to develop an industry specific guide.[19] For instance, the COVID-19 pandemic exposed vulnerabilities across the entire industry to disruptions in integrated chip manufacturing. The major automotive manufacturing companies failed to realize their lack of leverage with chip manufacturers compared with such companies as Apple and Samsung. So, when the demand for new automobiles began to surge, automakers were not able to surge supply of the chips needed to build their vehicles.[20]

An analysis of a large study in Brazil indicated that most companies point to three significant practices during SCRM implementation phase: better supply chain communication, an SCRM training program, and the creation of a chief risk officer.[21] The goal of creating a chief risk officer is to have someone with oversight and anticipation of possible chain reactions and ripple effects from one business unit to others. For the SCRM and business continuity management training programs, one of the main objectives is to analyze the impact of resource damage on the business through models of the interplay between the business processes of critical business activities.

How To Measure Risk

In a 2009 case study, the authors proposed a framework to broadly identify the disruptions to supply chains in the automotive sector.[22] These categories can be used to promote more preparedness and identify the elements to be measured. Their framework wrapped risk into the following four categories:

1. *Financial vulnerability* is the complication of financial flows due to the complexity of the global market.
2. *Hazard vulnerability* includes internal risk drivers, such as malicious disruptions, terrorism, or natural hazards like flooding and earthquakes.
3. *Strategic vulnerability* usually results when new models are introduced (e.g., failures in project management that can delay product launch, poor manufacturing quality that might detract from the products performance or require re-work to fix).
4. *Operations vulnerability* can happen when there are failures with the dealer distribution networks and results in problems of lead time.

Figure A.1 presents a map of these different categories of vulnerabilities and how they can be thought about in terms of disruptions or events that trigger them. The center of the figure represents events that can happen inside or closer to the organization; as one moves toward the periphery, one sees events happening outside the organization.

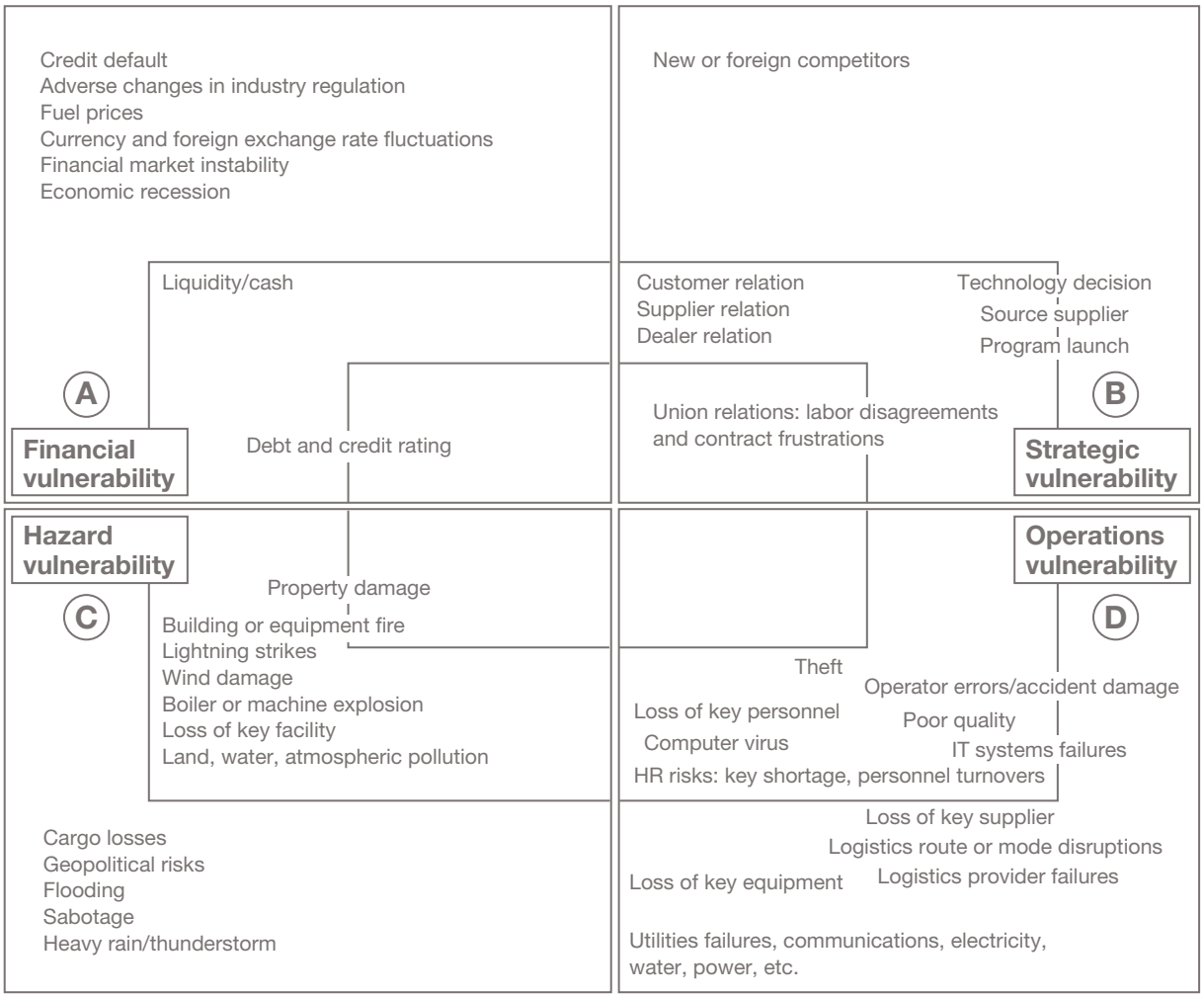
[19] Marc Helmold, Ayşe Küçük Yılmaz, Tracy Dathe, and Triant G. Flouris, "SCRM in the Automotive Industry: AutoSCRM," in *Supply Chain Risk Management: Cases and Industry Insights*, Springer International Publishing, 2022; Paula Santos Ceryno, Luiz Felipe Scavarda, and Katja Klingebiel, "Supply Chain Risk: Empirical Research in the Automotive Industry," *Journal of Risk Research*, Vol. 18, No. 9, 2015; Mauricio F. Blos, Mohammed Quaddus, H. M. Wee, and Kenji Watanabe, "Supply Chain Risk Management (SCRM): A Case Study on the Automotive and Electronic Industries in Brazil," *Supply Chain Management*, Vol. 14, No. 4, 2009.

[20] Arthur Sullivan, "Why the Auto Chip Crisis Could Get More Complex," Deutsche Welle, February 2, 2021.

[21] Blos et al., 2009.

[22] Blos et al., 2009.

FIGURE A.1
A View of Supply Chain Vulnerabilities



SOURCE: Adapted from Blos et al., 2009, p. 249.

Electronics Industry Case Study

The electronics industry has been described in terms of the following six key segments: (1) semiconductor supply and manufacturing services, (2) consumer electronics and appliances, (3) networking and communications, (4) industrial systems, (5) computer and office products, and (6) medical devices.[23] Each segment has unique supply chain challenges and vulnerabilities. It is not our intent to capture all the potential supply chain risks applicable to the electronics sector; instead, we focus on an example that illustrates SCRM principles and trends for this industry.

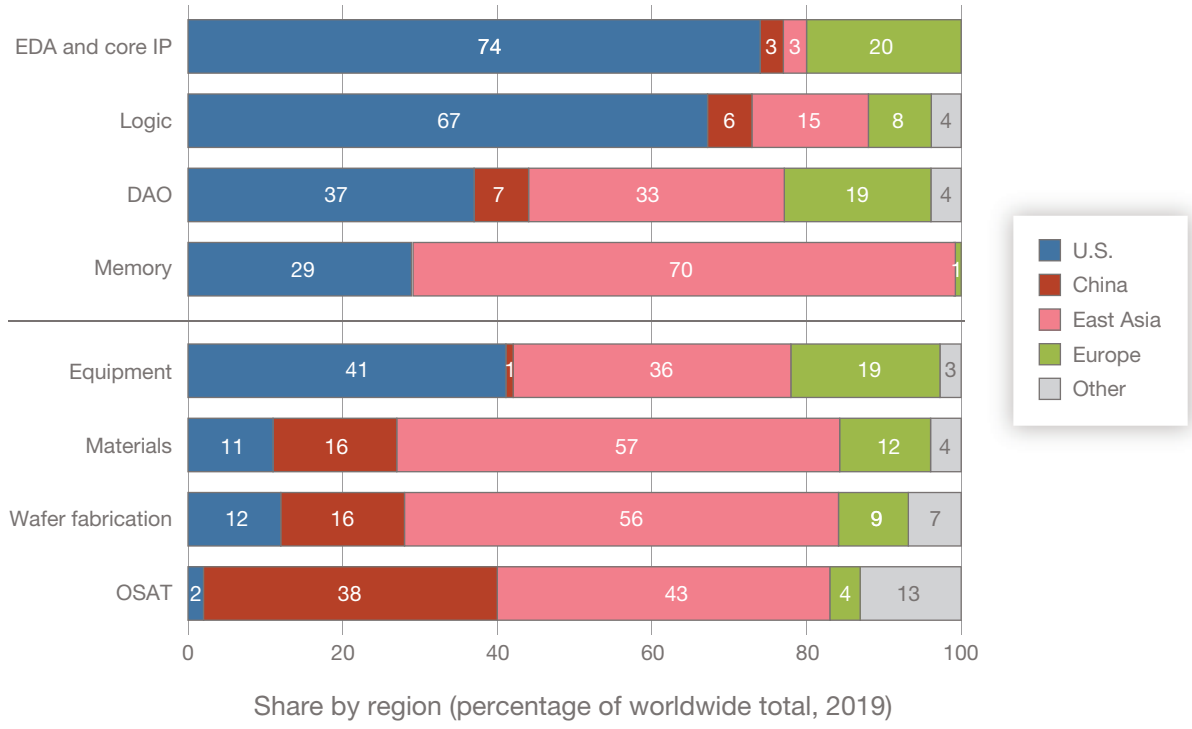
The electronics industry presents a highly dynamic and competitive environment that is still evolving. A working paper published by the East-West Center presented a comprehensive review of the historical evolution of completive dynamics and industrial organization within the electronics industry up to that

[23] Joshua Terry, "Key Segments of the Electronics Industry," webpage, Strategylab, undated.

point.[24] The working paper provides insights into the strategic decisions of major players, such as Apple, IBM, Seagate, and Dell, across key segments of the information communication technology (ICT) markets. The paper explains how the drive to continuously innovate, reduce costs, and maintain market share has created a manufacturing organizational structure that is highly globalized but regionally concentrated in Asia.[25] The evolution of globalization and regionalization, which began in the 1980s, has created a specialized supply (or value chain) segmentation of the semiconductor industry (see Figure A.2).

Considering the stated objectives of the People's Republic of China to become a "global leader in terms of composite national strength and international influence,"[26] the regional concentration of the ICT industry in Asia creates a geopolitical risk for U.S. national interests. The increasingly competitive nature of the relationship between the United States and China will continue to drive policy decisions and perturbations in international trade structures. One recent example was the passage of the CHIPS Act of 2022, which is

FIGURE A.2
Semiconductor Supply Chain Segmentation



SOURCE: Adapted from Antonio Varas, Raj Varadarajan, Ramiro Palma, Jimmy Goodrich, and Falan Yinug, *Strengthening the Global Semiconductor Supply Chain in an Uncertain Era*, Boston Consulting Group and Semiconductor Industry Association, April 2021, p. 5.
NOTE: DAO = discrete, analog, and other; EDA = electronic design automation; OSAT = outsourced assembly and testing.

[24] Ernst Dieter, "The Economics of the Electronics Industry: Competitive Dynamics and Industrial Organization," East-West Center Working Papers, Economics Series, No. 7, October 2000.

[25] Dieter, 2000, p. 8.

[26] President Xi Jinping more than hinted at this goal in his landmark address to the 19th Party Congress in October 2017 (Tony Saich, "What Kind of World Does Xi Jinping Want?" Harvard Kennedy School, Summer 2022).

intended to incentivize the development of "onshore domestic manufacturing of semiconductors critical to U.S. competitiveness and national security."[27]

At the company-operations level, several publications examine how companies in this industry manage the unique supply chain challenges of global supply chains. For example, one study examines external risk factors related to Apple's key suppliers.[28] The study discusses the use of Bayesian networks to identify the conditional probability that one of Apple's suppliers will fail. The supply chain network supporting Apple was categorized based on its expenditure levels. The purpose was to determine the external risk probabilities for each of the suppliers used in the sample from the development of Bayesian networks; in doing so, supplier risk profiles can be generated.

---

[27] U.S. Senate Committee on Commerce, Science, and Transportation, "The CHIPS Act of 2022: Section-by-Section Summary," 2022, p. 1.

[28] Lockamy, 2017.

APPENDIX B

How Might Intellectual Property and Data Rights Be Considered in Order to Reduce Army Supply Chain Risk?

The inability to obtain IP or data rights early in the system's life cycle might have an adverse effect on the Army's ability to operate and maintain its systems. The lack of critical IP or data rights might amplify other supply chain risks outlined in Chapter 2, such as reliance on a single supplier, skills obsolescence, or diminishing sources of supplies. Unlike many of the other supply chain risks, the assessing IP and data rights risk is one area in which the Army should likely lead because OEMs would be unlikely to consider this risk from the Army's perspective.

Introduction

In this appendix, we will consider when determinations concerning the licensing or purchase of IP and data rights should occur in the Army's acquisition process. Specifically, we examine whether existing Army guidance explicitly identifies supply chain risk in the context of IP and data rights and the development of a program IP strategy. Finally, we address how supply chain risk might be reduced concerning IP and data rights. DAU provides the following explanation of an Army program's IP Strategy:

> Strategy to identify and manage the full spectrum of IP (e.g., technical data and computer software deliverables, patented technologies, and appropriate license rights) from program inception and throughout the life cycle. The IP Strategy will describe how program management will assess program needs for, and acquire competitively when possible, IP deliverables and associated license rights needed for competitive, affordable acquisition and sustainment over the life cycle. The IP Strategy is updated throughout the life cycle, summarized in the Acquisition Strategy, and in the Life-Cycle Sustainment Plan during the Operations and Support Phase.[1]

When Should Intellectual Property and Data Rights Be Considered in the Army's Acquisition Process?

The answer to this question might be summarized as "early and often." Army Directive 2018-26 provides that short- and long-term needs for data rights should be developed and updated before the issuance of a contract solicitation:

> 7. Program Managers of Acquisition Category I through IV Programs. These managers will:

[1] DAU Acquipedia, "Data Rights," webpage, undated-a.

> a. assess the short- and long-term needs for data and license rights consistent with the spirit of 10 U.S.C. § 2320(e) and Department of Defense Instructions 5000.02 (Operation of the Defense Acquisition System) and 5000.75 (Business Systems Requirements and Acquisitions). Document the assessment in the program's IP Strategy, *which should be developed and updated before the issuance of a contract solicitation.* [emphasis added]
>
> (1) The IP Strategy is part of the program's Acquisition Strategy. When using a Simplified Acquisition Management Plan in place of an Acquisition Strategy, the Simplified Acquisition Management Plan should include the IP Strategy.[2]

Paragraphs 6.b. and c. of the directive further provide that the availability and delivery of identified data and license rights should be considered as a source selection factor:

> b. conduct early planning for the data and license rights needed to acquire, sustain, and dispose of Army materiel and non-materiel (solutions or systems). At a minimum, planning will address considerations at paragraph 7b of this policy.
>
> c. identify the Government's minimum needs for the technical data, computer software documentation, computer software, and license rights. *Consider including availability and delivery of identified data and rights as a source selection evaluation factor.*[3] [emphasis added]

Interviews with subject matter experts indicate that, for major weapons system acquisition, development of an IP strategy would happen before Milestone A of the acquisition process and would be part of the "analysis of alternatives," which would include the decision to license or buy IP and data rights.[4] Experts also explained the importance and difficulty of valuation of data rights and IP, which can change over time as technology changes and advances.[5] IP and data rights valuation is especially important for the sustainment phase of a major weapons system. As explained in a DAU reference document, sustainment can represent up to 70 percent of the total cost of a major weapons system; the cost of data rights licensing or purchase might represent a large portion of sustainment costs.[6] Specifically, DAU states:

> Historically product support or acquisition program operating sustainment costs are approximately 70% of the total ownership cost of the system over its entire "cradle to grave" lifecycle. Deficiencies in technical data present a significant impediment to DoD's ability to maximize competition for both acquisition and sustainment of programs. It also severely affects the government enterprise's ability to properly plan and execute effective and efficient sustainment strategies. The [. . .] discrepancy has led to the government's inability to reduce total ownership costs throughout its life cycle. Hence the value of the technical data across the government enterprise is critical for meeting key operating and sustainment requirements.[7]

---

2 Army Directive 2018-26, 2018, p. 3.

3 Army Directive 2018-26, 2018, p. 2.

4 RAND government contracting expert, interview with the authors, February 18, 2022.

5 RAND valuation expert for major weapons systems, interview with the authors, February 17, 2022.

6 DAU Acquipedia, "Intellectual Property Strategy," webpage, undated-b.

7 DAU Acquipedia, undated-b.

Is Supply Chain Risk Considered in the Context of Army Acquisition of Intellectual Property and Data Rights?

Army guidance on the acquisition of IP and data rights in DoDI 5010.44, *Intellectual Property (IP) Acquisition and Licensing*, sets out core principles, but none of the principles explicitly identifies supply chain risk during the program life cycle. For example, DoDI 5010.44 provides six core principles in Section 1.2.b.). Three of the principles concerning inclusion of IP strategy in life-cycle planning are set forth below:

> b. The following core principles govern the DoD acquisition, licensing, and management of IP:
>
> (1) Integrate IP planning fully into acquisition strategies and product support strategies to protect core DoD interests over the entire life cycle. Seek to acquire only those IP deliverables and license rights necessary to accomplish these strategies, bearing in mind the long-term effect on cost, competition, and affordability.
>
> (2) Ensure acquisition professionals have relevant knowledge of how IP matters relate to their official duties. Cross-functional input and coordination is critical to planning and life-cycle objectives.
>
> (3) Negotiate specialized provisions for IP deliverables and associated license rights whenever doing so will more effectively balance DoD and industry interests than the standard or customary license rights. This is most effective early in the life cycle when competition is more likely.[8]

A review of selected DoD and Army supply chain security guidance did not explicitly address how to formulate data rights acquisition strategies to offset supply chain risk.[9] As discussed previously, there is an emphasis on the early negotiation of IP and data rights and a discussion of an IP strategy assessment that must be contained in the acquisition process for Category I and II programs, but there is no clear linkage to supply chain vendors.

How Supply Chain Risk Might Be Reduced in the Context of Army Acquisition of Intellectual Property and Data Rights

There are several potential options to reduce supply chain risk linked to IP and data rights. These options include the use of a technology escrow account; the use of "specially negotiated" data rights early in an Army contract, which might provide greater certainty about the availability to the government of specific, critical data rights; and a user-friendly method to access and record the data rights that have been licensed or purchased by the Army. Finally, lawyers in the IP Cadre or other Army IP lawyers could assist PMs in identifying supply chain risks early in the IP strategy development process.

A Technology Escrow Account Might Help Reduce Supply Chain Risk

The Army and DoD need to incorporate new and emerging technologies to counter near-peer adversaries, as indicated in the 2020 National Defense Authorization Act. However, incorporating new technologies from small or nontraditional government suppliers and contractors can increase supply chain risk if those companies file for bankruptcy, can no longer support a particular version of the technology purchased by the gov-

[8] DoDI 5010.44, 2019, p. 4.

[9] Specifically, these documents included Army Directive 2018-26, 2018; AR 70-77, *Program Protection*, Department of the Army, June 8, 2018; DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)*, Office of the Under Secretary of Defense for Acquisition and Sustainment, May 28, 2015, change 3, October 1, 2020; and U.S. Code, Title 50, Section 3334e, Enhanced Procurement Authority to Manage Supply Chain Risk.

ernment, or in any other way cannot provide the necessary technology for a defense program. Establishing a technology escrow account is a broadly accepted method to address and reduce these supply chain risks. A technology escrow agreement consists of a legal agreement between all parties involved in the government's procurement of the technology, a neutral third-party escrow agent that can secure the technology developer's IP, and a specific agreement about when and under what conditions the escrow agent can release the escrowed IP to the government (e.g., bankruptcy, merger, acquisition, or inability to support the technology).[10]

The process to establish a technology escrow was described in a 2020 article:

- **Step 1.** An escrow agreement is established among the parties that secures the IP rights and identifies the release conditions. This is accomplished alongside the contracting agreement.
- **Step 2**. Prime and sub-contractors submit their deposit material for the associated IP.
- **Step 3**. The escrow agent receives, verifies and stores the deposit material in National Archives and Records Administration-compliant storage space with classified-level certifications.
- **Step 4.** Deposit materials are sent to the agency and/or prime contractor if a specified release condition occurs.[11]

DoD or Army intended use of a technology escrow agreement for a particular acquisition should be announced to potential contractors as early as the RFI and included in the RFP. The benefits for DoD or the Army will be to provide greater assurance that necessary IP will be available when needed, despite the many possible supply chain obstructions that could occur over the life cycle of a weapons program.

Use of Specially Negotiated Data Rights Might Provide Greater Certainty About the Availability to the Army of Key Intellectual Property and Data Rights

As explained previously, DoDI 5010.44 provides six core principles governing the DoD acquisition, licensing, and management of IP. Section 1.2.b.(3) authorizes DoD to:

> (3) Negotiate specialized provisions for IP deliverables and associated license rights whenever doing so will more effectively balance DoD and industry interests than the standard or customary license rights. This is most effective early in the life cycle, when competition is more likely.[12]

The approval to negotiate "specialized provisions for IP deliverables and associated license rights" could be used by Army PMs and IP lawyers to set up a technology escrow account or use other contractual methods to assure that key IP deliverables and associated data rights would be available to the Army to support its weapons systems, in the case of protracted delays or failure in a prime contractor's supply chain.

[10] See Antonelli, 2020. See also Deparment of Defense Enterprise Software Initiative, *Software Buyer's Checklist*, January 2016, Section 3.1, Source Code Escrow.

[11] Antonelli, 2020.

[12] DoDI 5010.44, 2019.

Legal Assessment and Evaluation of Data Rights and Licensing of Intellectual Property Will Be Important for Identifying and Reducing Supply Chain and Other Risks

A 2021 GAO report takes a comprehensive look at significantly increasing the legal and IP expertise available to negotiate Army contracts and licenses concerning data rights and determining the data rights the Army will need for sustainment very early in the acquisition process.[13]

The GAO report assessed the progress of the new IP Cadre of legal and other professionals who are tasked to assist with DoD acquisitions. Although a graphic in the GAO Report indicated that the IP Cadre envisions having a 15-person virtual team supporting the Army's IP efforts, currently, the IP Cadre has only one permanent civilian senior-level position for the director, four civilian "term" government positions, and approximately eight contractor full-time equivalent positions to serve all of DoD. The GAO report observed that the fact that the government positions are temporary (i.e., "term") will be a disincentive for IP lawyers and other experts to join the IP Cadre. Clearly, the IP Cadre will need experienced IP lawyers to negotiate with seasoned lawyers from major law firms who represent defense contractors. Therefore, DoD and the Army need to provide significant incentives to attract and retain top IP legal talent.

When asked about IP Cadre staffing and resources, lawyers in the OSD IP Cadre explained that the overall DoD-wide IP Cadre function uses a "federated model," consisting of the "OSD IP Cadre" (i.e., a small office within OUSD A&S), along with the larger collection of offices and personnel that are working IP matters, either as their primary duties or as a portion of their official duties, and that are located in other OSD offices (e.g., OUSD Research and Engineering [R&E]), Defense Pricing and Contracting, and in other DoD component offices. The OSD Cadre lawyers noted that the GAO report outlines staffing for such functions at DAU and the military departments.

Army IP professionals told us that new Army guidance directs acquisition professionals to use "specifically negotiated license rights" as much as possible.[14] However, the Army lawyer told us that they were short staffed and lacking the expertise and resources to negotiate these types of licensing rights on a broad scale. A 2017 report by the Institute for Defense Analyses observed in its conclusions that "[a]mbiguous terms and loosely defined constructs impair the implementation of IP for sustainment."[15] In brief, legal training and experience are required to eliminate the "ambiguous terms and loosely defined constructs" in contracts and licenses that can create risks to supply chain support during implementation and sustainment of major defense systems.

A User-Friendly Method to Access Data Rights Licensed or Purchased by the Army Would Assist Program Managers in Better Negotiating Intellectual Property and Data Rights and Avoiding Risk of Oversights

The 2021 GAO report provided an update on an effort to create a DoD-wide database of IP and data rights:

> DOD does not currently have a capability to track IP or data rights it previously acquired, but the department is piloting an effort to develop this capability. The Section 813 Panel concluded that federal agencies need to maintain relevant contract documents and IP documentation to avoid purchasing IP and corresponding IP rights more than once, and to avoid losing IP rights over time.

[13] U.S. Government Accountability Office, 2021.

[14] Army IP professionals, interview with the authors, December 2, 2021. See also DoDI 5010.44, 2019, Section 1.2.b.(2) and (3).

[15] Richard Van Atta, Royce Kneece, Michael Lippitz, and Christina Patterson, *Department of Defense Access to Intellectual Property for Weapon Systems Sustainment,* Institute for Defense Analyses, P-8266, May 2017, p. vi.

> Officials from the OSD IP Cadre, Army, Air Force, and Defense Advanced Research Projects Agency told us that DOD has purchased voluminous amounts of IP deliverables and licenses, but has no means of tracking them across the department or within components. The OSD IP Cadre is working with the Joint Artificial Intelligence (AI) Center to pilot an artificial intelligence knowledge-sharing model through February 2022. This model is intended to mine existing DOD databases to locate IP that DOD owns or has licensed. The Joint AI Center, the OSD IP Cadre, and a team of cross-functional subject matter experts are currently working to develop common terms and definitions that will facilitate DOD-wide searches. Members of the OSD IP Cadre told us this capability would enable users to identify IP already acquired by DOD personnel and work with the current owner to leverage that IP to meet additional needs.[16]

Lawyers in the OSD IP Cadre provided an update on the collaboration described in the GAO report. As of 2021, the OSD IP Cadre is working to develop an "enterprise knowledge model" that would establish a collection of definitions and relationships that could be used (e.g., by artificial intelligence tools) to better enable identification and data analytics on existing IP-related data or information that might reside in various data repositories already established and operated in DoD components. This effort is underway with continuing development activities planned through fiscal year 2023.

As the GAO report explained, this capability would allow users to identify IP already acquired and leverage IP to meet any additional requirements.[17] A DoD-wide method to access existing IP documentation and data rights could assist PMs and Army IP lawyers in preventing oversights concerning IP and data licensing arrangements that could lead to supply chain risk, among other risks to major defense systems.

Conclusion

In this appendix, (1) we considered when determinations concerning the licensing or purchase of intellectual property and data rights should occur in the Army's acquisition process, (2) we examined whether existing Army guidance explicitly identifies supply chain risk in the context of IP and data rights and the development of a program IP strategy, and (3) we addressed several options for how supply chain risk might be reduced concerning IP and data rights. These options included the use of a technology escrow account; the use of "specially negotiated" data rights early in an Army contract, which might provide greater certainty about the availability to the government of specific, critical data rights; and a user-friendly method to access and record the data rights that have been licensed or purchased by the Army. Additionally, lawyers in the IP Cadre or other Army IP lawyers could assist PMs in identifying supply chain risks early in the IP strategy development process.

[16] GAO, 2021, p. 28.

[17] GAO, 2021, p. 28.

APPENDIX C

Details on Army Regulations, NIST Special Publications, and Contracting Related to Supply Chain Risk Management

This appendix covers details related to Army regulations, the risk exposure framework contained in NIST SP 800-161r1, and the Defense Federal Acquisition Regulation Supplement (DFARS) discussed in Chapter 3.

A Brief Overview of Relevant Army Acquisition Regulations

For context of the critical SCRM aspects, the following are some passages of the relevant Army regulations governing SCRM:

> Where possible, all commands, DRUs [direct reporting units], and MAs [mission areas] must begin the planning phase by developing a strategy that describes their technology and information resource goals that align to the appropriate Army strategy (for example, The Army Plan and The Army Campaign Plan) and demonstrate how the technology and information resources goals map to the Army's mission and organizational priorities.
> a. *Risk management*. Part of planning, through the life cycle of IT investments, risks to be considered:
> (1) Security.
> (2) Privacy.
> (3) Records Management.
> (4) Public Transparency.
> (5) Supply Chain Security.[1]
>
> Refer to DoDI 5000.02, Enclosure 3. AR 70–77 assigns responsibilities and prescribes additional Army policies for developing plans to protect critical program information (CPI), conducting supply chain risk management, and performing damage assessment activities resulting from a compromise of unclassified program information.[2]
>
> b. *Activities to mitigate cybersecurity risks.* PMs will rely on existing cybersecurity standards tailored to reflect analysis of specific program risks and opportunities to determine the level of cyber protections needed for their program information, the system, enabling and support systems, and information types that reside in or transit the fielded system. Appropriate cyber threat protection measures include information safeguarding, designed in system protections, supply chain risk management, software assurance, hardware assurance, anti-counterfeit practices, anti-tamper, and program security related activities such

[1] AR 25-1, 2019, p. 26.

[2] AR 70-1, 2018, p. 16.

as information security, operations security, personnel security, physical security, and industrial security. Refer to DODI 5000.02 and AR 70–77 for additional details.[3]

Reliability, availability, and maintainability emphasis during source selection
Sustainment factors, including reliability and maintainability will be identified in the source selection plan as a technical evaluation subfactor in making a source selection. When operations and support costs can be accurately estimated and evaluated, these costs will be considered during the source selection decision. Whenever [reliability, availability, and maintainability] RAM and logistics are evaluated the source selection board should include a reliability engineer, reliability evaluator, or reliability manager for all major defense acquisition programs. [. . .]

g. Materiel developers, with the support of the [Combat Capability Development Centers] CCDCs, will emphasize management of parts, materials, and processes (PM&Ps) to ensure hardware high reliability performance in operating and non-operating environments (for example, storage) across the acquisition life cycle. The approach will address the requirements of MIL–STD–3018 and standard (SD)–19 including: supply chain disruption, counterfeit PM&P, lead-free usage, and the validation and acceptance test approaches for PM&P items.[4]

NIST SP 800-161r1 Risk Exposure Framework

The following is from the 2022 version of NIST SP 800-161r1, Appendix C:[5]

Step 1: Create a Plan for Developing and Analyzing Threat Scenarios

- Identify the purpose of the threat scenario analysis in terms of the objectives, milestones, and expected deliverables.
- Identify the scope of enterprise applicability, level of detail, and other constraints.
- Identify resources to be used, including personnel, time, and equipment.
- Define a Risk Exposure Framework to be used for analyzing scenarios.

Step 2: Characterize the Environment

- Identify core mission and business processes and key enterprise dependencies.
- Describe threat sources that are relevant to the enterprise. Include the motivation and resources available to the threat source, if applicable.
- List known vulnerabilities or areas of concern. (Note: Areas of concern include the planned outsourcing of a manufacturing plant, the pending termination of a maintenance contract, or the discontinued manufacture of an element).
- Identify existing and planned controls.
- Identify related regulations, standards, policies, and procedures.
- Define an acceptable level of risk (risk threshold) per the enterprise's assessment of tactics, techniques, and procedures (TTPs); system criticality; and a risk owner's set of mission or business priorities. The level of risk or risk threshold can be periodically revisited and adjusted to reflect the elasticity of the global supply chain, enterprise changes, and new mission priorities.

[3] AR 70-1, 2018, p. 24.

[4] AR 702-19, 2020, p. 8.

[5] Boyens et al., 2022, pp. 167–168.

Step 3: Develop and Select Threat Events for Analysis

- List possible ways that threat sources could exploit known vulnerabilities or impact areas of concern to create a list of events. (Note: Historical data is useful for determining this information.)
- Briefly outline the series of consequences that could occur because of each threat event. These may be as broad or specific as necessary. If applicable, estimate the likelihood and impact of each event.
- Eliminate those events that are clearly outside the defined purpose and scope of the analysis.
- In more detail, describe the remaining potential threat events. Include the TTPs that a threat source may use to carry out attacks. (Note: The level of detail in the description is dependent on the needs of the enterprise.)
- Select for analysis those events that best fit the defined purpose and scope of the analysis. More likely or impactful events, areas of concern to the enterprise, and an event that can represent several of the other listed events are generally useful candidates.

Step 4: Conduct an Analysis using the Risk Exposure Framework

- For each threat event, note any immediate consequences of the event and identify those enterprise units and processes that would be affected, taking into account applicable regulations, standards, policies, and procedures; existing and planned controls; and the extent to which those controls are able to effectively prevent, withstand, or otherwise mitigate the harm that could result from the threat event.
- Estimate the impact these consequences would have on the mission and business processes, information, assets, enterprise units, and other stakeholders affected, preferably in quantitative terms from historical data and taking into account existing and planned controls and applicable regulations, standards, policies, and procedures. (Note: It may be beneficial to identify a "most likely" impact level and a "worst-case" or "100-year" impact level.)
- Identify those enterprise units, processes, information (access or flows), and/or assets that may or would be subsequently affected, as well as the consequences and the impact levels until each affected critical item has been analyzed, taking into account existing and planned controls and applicable regulations, standards, policies, and procedures (e.g., if a critical server goes down, one of the first processes affected may be the technology support department, but if they determine a new part is needed to bring the server back up, the procurement department may become involved).

Step 5: Determine C-SCRM Applicable Controls

- Determine if and which threat scenario events create a risk level that exceeds a risk owner's acceptable level of risk (risk threshold). (Note: In some cases, the level of acceptable risk may be dependent on the capability to implement or the cost of mitigating strategies.) Identify opportunities to strengthen existing controls or potential new mitigating controls. Using a list of standards or recommended controls can simplify this process. […]
- Estimate the effectiveness of existing and planned controls at reducing the risk of a scenario.
- Estimate the capability and resources needed (in terms of money, personnel, and time) to implement potential new or strengthened controls.
- Identify those C-SCRM controls or combinations of C-SCRM controls that could cause the estimated residual risk of a threat event to drop to an acceptable level in the most resource-effective manner, taking into account any rules or regulations that may apply. (Note: Consider the potential that one control will help mitigate the risk of more than one event or that a control may increase the risk of a separate event.)

Step 6: Evaluate/Feedback

- Develop a plan to implement the selected controls and evaluate their effectiveness.
- Evaluate the effectiveness of the Risk Exposure Framework, and make improvements as needed.

LSCRM Contract Provisions

The following contract provisions should be considered in an Army RFP involving cyber and cyber-physical systems. These are relevant examples and do not constitute an exhaustive listing, which would depend upon the details and components of a specific system acquisition.

DFARS Subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS subpart 204.73 and its associated contract clauses require contractors and subcontractors to protect defense information that resides in or transits through covered contractor information systems by applying specified network security requirements. It also requires reporting of cyber incidents. These requirements are implemented through three clauses in DFARS subpart 252.204 required to be included in contracts for covered items and services.

The workhorse clause, DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, imposes the requirements to provide "adequate security" for covered contractor information services. DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, establishes NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, as the primary standard against which "adequate security" is determined. DFARS 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information, protects entities disclosing cyber incidents from disclosure by other firms in the supply chain.[6]

This subpart also includes the following:

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, which adds additional cybersecurity measures to those already required under DFARS 252.204-7012 by establishing enforcement methodologies for ensuring contractors have implemented the NIST Special Publication 800-171 DoD assessment methodology. This is related to contract cybersecurity requirements for DoD contractors. Assessments related to the cybersecurity requirements are posted to the Supplier Performance Risk System].
- DFARS 252.204-7018, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services.

DFARS Subpart 239.73, Requirements for Information Relating to Supply Chain Risk

DFARS subpart 239.73 requires DoD and contractors to conduct SCRM for acquisition of *covered systems* (information systems handling particularly sensitive information or cyber equipment required for high-priority missions.)

[6] The DoD emphasis on NIST SP 800-171 provides excellent guidance for CUI processing cyber security but has taken on general SCRM importance beyond its original scope.

This subpart requires DoD program offices and contracting officers to manage supply chain risk for the "acquisition of information technology for covered systems."[7] It implements 10 U.S.C. 2339a (which began as Section 881 of the National Defense Authorization Act for Fiscal Year 2019) and elements of DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*. As we understand it, this subpart authorizes the Secretary of Defense and service secretaries to exclude sources of supply (prime or subcontractors) for reasons related to supply chain risk and makes such actions not subject to review in bid protests.

As defined in the subpart, *supply chain risk* means

> [t]he risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.[8]

DFARS subpart 239.73 requires the addition of two clauses (DFARS 252.239-7017 and 252.239-7018) in all solicitations and contracts for cyber systems and cyber-physical systems (e.g., information technology services or supplies, including commercial item acquisitions). These clauses require contractors to accept the authority provided by the subpart described above. Also, DFARS 252.239-7018 states that "[t]he Contractor shall mitigate supply chain risk in the provision of supplies and services to the Government" but does not define the mechanisms for doing so, nor does it provide a standard establishing sufficient mitigation.[9]

DFARS Subpart 246.870, Contractors Counterfeit Electronic Part Detection and Avoidance

DFARS subpart 246.870 "[p]rescribes policy and procedures for preventing counterfeit electronic parts and suspect counterfeit electronic parts from entering the supply chain when procuring electronic parts or end items, components, parts, or assemblies that contain electronic parts."[10] It requires the inclusion of clauses 252.246-7007 and 252.246-7008 when procuring electronic parts, end items including electronic parts, or services for which the contractor will supply electronics parts (contracts set aside for small business do not incorporate 252.246-7007).

DFARS 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, requires contractors to establish and maintain a counterfeit electronic part detection and avoidance system. It requires risk-based policies, such as personnel training; the inspection and testing of electronic parts; "[p]rocesses to abolish counterfeit parts proliferation"; a process enabling the tracking of electronic parts from OEM to product acceptance by the government; use of contractor-authorized suppliers (as defined by DFARS 252.246-7008); and reporting of suspected counterfeit electronic parts to the Government-Industry Data Exchange Program. It requires "flow down of counterfeit detection and avoidance requirements" to subcontractors at all levels.[11]

DFARS 252.246-7008, Sources of Electronic Parts, focuses on sources of electronic parts and requires prime contractors to follow certain procedures for the selection and vetting of electronic parts suppliers. It

---

[7] DFARS, Part 239, Acquisition of Information Technology; Subpart 239.73, Requirements for Information Relating to Supply Chain Risk; Section 239.7302, Applicability.

[8] DFARS, Part 239, Acquisition of Information Technology; Subpart 239.73, Requirements for Information Relating to Supply Chain Risk; Section 239.7301, Definitions.

[9] DFARS, Part 252, Solicitation Provisions and Contract Clauses; Section 252.239-7018, Supply Chain Risk.

[10] DFARS, Part 246, Quality Assurance; Section 246.870, Contractors Counterfeit Electronic Part Detection and Avoidance.

[11] DFARS, Part 252, Solicitation Provisions and Contract Clauses; Section 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System.

also requires the contractor to assume responsibility for the authenticity of parts provided by contractor-approved suppliers.

FAR Part 39, Acquisition of Information Technology

FAR Part 39 establishes privacy and security safeguards on federal contracts for IT systems. Section 39.106 requires the contracting officers to insert a broad clause addressing privacy and security safeguards "in solicitations and contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services."[12] As we interpret it, the standard FAR clause for privacy and security safeguards, FAR 52.239-1, requires the contractor to afford the government access to contractor assets "to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data," and to inform the government if it finds "unanticipated threats or hazards" or if existing safeguards fail.[13]

These are examples of the required contract clauses, current as of the date of this report, but not comprehensive: Each system acquisition program will require the contracting officer and contracting officer's representative to consider specifics for SCRM in the context of the ICD, CDD, and CONOPS. Alignment of the respective CDRLs with the ASA (ALT) requirements (e.g., AR 770-2, AR 770-3) and other acquisition requirements should be succinctly spelled out in the RFP to provide format, context, and transferability of the documentation.

---

[12] FAR, Part 39, Acquisition of Information Technology; Section 39.106, Contract Clause.

[13] FAR, Part 52, Solicitation Provisions and Contract Clauses; Section 52.239-1, Privacy or Security Safeguards.

APPENDIX D

Cyber Supply Chain Risk Management

Virtually everything the Army develops and acquires involves software. The term of art has shifted from *software* to *cyber* because of the lack of clear delineation between hardware and software in many cases, such as firmware, field-programmable gate arrays, cloud-based services, and the rise of the cyber-physical systems paradigm. The domain ranges from highly complicated to complex, requiring a systems approach to supply chains and supply chain risk. The current term of art for this systemic approach is *cyber supply chain risk management* (C-SCRM), formerly called *information and communications technology supply chain risk management* (ICT-SCRM) in the literature.

Vulnerabilities of the Cyber Supply Chain

By their nature, software or cyber supply chains contain a high degree of complexity and nebulousness. Among the factors that contribute to this state is the use of open-source code, the complicated origins of which might not be known, and the Agile development manifesto that is structured to rapidly develop code in a multi-stakeholder environment.

Software code developers rely on open-source libraries of functions, hosted by academic institutions and for-profit code libraries, to avoid reinventing the wheel where common functions are required. An example would be random forest analysis (RFA), the commonly used statistical function. A coder needing an RFA function would go to Google or GitHub and search the open-source, available RFA modules (ignorant of their respective origins or histories) or perhaps would go directly to a prominent statistical tool library, such as ALGLIB. Not unusual among function libraries, ALGLIB is a for-profit, Python function library that is hosted in the Russian Federation.[1] Developers also often embed older blocks of their own code into their new software functions that they then post in a library, which might then become a part of another new function in yet another library. Thus, a block of open-source code from a series of nebulous sources located all over the world would be embedded within millions of lines of other code and passed along as a working module to multiple projects requiring similar functionality.

This is where the Agile software development approach contributes to the complexity of the cyber supply chain. One aspect of the Agile process includes teams of contributors, each representing different aspects of the system goals, working together in two-week sprints of coding to produce software that accomplishes a goal, called a *story*. Many stories are combined into the finished software product and many teams work concurrently and in parallel during the Agile process.[2] The Agile process lends itself to the heavy reuse of code and the reliance on open-source code libraries to meet the goal (i.e., the *definition of done*) quickly. Although documentation is promoted as a hallmark of Agile, the documentation virtually never includes the provenance of the open-source code used, which is as much a result of such knowledge being unavailable to the user of the code as the rapid pace of the Agile sprint process.

[1] See ALGLIB Project, "Decision Forest," webpage, undated.

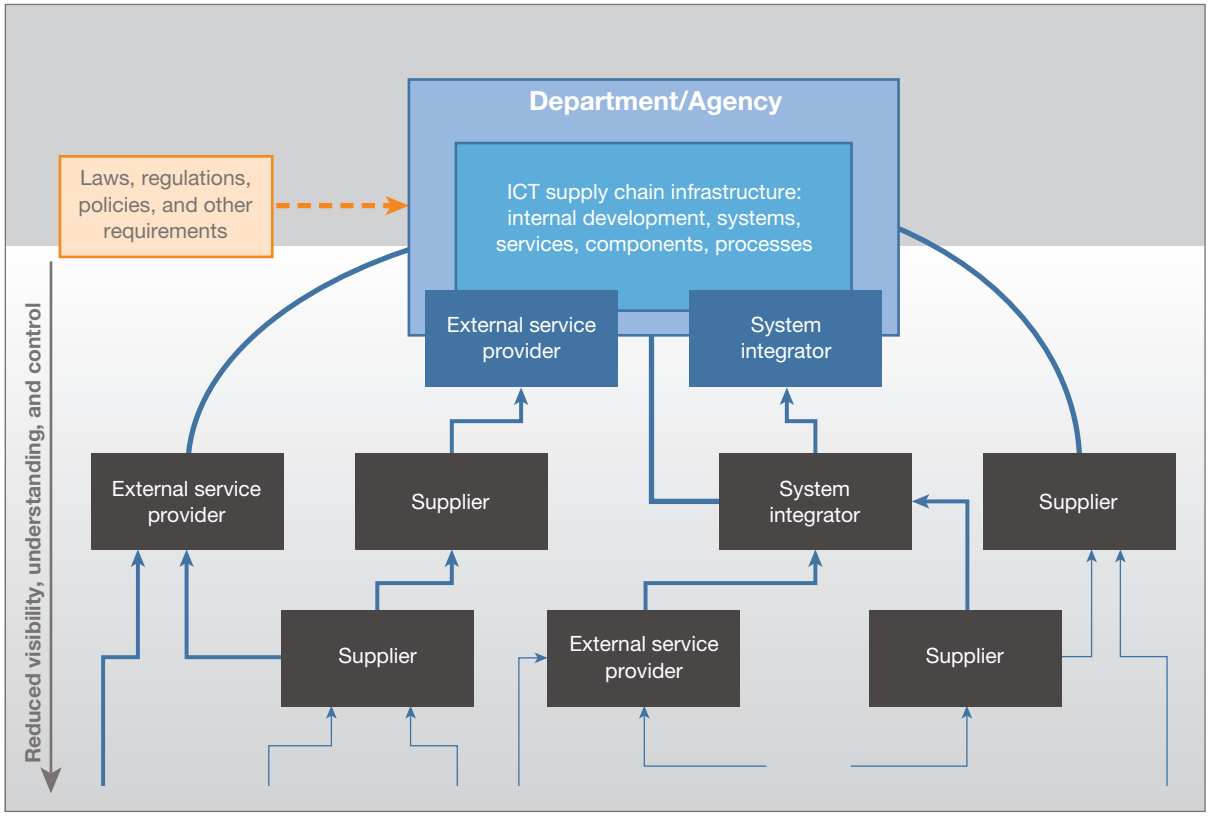
[2] Agile Alliance, "Agile 101," webpage, undated.

Finally, government contractors often reuse cyber program packages. Streamlining the process of developing and testing functional software through the reuse of proven code saves the government time and money and provides a product of known reliability. These program packages might have been developed prior to current standards for C-SCRM, so they could also introduce unknown vulnerabilities along with their cost savings.

Contracting and subcontracting for a cyber system result in the network shown in Figure D.1. This network diagram depicts the tip of a pyramid; each of the suppliers and providers in that pyramid are using Agile and open-source libraries. To accomplish comprehensive LSCRM in software code, all the code requires complete documentation of provenance at all levels of development, especially the open-source code. Such documentation is no small or inexpensive task. Capability maturity model integration (CMMI) and cybersecurity maturity model certification (CMMC) are considered the industry-standard media (or approaches) for achieving the cybersecurity and LSCRM goals of code provenance knowledge, but those approaches cannot document or measure what is effectively unknown.

FIGURE D.1

Federal Agency Relationships with System Integrators, Suppliers, and External Service Providers with Respect to the Scope of NIST SP 800-161



SOURCE: Adapted from Jon Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NIST, SP 800-161, April 2015, p. 5.

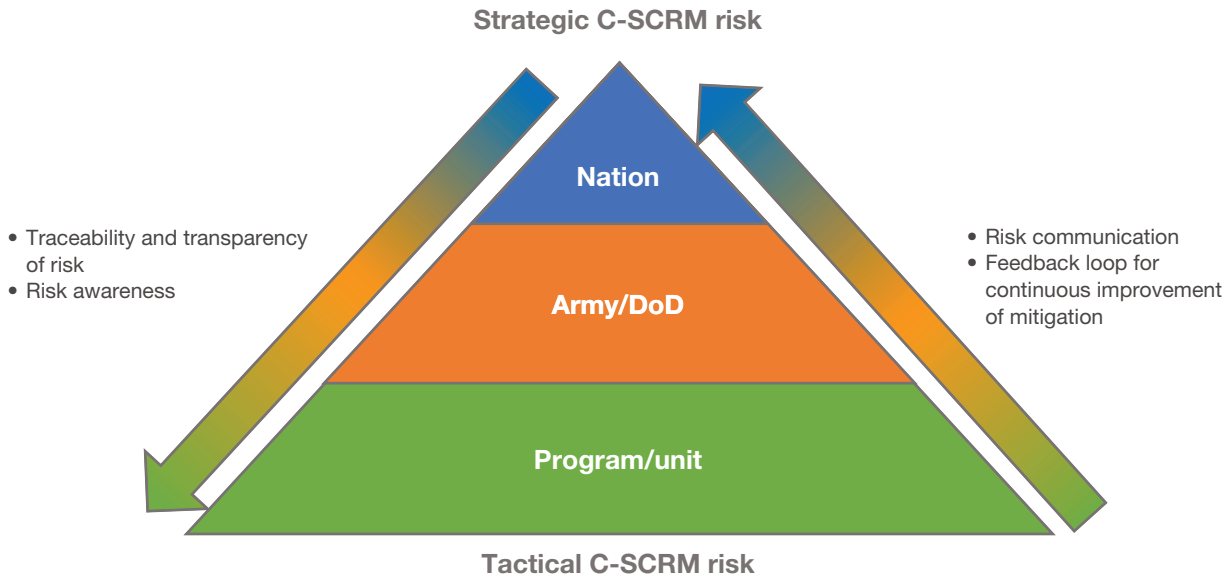
Multilevel Software Supply Chain Risk

Once software code enters the Army system, it becomes a part of a hierarchy of multilevel supply chain risk. Software in a rifle scope, a howitzer, or a helicopter enters the Army cyber network, requiring network interface for communication and periodic software updates. Thus, when this software is connected, however briefly, to the enterprise, it poses a risk of spreading cyber vulnerabilities to other systems and operations throughout the hierarchy. As shown in Figure D.2, detection of risks at the system level will flow up the chain to inform the management of risk. Likewise, information on vulnerabilities and countermeasures will flow down the chain to protect systems at all levels, and the feedback loop of mitigation effectiveness will refine the overall protection process.

Complexity in C-SCRM

Most system risks are not independent; rather, they are conditional on other variables that lead to specific impacts. Deciding where to build a factory, whom to hire to develop software, how to transport materials, or how to finance a venture all lead to conditional risks, as do pandemics, wars, and solar weather, among countless other factors. Nuclear plant accidents and manned spacecraft accidents are classic examples of complexity in risk, studied by engineers and academics for better approaches to risk analysis. One such powerful approach to accounting for risk complexity in supply chains involves the Bayesian aspects of conditional risk and modeling techniques, such as Bayesian Belief Networks.[3] Supported by risk exposure framework activities as described in NIST SP 800-161r1, Bayesian Networks should provide the Army with the optimal leverage points for risk management in complex systems and the Army enterprise.

FIGURE D.2
Multilevel Risk in Army C-SCRM



SOURCE: Adapted from Boyens et al., 2022, p. 22.

[3] Norman Fenton and Martin Neil, *Risk Assessment and Decision Analysis with Bayesian Networks*, CRC Press, 2018.

C-SCRM in Army Acquisition

The noted approaches for achieving the SCRM standards in the Army regulations remain program dependent, and the cyber aspects require some interpretation. We propose the following as a baseline approach to achieve these criteria during system acquisition as a part of the critical LSCRM aspects.

Because of the complicated nature of C-SCRM, active and continuous engagement of all stakeholders during the life cycle is required. In the context of the critical LSCRM aspects discussed in Chapter 3, the new acquisition documents shown in orange in Figures 3.5 and 3.6 should include specific requirements to address the most recent (2022) version of NIST SP 800-161r1, especially the Risk Exposure Framework. Critical passages of that exposure framework are in Appendix C of this report.

In the acquisition program concept phase, the NIST SP 800-161r1 concepts and practices should be leveraged as much as possible in the RFI and in the AoA to inform the solution trade study. For the initial and subsequent program RFPs, key program-relevant aspects of the NIST SP 800-161r1 practices and all NIST frameworks should be included in the SCRM requirements and the source selection SCRM decision matrix. The SCRM section of the submitted proposals should be carefully reviewed by the Army or other government cybersecurity experts as part of the source selection, modified in the awardee contract where necessary according to the MDCITA and other supporting program protection documentation, and followed up on in the respective acquisition phase SCRM CDRLs. These CDRLs should also be reviewed by the appropriate government cybersecurity experts. An informed C-SCRM feedback loop between the Army and the awardee will be critical to systemic life-cycle risk management.

Abbreviations

AA	American Airlines
ACC	Army Contracting Command
AFC	Army Futures Command
AMC	Army Materiel Command
AoA	analysis of alternatives
APA	additional performance attributes
ASA (ALT)	Assistant Secretary of the Army for Acquisition, Logistics, and Technology
CDD	capabilities development document
CDRL	contract data requirements list
CFIUS	Committee on Foreign Investment in the United States
CIP	critical intelligence parameters
CONOPS	concept of operations
COVID-19	coronavirus disease 2019
CPD	capability production document
CPI	critical program information
C-SCRM	cyber supply chain risk management
DASA-S	Deputy Assistant Secretary of the Army for Sustainment
DAU	Defense Acquisition University
DFARS	Defense Federal Acquisition Regulation Supplement
DIA	Defense Intelligence Agency
DLA	Defense Logistics Agency
DMSMS	diminishing manufacturing sources and material shortages
DoD	Department of Defense
DoDI	Department of Defense Instruction
DRFPRD	development request for proposals release decision
EMD	engineering and manufacturing development
FAR	Federal Acquisition Regulations
FCA	functional configuration audit
FIRRMA	The Foreign Investment Risk Review Modernization Act of 2018
FRP	full-rate production
GAO	Government Accountability Office
IBR	integrated baseline review
ICD	initial capabilities document
ICT	information communication technology
ICT-SCRM	information and communications technology supply chain risk management
INSCOM	Intelligence and Security Command
IoT	internet of things
IOT&E	initial operational test and evaluation

IP	intellectual property
IT	information technology
ITRA	independent technology risk assessment
JCIDS	Joint Capabilities Integration and Development System
JROC	Joint Requirements Oversight Council
KPP	key performance parameter
KSA	key system attribute
LCMC	Life Cycle Management Commands
LCSP	life-cycle sustainment plan
LFT&E	live fire test and evaluation
LMDP	life-cycle mission data plan
LMP	logistics modernization program
LRIP	low-rate initial production
LSCRM	life-cycle supply chain risk management
MAIS	major automated information system
MDA	milestone decision authority
MDCITA	multidisciplinary counterintelligence threat assessment
MDD	material development decision
MS	milestone
NHSTA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OEM	original equipment manufacturer
OSD	Office of the Secretary of Defense
OUSD A&S	Office of the Under Secretary of Defense for Acquisition and Sustainment
OUSD(R&E)	Office of the Under Secretary of Defense for Research and Engineering
PBOM	preliminary bill of materials
PEO	Program Evaluation Office
PM	program manager
PMB	performance measurement baseline
PPE	personal protective equipment
PPP	program protection plan
PSS	product support strategy
RFA	random forest analysis
RFI	request for information
RFP	request for proposal
RDT&E	research, development, test, and evaluation
SAM	System for Award Management
SCRM	supply chain risk management
SEP	systems engineering plan
SFR	system functional review
SME	subject matter expert

SOW	statement of work
SP	Special Publication
SRD	systems requirements document
SRM	supplier relationship management
SRR	systems requirements review
SSWG	Strategic Sourcing Working Group
SVR	system verification review
TMRR	technology maturation and risk reduction
TRL	technology readiness level
TTP	tactics, techniques, and procedures
TTR	time to recovery
USAF	United States Air Force
VATEP	value adjusted total evaluated price
VOLT	validated online life cycle threat

References

"American Airlines' Approach to Examining Supplier Performance," *Aviation Week & Space Technology*, Vol. 176, No. 35, October 6, 2014.

AcqNotes, "Capability Production Document (CPD)," webpage, February 12, 2020. As of March 11, 2022: https://acqnotes.com/acqnote/acquisitions/capability-production-document

AcqNotes, "Critical Design Review (CDR)," webpage, June 1, 2021a. As of March 11, 2022: https://acqnotes.com/acqnote/acquisitions/critical-design-review

AcqNotes, "Statement of Work (SOW)," webpage, June 6, 2021b. As of March 11, 2022: https://acqnotes.com/acqnote/tasks/statement-of-work

AcqNotes, "Performance Measurement Baseline (PMB)," webpage, June 24, 2021c. As of March 11, 2022: https://acqnotes.com/acqnote/tasks/performance-measurement-baseline

AcqNotes, "Integrated Baseline Review (IBR), webpage," June 26, 2021d. As of March 11, 2022: https://acqnotes.com/acqnote/acquisitions/integrated-baseline-review

AcqNotes, "Functional Configuration Audit (FCA)," webpage, June 29, 2021e. As of March 11, 2022: https://acqnotes.com/acqnote/tasks/functional-configuration-audit-2

AcqNotes, "Low-Rate Initial Production (LRIP)," webpage, June 30, 2021f. As of March 11, 2022: https://acqnotes.com/acqnote/acquisitions/low-rate-initial-production

AcqNotes, "Life-Cycle Sustainment Plan (LCSP)," webpage, July 2, 2021g. As of March 11, 2022: https://acqnotes.com/acqnote/careerfields/life-cycle-sustainment-plan-lcsp

AcqNotes, "Initial Operational Test & Evaluation (IOT&E)," webpage, July 8, 2021h. As of March 11, 2022: https://acqnotes.com/acqnote/careerfields/initial-operational-test-and-evaluation-te

AcqNotes, "Product Support Strategy (PSS)," webpage, July 14, 2021i. As of March 11, 2022: https://acqnotes.com/acqnote/careerfields/product-support-strategy

AcqNotes, "Live-Fire Test and Evaluation (LFT&E)," webpage, July 17, 2021j. As of March 11, 2022: https://acqnotes.com/acqnote/careerfields/live-fire-test-and-evaluation-2

AcqNotes, "System Verification Review (SVR)," webpage, July 26, 2021k. As of March 11, 2022: https://acqnotes.com/acqnote/acquisitions/system-verification-review-svr

Agile Alliance, "Agile 101," webpage, undated. As of March 21, 2022: https://www.agilealliance.org/agile101

ALGLIB Project, "Decision Forest," webpage, undated. As of March 21, 2022: https://www.alglib.net/dataanalysis/decisionforest.php

Al-Mansour, Jarrah F., and Sanad A. Al-Ajmi, "Coronavirus 'COVID-19'—Supply Chain Disruption and Implications for Strategy, Economy, and Management," *Journal of Asian Finance, Economics and Business,* Vol. 7, No. 9, 2020.

Altman, Edward I., "Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy," *Journal of Finance*, Vol. 23, No. 4, September 1968.

Antonelli, Julie, "Protecting Emerging and Existing Technology Investments with Escrow," *Defense One*, August 14, 2020. As of March 11, 2022: https://defensesystems.com/it-infrastructure/2020/08/protecting-emerging-and-existing-technology-investments-with-escrow/194760

Aqlan, Faisal, and Sarah S. Lam, "Supply Chain Risk Modelling and Mitigation," *International Journal of Production Research,* Vol. 53, No. 18, 2015.

AR—*See* Army Regulation.

Army Directive 2018-26, *Enabling Modernization Through the Management of Intellectual Property*, Secretary of the Army, December 7, 2018.

Army Regulation 25-1, *Army Information Technology*, Department of the Army, July 15, 2019.

Army Regulation 70-1, *Army Acquisition Policy*, Department of the Army, August 10, 2018.

Army Regulation 70-77, *Program Protection*, Department of the Army, June 8, 2018.

Army Regulation 702-19, *Reliability, Availability, and Maintainability*, Department of the Army, February 12, 2020.

Army Regulation 770-2, *Materiel Fielding*, Department of the Army, July 16, 2021.

Army Regulation 770-3, *Type Classification and Materiel Release*, Department of the Army, July 16, 2021.

Bailey, Tucker, Edward Barriball, Arnav Dey, and Ali Sankur, "A Practical Approach to Supply-Chain Risk Management," McKinsey and Company, March 8, 2019.

Bains, Patrick, Kyle Ferris, Justin Gregoire, James Kim, Jacob Kozloski, Jonathan Lazenby, Dimitri Ofiesh, Evan Shank, Kevin Wu, Peter Beling, and Cody Fleming, "Risk Analysis of Globalized Airline Supply Chains," *IEEE Systems and Information Engineering Design Symposium*, June 13, 2016.

Bisceglie, Jennifer, and Mark Weatherford, "New Technologies Bring New Risks to the Supply Chain," *Journal of Supply Chain Management, Logistics and Procurement,* Vol. 2, No. 2, Winter 2019–2020.

Blos, Mauricio F., Mohammed Quaddus, H. M. Wee, and Kenji Watanabe, "Supply Chain Risk Management (SCRM): A Case Study on the Automotive and Electronic Industries in Brazil," *Supply Chain Management,* Vol. 14, No. 4, June 19, 2009.

Boston, William, Asa Fitch, Mike Colias, and Ben Foldy, "How Car Makers Collided with a Global Chip Shortage," *Wall Street Journal*, February 12, 2021.

Bourlakis, Michael, and Johanne Allinson, "The Aftermath of the Foot and Mouth Crisis in Agricultural Logistics: The Case of the UK Fat Lamb Supply Chain," *International Journal of Logistics Research and Applications,* Vol. 6, No. 4, 2003.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Electronics Company*, National Institute of Standards and Technology, February 2020a.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Goods Company*, National Institute of Standards and Technology, February 2020b.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Anonymous Renewable Energy Company*, National Institute of Standards and Technology, February 2020c.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic*, National Institute of Standards and Technology, February 2020d.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Palo Alto Networks, Inc.*, National Institute of Standards and Technology, February 2020e.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Seagate Technology*, National Institute of Standards and Technology, February 2020f.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Case Studies in Cyber Supply Chain Risk Management: Summary of Findings and Recommendations*, National Institute of Standards and Technology, February 2020g.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*, National Institute of Standards and Technology, February 2021.

Boyens, Jon, Celia Paulsen, Rama Moorthy, and Nadya Bartol, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Special Publication 800-161, April 2015.

Boyens, Jon, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, and Matthew Fallon, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, National Institute of Standards and Technology, Special Publication 800-161r1, May 2022.

Boyson, Sandor, "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems," *Technovation,* Vol. 34, No. 7, July 2014.

Canis, Bill, *The Motor Vehicle Supply Chain: Effects of the Japanese Earthquake and Tsunami*, Congressional Research Service, R41831, May 23, 2011.

Castellan, *Supply Chain Continuity: The Impact of Global Labor—How COVID-19 Exposed Risk for Disruption*, White Paper, 2020.

Ceryno, Paula Santos, Luiz Felipe Scavarda, and Katja Klingebiel, "Supply Chain Risk: Empirical Research in the Automotive Industry," *Journal of Risk Research,* Vol. 18, No. 9, 2015.

Chen, Jingzhe, Hongfeng Wang, and Ray Y. Zhong, "A Supply Chain Disruption Recovery Strategy Considering Product Change Under COVID-19," *Journal of Manufacturing Systems,* Vol. 60, July 2021.

Chopra, Sunil, and Manmohan S. Sodhi, "Managing Risk to Avoid Supply-Chain Breakdown," *MIT Sloan Management Review*, Vol. 46, No. 1, Fall 2004.

Committee on Critical Mineral Impacts on the U.S. Economy, National Research Council of the National Academies, *Minerals, Critical Minerals, and the U.S. Economy*, National Academies Press, 2008.

Costantino, Nicola, and Roberta Pellegrino, "Choosing Between Single and Multiple Sourcing Based on Supplier Default Risk: A Real Options Approach," *Journal of Purchasing and Supply Management,* Vol. 16, No. 1, March 2010.

Dai, Tinglong, Ge Bai, and Gerard F. Anderson, "PPE Supply Chain Needs Data Transparency and Stress Testing," *Journal of General Internal Medicine*, Vol. 35, No. 9, September 2020.

DAU—*See* Defense Acquisition University.

Defense Acquisition University, "Ask a Professor," webpage, undated-a. As of February 14, 2022: https://www.dau.edu/training/career-development/contracting/p/Ask-A-Professor

Defense Acquisition University, "Engineering and Manufacturing Development (EMD) Phase," webpage, undated-b. As of March 11, 2022:
https://aaf.dau.edu/aaf/mca/emd-phase

Defense Acquisition University, "Systems Engineering Plan (SEP)," webpage, undated-c. As of March 11, 2022: https://aaf.dau.edu/aaf/mca/sep

Defense Acquisition University, *Product Support Strategy Development Tool*, 2022a. As of March 30, 2023: https://www.dau.edu/tools/Lists/DAUTools/Attachments/16/Product%20Support%20Strategy%20Development%20Tool-Revised-20230222.pdf

Defense Acquisition University, "Major Capabilities Acquisition (Pre-Tailoring): Acquisition & Procurement Milestones, Phases and Decision Points," chart, Ver. 2.1, October 21, 2022b. As of March 30, 2023: https://www.dau.edu/tools/Documents/Lifecycle%20Chart%20-%20Major%20Capability%20Lane_print.pdf

Defense Acquisition University Acquipedia, "Data Rights," webpage, undated-a. As of March 2, 2022: https://www.dau.edu/acquipedia/pages/articledetails.aspx#!510

Defense Acquisition University Acquipedia, "Intellectual Property Strategy," webpage, undated-b. As of March 3, 2022:
https://www.dau.edu/acquipedia/pages/articledetails.aspx#!508

Defense Federal Acquisition Regulation Supplement, Part 204, Administrative and Information Matters; Subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Defense Federal Acquisition Regulation Supplement, Part 239, Acquisition of Information Technology; Subpart 239.73, Requirements for Information Relating to Supply Chain Risk.

Defense Federal Acquisition Regulation Supplement, Part 246, Quality Assurance; Section 246.870, Contractors Counterfeit Electronic Part Detection and Avoidance.

Defense Federal Acquisition Regulation Supplement, Part 252, Solicitation Provisions and Contract Clauses; Section 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Defense Federal Acquisition Regulation Supplement, Part 252, Solicitation Provisions and Contract Clauses; Section 252.239-7018, Supply Chain Risk.

Defense Federal Acquisition Regulation Supplement, Part 252, Solicitation Provisions and Contract Clauses; Section 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System.

Deleris, Léa A., Debra Elkins, and M. Elisabeth Paté-Cornell, "Analyzing Losses from Hazard Exposure: A Conservative Probabilistic Estimate Using Supply Chain Risk Simulation," in Ricki G. Ingalls, Manuel D. Rossetti, Jeffrey S. Smith, and Brett A. Peters, eds., *Proceedings of the 2004 Winter Simulation Conference*, Institute of Electrical and Electronics Engineers, December 2004.

Department of Defense Enterprise Software Initiative, *Software Buyer's Checklist*, January 2016.

Department of Defense Instruction 4140.01, *DoD Supply Chain Materiel Management Policy*, Office of the Under Secretary of Defense for Acquisition and Sustainment, March 6, 2019.

Department of Defense Instruction 4140.67, *DoD Counterfeit Prevention Policy*, Office of the Under Secretary of Defense for Acquisition and Sustainment, April 26, 2013, change 3, March 6, 2020.

Department of Defense Instruction 4245.15, *Diminishing Manufacturing Sources and Material Shortages Management*, Office of the Under Secretary of Defense for Acquisition and Sustainment, November 5, 2020.

Department of Defense Instruction 5000.02T, *Operation of the Defense Acquisition System*, Office of the Under Secretary of Defense for Acquisition and Sustainment, January 7, 2015, change 3, August 10, 2017.

Department of Defense Instruction 5010.44, *Intellectual Property (IP) Acquisition and Licensing*, Office of the Under Secretary of Defense for Acquisition and Sustainment, October 16, 2019.

Department of Defense Instruction 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)*, Office of the Under Secretary of Defense for Acquisition and Sustainment, May 28, 2015, change 3, October 1, 2020.

Department of Defense Instruction 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, November 5, 2012.

Department of Defense Instruction 8500.01, *Cybersecurity*, March 14, 2014, change 1, October 7, 2019.

Department of Defense Manual 4140.01, Volume 1, *DoD Supply Chain Materiel Management Procedures: Operational Requirements*, December 13, 2018.

Department of Defense 7000.14-R, *Financial Management Regulation,* Volume 2A, "Budget Formulation and Presentation (Chapters 1–3)," Office of the Under Secretary of Defense (Comptroller), June 2017.

Department of the Army, Draft SCRM Directive, provided to the authors for this project, November 17, 2021.

Department of the Army Pamphlet 70-3, *Army Acquisition Procedures*, Department of the Army, September 17, 2018.

DFARS—*See* Defense Federal Acquisition Regulation Supplement.

Dieter, Ernst, "The Economics of the Electronics Industry: Competitive Dynamics and Industrial Organization," East-West Center Working Papers, Economics Series, No. 7, October 2000.

DoDI—*See* Department of Defense Instruction.

DoDM—*See* Department of Defense Manual.

DuHadway, Scott, Steven Carnovale, and Benjamin Hazen, "Understanding Risk Management for Intentional Supply Chain Disruptions: Risk Detection, Risk Mitigation, and Risk Recovery," *Annals of Operations Research,* Vol. 283, No. 1–2, December 2019.

Enyinda, Chris I., Chris H. N. Mbah, and Alphonso Ogbuehi, "An Empirical Analysis of Risk Mitigation in the Pharmaceutical Industry Supply Chain: A Developing-Country Perspective," *Thunderbird International Business Review,* Vol. 52, No. 1, January/February 2010.

Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," Executive Office of the President, July 21, 2017.

Executive Order 14017, "Securing America's Defense Critical Supply Chains," Executive Office of the President, February 24, 2021.

FAR—*See* Federal Acquisition Regulation.

Federal Acquisition Regulation, Part 9, Contractor Qualifications; Subpart 9.1, Responsible Prospective Contractors.

Federal Acquisition Regulation, Part 22, Application of Labor Laws to Government Acquisitions; Section 22.101-2, Contract Pricing and Administration.

Federal Acquisition Regulation, Part 39, Acquisition of Information Technology; Section 39.106, Contract Clause.

Federal Acquisition Regulation, Part 52, Solicitation Provisions and Contract Clauses; Section 52.239-1, Privacy or Security Safeguards.

Fenton, Norman, and Martin Neil, *Risk Assessment and Decision Analysis with Bayesian Networks*, CRC Press, 2018.

Finch, Joel, "Toyota Sudden Acceleration: A Case Study of the National Highway Traffic Safety Administration—Recalls for Change," *Loyola Consumer Law Review*, Vol. 22, No. 4, 2010.

GAO—*See* U.S. Government Accountability Office.

Goddin, James R. J., "Identifying Supply Chain Risks for Critical and Strategic Materials," in S. Erik Offerman, ed., *Critical Materials: Underlying Causes and Sustainable Mitigation Strategies*, World Scientific, 2019.

Gravier, Michael J., and Stephen M. Swartz, "The Dark Side of Innovation: Exploring Obsolescence and Supply Chain Evolution for Sustainment-Dominated Systems," *Journal of High Technology Management Research,* Vol. 20, No. 2, 2009.

Gregson, Sarah, Ian Hampson, Anne Junor, Doug Fraser, Michael Quinlan, and Ann Williamson, "Supply Chains, Maintenance and Safety in the Australian Airline Industry," *Journal of Industrial Relations,* Vol. 57, No. 4, September 2015.

Harapko, Sean, "How COVID-19 Impacted Supply Chains and What Comes Next," webpage, Ernst & Young, 2021. As of March 4, 2022:
https://www.ey.com/en_us/supply-chain/how-covid-19-impacted-supply-chains-and-what-comes-next

Helmold, Marc, Ayşe Küçük Yılmaz, Tracy Dathe, and Triant G. Flouris, "SCRM Strategy," in *Supply Chain Risk Management: Cases and Industry Insights*, Springer International Publishing, 2022.

Helmold, Marc, Ayşe Küçük Yılmaz, Tracy Dathe, and Triant G. Flouris, "SCRM in the Automotive Industry: AutoSCRM," in *Supply Chain Risk Management: Cases and Industry Insights*, Springer International Publishing, 2022.

Hermoso-Orzáez, M. J., and J. Garzón-Moreno, "Risk Management Methodology in the Supply Chain: A Case Study Applied," *Annals of Operations Research*, Vol. 13, No. 2, June 2022.

Hillman, Mark, and Heather Keltz, *Managing Risk in the Supply Chain—A Quantitative Study*, AMR Research, Inc., January 2007.

Hoeksema, Michael, "Understanding and Managing Future Risk: Case Study on Managing Supply Chain Data," *Journal of Supply Chain Management, Logistics and Procurement,* Vol. 2, No. 2, Winter 2019–2020.

Hosseini, Seyedmohsen, and Dmitry Ivanov, "A Multi-Layer Bayesian Network Method for Supply Chain Disruption Modelling in the Wake of the COVID-19 Pandemic," *International Journal of Production Research*, Vol. 60, No. 17, 2022.

International Organization for Standardization, "ISO 31000:2018, Risk Management—Guidelines," 2018.

Kamarudeen, Niyazudeen, and Balan Sundarakani, "Business and Supply Chain Strategy of Flying Above the Dessert: A Case Study of Emirates Airlines," *9th International Conference on Operations and Supply Chain Management, Vietnam*, 2019.

Kane, Sean, Ellen Liberman, Tony DiViesti, and Felix Click, *Toyota Sudden Unintended Acceleration*, Safety Research & Strategies, February 5, 2010.

Kline, Ellen, "Canadian BSE Continues to Disrupt the Supply Chain for Beef," *Law and Business Review of the Americas,* Vol. 13, No. 3, 2007.

Kwon, Caleb, *Supply Chain Disruptions: Evidence from the Bankruptcy of Hanjin Shipping*, Social Science Research Network, July 17, 2021.

Larson, Paul D., and Jack D. Kulchitsky, "Single Sourcing and Supplier Certification: Performance and Relationship Implications," *Industrial Marketing Management,* Vol. 27, No. 1, January 1998.

Li, Xishu, Rommert Dekker, Christiaan Heij, and Mustafa Hekimoğlu, "Assessing End-Of-Supply Risk of Spare Parts Using the Proportional Hazard Model," *Decision Sciences,* Vol. 47, No. 2, April 2016.

Liker, Jeffrey K., and Gary L. Convis, *The Toyota Way to Lean Leadership: Achieving and Sustaining Excellence Through Leadership Development*, McGraw-Hill, 2011.

Lockamy, Archie, III, "An Examination of External Risk Factors in Apple Inc.'s Supply Chain," *Supply Chain Forum: An International Journal,* Vol. 18, No. 3, May 16, 2017.

Loredo, Elvira N., John F. Raffensperger, and Nancy Young Moore, *Measuring and Managing Army Supply Chain Risk: A Quantitative Approach by Item Number and Commercial Entity Code*, RAND Corporation, RR-902-A, 2015. As of February 24, 2023:
https://www.rand.org/pubs/research_reports/RR902.html

Luckstead, Jeff, Rodolfo M. Nayga, Jr., and Heather A. Snell, "Labor Issues in the Food Supply Chain Amid the COVID-19 Pandemic," *Applied Economic Perspectives and Policy,* Vol. 43, No. 1, March 2021.

McClean, Timothy, "How Do You Reduce Lead Time in Your Supply Chain?" TXM Lean Solutions blog, 2017. As of March 3, 2022:
https://txm.com/reduce-lead-time-supply-chain

Miocevic, Dario, and Biljana Crnjak-Karanovic, "The Mediating Role of Key Supplier Relationship Management Practices on Supply Chain Orientation—The Organizational Buying Effectiveness Link," *Industrial Marketing Management*, Vol. 41, No. 1, January 2012.

Mocenco, Daniela, "Supply Chain Features of the Aerospace Industry Particular Case Airbus and Boeing," *Scientific Bulletin – Economic Sciences,* University of Pitesti*,* Vol. 14, No. 2, 2015.

Moore, Nancy Y., Clifford A. Grammich, and Judith D. Mele, *Findings From Existing Data on the Department Of Defense Industrial Base*, RAND Corporation, RR-614-OSD, 2014. As of February 24, 2023:
https://www.rand.org/pubs/research_reports/RR614.html

Moore, Nancy Young, Elvira N. Loredo, Amy G. Cox, and Clifford A. Grammich, *Identifying and Managing Acquisition and Sustainment Supply Chain Risks*, RAND Corporation, RR-549-AF, 2015. As of February 24, 2023:
https://www.rand.org/pubs/research_reports/RR549.html

National Highway Traffic Safety Administration, *U.S. Department of Transportation Releases Results From NHTSA-NASA Study of Unintended Acceleration in Toyota Vehicles*, press release, February 8, 2011.

Nishiguchi, Toshihiro, and Alexandre Beaudet, "The Toyota Group and the Aisin Fire," *MIT Sloan Management Review,* Vol. 40, No. 1, Fall 1998.

NIST SP 800-161r1—*See* Boyens et al., 2022.

NIST SP 800-171—*See* Ross et al., 2020.

O'Connell, Caolionn, Elizabeth Hastings Roer, Rick Eden, Spencer Pfeifer, Yuliya Shokh, Lauren A. Mayer, Jake McKeon, Jared Mondschein, Phillip Carter, Victoria A. Greenfield, and Mark Ashby, *Managing Risk in Globalized Supply Chains*, RAND Corporation, RR-A425-1, 2021. As of February 24, 2023:|
https://www.rand.org/pubs/research_reports/RRA425-1.html

Office of the Deputy Assistant Secretary of Defense for Systems Engineering, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, January 2017.

Patel, Anita, Maryann M. D'Alessandro, Karen J. Ireland, W. Greg Burel, Elaine B. Wencil, and Sonja A. Rasmussen, "Personal Protective Equipment Supply Chain: Lessons Learned from Recent Public Health Emergency Responses," *Health Security*, Vol. 15, No. 3, May/June 2017.

Pettit, Timothy J., Joseph Fiksel, and Keely L. Croxton, "Ensuring Supply Chain Resilience: Development of a Conceptual Framework," *Journal of Business Logistics,* Vol. 31, No. 1, Spring 2010.

Phadnis, Shardul, and Nitin Joglekar, "Configuring Supply Chain Dyads for Regulatory Disruptions: A Behavioral Study of Scenarios," *Production and Operations Management*, Vol. 30, No. 4, April 2021.

Public Law 115-232, Title XVII—Review of Foreign Investment and Export Controls, The Foreign Investment Risk Modernization Act of 2018, August 13, 2018.

Rampersad, Giselle C., Ann-Louise Hordacre, and John Spoehr, "Driving Innovation in Supply Chains: An Examination of Advanced Manufacturing and Food Industries," *Journal of Business and Industrial Marketing,* Vol. 35, No. 5, April 23, 2020.

Ross, Ron, Victoria Pillitteri, Kelley Dempsey, Mark Riddle, Gary Guissanie, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, National Institute of Standards and Technology, Special Publication 800-171, Revision 2, February 2020.

Saich, Tony, "What Kind of World Does Xi Jinping Want?" Harvard Kennedy School, Summer 2022.

Sandborn, Peter, Varun J. Prabhakar, and Abisola Kusimo, "Modeling the Obsolescence of Critical Human Skills Necessary for Supporting Legacy Systems," *Proceedings of the ASME 2012 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, American Society of Mechanical Engineers, August 12–15, 2012.

Schoenherr, Tobias, Carlos Mena, and Thomas Choi, "Measuring and Managing Risks in the Supply Chain," CAPS Research, April 2019.

Schwartz, Samantha, "Cyber Needs to Be a Part of Supply Chain Risk Management, Federal Agency Says," *Supply Chain Dive*, October 6, 2021. As of March 7, 2022: https://www.supplychaindive.com/news/NIST-cyber-supply-chain-risk-management/607776

Shahed, Kazi Safowan, Abdullahil Azeem, Syed Mithun Ali, and Md. Abdul Moktadir, "A Supply Chain Disruption Risk Mitigation Model to Manage COVID-19 Pandemic Risk," *Environmental Science and Pollution Research*, January 2021.

Sheffi, Yossi, James B. Rice, Jr., Jonathan M. Fleck, and Federico Caniato, "Supply Chain Response to Global Terrorism: A Situation Scan," *Proceedings from the EurOMA POMS Joint International Conference, Cernobbio*, June 17, 2003.

Siegfried, Mary, *Critical Issue Report*: *Third Party Risk Management*, CAPS Research, September 2019.

Silberglitt, Richard, *Critical Materials and U.S. Import Reliance: Recent Developments and Recommended Actions*, RAND Corporation, CT-485, 2017. As of May 11, 2023: https://www.rand.org/pubs/testimonies/CT485.html

Silberglitt, Richard, James T. Bartis, Brian G. Chow, David L. An, and Kyle Brady, *Critical Materials: Present Danger to U.S. Manufacturing*, RAND Corporation, RR-133-NIC, 2013. As of March 1, 2023: https://www.rand.org/pubs/research_reports/RR133.html

Smith, L. Douglas, Anthony Vatterott, and Wesley Boyce, "Assessing Performance and Risk in Complex Supply Chains and Tying Performance Measures to Strategic Concepts," *Supply Chain Forum: An International Journal*, Vol. 23, No. 1, 2022.

Song, Tao, Yan Li, Jiashan Song, and Zhao Zhang, "Airworthiness Considerations of Supply Chain Management from Boeing 787 Dreamliner Battery Issue," *Procedia Engineering,* Vol. 80, 2014.

"Strategies to Build a Resilient Supply Chain and How to Manage the People to Keep It Operational," Supply Chain Management Review, Vol. 25, No. 4, May/June 2021.

Sullivan, Arthur, "Why the Auto Chip Crisis Could Get More Complex," Deutsche Welle, February 2, 2021.

Sund, Tobias, Claes Lööf, Simin Nadjm-Tehrani, and Mikael Asplund, "Blockchain-Based Event Processing in Supply Chains—A Case Study at IKEA," *Robotics and Computer-Integrated Manufacturing,* Vol. 65, October 2020.

Talluri, Srinivas, Thomas J. Kull, Hakan Yildiz, and Jiho Yoon, "Assessing the Efficiency of Risk Mitigation Strategies in Supply Chains," *Journal of Business Logistics,* Vol. 34, No. 4, 2013.

Tang, Christopher S., "Robust Strategies for Mitigating Supply Chain Disruptions," *International Journal of Logistics Research and Applications,* Vol. 9, No. 1, 2006.

Terry, Joshua, "Key Segments of the Electronics Industry," webpage, Strategylab, undated. As of March 20, 2023: https://strategylab.eu/key-segments-of-the-electronics-industry.html

Thomason, James S., Robert J. Atwell, Ylli Bajraktari, James P. Bell, D. Sean Barnett, Nicholas S. J. Karvonides, Michael F. Niles, and Eleanor L. Schwartz, *From National Defense Stockpile (NDS) to Strategic Materials Security Program (SMSP): Evidence and Analytic Support*, Institute for Defense Analyses, P-4593, May 2010.

Titman, Sheridan, "Risk Transmission Across Supply Chains," *Production and Operations Management,* Vol. 30, No. 12, December 2021.

Tummala, Rao, and Tobias Schoenherr, "Assessing and Managing Risks Using the Supply Chain Risk Management Process (SCRMP)," *Supply Chain Management*, Vol. 16, No. 6, September 27, 2011.

U.S. Code, Title 50, Section 3334e, Enhanced Procurement Authority to Manage Supply Chain Risk.

U.S. Government Accountability Office, *Defense Acquisitions: DOD Should Take Additional Actions to Improve How It Approaches Intellectual Property*, GAO-22-104752, November 2021.

U.S. Senate Committee on Commerce, Science, and Transportation, "The CHIPS Act of 2022: Section-by-Section Summary," 2022.

Van Atta, Richard, Royce Kneece, Michael Lippitz, and Christina Patterson, *Department of Defense Access to Intellectual Property for Weapon Systems Sustainment,* Institute for Defense Analyses, P-8266, May 2017.

Varas, Antonio Raj Varadarajan, Ramiro Palma, Jimmy Goodrich, and Falan Yinug, *Strengthening the Global Semiconductor Supply Chain in an Uncertain Era*, Boston Consulting Group and Semiconductor Industry Association, April 2021.

Villena, Veronica H., Andrew M. Novakovic, Mark Stephenson, and Charles Nicholson, "Management Lessons from the U.S. Dairy Sector's Pandemic Response," *Supply Chain Management Review,* Vol. 25, No. 5, September/October 2021.

Wang, Xiaojun, Puneet Tiwari, and Xu Chen, "Communicating Supply Chain Risks and Mitigation Strategies: A Comprehensive Framework," *Production Planning and Control,* Vol. 28, No. 13, May 22, 2017.

Wincewicz-Bosy, Marta, Adam Sadowski, Katarzyna Wąsowska, Zbigniew Galar, and Małgorzata Dymyt, "Military Food Supply Chain During the COVID-19 Pandemic," *Sustainability,* Vol. 14, No. 4, February 2022.

ARROYO CENTER

Although policy guidance is in place to manage some risks, there is no comprehensive procedure on how to manage the array of risks that can afflict U.S. Army supply chains. Because the Army lacks a comprehensive supply chain risk management (SCRM) system, there is limited ability to proactively identify and manage supply chain risks across a weapon system program's life cycle. In this report, the authors develop frameworks to support implementation of an Army common operating procedure for identifying and managing supply chain risks during the acquisition life cycle.

The authors surveyed the SCRM literature to catalog and define 10 supply chain risk categories and 31 supply chain risk drivers. They also documented lessons learned from three supply chain risk case studies. The authors reviewed the process steps and documents reflected in the Army acquisition life cycle; interviewed representatives from the acquisition and sustainment communities to understand the existing approach to SCRM; and then identified the steps along the process where supply chain risk activities might take place.

The authors recommend the adoption of three interconnected SCRM frameworks that span the weapon system's life cycle. By managing across three frameworks, the Army can focus SCRM activities within the organizations that have the most knowledge and information about the weapon system at that point in the life cycle. The interrelated nature of the frameworks promotes sharing knowledge and acknowledging the changing nature of risks across the life cycle.

$38.00

ISBN-10 1-9774-1451-6
ISBN-13 978-1-9774-1451-9

www.rand.org

RR-A2002-1