Supply Chain Risk Management Framework

Project Report – Phase I

Office of the Assistant Secretary
of Defense for Sustainment

CLEARED FOR OPEN PUBLICATION 15 Feb 2023

FOREWORD FROM ASSISTANT SECRETARY OF DEFENSE (SUSTAINMENT)

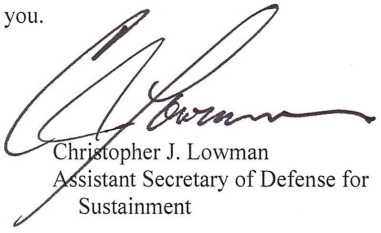
Part of delivering on the National Defense Strategy's Integrated Deterrence priority is providing a holistic, coordinated, cohesive approach to supply chain risk management (SCRM) that will strengthen the resiliency of our defense supply chain. As the Department of Defense (DoD) proponent for the development and implementation of SCRM policies, my office launched a project in May 2022 to develop a common SCRM framework and taxonomy in coordination with DoD components, interagency partners, academia, industry and related standards bodies.

Although multiple organizations across the DoD work to address the many risks impacting our supply chain, cross-functional coordination and information sharing will be required to deliver the Integrated Deterrence effects we seek. To begin institutionalizing this more coordinated approach, the Deputy Assistant Secretary of Defense for Logistics led an effort in partnership with the Defense Acquisition University over the past 15 months to develop a common SCRM framework. The goal was to clearly identify the roles, responsibilities, processes, gaps, and opportunities across the many stakeholder communities and functional areas working diligently to mitigate disruptions and secure our supply chains.

This report summarizes Phase I of our DoD SCRM framework development efforts to date, and validates our commitment to continuous learning and scrutiny of our defense supply chains and associated risk factors. The report includes a first-ever coordinated DoD SCRM Taxonomy that enables the DoD's cross-functional supply chain risk enterprise to speak in common terms when identifying, assessing, and mitigating supply chain risks. We developed the taxonomy, which includes 12 risk categories and 126 sub-risk categories, in coordination throughout the Department and with industry, academia, and related standards bodies. DoD Components now can incorporate this common taxonomy into information systems, databases, programs, and policies to assess, categorize, and share risk discussions across the enterprise.

Throughout 2023, we will continue refining and expanding the framework and ultimately codify the framework and taxonomy in an overarching DoD SCRM policy instruction. We will work with the Defense Acquisition University to develop a training and curriculum roadmap and lead and coordinate an overall SCRM data analytics strategy across the Department. My office is committed to delivering a holistic, coordinated DoD SCRM taxonomy, framework, strategy, and policy. These efforts will support the supply chain enterprise in identifying, managing, and mitigating risk in our defense supply chains necessary to ensure our national defense and security at home and abroad.

On behalf of the Department and the nation's defense, I am grateful for the contributions and advocacy of our defense supply chain stakeholders on this endeavor. I especially wish to thank the high-quality contributions of our nation's foremost academic institutions and industry partners. We couldn't have done it without you.



Christopher J. Lowman
Assistant Secretary of Defense for
Sustainment

March 2023

Office of the Secretary of Defense,
Assistant Secretary of Defense for Sustainment

Ms. Leigh E. Method
Deputy Assistant Secretary of Defense for Logistics

BG Michelle Link, USA Executive Director for OCS Office of the Deputy Assistant Secretary of Defense for Logistics	**Mr. Steven Karl** Professor of Logistics Management Defense Systems Management College Defense Acquisition University
Mr. Jared Andrews Senior Supply Chain Analyst Office of the Deputy Assistant Secretary of Defense for Logistics	**Dr. Robert Claflin** Professor of Requirements Management Defense Systems Management College Defense Acquisition University
Mr. Peter Battaglia Deputy Director, Mission Assurance (J351) J3 Logistics Operations Defense Logistics Agency	**Dr Chris D'Ascenzo DBA** Professor of Program Management Defense Systems Management College Defense Acquisition University
Ms. Stephanie Lopez Taxonomy Team Lead AFMC/A4/10 Headquarters Air Force Materiel Command	**Ms. Renee Settles** Management Analyst/Mission Assistance Defense Systems Management College Defense Acquisition University
Dr. Wayne Clark DSLDP Fellow, Senior Research Analyst Office of the Deputy Assistant Secretary of Defense for Logistics	**Mr. Alex Weaver** Supply Chain Analyst Office of the Deputy Assistant Secretary of Defense for Logistics

February 2023

Executive Summary

With our adversaries using our global supply chains as a non-standard tool to engage in competition below the level of armed conflict, the Department of Defense requires:

- a persistent and holistic approach for managing the risks associated with supply chains of the defense industrial base and national security innovation base (NSIB) as well as
- a consensus on the definition of supply chain risk lexicon as it pertains to DoD supply chain entities, relationships, and functions.

The purpose of this report is to provide the output of the Deputy Assistant Secretary of Defense for Logistics (DASD(Log)) and Defense Acquisition University (DAU) Supply Chain Risk Management (SCRM) project. The DASD(Log) asked DAU, in concert with academia and industry to facilitate deliberate, focused small group working sessions with key stakeholders to develop a common framework that clearly defines the compendium of supply chain risk management terms and lines of effort.

Deliberate working sessions were held with key stakeholders to further discuss and refine the draft framework over the last nine months. Each working session focused on identifying key stakeholders and their organizational SCRM related activities, authorities, policies, processes, opportunities, and gaps within each respective line of effort (LOE). DASD(Log) developed a draft framework with the Military Services, key Office of the Secretary of Defense (OSD) stakeholders and other government agencies in early FY22, ahead of focused small working sessions. As a result of the work, the overarching recommendation was to establish an enterprise level organizational structure to develop and implement an integrated SCRM framework, standard supply chain risk taxonomy, DoD SCRM policy, data integration strategy, and governance and oversight.

While many practitioners of supply chain management have long understood the global dependencies—and associated risks—of our supply chains, it took a pandemic and the resultant supply disruptions to fully expose the national security implications associated with these supply chain vulnerabilities.

Supply chain risks are not unique to the Department, but such risks take on greater urgency when considered in light of national security. For example, to keep aging weapon systems operational, we depend on a finite number of repair parts suppliers, some of which are precariously close to fiscal collapse. The proliferation of counterfeit items (particularly for microelectronics) increases the risk of mission delay or imperiled safety. Intellectual property vulnerabilities and lowered integrity of sensitive data and secure networks undermine the protections around our weapon system designs. Dependence on foreign entities for critical items and cyber disruptions to the manufacturing and transportation domains likewise jeopardize mission support and success.

The goals for the working sessions were twofold: 1) develop a compendium of supply chain terms to ensure a shared understanding and a common lexicon for risks and management strategies, and 2) develop specific lines of effort that focus organizational energies from across the DoD.

This report summarizes the methods, results, and recommendations of the DASD(Log)/DAU project:

- Recommendation 1: Integrate the SCRM taxonomy with policies, procedures, and governance processes.
- Recommendation 2: Execute an integrated gap closure initiative across the eight current lines of effort.
- Recommendation 3: Expand on the work completed to date by developing additional proposed lines of effort and identified gaps within each.
- Recommendation 4: Establish an enterprise-level organizational structure to develop and implement an integrated SCRM framework, standard supply chain risk taxonomy, DoD SCRM policy, data integration strategy, and governance and oversight.

A follow-on project (Phase II) is needed to further refine and develop the Department's supply chain ecosystem and expand on additional lines of effort identified but not defined during Phase I such as transportation, pharmaceutical/medical, environment, agriculture, data analytics, and chemical. Phase II will also include the integration of metrics, climate, and operational considerations across all lines of effort.

Table of Contents

Figures

Tables

1.0 Challenge

The very nature of a modern global supply chain has exposed the nation to increased foreign influence and control in the form of shadowy equity investments, a web of hard-to-trace associations that result from a multitude of mergers and acquisitions, and competitor infiltration deep within the supply chain sub-tiers. Our adversaries have also increased their control of strategic reserves of critical minerals and rare earth elements, just as we grow more dependent on economically fragile sole-source suppliers.

While many practitioners of supply chain management have long understood the global dependencies of our supply chains and all associated risks, it took a pandemic and the subsequent supply chain disruptions to fully expose the national security implications associated with such vulnerabilities. The February 2022 Russian invasion of Ukraine compounded an already stressed supply ecosystem experiencing wide-ranging effects, including energy interruptions across Europe, disruptions to key sources of supply (such as neon gas) critical to micro-chip production, and delayed shipments of a sizable portion of the world's grain supply.

Our adversaries are using supply chains as a non-standard tool to engage in competition below the level of armed conflict. It is, therefore, imperative the DoD identify risks, threats, and vulnerabilities and prioritize mitigation strategies in the form of

- strategic economic investments,
- in-depth sector analyses,
- increased training and education of the DoD workforce and partners,
- information sharing across the enterprise and with interagency partners and industry (as applicable),
- additional authorities for addressing SCRM throughout the acquisition lifecycle,
- clear SCRM roles and responsibilities codified within updates to relevant policies and procedures, and
- the establishment of a government structure to actively identify opportunities and gaps while monitoring for new areas of potential risk.

2.0 Problem Statement

The Department of Defense requires a persistent, holistic, and comprehensive approach to effectively manage the disparate risks associated with the defense industrial base and national security innovation base (NSIB) supply chain, as well as, a consensus on the definition of supply chain risk lexicon as it pertains to supply availability, original equipment manufacturers (OEMs), Defense Logistics Agency (DLA), Academia, Committee on Foreign Investment in the United States (CFIUS), supply chain resiliency, and supply chain risk management.

The DoD currently lacks a coordinated, holistic framework to effectively manage the risks within the broader defense supply chain, including counterfeit items, diminishing manufacturing sources and material shortages (DMSMS), obsolescence, supply chain disruptions, cyber

vulnerabilities, foreign sourced components, foreign investments, financial distress, and sourcing of critical technologies from entities within or associated with potentially adversarial nations. These risks are currently managed by myriad organizations across the Department, with little cross-functional coordination and sharing of common supply chain information or initiatives. Cross-functional coordination efforts are also inhibited by the simple lack of common supply chain risk terminology and definitions. A holistic approach is needed to ensure integrated deterrence for the defense supply chain.

3.0 Approach

Within the Office of the Secretary of Defense (OSD), the Assistant Secretary of Defense for Industrial Base Policy (ASD(IBP)) and the Assistant Secretary of Defense for Sustainment (ASD(S)) have mutually reinforcing roles providing guidance and oversight for the Defense Industrial Base and its supply chains.[1] Within ASD(IBP), the Deputy Assistant Secretary of Defense for Industrial Base Resiliency ((DASD(IBR)), in response to executive orders and congressional direction, focused on developing mitigation strategies for five critical sectors—kinetic capabilities, energy storage, castings/forgings, microelectronics, and strategic and critical materials. Within ASD(S), the Deputy Assistant Secretary of Defense (DASD(Log)) addressed internal processes and began by better defining the SCRM ecosystem to increase both the efficiency and agility of systems and material delivery within the Department. The expectation was that a common framework would enable a holistic and coordinated approach for managing disparate risks within the Department's supply chain. The supporting taxonomy would provide a common lexicon of supply chain terms that would enable the collective pursuit of objectives along focused lines of efforts (see Figure 3-1). This Phase I effort and report addresses the taxonomy and framework. The proposed Phase II (see Section 11.0) effort addresses the organizing elements of governance and oversight.

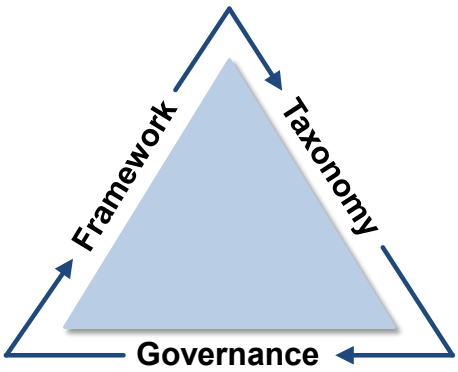


Figure 3-1. *SCRM Project Approach*

To that end, DASD(Log) initiated a series of interviews with senior leaders from across several functional communities of interest to understand their respective SCRM-related roles and

[1] ASD(IBP) has delivered several reports to Congress and the White House and created enterprise-level products. These were used as a starting point in the development of supply chain risk definitions and supply chain tool capabilities.

responsibilities as well as existing policies, authorities, challenges, and opportunities to mitigate supply chain risk. Based on those interviews, DASD(Log) identified eight initial lines of effort (LOEs)—three operational LOEs and five functional LOEs—that could be integrated across the Department (see Table 3-1).[2] The responsibility for the three operational LOEs resides within the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) as it encompasses all acquisition and sustainment operations. Functional LOEs are focused on specific areas with responsibilities outside OUSD(A&S). It is important to note, however, that acquisition authority and support of the five functional SCRM-related LOEs remains an OUSD(A&S) responsibility. Each line of effort is defined in more detail in Section 7.0.

Table 3-1. *Phase I Lines of Effort*

Operational	Functional
LOE 1: Industrial base capabilities	LOE 4: Technology protection
LOE 2: Acquisition security	LOE 5: Cybersecurity **(combined with LOE 6)**
LOE 3: Supply chain sustainment	LOE 6: Information & communication technology
	LOE 7: Intelligence & security
	LOE 8: Installation & critical infrastructure

With each interview or listening session it became clear the Department of Defense lacked a deliberate, holistic, and coordinated approach to managing the disparate risks associated with the supply chains of the defense industrial base (DIB). Also lacking was consensus on the definition of SCRM across and between DoD and the intelligence community. Organizations and individual logisticians[3] understood and supported their supply chains in terms of their experiences and requirements rather than a common enterprise perspective.

As DASD(Log) considered the problem of what SCRM meant across the Department, two primary truths became evident:

- First, organizations routinely conflated terms and lacked a common supply chain language, which led to conflicting roles and responsibilities.
- Second, DoD components narrowly addressed their role in the supply chain and rather than considering supply chain risk within a system of systems as part of an evolving ecosystem.

[2] There were eight LOEs initially identified; however, after further research and discussion with stakeholders, the project team combined LOE 5: Cybersecurity and LOE 6: Information & communication technology as they were too closely related to be stand-alone LOEs.

[3] DoD logisticians are required to complete professional certification based on 12 foundational product support elements, including supply availability, cataloging requirements, supply support or support equipment among other life cycle sustainment, technical management, and infrastructure management processes.

Organizations across the department were doing significant work within the broader supply chain space, but those pockets of excellence were fragmented—and being executed from the ground up. The Department had neither a coordinated top-down approach with clear policy and requirements that could be replicated at echelon, nor a consistent application of supply chain tools, processes, or data analyses and assessments; both of which subverted the development of appropriate mitigation strategies.

Thus, DASD(Log) asked the Defense Acquisition University (DAU) to facilitate small working group sessions with key stakeholders to develop a common framework that clearly defined the compendium of supply chain risk management terms and lines of effort. The DAU-facilitated effort had the following desired end states:

- Develop a whole-of-DoD approach to SCRM, starting with a detailed review of OSD's roles and responsibilities, with appropriately scoped lines of effort that enable collaboration, real-time information sharing, and mitigation across the whole of government (WOG).
- Refine the proposed framework and definitions to structure the DoD supply ecosystem.
- Create a policy roadmap for identifying gaps, required changes, or updates to policy.
- Create a process roadmap that emphasizes interagency supply chain threats and related information sharing.
- Develop a training and curriculum roadmap for both civilian and military education.
- Propose an ideal SCRM organizational framework, with clear roles and responsibilities.
- Propose a SCRM governance and oversight framework.
- Identify best practices and current efforts, studies, pilot programs, and supply chain tools that enable enterprise-level supply chain collaboration.

After engaging with the military services, defense agencies, OSD, and other government agencies, the DASD(Log)/DAU team developed a preliminary framework to represent how supply chain LOEs are currently viewed and managed within the DoD.

3.1 SCRM Policy, Definitions, and Standards

The DASD(Log)/DAU team began its research of key supply chain terms by reviewing several DoD directives, instructions, and manuals (see Section 8.0 for a complete listing); Joint Staff policy; guidance from the Office of Management and Budget (OMB); U.S. Code; Code of Federal Regulations; and executive orders to identify definitions and disconnects. The team also assessed products completed to respond to Executive Order (EO) 14017 and leveraged the policy map and taxonomy deliverables from those documents.

The team conducted additional research to determine the supply chain standards of the National Institute of Standards & Technology (NIST), American National Standards Institute (ANSI), and International Organization for Standardization (ISO).

Two DoD Instructions highlight SCRM roles and responsibilities:

- Per **DoDI 4140.01**, *DoD Supply Chain Materiel Management Policy*, the Assistant Secretary of Defense for Sustainment (ASD[S]) develops and implements SCRM policies in coordination with the Under Secretary of Defense for Research and Engineering (USD[R&E]).
- Per **DoDI 5200.44**, *Protection of Trusted Systems Networks*, the DoD Chief Information Officer (CIO)—in coordination with the Director, Defense Intelligence Agency (DIA), heads of the DoD components, and the Under Secretary of Defense for Acquisition and Sustainment (USD[A&S])—integrates TSN concepts into security controls, policies, and processes and develops programming recommendations to ensure the integration of TSN concepts and processes into the acquisition and maintenance of DoD information systems, enclaves, and services. This includes developing strategies for managing risk in the supply chain for integrated circuit-related products and services.

3.2 Service Colleges

As part of the discovery process, DASD(Log) interviewed service-affiliated academic institutions and reviewed their curricula to identify SCRM-related content:

- **Army War College (AWC).** The Army War College does not have a formal SCRM curriculum. It does, however, provide instruction on vulnerabilities within the military's supply chain and how those vulnerabilities may affect readiness. For example, curriculum considers which global issues could negatively affect DoD's acquisition of materials and how adversaries might exploit those vulnerabilities as a "chess move" to thwart DoD's efforts; how and where materials are sourced and manufactured into finished products; how the construction of the supply chain introduces risk (i.e., the complexity and mixture of entities); and the lack of visibility and oversight of the multiple tiers responsible for providing support.
- **Air War College.** The Air War College is exploring ways to increase their coverage of supply chain risk in its curriculum, recognizing the fragile yet essential strategic aspects of supply chain issues to national defense. At the time of interview, the Air War College was in the process of a major curriculum overhaul and exploring ways to bolster coverage of supply chain and related acquisition topics. The current National Security Decision Making curriculum includes lessons on defense suppliers and the factors influencing defense procurement as part of the broader "Ends, Ways, and Means" lesson. World War I supply chain shortages are also included in one of its Foundations of Strategy lessons. The Air War College also broadly examines sustainability and transportation feasibility related to the South China Sea in its Global Campaigning course. Plans are in place to increase coverage of supply chain risk through the guest speakers, as well.

- **Navy War College (NWC).** The Navy War College does not specifically cover supply chain management (SCM) in its curriculum, but it does cover the operations of the Defense Transportation System (DTS). The DTS curriculum includes information on the commercial maritime industry and its role relative to supply chain resilience and risk. For example, identifying and countering threats to the movement of equipment and supplies from factory or fort to final destination via port, ocean, and global intermodal transport links; the potential risks posed by foreign direct investment in domestic ports (Committee on Foreign Investment in the United States, or CFIUS); adversarial investment in overseas ports and overland transport systems; understanding of SCRM-related cybersecurity challenges; and reliance on foreign flag shipping and the need to strengthen U.S.-flag commercial shipping and sealift capacity. Preparing U.S. merchant mariners and commercial sealift ships for operations in a contested environment is another a critical focus area.
- **National Defense University (NDU)**. The Global Supply Chain & Logistics concentration within the NDU provides military officers and civilians with a strategic-level understanding of global supply chain and logistics concepts and prepares them for the most challenging senior positions within the DoD, government agencies, and the private sector. However, NDU does not offer courses specifically addressing SCRM.
- **National Intelligence University (NIU).** The National Intelligence University currently does not teach supply chain risk, but a pilot course seeks to explore the effect U.S. investments in foreign interests on achieving national policy objectives. Part of the NIU curriculum includes SCRM as it relates to economic competition.

3.3 Industry and Academia

The DASD(Log)/DAU team met with representatives from the National Defense Industry Association (NDIA), the National Technology and Industrial Base (NTIB), and established SCRM-related consortiums to discuss known gaps in the national SCRM strategy as well as discuss opportunities to collaborate and identify potential participants from academia and industry for targeted working group sessions.

A key project goal was to include companies that did not directly support the DoD—thus ensuring a broader review of SCRM best practices outside of the DIB. The team met with the Supply Chain Risk Leadership Council (SCRLC) and the Supply Chain Risk Management Consortium (SCRMC) to consider the joint development of SCRM best practices and standards for enterprise-wide synchronization and risk mitigation. SCRLC comprises several leading supply chain universities and Fortune 500 companies; SCRMC consists of more than 30 global companies.

The team also coordinated with several leading SCRM practitioners from academia to identify how they teach SCRM. The sessions were integral to understanding SCRM commercial best practices and common terminology and definitions. Table 3-2 summarizes industry and academia participants and why they were included in this project.

Table 3-2. *Industry and Academia Participants*

Organization	Objective criteria
Supply Chain Operations Preparedness Education (also SCRM Consortium)	Courses focus on supply chain management, transportation management, and risk management.
SCRMC, Villanova, Lehigh Universities	More than 30 companies with different skill sets, solutions, and methods in an effort to identify, assess, mitigate, and manage supply chain risks.
Michigan State University (MSU)	Ranked #1 by the *US News and World Report f*or supply chain management; MSU offers several supply chain risk management-related courses and certifications.
Penn State University, Center for Supply Chain Research	Ranked #4 by the *US News and World Report* for supply chain management; Penn State offers several SCRM-related courses and certifications.
Massachusetts Institute of Technology (MIT)	Ranked #5 by the *US News and World Report* for supply chain management; MIT offers several SCRM-related courses and certifications.
University of Michigan (UofM)	Ranked #7 by the *US News and World Report* for supply chain management. U ofM developed several SCRM-related courses and certifications.
Cisco	An American Multinational digital communication corporation that delivers innovative software-defined networking, cloud and security solutions.
General Dynamics	Among the top 10 largest defense contractors in the United States; manufacturing numerous weapon systems in support of national defense. General Dynamics supply chain is global in nature, sourcing numerous raw materials and other products from vendors throughout the world.
General Motors (GM)	An American multinational automotive manufacturing corporation. GM is the largest automobile manufacturer based in the United States and one of the largest worldwide. It sources raw materials and other items, to include microelectronics and semi-conductors, globally.
Huntington Ingalls Industries (HII)	The largest military shipbuilding company in the U.S. HII sources numerous raw materials and other products from vendors throughout the world.
Johnson and Johnson (J&J)	An American multinational corporation that develops medical devices, pharmaceuticals, and consumer packaged goods. J&J has more than 78,000 suppliers around the world and sources a variety of materials, including chemicals, plastics, machinery, and packaging.
McNally Industries	A small-to-medium-sized company that provides a broad range of manufacturing, assembly, and value-added engineering services for ships, ground vehicles, aircraft, and soldier systems. McNally machines a wide range of ferrous and non-ferrous materials and routinely works with high performance and exotic alloys to build complex, precision parts, castings, and forgings.
The Boeing Company	An American multinational corporation that designs, manufactures, and sells airplanes, rotorcraft, rockets, satellites, telecommunications equipment, and missiles worldwide. Boeing serves both the military and commercial sectors and sources numerous material types, to include microelectronics and semi-conductors, globally.

In May 2022, the DASD(Log)/DAU team, in conjunction with NDU, and the Defense Logistics Agency (DLA), held three working group sessions with industry and academia to review the proposed DoD SCRM taxonomy and discuss other strategic supply chain topics. During the sessions, participating industry partners and academic institutions provided critical insight related to current supply chain areas of focus and education. The team distributed surveys to gather additional information on the proposed taxonomy and supply chain areas of concern. The survey and summary results can be found in Appendix B. The consolidated discussion points of the industry and

academia sessions can be found in Appendix A, with the taxonomy survey results in Appendix D. As an outcome of the survey exercise, four risk sub-categories were added to the proposed DoD supply chain risk management taxonomy:

- Adjacency risk
- Reclamation and utilization risk
- Unreported supplier-recall risk
- Government policy risk.

3.4 Methodology

The broad scope of the taxonomy and framework development endeavor was divided into two phases. Figure 3-2 depicts the approach for Phase I, which focuses on small working group sessions with key stakeholders to further refine the draft framework.

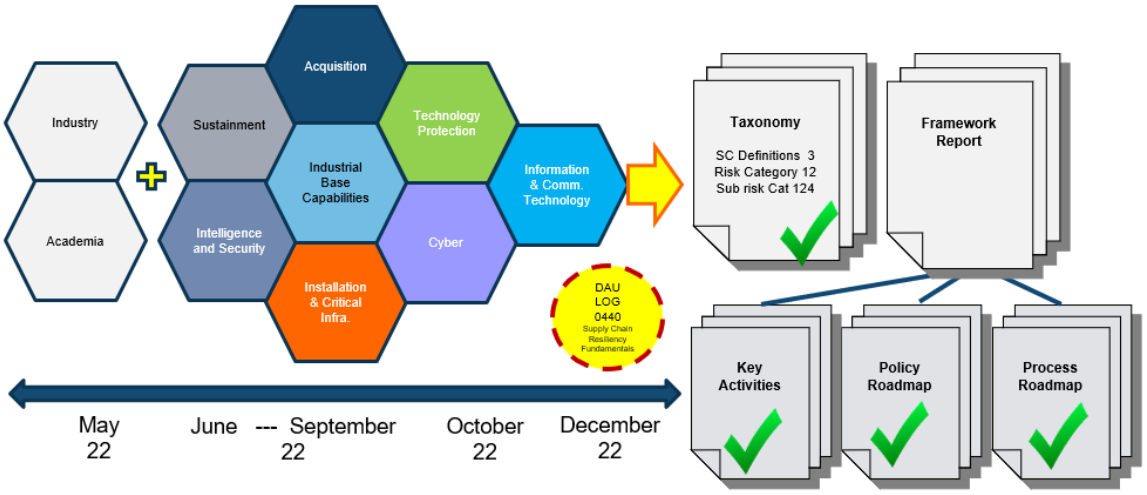


Figure 3-2. *Common DoD SCRM Framework and Taxonomy Initiative (Phase I)*

The team subsequently published the list of eight lines of effort (represented by the colored hexagons in Figure 3-2) to be completed under Phase I and conducted follow-on working group sessions from June through October 2022 with key stakeholders within each functional LOE. The working group sessions, which included participants from both the executive and action officer levels, helped identify the appropriate stakeholders and SCRM-related activities, authorities, policies, processes, opportunities, and gaps within each LOE. The key takeaways of each session were consolidated into session notes, which can be found in Appendix A.

The team then consolidated all the information received during the working group sessions to refine the framework; document process, strategy, and policy gaps; and provide recommendations for execution during Phase II. The team completed and published version 1.0 of a common SCRM taxonomy (see Appendix D) and is currently developing several other deliverables, including a policy, process, and training roadmap.

4.0 Stakeholders

Table 4-1 lists the organizations from across the government, academia, and industry that contributed valuable insights and expertise to this study. The project team is very appreciative of their contributions to surveys, working group sessions, and adjudication meetings.

Table 4-1. *Framework Contributors*

Military Services	U.S. Army	U.S. Navy	U.S. Marine Corps
	U.S. Air Force	U.S. Space Force	
OUSD(A&S)	Acquisition	Industrial Base Policy	Logistics
	VTM	DLA	DPC/DCMA
OUSD(R&E)	SBIR/STTR	MTA	SysSec
OUSD CIO	CMMC/CIO	Cybersecurity	
OUSD I&S	CTPIC	DCSA	DIA
	Special Programs	NRO	NGA
	NSA		
DoD	Joint Staff	CDAO	
Combatant Commands	CENTCOM	TRANSCOM	AFRICOM
	EUCOM	SOCOM	CYBERCOM
	STRATCOM	SPACECOM	INDOPACOM
	SOUTHCOM	NORTHCOM	
Federal Departments	Homeland Security	State	Energy
	Commerce	Treasury	DFC
	Health & Human Services		
Other DoD & Government	ODNI	DISA	GSA
	DARPA	MDA	NRC
	OMB	NIST	CIA
	NASA		
FVEY (Five Eyes)	Canada	Australia	New Zealand
	United Kingdom		
Academia	DAU	NDU	NIU
	AWC	NWC	Air War College
	MSU	PSU	MIT
	Villanova	U of M	Lehigh University
Industry	Johnson & Johnson	Huntington Ingalls Industries	McNally
	GM	GDLS	
	Boeing	Cisco	

5.0 Supply Chain Risk Management (SCRM) Taxonomy

To develop the SCRM taxonomy the DASD(Log)/DAU team organized and categorized supply chain risks into a common lexicon to enable communication and streamline risk mitigation activities across the DoD enterprise. DoD components can use the taxonomy to assess and categorize risks and incorporate the taxonomy into information technology systems, databases, programs, policies, and processes to share information about supply chain risks and mitigation strategies across the DoD enterprise.

The SCRM taxonomy team leveraged the work previously completed by the EO 14017 Working Group led by ASD(IBP), then broke the additional effort into three stages.

- **Stage 1.** The team requested all existing SCRM taxonomies currently being used across the Department. A total of 12 taxonomies were provided (by the participants listed in Table 5-1) for decomposition and analysis, with the goal to create a single standard taxonomy. Although challenged by the different lenses through which risks were viewed, the team derived a base taxonomy of 12 risk categories with 116 sub-risk categories.

Table 5-1. *SCRM Taxonomy Participants (Stage 1)*

Military services, assistant secretaries & key agencies
United States Army
United States Navy
United States Air Force
United States Marine Corps
OSD, Assistant Secretary of Defense for Industrial Base Policy
OSD, Assistant Secretary of Defense for Sustainment
Defense Intelligence Agency
United States Transportation Command

- **Stage 2.** The team then socialized the derived taxonomy with industry, academia, as well as a few US-allied countries (Five Eyes). An additional 4 sub-risk categories were adopted as a result of those discussions, thus increasing the DoD SCRM taxonomy to 12 risk categories and 120 sub-risk categories.
- **Stage 3**. During adjudication, 8 additional sub-risk categories were considered (by the participants listed in Table 5-2). Some sub-risk categories were duplicated, merged, or deferred, bringing the total taxonomy to 12 risk categories and 124 sub-risk categories.

  The adjudicated taxonomy was compared existing OMB and NIST taxonomies as well as to lists of risk categories developed through other DoD studies and pilot programs.

Table 5-2. *SCRM Taxonomy Participants (Stage 3)*

OUSD(A&S)	OUSD(R&E)	OUSD(CIO)	OUSD(I&S)
Acquisition	SBIR/STTR	CMMC/CIO	CTPIC
Industrial Base Policy	MTA	Cyber Security	DCSA
VTM	SysSec		DIA
Logistics			NGA
DLA			
DPC/DCMA			

Note: CMMC = Cybersecurity Maturity Model Certification; CTPIC = Critical Technology Protection & Integration Cell; DCMA = Defense Contract Management Agency; DPC = Defense Pricing & Contracting; DCSA = Defense Counterintelligence and Security Agency; MTA = Maintaining Technology Advantage; NGA = National Geospatial Intelligence Agency; SBIR = Small Business Innovation Research; SysSec= Systems Security; STTR = SBIR & Technology Transfer Research; VTM = Vendor Threat Mitigation

The final taxonomy is provided as Appendix D.

6.0 Definitions

While DoD currently has definitions codified in policy (DoDI 4140.01) for *supply chain* and *supply chain management* (listed below), the team worked closely with all framework contributors to identify common definitions for the terms *supply chain resiliency* (SCR), *supply chain risk management* (SCRM), and *supply chain security* (SCS), and more importantly how those terms relate to one another, the key functions and organizations that contribute to supply chain resilience.

supply chain: The linked activities associated with providing materiel to end users for consumption. Those activities include supply activities (such as organic and commercial ICPs and retail supply activities), maintenance activities (such as organic and commercial depot level maintenance facilities and intermediate repair activities), and distribution activities (such as distribution depots and other storage locations, container consolidation points, ports of embarkation and debarkation, and ground, air, and ocean transporters).

supply chain management (SCM): Meeting 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.

Figure 6-1 lists the proposed definitions and hierarchy for these terms as well as the key functions and critical stakeholders that enable resiliency.[4]

[4] IBP proposes that Supply Chain Resilience be defined as "Resistance to disruptions and ability to recover quickly greatly limiting the effect of the disruption on the delivery of a good or service" As this report coincides with ASD(S) memo "Supply Chain Risk Management Draft Taxonomy Version 1.0 – Advance Copy" dated November 28, 2022 (see Appendix D), IBP's proposed definition will be incorporated as part of a formal configuration management process for the new Policy Instruction, Taxonomy, and definition updates.

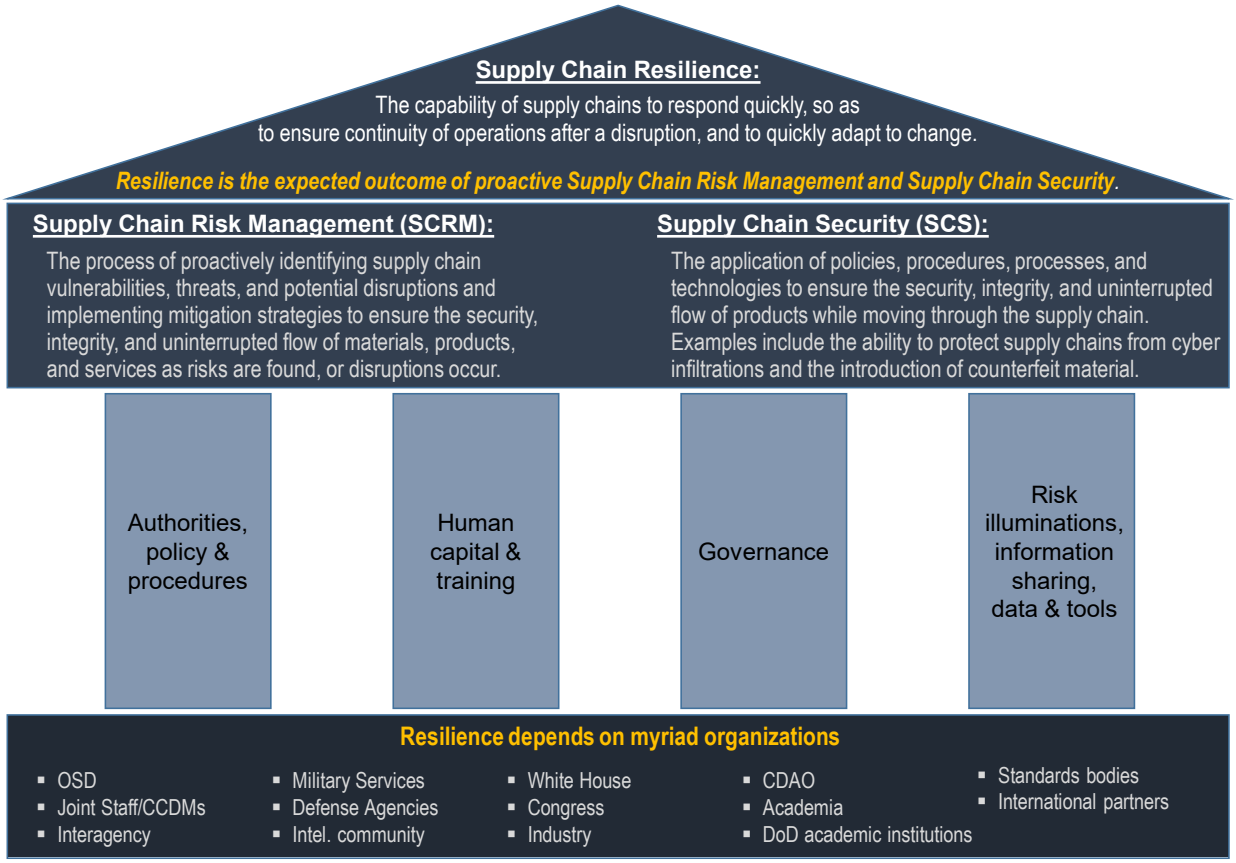


Figure 6-1. *Definitions and Requirements for Resiliency*

7.0 Findings from across the Ecosystem

All academia, industry, and government institutions recognize the global supply chain as a potential critical vulnerability. Despite this broad recognition, mitigation efforts are largely reactive and scoped to the immediate needs of individual organizations; therefore, a broader, integrated, and coordinated perspective of the supply chain ecosystem is still needed.

Academia has only recently extended its traditional logistics frameworks and curriculum to focus on supply chain management assets and tools. Industry, holistically, complies with contractual obligations, but individual companies struggle with SCRM as a cost center, which negatively impacts division-level profit and loss performance. Subsequent corporate-level efforts are often "too little, too late" and, given associated costs, are not fully adopted by the operating units they are intended to support.

Government policy can be erratic—and frequently reactive as supply chain disruptions occur. Without a department-wide framework or coordination across all lines of effort that comprise the supply chain ecosystem, government resources would be applied haphazardly. Therefore, the U.S. government has an opportunity and obligation to analyze, define, identify, structure, assign, integrate, coordinate, and execute activities (and resources) as part of a strategic framework and action plan. An immediate outcome will be increased efficiency and effectiveness of applied

resources, while proactive standard business processes will continue to protect and deliver timely and uncompromised products and services across the enterprise.

Partnering with academia and industry and using a common framework and action plan, will further the effectiveness of supply chain risk management. This will achieve supply chain resilience—a national priority—while using a common standard for ease of practice and implementation.

8.0 Lines of Effort

As mentioned previously, the draft framework consists of eight lines of effort. The first three are operational, with responsibility residing with OUSD(A&S). The remaining five focus on specific areas with responsibilities outside OUSD(A&S); however, acquisition authority and support of the five functional SCRM-related LOEs remains an OUSD(A&S) responsibility. LOE 5 and LOE 6 were combined to account for the overlap of focus and responsibility.

8.1 Line of Effort 1: Industrial Base Capabilities

The Assistant Secretary of Defense for Industrial Base Policy (ASD(IBP)) focuses on industrial base sectors and makes key investments that can enhance supply chains from a resilience and risk management perspective. Specific supply chains or program material are not the focus of Industrial Base Policy efforts, but they often benefit from IBP's work. Table 8-1 outlines the Industrial Base Policy activities within this LOE.

Table 8-1. *LOE 1: Industrial Base Capabilities Activities*

Key activities	
1	Conduct industrial base analyses to identify capacity and / or capability restrains in critical sectors. Leverage data and analysis to develop mitigation strategies and track progress.
2	Develop assessments of future industrial base capabilities; make investments to close gaps in defense capacity and capabilities; and create and sustain reliable sources of supply.
3	Organize engagements with industrial base.
4	Conduct international engagement efforts, including government-to-government dialogues with allies and partners on joint industrial base concerns and areas of potential collaboration.
5	Coordinate within the Department to identify priority areas and develop mitigation strategies; leverage appropriate authorities.
6	Collaborate with interagency partners to identify, mitigate, and monitor risks and issues across the industrial base.
7	Develop programs to increase participation of small, and medium, companies in the industrial base; maximize opportunities to ensure that the nation's small businesses remain responsive, resilient, secure, and diversified
8	Inform the Committee on Foreign Investment in the United States (CFIUS) on national security concerns.
9	Develop DoD policy and provide guidance, oversight, and technical assistance on assessing, or investing, in defense industrial capabilities to senior leadership.
10	Coordinate with components on any proposal to use U.S. government funds to preserve industrial capability.
11	Establish workforce development programs to meet the skilled workforce needs of the DIB.

8.2 Line of Effort 2: Acquisition Security

The Assistant Secretary of Defense for Acquisition (ASD(A)) has a large role in shaping the associated policies, regulations, acquisition workforce guidance, training, and how contracts are written to require supply chain illumination, transparency, and risk management from the final product to the raw materials. As the DoD lead for the Federal Acquisition Regulation (FAR) system, ASD(A)'s Defense Pricing and Contracting (DPC) is responsible for developing contracting policy and regulations. ASD(A) plays a pivotal role in shaping supply chain risk management and resilience. Table 8-2 outlines the key ASD(A) activities within this LOE.

Table 8-2. *LOE 2: Acquisition Security Activities*

Key activities	
1	Establish procurement policies, procedures, authorities, and guidance to mitigate supply chain risks; advocate for and enable DoD authority to waive requirements for accepting risk, when applicable.
2	Implement emerging SCRM policy into DFARS clauses and contracting guidance to support supply chain security, including information sharing and risk reduction strategies.
3	Ensure compliance of supply chain dependability and financial reliability, including Buy American Act, financial responsibility, criminality, FOCI, and subcontracts. Partner with industry to reduce supply chain risk across all sub-tiers in supply chain.
4	Support supply quality and reliability, counterfeit/nonconformance, obsolescence, inspection, warranty, and safety related DFARS provisions/clauses.
5	Create policy to support the forthcoming DHS, DoD, and the ODNI acquisition exclusion authorities, upon the recommendation of the FASC. These orders are issued to protect national security by excluding certain covered products, services, or sources from the federal supply chain.
6	Establish policy and assign responsibilities to support the identification of beneficial ownership, and assessment and FOCI mitigation of covered contractors and subcontractors to enhance supply chain resilience.
7	Improve supply chain security and protection efforts across all phases of acquisition, development, production, and sustainment; develop appropriate transition guidance and resourcing strategies for supply chain management of programs in sustainment
8	Establish policies and procedures that address vendor supply chain threats and enable mitigation of risks associated with commercial support to DoD operations outside of the United States. Implement acquisition authorities that enable termination and restriction of vendors that pose a significant threat to U.S. missions and forces.
9	Provide technology and cyber support to electronics and digital technologies supply chains, operational technology supply chains compliance with NIST SP 800-82 standards**,** cyber and cloud standards, incident reporting, 3252 exclusionary authorities, software maintenance, and patents/technical data. Ensure cyber compliance of the NIST SP-800-171 standards for information protection and cyber standards across the DIB, including support to the CMMC program.
10	Identify cyber vulnerabilities in our software supply chain through DIB reporting of source code exposure to foreign governments. Create a policy and procedures to test, assess, and mitigate the vulnerabilities created by that exposure. Establish and enhance cyber policies and procedures around weapon/control systems

Note: DFARS = Defense FAR Supplement; DHS = Department of Homeland Security; ODNI = Office of Director of National Intelligence; FASC = Federal Acquisition Security Council; FOCI = foreign ownership, control, or influence.

8.3 Line of Effort 3: Supply Chain Sustainment

On behalf of the Assistant Secretary of Defense for Sustainment (ASD(S)), the Deputy Assistant Secretary of Defense for Logistics (DASD(Log)) leads the DoD's efforts for both supply chain risk management and resilience. As the DoD supply chain manager and policy proponent, the DASD(Log) must synchronize the information, intelligence, and vulnerability analysis from key stake holders risk decisions and oversee risk mitigation strategies across the department. The DASD(Log) must also monitor overall supply chain performance since supply chain performance is impacted by risk management and resilience. Table 8-3 outlines the key sustainment-related activities within this LOE.

Table 8-3. *LOE 3: Supply Chain Sustainment Activities*

Key activities	
1	Develop and implement SCRM policies in coordination with the Under Secretary of Defense for Research and Engineering.
2	Assist with the supply chain illumination and resolution of high visibility SCRM for enterprise-level supply chain issues.
3	Develop and implement diminishing manufacturing sources and material shortages (DMSMS) and counterfeit prevention policies within the DoD to enhance supply chain resilience.
4	Develop and implement DoD materiel management and disposition policies; monitor the overall effectiveness and efficiency of the DoD materiel management systems and continually develop improvements.
5	Collect and monitor enterprise-wide supply chain performance metrics (e.g., customer wait time, non-mission capable rates, procurement lead-time).
6	Review life cycle sustainment plans for major weapon system acquisitions (e.g., F-35); develop requirements for addressing SCRM within lifecycle sustainment plans.
7	Regular engagement with, and ownership of, SCRM-related audits and congressional inquiries.
8	Monitor, assess, and mitigate vendor supply chain threats in support of combatant commands as part of vendor threat mitigation requirements.
9	Monitor and assess risk and the performance of organic industrial base and transportation industrial base to enhance supply chain resilience.

8.4 Line of Effort 4: Technology Protection

The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E))'s Science and Technology & Program Protection Office and Small Business Innovation Research/ Small Business Technology Transfer Office lead critical technology protection efforts. The early efforts of these teams in identifying companies and shortfalls in key technology areas set the stage for follow-on SCRM and resilience work. Several stakeholders within OUSD(R&E) perform a variety of technology protection functions, including the Maintain Technology Advantage, Systems Security, ManTech program, and the Joint Acquisition Protection & Integration Cell (JAPEC). Other DoD stakeholders that R&E participates with on technology protection include the Department of Defense Cyber Crime Center (DC3), the Joint Federated Assurance Center (JFAC), Defense Microelectronics Activity (DMEA), and CTPIC and Blue Advantage. Table 8-4 outlines the key USD(R&E) activities within this LOE in priority order.

Table 8-4. *LOE 4: Technology Protection Activities*

Key activities	
1	Serve as a collaboration hub and the DoD focal point for coordination, operational information–sharing, partnering proposals, and assessments of supply chain risk related to technology protection.
2	Assess technology protection efforts, identify best practices, develop innovative methodologies, and propose concepts and tools for operational fielding; make recommendations for supply chain security policy changes that can be leveraged across the DoD security and intelligence enterprises, federal government, private sector, and academia.
3	Conduct continuous discovery of supply chains for indicators of risks to/from individual suppliers; provide timely and accurate assessments across the technology protection portfolio (Department and DIB partners, NSIB)
4	Synchronize efforts across the DoD to create and support standard reporting thresholds of information that are needed in the application of security and protection activities of the supply chain.
5	Assess threats to the supply chain and how to make classified/CUI /threat assessments available to the enterprise; optimize the use of data to improve mission and business effectiveness.
6	Address manufacturing needs of critical technology and acquisition system; develop and enhance technologies and manufacturing capabilities that are independent of sole source suppliers, prohibited suppliers, and potential adversarial nations to enhance supply chain resilience.
7	Build DoD, DIB, and Organic Industrial Base (OIB) advanced manufacturing workforce capabilities and capacity through systems analysis, design, and key investments in foundational and enabling capabilities.
8	Work with DCSA and other relevant stakeholders to ensure secure transfer of technologies within the supply chain throughout the acquisition process.
9	Ensure sustainability is considered as part of technology development.
10	Prioritize critical programs and technologies for enhanced protection, develop and guide implementation of enhanced protection practices, and integrate sources and analysis of technical, counterintelligence, security, and law enforcement information to proactively mitigate exploitation and losses.
11	Develop and implement policy, guidance, education, and methods to ensure defense systems perform free of known vulnerabilities and exploitation.

8.5 Lines of Effort 5 & 6: Cybersecurity & Information Communication Technology

The DoD's Chief Information Officer (CIO) leads critical work in the cybersecurity and information communication technology (Cyber-ICT) sectors, concentrating on the major information technology systems (e.g., Joint Worldwide Intelligence Communication System, or JWICS, and other systems on the classified side). Much of the focus is on ensuring commercial off-the-shelf technology components come from secure production sources. The DASD(Log)/DAU team found the Cyber-ICT sector to be the most mature line of effort, with policies and processes developed and well socialized within both the DoD and across the federal government. The team leveraged many of the lessons learned from the Cyber-ICT community and modeled the overarching cyber-ICT strategy, policies, and processes based on their ongoing work. Table 8-5 outlines the key activities for the CIO within these LOEs.

Table 8-5. *LOEs 5 & 6: Cybersecurity & Information Communication Technology Activities*

Key activities	
1	Protect DoD network supply chains, issue policy for the protection of contractor networks and DoD systems
2	Conduct and maintain Cyber-SCRM assessments and evaluations; responsible for advisories and coordination across the enterprise. Conduct continuous discovery of dynamic supply chains for indicators of risks to/from individual suppliers
3	Implementation of congressional requirements and lead for interagency coordination of cyber and ICT related supply chain equities or related activities
4	Collaborate with enterprise stakeholders (CFIUS, Team Telecom, CMMC, DIB Cybersecurity Program); share information (classified and unclassified) across the enterprise
5	Lead cyber focused supply chain tool pilots, perform threat assessments of vendors, and conduct supply chain illuminations/deep dives. Provide assessment and analysis support to the Department in order to communicate strategic risk
6	Establish and maintain an operational Cyber/ICT SCRM program to enable acquisition risk owners to identify, assess, and manage Cyber/ICT supply chain risks.
7	Establish basic Cyber/ICT supply chain risk due diligence capabilities for decision support and continual monitoring of suppliers for high-interest commodity Cyber/ ICT and critical acquisitions.
8	Co-chair SMWG meetings- Principal to Federal Acquisition Security Council; participate in DSAWG/ISRMC.
9	Inform cyber security architecture SCRM section.
10	In coordination with Services and components, establish Cyber/ICT-SCRM metrics for the enterprise.

8.6 Line of Effort 7: Intelligence & Security

The Office of the Director of National Intelligence (ODNI), and the National Geospatial Intelligence Agency (NGA) lead the work in the intelligence and security line of effort, focusing on intelligence and security systems (mostly on the classified side). Like the Cyber-ICT area, much of the focus is on ensuring the commercial off-the-shelf technology components come from secure production sources. The Intelligence & Security LOE is well established, with policies and processes developed and well socialized within both the DoD and across the federal government. Table 8-6 outlines the key activities for the ODNI and NGA within this LOE.

Table 8-6. *LOE 7: Intelligence and Security Activities*

Key activities	
1	Understand the complex connections and dependencies across intelligence/counterintelligence organizations; improve WOG collaboration; and develop communication/reporting processes.
2	Conduct supply chain threat and vulnerability assessments; recommend countermeasures and mitigating strategies.
3	Update policies, standard forms, and systems of record notification (SORN) to facilitate the collection, usage, storage, and sharing of information and PII in support of acquisition, contracting, and supply chain monitoring.
4	Enhance the nation's supply chain and cyber security; leverage multidisciplinary counterintelligence and security expertise to inform, guide, and coordinate integrated risk decisions and responses with strategic partners.
5	Secure critical U.S. supply chains from foreign influence and attempts to compromise the integrity, trustworthiness, and authenticity of products and services; assess and mitigate the activities of foreign influence enterprise and other adversarial attempts aimed at compromising the global network of pathways and supply chains that provide mission-critical products, materials, and services.
6	In coordination with USD(R&E) and CIO, develop policies, programs, and systems to safeguard critical technologies throughout the supply chain.

8.7 Line of Effort 8: Installation & Critical Infrastructure

The Department of Homeland Security (DHS) leads the U.S. government efforts for installation & critical infrastructure, conducting early vulnerability assessments of key installations and critical infrastructure around the nation and identifying and mitigating vulnerabilities tied to supply chains. The Cybersecurity and Infrastructure and Security Agency (CISA) serves as the major subordinate agency of DHS in charge of these efforts. The DoD must work with DHS/CISA to cover the complex interagency connections and dependencies to improve collaboration and continuous discovery of dynamic supply chains for indicators of non-kinetic risks to individual DIB suppliers, installations and critical infrastructure that supports all of them. Table 8-7 outlines the key activities for DHS and CISA within this LOE.

Table 8-7. LOE 8: Installation & Critical Infrastructure Activities

Key activities	
1	Conduct supply chain threat and vulnerability assessments; recommend countermeasures and mitigation strategies
2	Assess physical and digital risks associated with installations and critical infrastructure supply chains
3	Perform mission analysis to identify components that can impact supply chain related missions, essential tasks and functions
4	Continuously monitor real estate encroachment (in proximity to installations and key infrastructures)
5	Implement SCRM strategies for military construction projects during the design phase
6	Provide help to private sector owners and operators (state and local) to secure their supply chains in support of mission readiness
7	Conduct vulnerability assessments and identify alternative means of fulfilling the mission if key supply chains are disrupted; ensure Mission Assurance plans are in place and exercised regularly
8	Share supply chain risks and threats across the enterprise

9.0 Policy

The two key policies for supply chain resilience and risk management are DoDI 4140.01 "DoD Supply Chain Materiel Management Policy" and DoDI 5200.44 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)". Table 9-1 lists the supporting policies identified during Phase I. Table 9-2 lists the primary policy gaps that should be addressed during Phase II.

Table 9-1. *Key DoD SCRM Related Policies by Line of Effort*

LOE 1: Industrial Base Capabilities	LOE 2: Acquisition Security	LOE 3: Supply Chain Sustainment	LOE 4: Technology Protection
DoDD 2010.09	DoDI 5000.74	DoDD 3000.16	DoDI 5000.83
DoDD 4100.01E	DoDI 5000.79	DoDD 4715.21	DoDD 5000.44
DoDD 4275.05	DoDI 5000.82	DoDI 4140.01	DoDD 5000.47
DoDD 5101.18	DoDI 5000.83	DoDI 4140.67	DoDI 5200.39
DoDI 2000.25	DoDI 5000.85	DoDI 4245.15	DoDM 4245.15
DoDI 2010.06	DoDI 5000.86	DoDI 5000.93	DoDD 5137.02
DoDI 2040.03	DoDI 5000.90	DoDI 8320.04	DoDI 5230.24
DoDI 4205.01	DoDI 5000.91	DoDM 4140.01 Vol 1-11	DoDD 5240.24
DoDI 5000.60			DoDI 5200.FH
DoDI 5134.04			
DoD 4400.01-M			
LOEs 5 & 6: Cybersecurity & Information Communication Technology		**LOE 7: Intelligence & Security**	**LOE 8: Installation & Critical Infrastructure**
DoDI 3020.45	NIST SP 800-53 Rev5	DoDD 5205.16	DoDD 3020.40
DoDI 5200.44	NIST SP 800-37	DoDI 2000.25	DoDI 3020.45,
DoDI 8500.01	NIST SP 800-161	DoDI 5000.83	DoDD 3020.45 CE-01
DoDI 8510.01	NIST-IR 8276	DoDI 5240.19	DoDI 5220.22
DISAI 630-230-19	CNSSD 505	(DNI) ICD 731	DoDI 8500.01
DISAI 240-110-42	NDAA 2019, Sec 889	(DNI) ICD 731-01-05	DoDI 8510.01
DISAI 240-110-44		NIST SP 800-161	

Table 9-2. *Key Policy Gaps*

Line of Effort	Identified gaps
LOE 1: Industrial Base Capabilities	• Promulgate policies to incorporate SCRM into acquisition decisions • Management of Acquisition and industrial resources • Oversight of service managed industrial base investments • Leverage interagency to look at national policies through a national security lens • Write a governance process and mechanism for risk management • Develop a security classification guide to address data aggregation concerns across functional lines of effort and organizations, and disclosure guide • Develop guidance on communicating downstream risks to prime contractors that do not have privity with n-tiered vendors
LOE 2: Acquisition Security	• Common contract data requirements list (CDRL) approach. Develop comprehensive SCRM policy and procedures
LOE 3: Supply Chain Sustainment	• Develop comprehensive SCRM policy and procedures • Expand Vendor Threat Mitigation oversight to include all vendor threats, rather than just Operational Contract Support contingency threats.
LOE 4: Technology Protection	• Develop a technology map/refresh policy, including supply chains that will be needed to support the scale-up of emerging capabilities
LOEs 5 & 6: Cybersecurity and ICT	• Articulate DoD's internal FASC processes in policy (e.g., how to execute based on FASC recommendation)
LOE 7: Intelligence & Security	• Consider CUI security requirements (e.g., expanding requirements for CI/insider threat training to uncleared personnel) • Establish Section 889 authority versus acquisition authority • Policy for direction to aggregate open-source data/information
LOE 8: Installation & Critical Infrastructure	• Resolve any conflict between ODNI waiver authority and acquisition authority • Establish DoD clearing house/authority for investments near installations and infrastructures • Establish DIB operational technology (OT) systems security CMMC

The largest policy-related gap is the lack of a single policy proponent to synchronize all supply chain management/supply chain risk management efforts across the Department. Akin to this is the lack of standardization in terminology, definitions, risk categories, and sub risk categories. A lot of work is going on in each sector reviewed, but in many cases those efforts are not integrated with the work other stakeholders are doing. An overarching policy and governance structure is needed to enable each stakeholder to continue their individual efforts while integrating and sharing data across the DoD enterprise.

An ancillary, but still important, policy-related gap is the lack of clear contracting guidance to drive required transparency further down the supply chain.

10.0 Findings and Recommendations

This project and report addressed the policy, organizational, and supply chain risk performance challenges across the Department of Defense. The initial assertions—that the Department lacks a deliberate, holistic, and coordinated approach to managing the disparate risks associated with the DIB supply chain and lacks consensus on the definition of SCRM—remains unchanged.

The following are the key findings and recommendations of the project team:

Finding 1. There is a clear validated need for well-articulated and coordinated common supply chain terminology, definitions, and taxonomy that can be used across the Department to develop policies, procedures, and accountabilities that affect supply chain risk management. Interviews across the Department supply chain ecosystem enabled the development of a proposed taxonomy (Appendix D) to bind all stakeholders to a common supply chain lexicon.

Recommendation 1: Integrate the SCRM taxonomy described in Section 5 and provided in Appendix D of this report into policies, procedures, and governance processes within the Department's supply chain ecosystem. This recommendation is to ensure common terminology is used for any subsequent policy actions and to eliminate ambiguous communications.

Finding 2. The Department's supply chain ecosystem identified seven interrelated categories of key process gaps and opportunities for enterprise-wide synchronization and supply chain risk mitigation. The gaps are listed in Table 9-2.

Recommendation 2: Execute a planned integrated gap closure initiative across the seven primary lines of effort to close the gaps listed in Table 9-2. This plan should be developed and resourced by OUSD A&S to conduct primary and secondary stakeholder engagements in modifying or enhancing policy, directives, and instructions that drive accountabilities for gap closure. This initiative should be executed using a gap closure program plan, with metrics for measuring progress and demonstrable changes to working guidance.

Finding 3. Although there are significant supply chain risk management—and ultimately supply chain resiliency—accomplishments resident in the OSD councils, working groups, committees, OUSD organizations, commercial organizations, and combatant commands, supply chain risk information and tools are not adequately shared or managed across the Department's supply chain ecosystem.

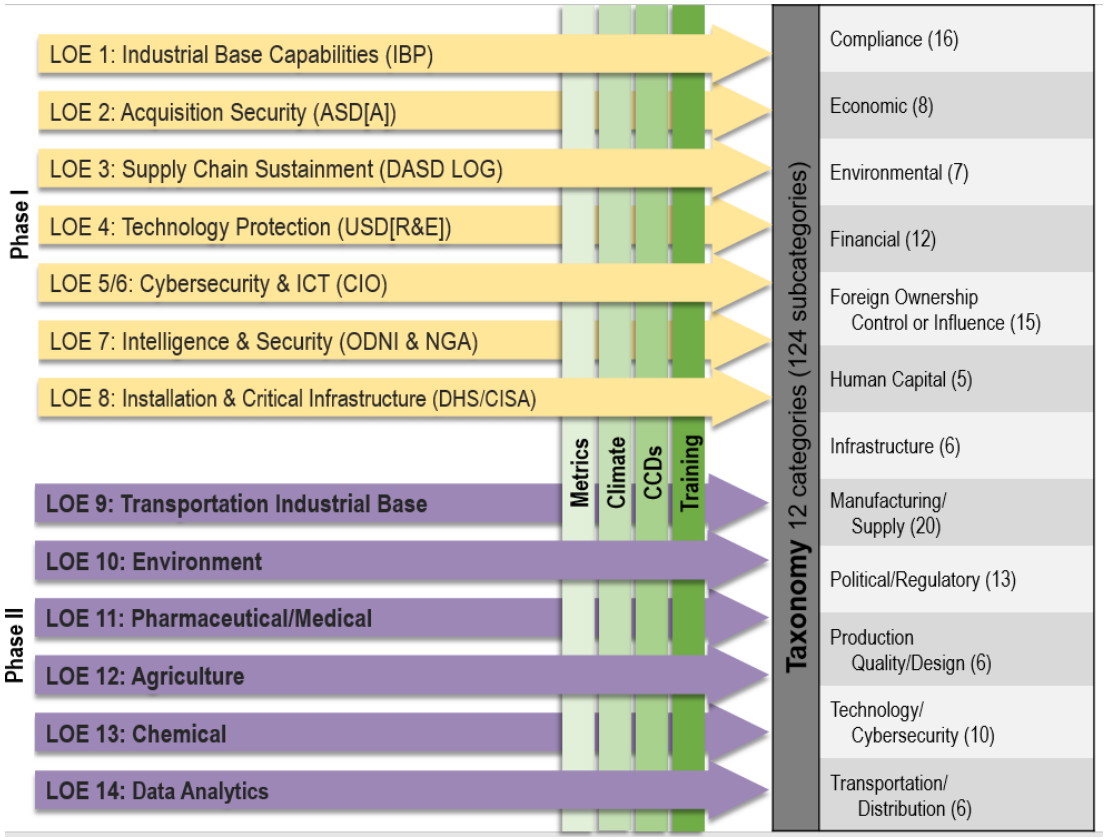
Recommendation 3: Expand on the work completed within the framework by developing and implementing roadmaps to address identified gaps. Also develop additional proposed lines of effort as identified in Table 11-1.

Finding 4. Supply chain risk is addressed by multiple organizations but without an enterprise coordination process to assign supply chain responses, responsibilities, and resources and inhibits the Department's ability to provide coordinated, holistic solutions across the myriad supply chain–related equities. This includes enterprise supply chain coordination for such things as appropriated funding and spend plans, executive orders, NDAA-related policy, congressional requests for information, House and Senate Armed Services Committee (HASC/SASC) taskers, GAO or DoD Inspector General audits and required responses, escalation of supply chain related concerns, supply chain illumination tools, and section 889 waivers.

Recommendation 4: Establish an enterprise-level organizational structure to develop and implement an integrated SCRM framework, standard supply chain risk taxonomy, DoD SCRM policy, data integration strategy, and governance and oversight structure.

11.0 Phase II and Next Steps

While the Department has made significant progress throughout this effort, more work remains to finalize the framework and develop the programs, policies, processes, governance structure, training plans, and data strategies and tools needed to implement an enterprise SCRM and supply chain resiliency program. A follow-on phase (Phase II) is needed to further refine and develop the Department's supply chain ecosystem and expand on additional lines of effort discussed during Phase I (see Figure 11-1). This includes the integration of metrics, climate, and operational considerations across existing LOEs and additional LOEs, which are listed in Table 11-1.



Note: For each LOE we will assess and identify related metrics, climate related impacts, combatant commands linkage, and training and education opportunities.

Figure 11-1. *SCRM Framework Phase I & Phase II*

Table 11-1. *Future Phase II LOEs*

Operational	Functional
LOE 9: Transportation Industrial Base	LOE 11: Pharmaceutical/Medical
LOE 10: Environment	LOE 12: Agriculture
LOE 14: Data Analytics	LOE 13: Chemical

Recommend Phase II actions be resourced and led by the Deputy Assistant Secretary of Defense for Logistics on behalf of the Assistant Secretary of Defense for Sustainment as the principal staff assistant for SCRM policy. Phase II deliverables will aid the Department's efforts to build resilient supply chains capable of addressing the national security challenges of the 21st century.

The goal for this next phase is a continuation of the goals for Phase I: *Develop a persistent, holistic, and comprehensive approach to risks across the DoD's supply chain ecosystem to further strengthen the DoD's integrated deterrence posture and support warfighter operations.*

The following are specific deliverables for Phase II:

1. Publish fully coordinated DoD Supply Chain Risk Taxonomy and SCRM Framework.

2. Establish enterprise SCRM roles and responsibilities and transition points; provide mechanisms for governance, oversight, and decisions on cross-functional and operational supply chain-related decisions.

3. Prioritize, assess, monitor, and mitigate risk; identify vulnerabilities and derive strategies. Develop Department priorities beyond the five key sectors listed in EO 14017 (chemical, agriculture, transportation, Rare Earth Elements, etc.).

4. Create scalable resourcing model that can be replicated at echelon; identify recurring funding requirements, personnel, structure, and tools.

5. Establish a standard process and methodology to identify and measure the maturity of component-level SCRM programs.

6. Define the additional LOEs not captured in phase I (see Figure 11-1); revisit LOE 8: Installation and Critical Infrastructure.

7. Develop a comprehensive curriculum and training roadmap.

8. Integrate supply chain activity into the Joint Concept for Contested Logistics, JP4.0 and JP3.0.

9. Purposefully integrate SCRM activities and requirements within operation plans (OPLANs).

10. Develop an integrated data strategy with sponsorship of enterprise-level supply chain tools and capabilities (e.g., Santa Maria/SCREEn, Advana, IDA, commercial tools) to procure supply chain data once and share that data consistently across the enterprise.

As phase II kicks off and matures the DASD(Log)/DAU team will work with the community to identify OPRs for the deliverables listed above.

12.0 Conclusion/Summary

The DoD lacks a holistic lacks a coordinated, holistic framework to effectively manage the risks within the broader defense supply chain. This report summarizes the Phase I work completed by a cross-functional team of SCRM stakeholders. Together, the team conducted multiple workshops and interviews and crafted the taxonomy and framework. The team established four recommendations:

1. Integrate the SCRM taxonomy described in Section 5 and provided in Appendix D of this report into policies, procedures, and governance processes within the Department's supply chain ecosystem,

2. Execute a planned integrated gap closure initiative across the seven primary lines of effort to close the gaps listed in Table 9-2,

3. Expand on the work completed within the framework by developing and implementing roadmaps to address identified gaps,

4. Establish an enterprise-level organizational structure to develop and implement an integrated SCRM framework, standard supply chain risk taxonomy, DoD SCRM policy, data integration strategy, and governance and oversight structure.

The outcomes for Phase II will provide the Department with an effective, scalable, process-based approach to address SCR and create integrated deterrence.

Appendix A. Industry and Academia Session Notes

Culture

Culture will be the hardest thing to change within the Department of Defense and with our Industry counterparts. The DoD can no longer do acquisition the way it has always been done – because the DoD must determine where they are vulnerable early during the design phase and plan the design and the supporting supply chain to be resilient despite these vulnerabilities.

- Culture = supply chain risk; a company's cultural and risk appetite.
- Culture tends to be associated with the prime and not the sub-tiers.
- Supply Chain Risk Management (SCRM) is considered overhead and eats at a company's profit. Therefore, there is no incentive to address this concern.
- Every action is charged to a cost accounting code. SCRM will be viewed as added cost.
- How the Department of Defense buys is how the primes will behave.
- How I do my ordering is very different than what parts are designed into the system.
- Changing culture from, "heroes in crisis" to "no heroes" will be hard. Resilience must be built-in to reduce the need for crisis management. The crisis manager heroes will resist this change.
- Supply Chain Risk Management is viewed as a support function.
- Supply Chain Risk Management is viewed as a program protection function.
- Design engineers are driven by their ego to see their product in action. Motivate the design engineer by sharing the supply chain risk profile upfront.

Governance and Oversight

Governance and oversight are key functions that include management, standards, statutes, regulations, and decision makers. As the DoD continues to emphasize supply chain resiliency, vulnerabilities, and risk management, ensuring that good policy is published to provide clear roles, responsibilities and processes will be key to the successful implementation.

- There are three categories of governance: management, accountability and taking an enterprise approach. This includes the people and framework with highly trained workforce who know their supply chains.
- Supply chain risk management must be built into the beginning of the acquisition process. When you are designing the item, review vendor profiles through a score key of how likely they will perform, review on-time deliveries, quality of product, etc.
- Decisions made by a centralized group, engineers, and PMs.
- Use of Standards. AS 9100 clearly defines risk management procedures that are closely integrated. This helps organizations ensure they meet customer and other stakeholder needs within statutory and regulatory requirements related to a product or service. But other companies should be adhering to these standards as well.

- Some government regulations make it harder to operate; a well-intended solution could hurt more than it helps.
- Government agency friction points – whole of government, agencies are not connected; sometimes laws are passed that conflict with each other and end goals. Example – some states are trying to secure the supply chain for their state only, which creates immediate conflicts.
- Engineers focus on creating a product, but the supplier may not be able to purchase this product
- Engineers will find the best item, not necessarily choose a stronger company; need to re-frame to why is this the only item that will fit the job?

Supply Chain Resiliency vs Supply Chain Risk Management

Organizations frequently conflate supply chain resiliency with supply chain risk management, using the terms interchangeably. However, SCR does not equal SCRM. Equating the two definitions demonstrates a lack of awareness about the complexities of supply chains, further, organizational naiveté about the differences between the two terms inhibits strategic decision making. It is difficult to find employees that understand the differences between resiliency and risk; these terms are generally not part of traditional purchasing, or supply chain curriculums. Supply Chain resilience is the capacity to persist, adapt and transform. Vulnerabilities and associated risk are omnipresent in supply chains. These vulnerabilities must be identified with assigned risk and developed plans to overcome supply chain failures. As a result of complex and dynamic supply chains, organizations must constantly review their supply chains, update the vulnerabilities and associated risk, and develop plans to make them resilient.

- Resilience – capacity invested in ahead of time, where the outcome is resident in an organization after making an investment. Supply chain network design can make you more resilient – or more susceptible to risk (i.e., baby formula). SCRM is required for a resilient supply chain; all affected organizations are responsible as supply chain risk managers.
- Resilience is the ability of the organization to respond should that adverse event occur. Localization risk on a certain theater connected but different all risks are local. Simple definition of risk: (exposure), = probability of an adverse occurrence, factored by the possible impact of that event.
- Resiliency is a term used to show pro-active continuity of supply (perception).
- SCR = taking actions before a disruption to ensure continuity of operations after a disruption; it is very difficult to connect SCRM to SCR.
- Biggest issue for practitioners is the conflation of risk with mitigation actions required to ensure resiliency.
- Resiliency includes actions taken after the fact, whereas, risk mitigation is assessing the likelihood and severity of a risk, with identification of possible actions to mitigate, or reduce, your risk.

- Risk Management = funding risk, quality risk, delivery risk, national disasters, geopolitical risk, etc. Managing the supplier at the tier 1 level is reactive within the SC; focus needs to be on fixing the problem. Resilience requires being proactive beyond the tier 1 suppliers, need to protect the continuity of supply in anticipation of problems.
- Risk management lives in several different functions within an organization.
- Address the risk farthest from you - outside of US - and focus on that first vs. closer - and understand what can be reacted to the easiest. Prioritize and learn from each choice.
- Effective risk mitigation is not necessarily about fixing risk each time, it's about awareness.
- Plan to use more than one source so that you don't have concentration risk; have multiple options.

Vulnerability vs Risk

When considering supply chain sources of risk, it may not always be apparent where that risk lies, and thus organizations should analyze and identify vulnerabilities within supply chains for such things as single-sourced components, or shared sourcing of components across multiple OEMs. Once an organization understands where its areas of most value, and risk, reside, it can work to develop mitigation plans.

- When viewed as individual product supply chains, each product has its own story, perhaps with points of aggregation, but the individual nature necessitates examining each product uniquely. Evaluate products to assess the most critical to prioritize; not all products carry the same level/types of risk. Product lines with higher reputational risk have priority - in order to maintain trust. This prioritization helps segment the portfolio.
- Vulnerability must consider normal market variations vs. disruption. Where are you vulnerable? Where do you have single sources? Normal market variation is managed and matured; however, vulnerabilities are key. Which materials are high risk? Where is an organization the most vulnerable? What are the single sources of failure?
- Rather than assessing the risks, a method to assess vulnerabilities, is to assume you've already lost supply chain availability, and then you can start quantifying impacts. Knowing your vulnerabilities in advance can help create resilience; understanding how vulnerable you are before a disaster occurs changes profile of risk. For example, a vulnerability assessment of a large network, like an airport, introduces risk. Significant product volumes travel through specific airports. If something happens to a critical airport, then how products get distributed to customers? In this example, transportation has vulnerabilities that would need to be considered - with identification of alternative solutions. These solutions need to be in alignment throughout the supply chain.

Return on Investment

Practitioners of SCRM understand the inherent value of integrating supply chain management strategies throughout the lifecycle of a product. However, it is difficult to quantify the benefit of SCRM implementation to an organization, or to develop a calculation of return on investment.

The resources, and overhead, required to effectively manage supply chains, and to further, assess, monitor and mitigate risk, are absorbed by program funding. This funding requirement is generally not established as part of a program's baseline. Thus, there are competing views of how to quantify SCRM. One view seeks to quantify the life cycle cost of SCRM and to integrate it into the overall cost of a product across its life cycle. Whereas, a contrasting view, establishes that it is too difficult to calculate ROI, and instead, shifts focus to demonstrating the value of effectively implementing SCRM. There are enough anecdotal examples of SCRM impacts to effectively demonstrate value (i.e., Solar Winds). What is the cost of "not" doing SCRM?

- Where and how you design SCRM from the beginning of the development is important.
- Supply Chain Risk Management community may understand the ROI – but others may not see the value. SCRM identifies risks that have not yet had an impact.
- SCRM return on investment (ROI) is not well defined or understood. How do stakeholders view return? ROI is viewed and defined by the person who is the decision maker. ROI in the organic DIB is much different than ROI for private industry.
- ROI calculations can be thought of in terms of buying insurance to protect yourself against adverse event. For profit you can calculate what it is going to cost if the thing happens, and you are not prepared. ROI calculation= insurance policy (like car insurance you hope to not get into a car accident, but you still need to purchase the insurance for coverage). Calculation of exposure to revenue, profit, and patients. How much is a single person's life worth? Other theoretical ways of calculating ROI: (1) cost to operate – (minus) the costs of lost production; (2) calculate the combined SCRM budget across the entire lifecycle of a system.
- One possibility is to add incentivized SCRM requirements into contracts and incorporate within the costs of the system to do SCRM. However, this is harder to leverage at lower tiers. Buyer should have some flexibility and discipline to motivate suppliers (raw materials).
- Determine ROI for a SCRM program or mitigation by weighing the cost of fixing a problem after it occurs.
- Figure out where the flashpoints are and make tangible for decision makers. Respond to risk and an adverse event; focus on today's risk but be willing to change for tomorrow. Risk exposure is dynamic. Nature of risk changes overnight so you need feedback loops and recovery plans. What happens if I lose a node how do I recover? Critical to this thought is the feedback loop.

Barriers

There is a reluctance to put resources to SCRM. Costs along with gathering information and traceability being some of the biggest barriers. In term of costs, intangible costs cannot be easily quantified and therefore applied to the appropriate costs categories (example overhead costs and/or material costs). Furthermore, applying costs to overhead/material could make industry's bid not as competitive. Therefore, losing the contract/award due to higher proposals.

Additionally, it has been challenging to capture supplier level data beyond level 1 (Prime) to raw materials. Two concerns shared with data capturing: 1) from an industry perspective sub-tier

suppliers do not want to provide this information because it might give the prime the information they need to by pass them in the future and/or create competition; 2) Internally, to the government the largest concern on sharing information to industry from within DLA is competitive advantage (by working to solve a certain risk does that give the contracted entity an advantage over other potential competitions within the DIB aka Competition Advocacy limitation?). Other barriers had to do with organizations (centralized verses decentralized management), and the resources required in terms of funding, positions, and training.

- There is a reluctant to put resources to SCRM. Where do you place these costs in the contract as overhead costs to the contract?
- The biggest challenges are in tier 2 to 3 to 4 suppliers. Systematic problems were identified getting information from tier 7/8 and 9 in the Supply Chain.
- The largest concern with sharing information to industry from within DLA, is the perception of competitive advantage: by working to solve a certain risk does that give the contracted entity an advantage over other potential competitions within the DIB? Aka Competition Advocacy limitation.

Training

Training the workforce is critical to addressing the cultural attitudes and biases. There must be some level of common training to help senior executives, managers and workforce members understand the urgency and impacts to the DoD. Next, focused training approaches must be tailored to different members of the acquisition and supply chain communities to provide a deeper understanding of their roles and provide the necessary skills to influence and manage the risk associated with decisions made at all levels.

- Some companies are using modular training and workforce members get assigned training modules with SCRM methodology and assessments built-in with sample types of risk including process and product risk.
- Teach SCRM by running a product through a value stream; leaders also will need this type of training.
- Conduct tabletop risk assessments with training focused on nodes and links, measure things like latency – how long does it take for you to recover; resilience has a time dimension, 2 days, 5 days, 10 days, etc.
- Train suppliers and work together with competitors; some believe that this area that could be a competitive advantage.
- Embed training into our annual compliance training particularly for procurement teams and other key stakeholders.
- Currently using an internal tool that has logic that maps vulnerabilities and nodes to assess continuity of operations.
- There is a constant dynamic of risk and the workforce changing; must help people understand their roles.
- Conduct training to map the nodes of a network; find data and use it to determine how a part flows through the network. Do I have a diamond shaped supply chain where second

tier suppliers are using the same third tier source? Understand what those nodes are and where they are placed in a map view? Use a visual command center-tool to conduct this type of training.

Metrics & Data

Interview findings show that accurate and full situational awareness metrics, and the underlying data over the entire acquisition lifecycle, need to be integrated with government and industry supply chain strategy, performance incentives, supply chain data collection and continuously monitoring SCRM tools. Executive support and alignment of metrics to the enterprise require: (1) buy in at the executive level; (2) appropriate resources; and (3) clearly defined success.

- SCRM metrics need to be defined to incentivize prime suppliers specific to supply chain outcomes over entire lifecycle just as typical cost schedule and scope program metrics do.
- Successful metrics for SCRM: visibility, standards, quality and be part of digital transformation.
- Metrics must be a corporate mandate aligned at executive level and part of management measures.
- Metrics to consider:
- Define core data needed
- Focus on qualifying suppliers
- Monthly audits
- Quality standards
- On-time deliveries
- Business continuity impact metrics and forecasting likelihood of risk
- Dependency mapping
- Visibility is important Supply chain intelligence – application of tools that can depict supply chain nodes, maps, ever stream analytics, risk methods, geospatial mapping of supply chain.

Resources

Resources will drive the ability to protect the supply chain. Resources are needed to pay for illumination, assessment, and mitigation of risks for critical items. Resources are also required to pay for supply chain risk management tools and the upkeep of data over the lifecycle of a product. Finally, resources are necessary to develop workforce training, required skills and expertise to manage and make decisions relevant to our supply chains.

- SCRM needs to be taught and resources provided to drive the right behavior.
- Develop supply chain expertise and establish portfolio managers.
- Implement training and education related to SCRM.

Other Strategic Takeaways

Industry and Academia are on a journey to figure out how to build resilient supply chains, while determining where they have vulnerabilities and how to best manage different types of associated risk. Each organization is trying different approaches to the same problems. There is no well-defined play book but there are several exemplars who are on the right track.

- Organizations are on a journey to figure out an effective supply chain risk management program, it is not well-defined in practice.
- Companies need playbooks for tsunamis, pandemics, wars, civil unrest, etc.
- People get into technical solutions too quickly! Need to set up the right structure. This is important and provides the foundation for how to manage in a crisis. Focusing on the right structure allows people to solve the problem in a coordinated fashion - given each crisis will be unique.
- Timescales are important. Vigilance is needed to watch what is happening across the world over time; things are shifting very slowly, who is observing? Vigilance equals National security – perception that there is no coordinated vigilance in the country. Vigilance is the price of economic security.
- Just because a company is secure does not mean the country is.
- What gets measured gets done. Consciously make sure that the visibility is there from the command suite down.
- Keep it simple, keep it focused, build a coherent strategy, and be very practical on what you can take on.
- Sometimes an organization must pick up the phone and talk to other companies (competitors) even though there is a concern over competitive advantage, organizations must work together as a team.
- There are multiple tier 1's contracting to the same tier 2 - which creates a diamond shaped supply chain. This creates huge concentrations at the tier 2 level no matter how much companies try to prevent it; they cannot mask it and it is possible to learn something from the near misses.

This Page Intentionally Left Blank

Appendix B. Survey & Summaries

Academia survey:

https://forms.office.com/Pages/ResponsePage.aspx?id=RL4hHDUkv0m8H8ujFxhwWHM8os2IZRJFvHBOVzWpSFdUN1RBTzNIVjlaOERJWEZYUk9ZRVJRNDVRVC4u

Industry survey:

https://forms.office.com/Pages/ResponsePage.aspx?id=RL4hHDUkv0m8H8ujFxhwWHM8os2IZRJFvHBOVzWpSFdURjRCSU1BUDE2STIxOTJMWTczNzEyTUlVMi4u

Survey Results:

Academia

4
Responses

Please select the level of instruction you teach/cover for Supply Chain Risk Management.

Undergraduate	1
Graduate	3
Professional Certification	2
other	1

17

DAU

How do you assess and prioritize risks?

Assess Using:

- An integrated supply chain - Not in isolation
- Market and industry information
- Third party SCRM tools
- Direct supplier intelligence
- Risk/Reward methodology
- Program needs and alignment with established supply chain
- Customer value
- Contract value
- Goals of the organization's supply chain
- Measures/Metrics:
  - Probability of disruption
  - Duration of disruption (Time to recover)
  - Risk Priority Numbering (RPN)
  - Value-at-Risk (VaR)
  - Failure Mode Effects Analysis (FMEA)
  - Quality
  - On-Time Delivery

Prioritize based on:

- Customer deliveries
- Sales
- Earnings
- Contract relationship(s)

18

DAU

What does a successful SCRM organization look like?

Organization:
- Central team (strategy, policy, standards, process, training, workforce development, etc.)
- Decentralized roles and responsibilities for all departments
- Dedicated resources (aligned with goals)
- Requires skilled workforce (analysts, managers, etc.)

Governance:
- Embraced by leadership
- Embedded organizational strategies to minimize loss
- Uses metrics, monitoring and predictive analysis that aligns risk with corporate goals
- Risk information integrated into core decision making; included in all decision-making processes
- Leverages a tailored policy and approach based on phase of lifecycle
- Management accountability for risk management activities within governance framework
- Clear communication of risk information (policies, practices, thresholds) with ability to conduct change analysis

Process/Technology:
- Optimizes supply chain performance while simultaneously minimizing supply chain vulnerabilities
- Use of query and reporting tools, dashboards, balanced scorecard, event management and triggers
- Proactive vice reactive
- Shares and accesses information from multiple sources
- Embeds SCRM processes within SCOR model
- Processes and evaluations imbedded in company aerospace quality management system standard (AS91000)

19 DAU

Challenges:

- Culture!
- Rigidity of requirements and competing requirements
- Limited resources or lack of funding
- SCRM viewed as "overhead costs"; all actions are charged
- PM normally rated on cost & schedule, not necessarily how well it will work particularly in sustainment
- Decisions made by a centralized group; Program managers and engineers
- Risk created by utilization of sole source suppliers
- Insufficient data to manage processes
- Insufficient standards within design and acquisition
- Inadequate tools to scrub contradictory data
- No incentives to mitigate long-term risks since program managers are often graded on cost and schedule
- DoD buying practices; may not be allowed to spend at-risk dollars on long lead items until contract is in place
- Design to DoD performance specifications which often limits choice in suppliers
- Conflicting and inconsistent knowledge within the organization's workforce, senior leaders, suppliers and customers leads to divergent paths to manage the SCRM process.
- Contradictory government global SCRM policies discourage long-term planning for sourcing commodities and critical components
- Competitive environment expands risk acceptance
- Return on Investment – viewed as a good return only by the decision maker
- Carrying cost of supply chain resilience

20 DAU

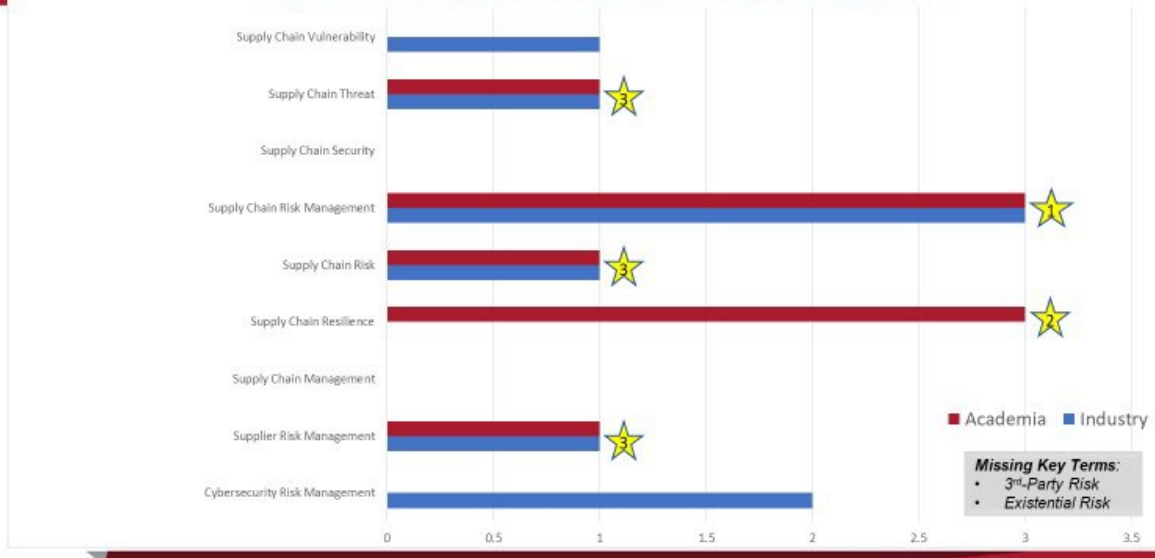
Challenges (Continued):

- Lack of:
  - Executive Sponsors
  - Tools
  - Compelling Business Case
  - Workforce training (which leads to decision making without full consequence of risk)
  - Understanding of interconnectedness of supply chain across the landscape
- Metrics:
  - No metrics or bad metrics
  - Lagging metrics

21

DAU

Top 3 Terms that are most used to manage risk



22

DAU

Supply Chain Risk:

- Any factor that may alter the course of the expected or desired outcome in the end-to-end cycle or mission
- Risk that you can't have what you need when you need it.
- Decisions and activities that have outcomes that could negatively affect information, goods and performance within a supply chain.
- Any factor that affects balance between supply and demand through its impact on: Quantity Price Quality Reputation Responsiveness.
- Identifying the root cause of whatever the current risks are.
- The potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products or services. Supply chain risks include INTENTIONAL, ACCIDENTAL OR ACTS OF GOD exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain. (NIST SP 800-53 Rev. 5.)I would modify NIST's definition based on my comments in caps.

23 DAU

Supply Chain Risk Management:

- Managing the supply chain by identifying, anticipating, mitigating, prevent the vulnerabilities and disruptions that cause or may cause impacts to the cost, schedule and performance of the mission. Includes readiness, preparedness, prevention, mitigation, acceptance, avoidance and recovery.
- The ability to project supply chain problems and make programmatic changes (both proactively and reactively) to mitigate the negative impact of those problems.
- The implementation of strategies to manage every day and exceptional risks along the supply chain through continuous risk assessment with the objective of reducing vulnerability and ensuring continuity. One way to view SCRM is to think of it as the intersection of supply chain management and risk management. from our book, "Supply Chain Risk Management: An Emerging Discipline"
- The management of supply chain risk.
- Processes that adopt the solutions identified by the root causes analysis from past challenges and developing a team that understands how to execute going forward.
- A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal). (CNSSI 4009-2015, The Committee on National Security Systems)

24 DAU

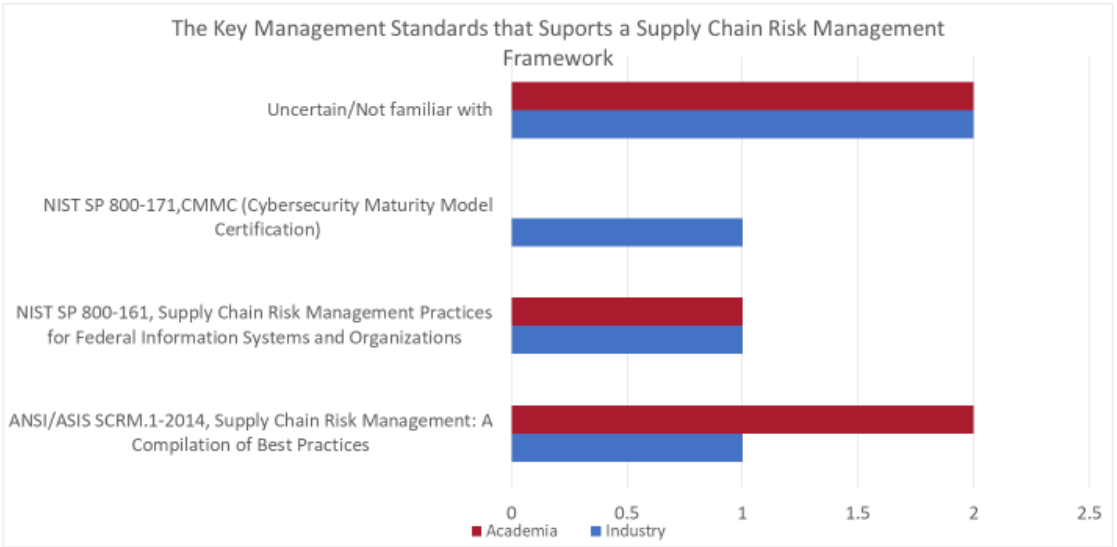
Supply Chain Resiliency:

- The fortitude in which your supply chain is prepared, can withstand and recover from vulnerabilities or disruptions. Includes readiness and recovery. The robust nature of your supply chain to weather the storm.
- The ability to still meet mission requirements when a problem occurs. For example, the ability to still deliver a system on time when a part is later. Or the ability to find a replacement part/vendor when a supplier goes out of business and still build a system that meets mission requirements.
- The capacity to overcome disruptions and continually transform itself to meet the changing needs and expectations of its customers.
- Ability to recover from a downturn and scalability.
- The capacity for resistance and recovery. That means having the capability to resist or even avoid the impact of disruptions.
- The ability of a supply chain to both resist disruptions and recover operational capability after disruptions occur.

25

DAU

Key Management Standards that Supports a SCRM Framework



26

DAU

Missing Key Standards

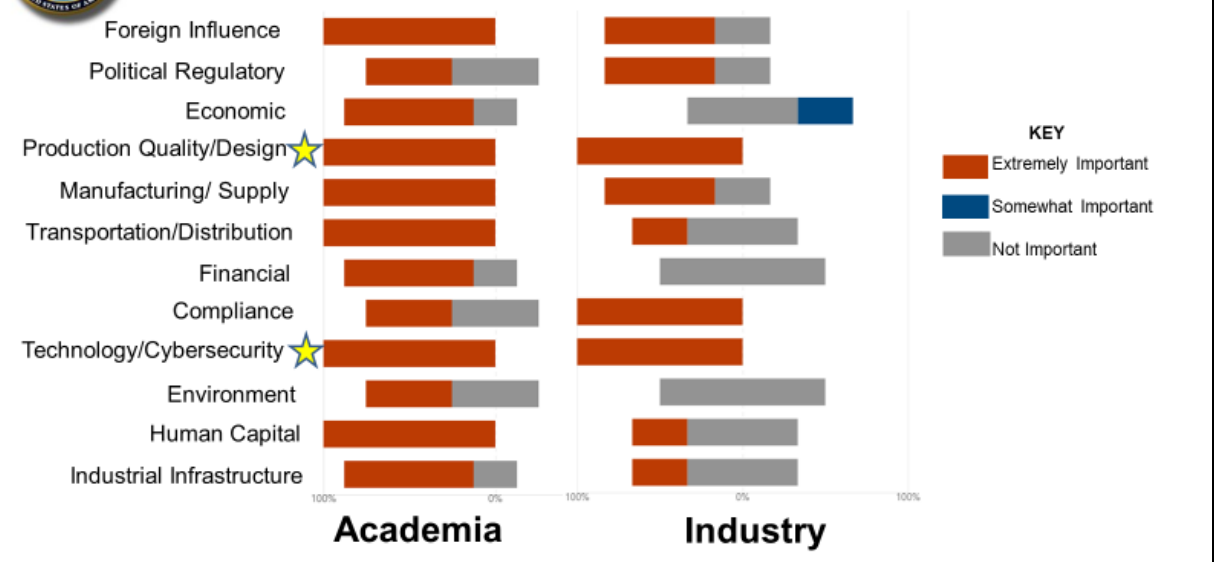
- **ISO 28000:** Supply Chain Security Management System
- **ISO 28002:** Security Management Systems for the Supply Chain – Development of Resilience in the Supply Chain
- **ISO 31000:** Risk Management
- **ISO 73:** Risk Management Vocabulary
- **AS 9100:** Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing

27

ISO – International Standards Organization

DAU

Importance of Risk Categories



Missing Risk Categories

- Raw Materials
- Metals
- Mineral Sourcing
- Sourcing Limitations
- Adjacency risk; Hidden or material deviation risk.
- Operational and Tactical Risks *within your own four walls...your own supply chain network. Things you say you control.*

29

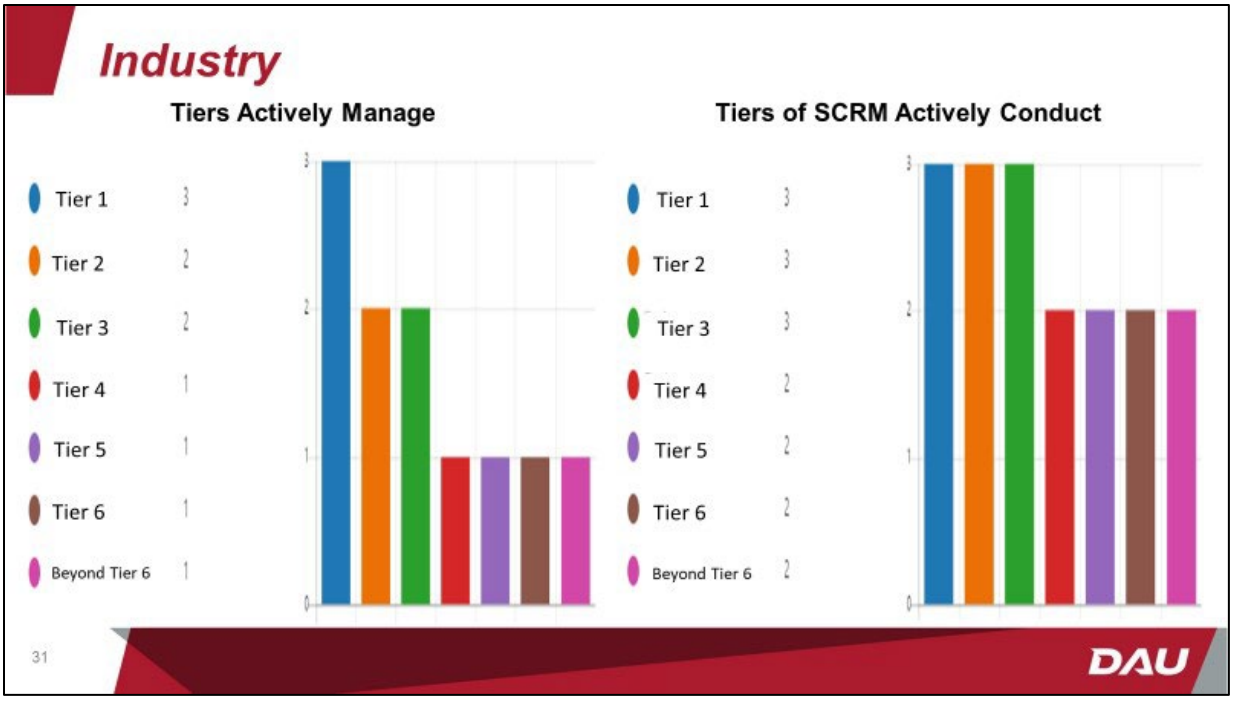
DAU

Missing Sub-Risk Categories

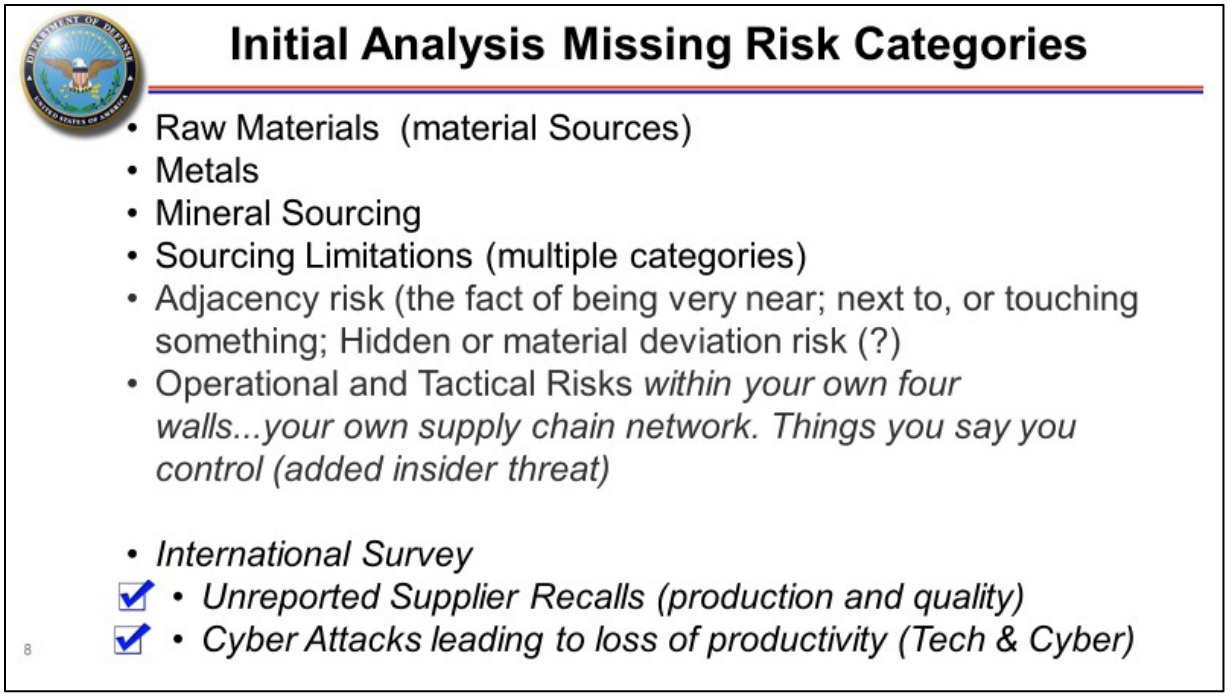
Risk Category	Recommended Subcategories
Foreign Influence	None
Political Regulatory	DoD Acquisition process, DoD Acquisition regulations, Domestic and global transportation regulations
Economic	None
Environment	Oil spills, nuclear reactors
Production Quality/Design	Sole sourced parts, single sourced parts, high performance system design at the expense of risk – availability of commodities, overlap with cyber
Manufacturing/ Supply	None
Transportation/Distribution	Transportation Cyber threats, blockchain implementation, labor shortages, Transportation oligopolies
Financial	None
Compliance	None
Technology/Cybersecurity	Nation state threats, public private partnerships effectiveness
Human Capital	Workforce training
Industrial Infrastructure	None

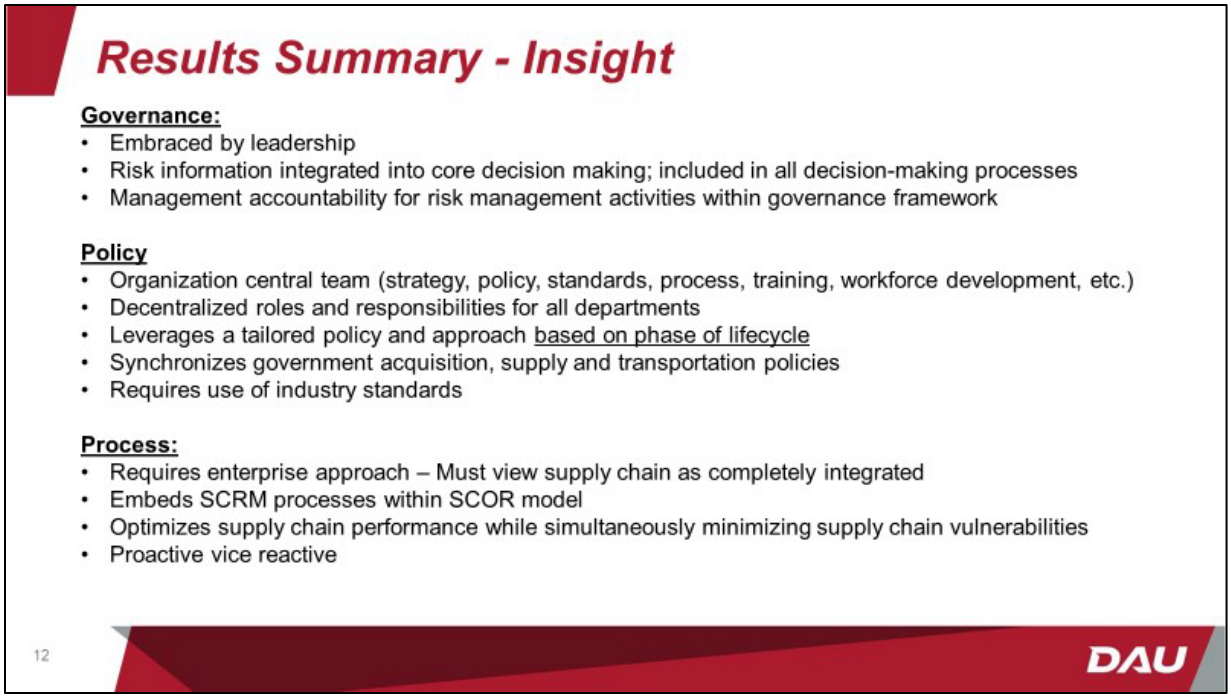
30

DAU


Industry
Tiers Actively Manage
Tier 1 3
Tier 2 2
Tier 3 2
Tier 4 1
Tier 5 1
Tier 6 1
Beyond Tier 6 1
Tiers of SCRM Actively Conduct
Tier 1 3
Tier 2 3
Tier 3 3
Tier 4 2
Tier 5 2
Tier 6 2
Beyond Tier 6 2
31
DAU


Academia
The Percentage Supply Chain Management Curriculum Devoted to Supply Chain Risk Management
• 5%
• One, three-hour credit course
• About 30%
32
DAU


Initial Analysis Missing Risk Categories
• Raw Materials (material Sources)
• Metals
• Mineral Sourcing
• Sourcing Limitations (multiple categories)
• Adjacency risk (the fact of being very near; next to, or touching something; Hidden or material deviation risk (?)
• Operational and Tactical Risks within your own four walls...your own supply chain network. Things you say you control (added insider threat)
• International Survey
• Unreported Supplier Recalls (production and quality)
• Cyber Attacks leading to loss of productivity (Tech & Cyber)
8


Results Summary - Insight
Governance:
• Embraced by leadership
• Risk information integrated into core decision making; included in all decision-making processes
• Management accountability for risk management activities within governance framework
Policy
• Organization central team (strategy, policy, standards, process, training, workforce development, etc.)
• Decentralized roles and responsibilities for all departments
• Leverages a tailored policy and approach based on phase of lifecycle
• Synchronizes government acquisition, supply and transportation policies
• Requires use of industry standards
Process:
• Requires enterprise approach – Must view supply chain as completely integrated
• Embeds SCRM processes within SCOR model
• Optimizes supply chain performance while simultaneously minimizing supply chain vulnerabilities
• Proactive vice reactive
12
DAU

Appendix C. SCRM Draft Taxonomy Version 1.0

ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3500

SUSTAINMENT

NOV 2 8 2022

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Supply Chain Risk Management Draft Taxonomy Version 1.0 – Advance Copy

As the Department of Defense (DoD) proponent for development and implementation of supply chain risk management (SCRM) policies, in May 2022, my office initiated a project to develop a common SCRM framework and taxonomy in coordination with DoD components, interagency partners, academia, industry, and standards bodies. While we continue to develop and coordinate the common framework, which will clearly identify SCRM roles and responsibilities across the DoD, we have completed the development of a draft SCRM Taxonomy Version 1.0, detailed in the attachment, consisting of 12 risk categories and 124 sub-risk categories. In addition, the Taxonomy includes proposed definitions for Supply Chain Resilience, SCRM, and Supply Chain Security.

I am providing an advance copy of the draft SCRM Taxonomy Version 1.0 to facilitate the communication of risk information across the DoD. Many DoD Components are currently using the Taxonomy to assess and categorize risks, to include incorporating the taxonomy into information technology systems, databases, programs, policies, and processes. My office will officially publish the Taxonomy as part of a new SCRM DoD Instruction, with estimated publication planned for early Fiscal Year 2024.

Your organizations have been instrumental in completing the draft SCRM Taxonomy Version 1.0 and I greatly appreciate your ongoing support as we develop and refine it as well as other key products for management of the risks within the DoD supply chain. My points of contact for this effort are BG Michelle Link, michelle.a.link2.mil@mail.mil; Mr. Jared Andrews, jared.m.andrews6.ctr@mail.mil; and Ms. Stephanie Lopez, stephanie.lopez.27@us.af.mil.

Christopher J. Lowman

Attachment:
As stated

Definitions

Terms	PROPOSED DEFINITIONS
Supply Chain Resilience (SCR)	The capability of supply chains to respond quickly, so as to ensure continuity of operations after a disruption, and to quickly adapt to change. Resilience is the expected outcome of proactive Supply Chain Risk Management and Supply Chain Security.
Supply Chain Risk Management (SCRM)	The process of proactively identifying supply chain vulnerabilities, threats, and potential disruptions and implementing mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services as risks are found or disruptions occur.
Supply Chain Security (SCS)	The application of policies, procedures, processes, and technologies to ensure the security, integrity, and uninterrupted flow of products while moving through the supply chain. Examples include the ability to protect supply chains from cyber infiltrations and the introduction of counterfeit material.

Risks

RISK CATEGORY	PROPOSED DEFINITIONS
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	A company is considered to be operating under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts and/or programs which support national security.
POLITICAL & REGULATORY	The weakness of the political powers and their legitimacy and control. Inadequacy of the control schemes, policies and planning, or broad political conditions. Includes terrorism, government policy changes, systematic corruption, and energy crises in the international marketplace. This can occur when changes in laws or regulations materially impact a security, business, sector or market. New laws and regulations enacted by the government or regulatory body can increase costs of operating a business, reduce the attractiveness of investment, or change the competitive landscape. Includes issues such as civil unrest or conflict and acts of terrorism that negatively impact supply chain operations. A certified act of terrorism must fall within the four identified descriptors determined by the Terrorism Risk Insurance Act (TRIA) and the Secretary of Treasury.
ECONOMIC	Currency fluctuations, instability in demand and prices, changing labor costs and inflationary pressures present challenges for suppliers to accurately plan their investment in foreign markets.
ENVIRONMENT	Include natural and manmade disasters that may disrupt supply chains. Natural disasters and other extreme weather conditions comprise the bulk of external environmental risk. Manmade disasters can arise from improper health and safety, fires, spills, chemical leaks, and other environmental hazards.
PRODUCT QUALITY & DESIGN	Occurs due to inherent design and quality problems (e.g., raw materials, ingredients, production, logistics, packaging) in which the part does not meet performance specifications and quality standards set by industry or DoD. Includes the detection of a part that was illegally created and sold under false pretenses. The part has not faced industry standard tests during the production phase (e.g., pressure testing) to ensure sustainability during usage. Counterfeit and non-MILSPEC parts pose significant risk to the function and safety of the system through malicious intrusion via backdoor exposures; increased maintenance costs due to depreciation in quality; and added stresses due to the parts inability to function at true capacity.
MANUFACTURING & SUPPLY	Occurs when a supplier cannot fulfill the supply of a product to meet market demand. This can be due to reduced throughput or production delays caused by equipment down-time, capacity constraints, and delays in material delivery.

RISK CATEGORY	PROPOSED DEFINITIONS
	Additional concerns include availability of supply, sole-source, and concentration within a singular country creating over-reliance.
TRANSPORTATION & DISTRIBUTION	Occurs when there is a dynamic disruption within the transportation and logistics of a product from one point to another. The transportation industry is among the most risk-prone of all industries, due to accidents, losses of cargo, driver shortages, and deteriorating infrastructure. These risks can cause shipment delays, supply chain disruptions, increased costs, and damaged reputations. In addition, the inability to predict and plan for disruptions in the logistics plan presents risk in meeting delivery requirements and maintaining operations.
FINANCIAL	The condition in which a supplier cannot generate revenue or income resulting in the inability to meet financial obligations. This is generally due to high fixed costs, illiquid assets, or revenues sensitive to economic downturns. Financial distress can lead to the inability to meet contractual obligations, hostile takeovers, or bankruptcy.
COMPLIANCE	Inability to comply with a wide-arching set of guidelines, policies, laws, and/or agreements established to avoid impact to national security.
TECHNOLOGY & CYBER SECURITY	Involves the management of cybersecurity requirements for information technology systems, software and networks, which are driven by threats such as cyber-terrorism, malware, data theft and the advanced persistent threat (APT). Technology risks include vulnerabilities and exposures of systems components and information systems produced by a specific supplier. Common risks include weaknesses in computation logic (code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity or availability.
HUMAN CAPITAL	Associated with human skills, knowledge and ethical conduct of an organization, including industrial disputes and labor unrest.
INFRASTRUCTURE	Infrastructure required to support supply chains within a country (e.g., buildings, water, electricity, roads).

Sub-Risk Categories

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
COMPLIANCE	Trafficking in Persons	"Trafficking in persons," "human trafficking," and "modern slavery" are umbrella terms – often used interchangeably – to refer to a crime whereby traffickers exploit and profit at the expense of adults or children by compelling them to perform labor or engage in commercial sex.
COMPLIANCE	SEC Enforcement Action	Actions that take place by the SEC to address misconduct that arose from or led to financial crimes.
COMPLIANCE	Past suspension or Debarment	Suspend - to temporarily pause or delay work with the option to continue later. This action must be taken by a suspending official and executed in accordance with FAR 9.4.Debar - to disqualify the person or company from receiving contracts. Must be completed by a debarring official and executed in compliance with FAR 9.4.
COMPLIANCE	Occupational Workers Health and Safety (OSHA)	Safe and healthful working conditions for workers by setting and enforcing standards and by providing training, outreach, education and assistance.

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
COMPLIANCE	Legal and Reputational	Examples include lawsuits, discrimination, and other law enforcement actions.
COMPLIANCE	Insider Threat	Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization.
COMPLIANCE	Import/Export Violation	Both the deliberate and non-deliberate violation of the customs laws of the United States.
COMPLIANCE	Human Rights	Rights regarded as belonging fundamentally to all persons (e.g., freedom from unlawful imprisonment, torture, and execution).
COMPLIANCE	Fraud (Procurement and Government)	Fraudulent activities by Federal or State employees, contractors, subcontractors, or any other participants on government contracts. Suspected fraudulent activities include, but are not limited to: • falsifying information on contract proposals • using Federal funds to purchase items that are not for Government use • billing more than one contract for the same work • billing for expenses not incurred as part of the contract • billing for work that was never performed, falsifying data • substituting approved materials with unauthorized products • misrepresenting a project's status to continue receiving Government funds • charging higher rates than those stated or negotiated for in the bid or contract • influencing government employees to award a grant or contract to a particular company, family member, or friend.
COMPLIANCE	Forced Labor	Forced labor occurs when individuals are compelled to provide work or service through the use of force, fraud, or coercion.
COMPLIANCE	Ethics Violation	A violation of moral principles that govern a person's behavior or the conducting of an activity.
COMPLIANCE	Defective Pricing	Result of Cost/Pricing Data (C/PD) that was certified by a contractor to be accurate, current, and complete but was not.
COMPLIANCE	Contractor Misconduct	When companies that sell goods or services to the government violate laws or regulations or are the subject of misconduct allegations in their dealings with the government, individuals, or private entities.
COMPLIANCE	Contract Non-Compliance	Non-compliance occurs when one party in a contract does not fulfill his or her obligations.
COMPLIANCE	Conflict Minerals and Raw Materials in Supply Chain	Natural resources extracted in a conflict zone. In the United States, companies must report on their use and sourcing of tin, tantalum, tungsten and gold and raw materials.

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
COMPLIANCE	Anti-trust / Monopolistic Practices	Practices that unduly restrain competitive trade. Monopolistic practices - Companies' actions to create a monopoly. A monopoly refers to when a company and its product offerings dominate a sector or industry. Monopolies can be considered an extreme result of free-market capitalism in that, absent any restriction or restraints, a single company or group becomes large enough to own all or nearly all of the market (goods, supplies, commodities, infrastructure, and assets) for a particular type of product or service. The term monopoly is often used to describe an entity that has total or near-total control of a market.
ECONOMIC	Recession, Economic Slowdown	A period of temporary economic decline during which trade and industrial activity are reduced, generally identified by a fall in GDP in two successive quarters.
ECONOMIC	Price Volatility/Market Risk	The sensitivity of the financial institution's earnings or the economic value of its capital to adverse changes in interest rates, foreign exchanges rates, commodity prices, or equity prices.
ECONOMIC	Inflation	Inflation is the increase in the prices of goods and services over time.
ECONOMIC	High Unemployment	The term unemployment refers to a situation where a person actively searches for employment but is unable to find work. Unemployment is considered to be a key measure of the health of the economy.
ECONOMIC	Economic Sanctions	Economic sanctions are defined as the withdrawal of customary trade and financial relations for foreign- and security-policy purposes. Sanctions may be comprehensive, prohibiting commercial activity with regard to an entire country, like the long-standing U.S. embargo of Cuba, or they may be targeted, blocking transactions by and with particular businesses, groups, or individuals.
ECONOMIC	Economic instability	Economic instability occurs when the factors that influence an economy are out of balance. When an economy becomes unstable, there is inflation, which is a decrease in the value of money. This leads to higher prices, higher unemployment rates, and general angst among consumers and businesses that are trying to survive financially. Causes of Economic Instability: Stock Market Fluctuations, Fall in Home Prices, Interest Rate Changes, Black Swan Events (Hurricane, Terrorist attack, etc.)
ECONOMIC	Demand Shocks	A demand shock is a sudden unexpected event that dramatically increases or decreases demand for a product or service, usually temporarily.

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
ECONOMIC	Currency Fluctuations	Currency fluctuations are a natural outcome of floating exchange rates, which is the norm for most major economies. Numerous factors influence exchange rates, including a country's economic performance, the outlook for inflation, interest rate differentials, capital flows and so on. A currency's exchange rate is typically determined by the strength or weakness of the underlying economy. As such, a currency's value can fluctuate from one moment to the next.
ENVIRONMENT	Wildfire	A large, destructive fire that spreads quickly over woodland or brush.
ENVIRONMENT	Pandemic	A pandemic is the worldwide spread of a new disease.
ENVIRONMENT	Natural Disaster	Natural disasters include all types of severe weather, which have the potential to pose a significant threat to human health and safety, property, critical infrastructure, and homeland security. Natural disasters occur both seasonally and without warning, subjecting the nation to frequent periods of insecurity, disruption, and economic loss.
ENVIRONMENT	Man-made Risk	The exposure to dangerous or harm as a result of human intent, negligence, or error involving a failure of a man-made process or system, as opposed to natural disasters resulting from natural hazards.
ENVIRONMENT	Extreme Weather Event	Refers to weather phenomena that are at the extremes of the historical distribution and are rare for a particular place and/or time, especially severe or unseasonal weather. Such extremes include severe thunderstorms, severe snowstorms, ice storms, blizzards, flooding, hurricanes, and high winds, and heat waves. For example, although flooding is common in the United States, the impacts of flooding are not consistent from year to year through time. Many years of small floods with little impact may be followed by a single large flood with a sizable loss.
ENVIRONMENT	Climate	The impact that adverse climate-related conditions can impact the supply chain.
ENVIRONMENT	Chemical Spill (Hazmat)/chemical, biological, radiological, or nuclear incident	Chemical spills are the uncontrolled release of a hazardous chemical, either as a solid, liquid or a gas. Any occurrence, resulting from the use of chemical, biological, radiological, and nuclear weapons and devices; the emergence of secondary hazards arising from friendly actions; or the release of toxic industrial materials or biological organisms and substances into the environment, involving the emergence of chemical, biological, radiological, and nuclear hazards.
FINANCIAL	Unstable Payment Performance	When a company does not consistently "transfer money, goods or services in exchange for goods and

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
		services in acceptable proportions that have been previously agreed upon by all parties involved".
FINANCIAL	Solvency, Credit Risk	Solvency is the ability of a company to meet its long-term debts and financial obligations. Solvency can be an important measure of financial health, since its one way of demonstrating a company's ability to manage its operations into the foreseeable future. The quickest way to assess a company's solvency is by checking its shareholders' equity on the balance sheet, which is the sum of a company's assets minus liabilities.
FINANCIAL	Profitability Measures	Profitability ratios are a class of financial metrics that are used to assess a business's ability to generate earnings relative to its revenue, operating costs, balance sheet assets, or shareholders' equity over time, using data from a specific point in time.
FINANCIAL	Operational Efficiency Risk	In a business context, operational efficiency is a measurement of resource allocation and can be defined as the ratio between an output gained from the business and an input to run a business operation. When improving operational efficiency, the output to input ratio improves. Operational risk summarizes the uncertainties and hazards a company faces when it attempts to do its day-to-day business activities within a given field or industry. A type of business risk, it can result from breakdowns in internal procedures, people and systems—as opposed to problems incurred from external forces, such as political or economic events, or inherent to the entire market or market segment, known as systematic risk. Operational risk can also be classified as a variety of unsystematic risk, which is unique to a specific company or industry.
FINANCIAL	Offshore Leaks/Database	The ICIJ Offshore Leaks Database represents a large set of relationships between people, companies, and organizations involved in the creation of offshore companies in tax-heaven territories, mainly for hiding their assets.
FINANCIAL	Liquidity Risk	The risk of incurring losses resulting from the inability to meet payment obligations in a timely manner when they become due or from being unable to do so at a sustainment cost
FINANCIAL	Lack of Funding Sources	(1) Funding is money which a government or organization provides for a particular purpose. If sufficient funding is unavailable, it will limit the provider's ability to meet requirements. (2) An absence or limit in the assortment of capital a

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
		business can access to reinvest into business operations.
FINANCIAL	Financial Crimes	Financial crime refers to all crimes committed by an individual or a group of individuals that involve taking money or other property that belongs to someone else, to obtain a financial or professional gain.
FINANCIAL	Dependence on Defense Contracts	Consider DoD sales relative to total global sales for the facility. "Mixed" market is ~50% DoD; "Significant" is ~>60% for DoD or >60% for non-DoD; Very Strong or very weak DoD dominance can be risky for different reasons: High dependence on DoD contracts makes a facility more susceptible to DoD funding decisions. Low dependence on contracts makes the DoD more susceptible to business decisions by the facility.
FINANCIAL	Cyclical Risk	Cyclical risk is the risk of business cycles or other economic cycles adversely affecting the returns of an investment, an asset class or an individual company's profits.
FINANCIAL	Costs Overruns	A cost overrun, also known as a cost increase or budget overrun, involves unexpected, incurred costs. When these costs are in excess of budgeted amounts due to a value engineering underestimation of the actual cost during budgeting, they are known by these terms. Cost overruns are common in infrastructure, building, and technology projects and Weapon Systems.
FINANCIAL	Bankruptcy	The state of being completely lacking particular quality or value.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Weaponized Mergers and Acquisitions (M&A)	The use by national governments of the tools of regulation of M&A to advance, explicitly or implicitly, domestic political and trade agendas.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Veiled Venture	An acquisition or economic-related action designed to camouflage nefarious intent of an individual, company, or country.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Theft of Trade Secrets	Trade secrets are a type of intellectual property that comprise formulas, practices, processes, designs, instruments, patterns, or compilations of information that have inherent economic value because they are not generally known or readily ascertainable by others, and which the owner takes reasonable measures to keep secret. In some jurisdictions, such secrets are referred to as confidential information.

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	State-owned Company	A state-owned enterprise (SOE) is a legal entity that is created by a government in order to partake in commercial activities on the government's behalf. A state-owned enterprise or government-owned enterprise is a business enterprise where the government or state has significant control through full, majority, or significant minority ownership.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Sabotage	1: destruction of an employer's property (such as tools or materials) or the hindering of manufacturing by discontented workers 2: destructive or obstructive action carried on by a civilian or enemy agent to hinder a nation's war effort 3a: an act or process tending to hamper or hurt 3b: deliberate subversion
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Provenance	The extent to which a supplier relies on parts that are manufactured, sold, or distributed by companies that have part or whole foreign ownership or significant foreign influence.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Partnership with State-owned Entity	A state-owned enterprise (SOE) or government-owned enterprise (GOE) is a business enterprise where the government or state has significant control through full, majority, or significant minority ownership. Defining characteristics of SOEs are their distinct legal form and operation in commercial affairs and activities. While they may also have public policy objectives (e.g., a state railway company may aim to make transportation more accessible), SOEs should be differentiated from government agencies or state entities established to pursue purely nonfinancial objectives.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Nationalization	A national government can transform privately-owned businesses into state-owned businesses, which can enable foreign governments to enter existing supply chains.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Industrial Espionage	Industrial espionage, economic espionage, corporate spying or corporate espionage is a form of espionage conducted for commercial purposes instead of purely national security. While economic espionage is conducted or orchestrated by governments and is international in scope, industrial or corporate espionage is more often national and occurs between companies or corporations.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Foreign Intelligence Entity (FIE)	Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
		intelligence and security services and international terrorists.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Executive Poaching	The intentional action of one company to hire an employee or group of employees currently employed at another company (many times a competing company).
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Cyber Espionage	Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Counterintelligence	Information gathered, and activities conducted to detect, identify, exploit and neutralize the intelligence capabilities and activities of terrorists, foreign powers and other entities directed against US national security.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	CI Collection	The systemic acquisition of intelligence information to answer CI collection requirements.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	CI Analysis	The process of examining and evaluating raw information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of a foreign intelligence entity (FIE).
HUMAN CAPITAL	Work Stoppage	A cessation of work by employees as a job action. Work stoppage is often used to refer to a cessation of work that is less serious and more spontaneous than one referred to as a strike.
HUMAN CAPITAL	Loss of Talent/Skill, Mass Lay-offs	An absence or decline in workforce knowhow resulting in diminished domestic capabilities.
HUMAN CAPITAL	Lack of Access to Capable Workforce/Labor Shortages	When a labor shortage occurs, it means that employers are having a difficult time recruiting qualified applicants for available job openings. There are not enough candidates to fill the roles employers are hiring for or there only a few available candidates and are hard to find.
HUMAN CAPITAL	Labor Dispute	The term “labor dispute” includes any controversy concerning terms, tenure or conditions of employment, or concerning the association or representation of persons in negotiating, fixing, maintaining, changing, or seeking to arrange terms or conditions of employment, regardless of whether the disputants stand in the proximate relation of employer and employee.
HUMAN CAPITAL	Boycotts	Withdraw from commercial or social relations with (a country, organization, or person) as a punishment or protest

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
INFRASTRUCTURE	Utilities	Any and all utility services and installations including, but not limited to, gas, water, electricity, telephone, other telecommunications, steam, sewer and storm sewer, and all piping, wiring, conduit and/or other fixtures related thereto or used in connection therewith. To include Water – includes the material and availability therein of irrigation, sanitation, production and transportation (see waterway) of material and/or products. Water Supply sources and their surroundings from which water is supplied for drinking, manufacturing, production, industrial, or domestic purposes.
INFRASTRUCTURE	Security	1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 3-10) 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JP 3-10) 3. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.
INFRASTRUCTURE	Roads, Rail, Water etc.	Railroads are of particular importance for the movement of commodities that are heavy and moved in bulk over long distances. This also includes the use of water as a mode of transportation and roadways in and out of industrial facilities. Waterway – a river, canal, or other body of water serving as route or way to travel or transport.
INFRASTRUCTURE	Equipment	Equipment — In logistics, all nonexpendable items needed to outfit or equip an individual or organization. See also component, supplies. (JP 4-0)
INFRASTRUCTURE	Energy Scarcity	Energy scarcity - any significant bottleneck in the supply of energy resources to manufacturing, production, or economy. Additionally, in economics, a commodity is called scarce if using that commodity in one specific way implies that it can no longer be used in any other way.
INFRASTRUCTURE	Building/Facilities conditions	Facility — A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land. (JP 3-34). Building conditions- the state of facilities and buildings measured through various metrics such as Building Condition Index (engineering assessment) or Facilities Condition Index (cost of repair divided by cost of replacement). Generally, the lower the score

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
		the lower the quality of building and expected storage capabilities and productive output.
MANUFACTURING & SUPPLY	Underdeveloped Product Pipeline	Used to transmit fuel and natural gas or derivatives to manufacturing and supply facilities. The extent to which the OEM is resilient to delays in supply chain capacity and development needed to meet extant and nascent manufacturing requirements
MANUFACTURING & SUPPLY	Throughput/Production Delays	A delay in the amount of a product or service that a company can produce and deliver to a client within a specified period of time.
MANUFACTURING & SUPPLY	Sole Source Dependency	Only one supplier for the required item is available.
MANUFACTURING & SUPPLY	Single Source	A particular supplier is purposefully chosen by the buying organization, even when other suppliers are available
MANUFACTURING & SUPPLY	Reseller/3rd Party Vendor/Middleman	A person or company that sells something they have bought from someone else.
MANUFACTURING & SUPPLY	Reclamation/Utilization	Process to reclaim whole or essential components and materials for manufacturing either the same or alternate products. Reutilization is using components and materials for the same, similar, or differing purpose (e.g., using ships again in different missions or sinking to build reefs)
MANUFACTURING & SUPPLY	Parts/Spares Inventory Shortages	Inadequate supplies of spare parts on hand for maintenance and repairs.
MANUFACTURING & SUPPLY	Outsourcing	Outsourcing is the business practice of hiring a party outside a company to perform services and create goods that traditionally were performed in-house by the company's own employees and staff.
MANUFACTURING & SUPPLY	Order Fulfillment	The complete process from point of sales inquiry to delivery of a product to the customer.
MANUFACTURING & SUPPLY	Material Sources	The origin of materials which have been used to form or manufacture a product generally represented as the N-1 Supply Tier. This includes direct material used in the product and indirect material used in production and manufacturing, e.g., castings.
MANUFACTURING & SUPPLY	Inventory Stockout/Material Shortages	A stockout, or out-of-stock (OOS) event is an event that causes inventory to be exhausted.
MANUFACTURING & SUPPLY	Inventory or Capacity Incidents	Loss of inventory or capacity from events. This may be a loss from building failure, access restrictions, etc.
MANUFACTURING & SUPPLY	Industrial Capacity	Industrial capacity is “the amount (e.g., quantity) of industrial capability” or “the amount (e.g., quantity) of the ability of industry to accomplish a result”. This could include products (e.g., industry can make one item per month with existing lines), services (e.g., industry can service one plane per hour), and changes (e.g., if industry received $XX this month

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
		they could increase by YY production lines next month to make 50 items per month).
MANUFACTURING & SUPPLY	Industrial Capability	Industrial capability is "the ability of industry to accomplish (make, create, destroy, etc.) a result (product, information, objective, etc.)." This drives both the larger products (e.g., can we make airplanes?) and more specifics (e.g., can we make a stealth covering for legacy airplanes to avoid aerial reconnaissance while on the tarmac?)
MANUFACTURING & SUPPLY	Extended Lead Times	Unplanned and/or unexpected time it takes between order initiation and product delivery.
MANUFACTURING & SUPPLY	Equipment Down Time	Equipment downtime refers to the amount of time that equipment is not operating, whether that is a result of unplanned equipment failure (e.g., a fault or broken part) or planned downtime (e.g., necessary downtime for preventive maintenance).
MANUFACTURING & SUPPLY	Obsolescence/DMSMS	Obsolescence is defined as the loss or impending loss of original manufacturers of items or suppliers of items or raw materials. This type of obsolescence is commonly referred to as DMSMS (Diminishing Manufacturing Sources and Material Shortages) within the Department of Defense, which is caused by the unavailability of technologies or parts that are necessary to manufacture or sustain a system. Due to the length of the system's manufacturing and support life, and unforeseen life extensions to the support of the system longer than its planned end of support date, the parts and other resources necessary to support the system become unavailable before the system's demand for the parts or other resources ends.
MANUFACTURING & SUPPLY	Concentration Risk	The probability of loss likely to arise due to over-dependence on a single vendor, concentration risk is further exacerbated when such a vendor specializes in a specific industry.
MANUFACTURING & SUPPLY	Agriculture	Agriculture is the art and science of cultivating the soil, growing crops and raising livestock. It includes the preparation of plant and animal products for people to use and their distribution to markets. Agriculture provides most of the world's food and fabrics.
MANUFACTURING & SUPPLY	Adjacency Risk	When separate industries (e.g., auto industry and defense sector) compete for limited resources (e.g., microchips).

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
POLITICAL & REGULATORY	Watch List	The watchlist is used by government agencies with a national security mission to support Visa and passport screening (Department of State), International travel into the U.S. (U.S. Customs and Border Protection), and air passenger screening for terrorism (Transportation Security Administration).
POLITICAL & REGULATORY	Trade Wars	Trade war happens when one country retaliates against another by raising import tariffs or placing other restrictions on the other country's imports.
POLITICAL & REGULATORY	Terrorism	The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives
POLITICAL & REGULATORY	Territorial Disputes on trade routes	A trade route is a logistical network identified as a series of pathways and stoppages used for the commercial transport of cargo. Territorial disputes involve disagreement about who controls a particular territory or trade route.
POLITICAL & REGULATORY	Political/Government Changes	The risk that political changes or instability in a country could pose to a supply chain. Instability could stem from a change in government, legislative bodies, other foreign policymakers or military control. Political risk is also known as "geopolitical risk," and becomes more of a factor as the time horizon of investment gets longer. Government risk manifests when the actions of government increase uncertainty with respect to an organization, project or activity. An example of government risk is when poor behavior of an industry or sector leads to a government policy or regulatory response.
POLITICAL & REGULATORY	Interstate conflict (War or Armed Conflict)	Interstate conflict involves violence between two or more states.
POLITICAL & REGULATORY	Government Policies	All DoD Polices/Regulations such as: DoD Acquisition process, DoD Acquisition and Supply regulations, Intel, Information Technology, Industrial Base, Domestic and global transportation regulations
POLITICAL & REGULATORY	Government Collapse	State collapse, breakdown, or downfall is the complete failure of a mode of government within a sovereign state.
POLITICAL & REGULATORY	Exposure (Potential Political)	The condition of being exposed to several events: such as: • the condition of being presented to view or made known • the condition of being unprotected especially from severe weather • the condition of being subject to some effect or influence

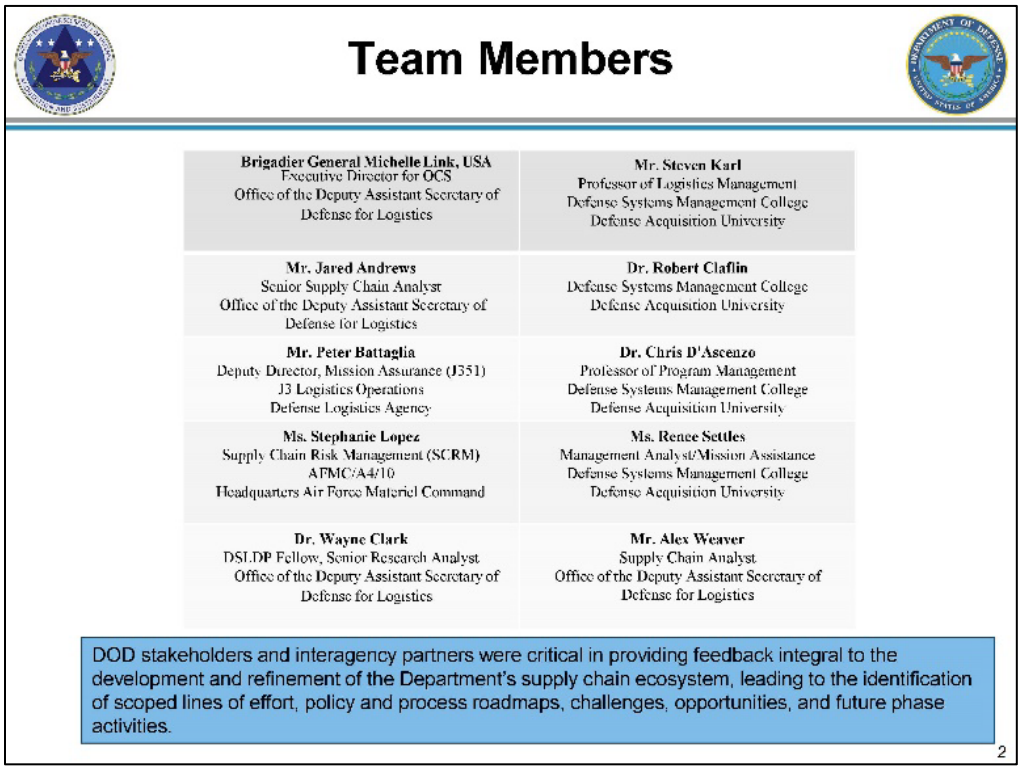
RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
		• the condition of being at risk of financial loss
POLITICAL & REGULATORY	Environmental Protection Agency (EPA)	The mission of EPA is to protect human health and the environment.
POLITICAL & REGULATORY	Corruption	Corruption is dishonest behavior by those in positions of power, such as managers or government officials. Corruption can include giving or accepting bribes or inappropriate gifts, double-dealing, under-the-table transactions, manipulating elections, diverting funds, laundering money, and defrauding investors.
POLITICAL & REGULATORY	New Regulations, Changes in Policy (e.g., Trade Policy)	Changes in government policies or regulations that impact the supply chain.
POLITICAL & REGULATORY	Border Delays	Border delays can result in the timely delivery of materials/items.
PRODUCT QUALITY & DESIGN	Unreported Supplier Recalls	Unsupported Product Recall means recalls unsubstantiated by documentation or receipts incurred by third parties selling a Product(s) that is included in a Recall(s) to the end user(s).
PRODUCT QUALITY & DESIGN	System/Parts Performance Failure	Performance is a measurement of either work or time, for example, system-related work accomplished within a given time and the time required to complete a task or job, based upon past performance.
PRODUCT QUALITY & DESIGN	Product Characteristics	Product characteristics can inform decisions on whether products can be interchangeable or substitutable.
PRODUCT QUALITY & DESIGN	Non-MILSPEC Parts	Non-MILSPEC parts items may not conform to military specifications and could result in product failure.
PRODUCT QUALITY & DESIGN	Non-Conforming Parts	Non-conforming materials are any product or parts that are defective, counterfeit or do not meet the requirements.
PRODUCT QUALITY & DESIGN	Counterfeit Parts	The unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
TECHNOLOGY & CYBER SECURITY	Unsecure Networks or Systems	An unsecured network or system lacks intrusion detection and prevention capability.
TECHNOLOGY & CYBER SECURITY	OPSEC / INFOSEC Violation	OPSEC (operational security) is an analytical process that classifies information assets and determines the controls required to protect these assets. After vulnerabilities have been determined, the next step is to determine the threat level associated with each of them. OPSEC encourages managers to view operations or projects from the outside-in, or from the perspective of competitors (or enemies) in order to identify weaknesses. If an organization can easily extract their own information while acting as an outsider, odds are adversaries outside the organization can as well. Completing regular risk assessments and OPSEC is key to identifying vulnerabilities.
TECHNOLOGY & CYBER SECURITY	Malicious Intrusion	Intrusions that take place anytime a bad actor gains access to an application with the intent of causing harm to or steal data from the network or user.
TECHNOLOGY & CYBER SECURITY	Loss or Theft Of DCI/PII Discharge of Classified Information = DCI; Personally Identifiable Information = PII	PII---- The removal or unlawful taking of information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. CII--- The removal or unlawful taking of information that a defense organization has determined to be valuable to an adversary. This information may vary based on the organization's role.
TECHNOLOGY & CYBER SECURITY	IT Obsolescence	When a technical product or service is no longer needed or wanted even though it could still be in working order. Technological obsolescence generally occurs when a new product has been created to replace an older version.
TECHNOLOGY & CYBER SECURITY	IT Implementation Failure	A new system implementation or upgrade that fails to a degree where normal business operations are negatively impacted
TECHNOLOGY & CYBER SECURITY	IT Disruption/Connectivity Issues	An IT issue that disrupts normal business operations such as an outage, errors while implementing new technology, ransomware, or IT overloads
TECHNOLOGY & CYBER SECURITY	Data Breach	A data breach is a security violation, in which sensitive, protected or confidential data is copied,

RISK CATEGORY	RISK SUB-CATEGORIES	PROPOSED DEFINITIONS
		transmitted, viewed, stolen or used by an individual unauthorized to do so.
TECHNOLOGY & CYBER SECURITY	Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information.
TECHNOLOGY & CYBER SECURITY	Critical Hardware/Software Vulnerability	A weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.
TRANSPORTATION & DISTRIBUTION	Transportation Network Disruption	Disruptions to the transportation network can cause delays or missed shipments of material and items.
TRANSPORTATION & DISTRIBUTION	Poor Shipment and Delivery Accuracy	Shipment accuracy implies that items are properly fulfilled, packed, and delivered in accordance with the customer’s requirements.
TRANSPORTATION & DISTRIBUTION	Poor Delivery Performance	Poor delivery performance includes incorrect and incomplete shipments, shipments to the wrong location, and late shipments.
TRANSPORTATION & DISTRIBUTION	Loss of Cargo	Cargo loss means any loss or destruction that occurs while the cargo is moved within distribution channels.
TRANSPORTATION & DISTRIBUTION	Changes in Trade Policy (Containers in Ports)	See Office of the U.S. Trade Representative (https://ustr.gov/)
TRANSPORTATION & DISTRIBUTION	Accidents	An incident that happens unexpectedly and unintentionally, typically resulting in damage, injury, and negatively impacts the transportation network.

This Page Intentionally Left Blank

Appendix D. SCRM Phase I Outbrief



Agenda

Purpose: To brief the output of the DASD Log/DAU SCRM project.

Executive Summary:

- OSD DASD Log asked DAU, in concert with academia and industry to facilitate deliberate, focused small group working sessions with key stakeholders to develop a common framework that clearly defines the compendium of supply chain risk management terms and lines of effort
- OSD DASD Log developed a draft framework with the Military Services, key OSD stakeholders and other government agencies in early FY22, ahead of focused small working sessions
- Deliberate working sessions were held with key stakeholders to further discuss and refine the draft framework over the past 9 months. Each working session focused on identifying key stakeholders and their organizational SCRM related activities, authorities, policies, processes, opportunities, and gaps within each respective LOE

Recommendation: Establish an enterprise level organizational structure to develop and implement an integrated SCRM framework, standard supply chain risk taxonomy, DoD SCRM policy, data integration strategy, and governance and oversight.

3

Project Overview

Problem Statement: The Department of Defense requires a persistent, holistic, and comprehensive approach to manage the disparate risks associated with the defense industrial base and national security innovation base (NSIB) (PJL) supply chain, as well as, a consensus on the definition of supply chain risk lexicon as it pertains to supply availability, original equipment manufacturers (OEMs), Defense Logistics Agency (DLA). Academia, Committee on Foreign Investment United States (CFIUS), supply chain resiliency, and supply chain risk management.

NOTE – NSIB is defined as the American network of knowledge, capabilities, and people—including academia, National Laboratories, and the private sector—that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life (2017 National Security Strategy). It is broader than the DIB, but feeds into the DIB and the supply chain.

Guidance

- US Code
- SCRM Policies
- Joint Doctrine
- FAR
- NDAA
- NSS
- NDS
- Executive Orders
- Congressional Committees

Approach

Taxonomy

Framework

Governance

End State

Phase One

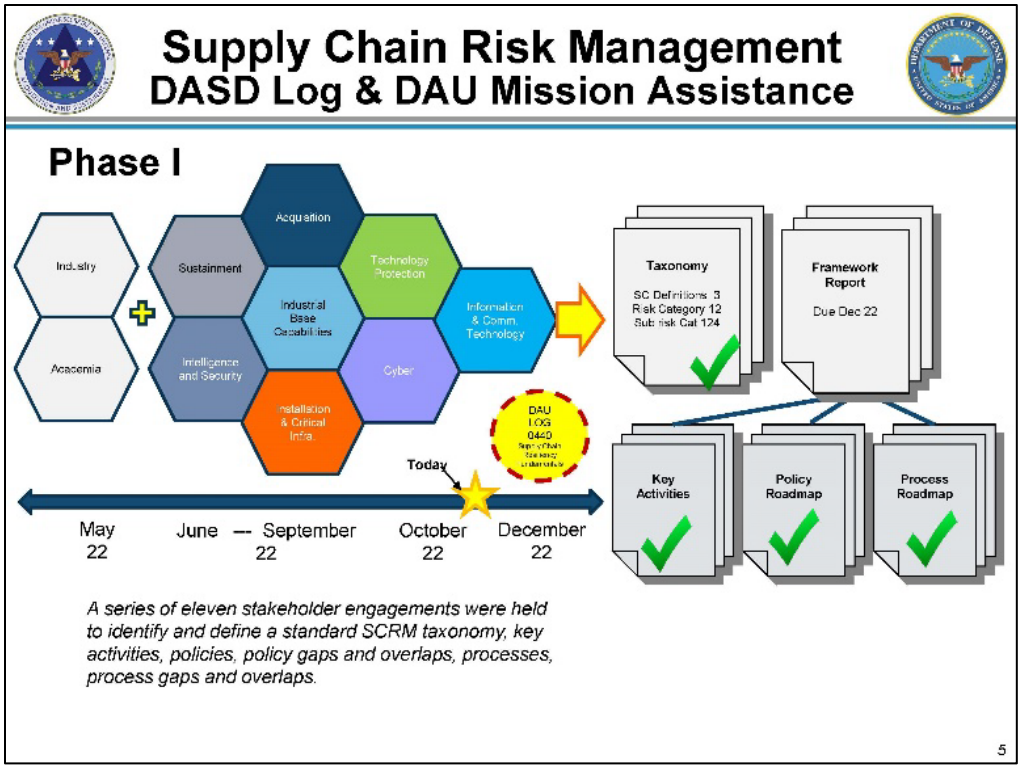
- Develop supply chain eco-system and **SCRM framework**
- Develop initial enterprise **taxonomy**
- **Leverage best practices**, pilots, or other efforts already in process
- Develop/update appropriate **policies**
- Identify **process gaps**
- Interim policy guidance as appropriate

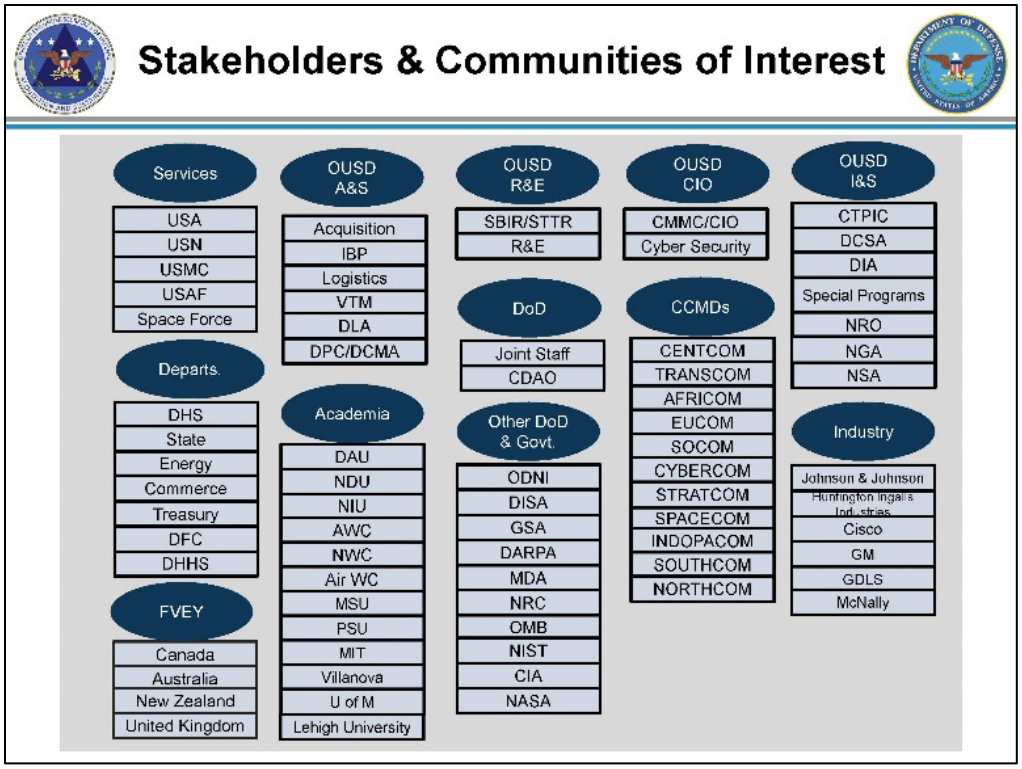
Phase Two

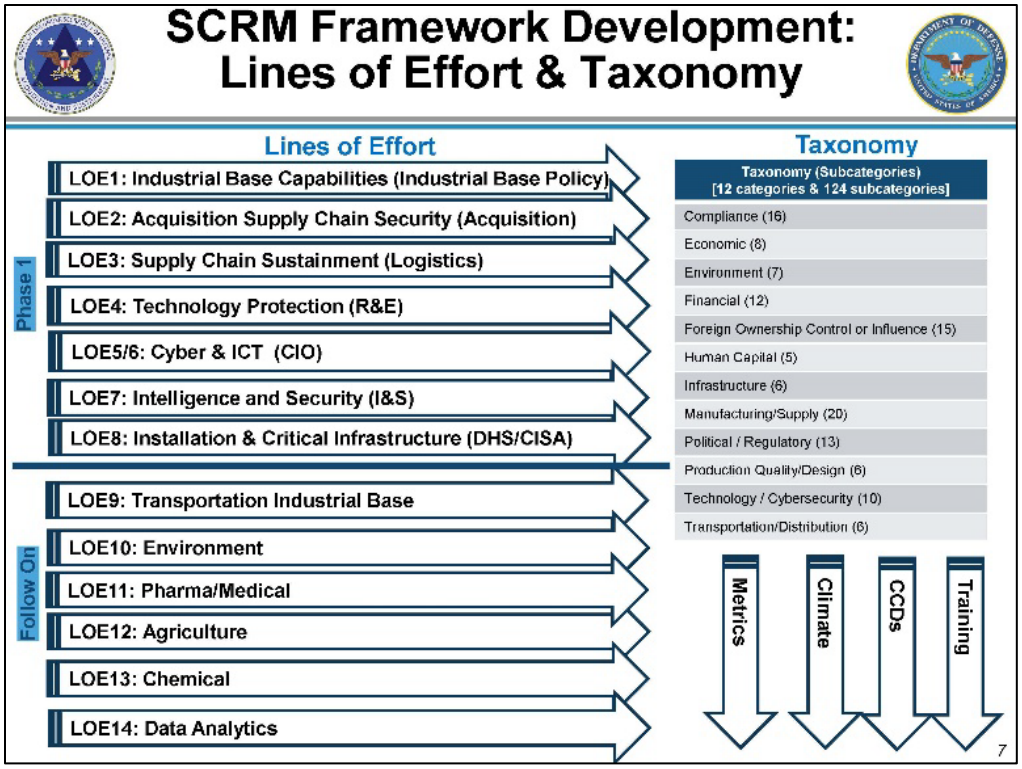
- Develop scalable resource model
- Establish DoD SCRM **organizational structure, governance & oversight**
- Create training & curriculum roadmap
- Enable efficiencies, **cross-organization collaboration**, and consistent data analysis.
- Integrate **additional LOEs** (climate, transportation)
- Organization replication at echelon

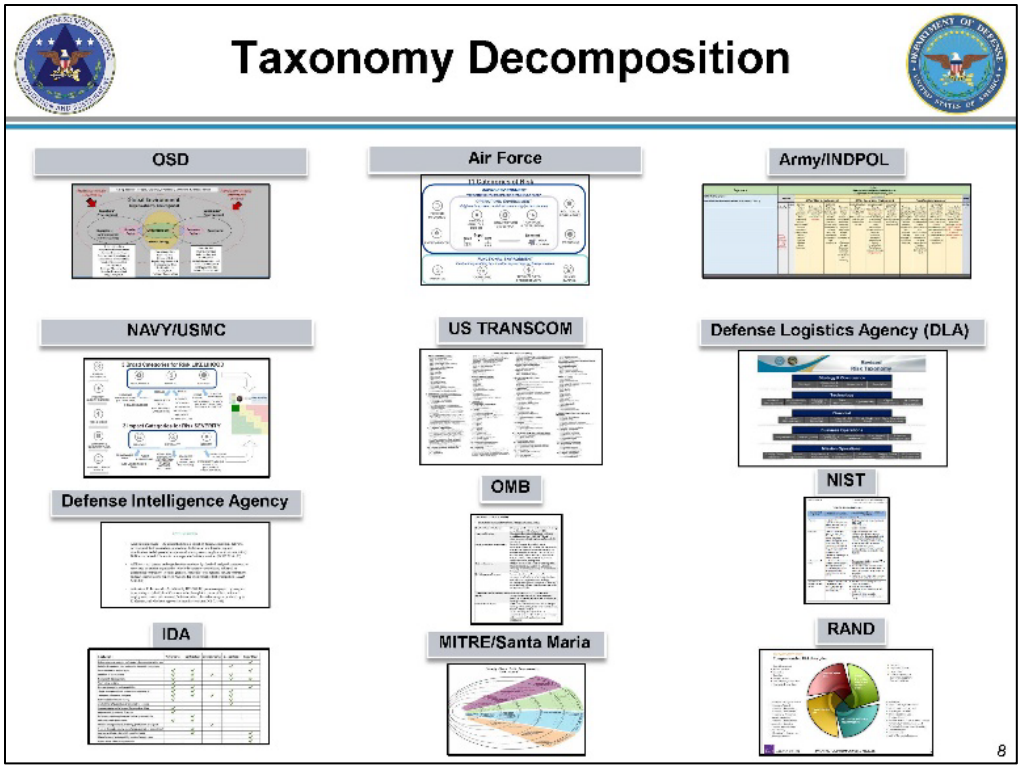
1Q22	2Q22	3Q22	4Q22/1Q23	1Q23
Draft Taxonomy and Framework	Phase One Project Scope	Working Group Sessions	Phase One Completion	Phase Two Project Scope

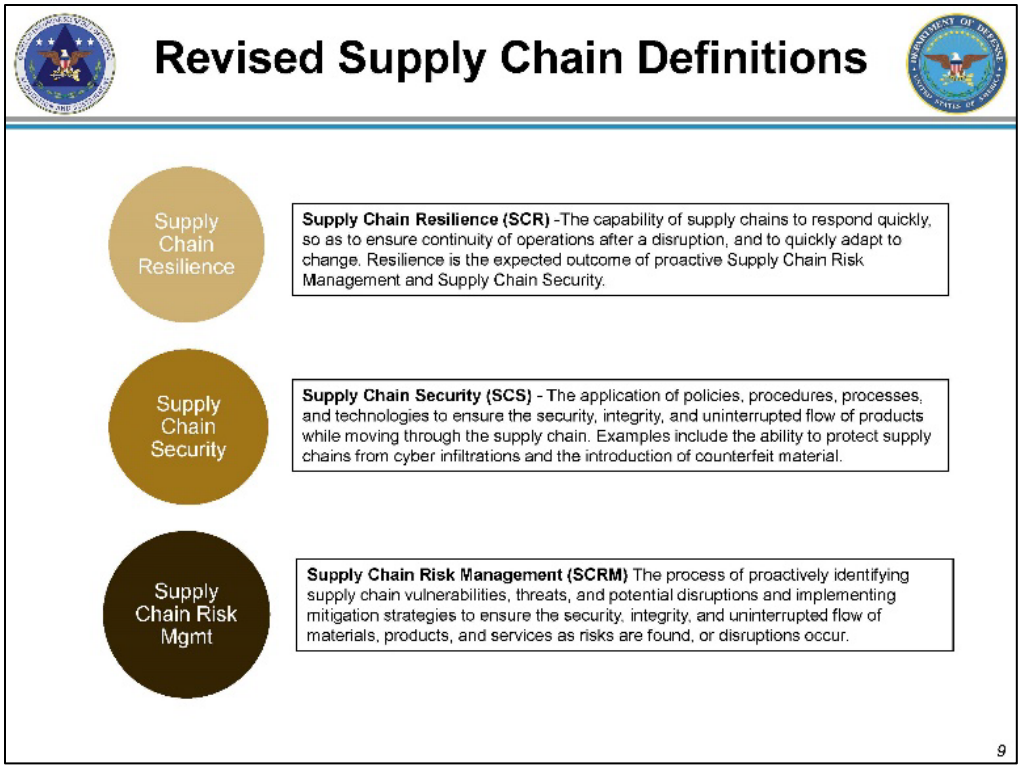
4

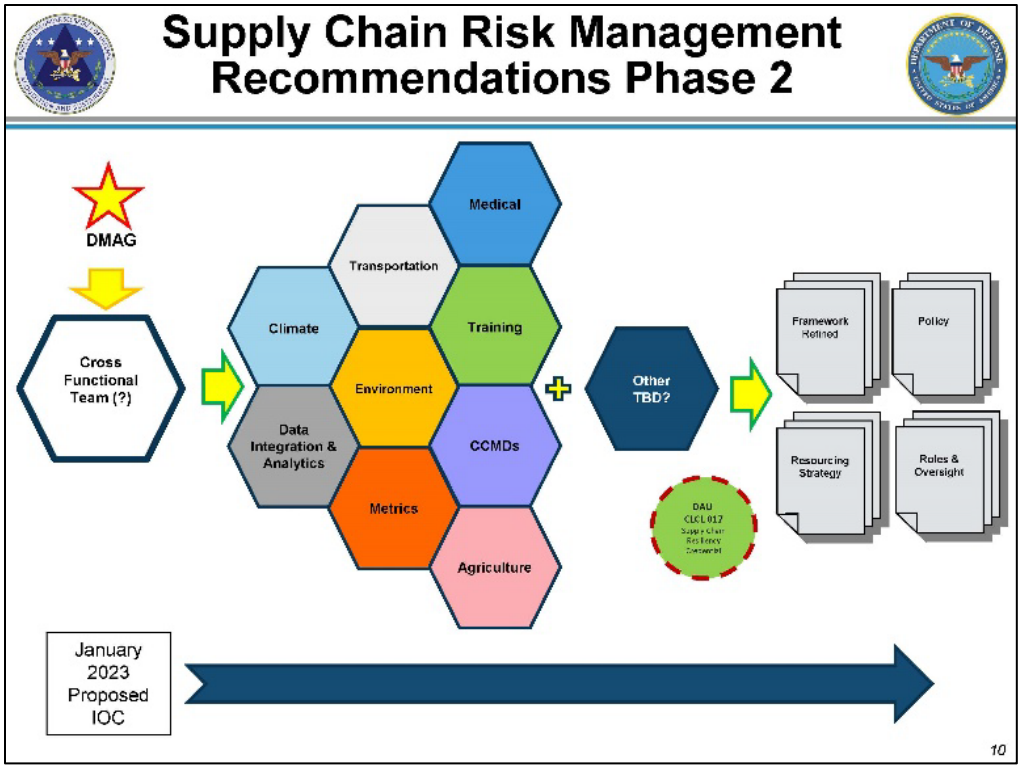

Supply Chain Risk Management
DASD Log & DAU Mission Assistance
Phase I
Industry
Academia
Acquisition
Sustainment
Technology Protection
Industrial Base Capabilities
Information & Comm. Technology
Intelligence and Security
Cyber
Installation & Critical Infra.
DAU LOG 0440
Today
May 22
June — September 22
October 22
December 22
Taxonomy
SC Definitions: 3
Risk Category 12
Sub risk Cat 124
Framework Report
Due Dec 22
Key Activities
Policy Roadmap
Process Roadmap
A series of eleven stakeholder engagements were held to identify and define a standard SCRM taxonomy, key activities, policies, policy gaps and overlaps, processes, process gaps and overlaps.
5

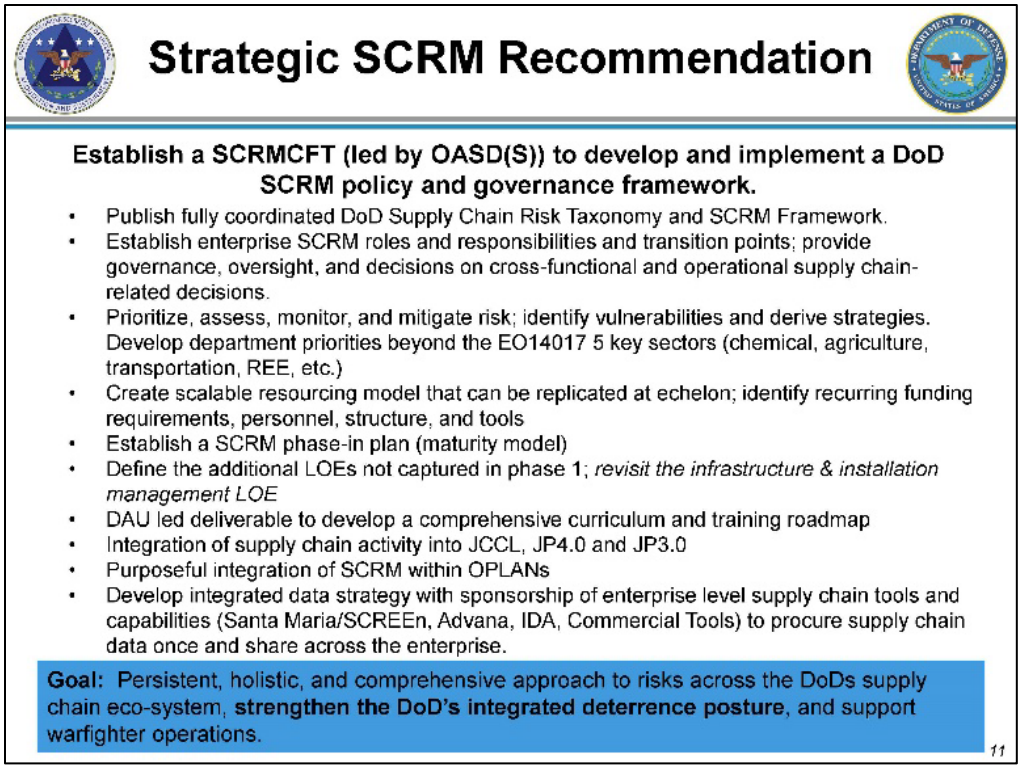

Stakeholders & Communities of Interest
Services
USA
USN
USMC
USAF
Space Force
Departs.
DHS
State
Energy
Commerce
Treasury
DFC
DHHS
FVEY
Canada
Australia
New Zealand
United Kingdom
OUSD A&S
Acquisition
IBP
Logistics
VTM
DLA
DPC/DCMA
Academia
DAU
NDU
NIU
AWC
NWC
Air WC
MSU
PSU
MIT
Villanova
U of M
Lehigh University
OUSD R&E
SBIR/STTR
R&E
DoD
Joint Staff
CDAO
Other DoD & Govt.
ODNI
DISA
GSA
DARPA
MDA
NRC
OMB
NIST
CIA
NASA
OUSD CIO
CMMC/CIO
Cyber Security
CCMDs
CENTCOM
TRANSCOM
AFRICOM
EUCOM
SOCOM
CYBERCOM
STRATCOM
SPACECOM
INDOPACOM
SOUTHCOM
NORTHCOM
OUSD I&S
CTPIC
DCSA
DIA
Special Programs
NRO
NGA
NSA
Industry
Johnson & Johnson
Huntington Ingalls Industries
Cisco
GM
GDLS
McNally

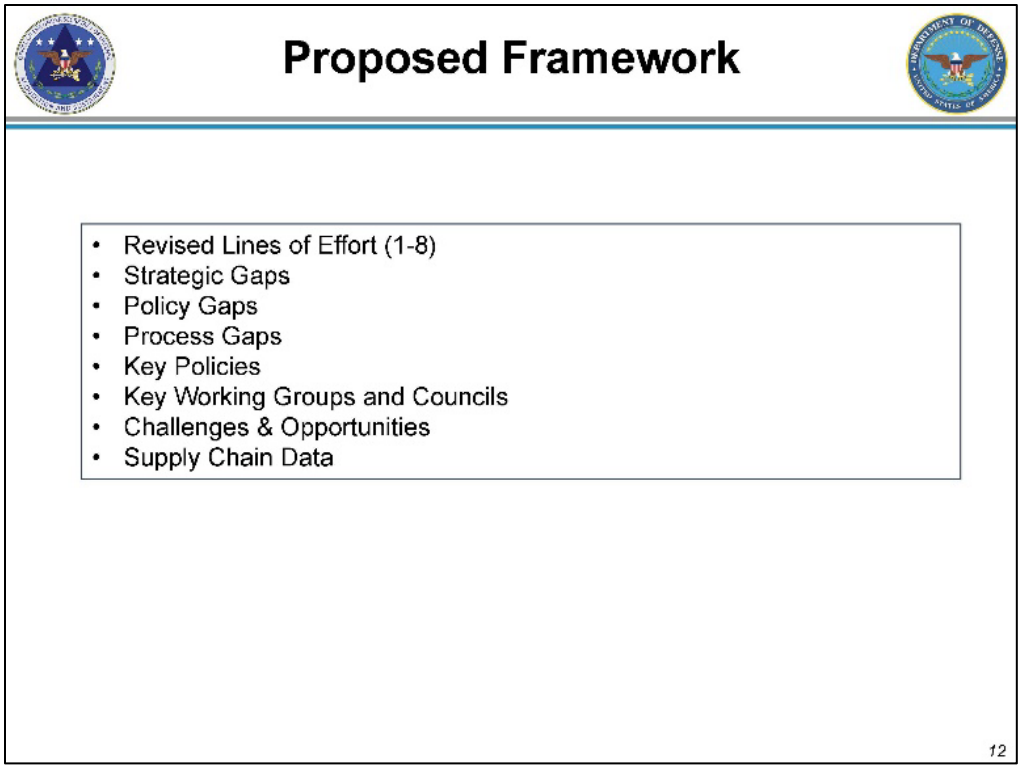

SCRM Framework Development:
Lines of Effort & Taxonomy
Lines of Effort
Taxonomy
Phase 1
LOE1: Industrial Base Capabilities (Industrial Base Policy)
LOE2: Acquisition Supply Chain Security (Acquisition)
LOE3: Supply Chain Sustainment (Logistics)
LOE4: Technology Protection (R&E)
LOE5/6: Cyber & ICT (CIO)
LOE7: Intelligence and Security (I&S)
LOE8: Installation & Critical Infrastructure (DHS/CISA)
Follow On
LOE9: Transportation Industrial Base
LOE10: Environment
LOE11: Pharma/Medical
LOE12: Agriculture
LOE13: Chemical
LOE14: Data Analytics
Taxonomy (Subcategories)
[12 categories & 124 subcategories]
Compliance (16)
Economic (8)
Environment (7)
Financial (12)
Foreign Ownership Control or Influence (15)
Human Capital (5)
Infrastructure (6)
Manufacturing/Supply (20)
Political / Regulatory (13)
Production Quality/Design (6)
Technology / Cybersecurity (10)
Transportation/Distribution (6)
Metrics
Climate
CCDs
Training
7


Taxonomy Decomposition
OSD
Air Force
Army/INDPOL
NAVY/USMC
US TRANSCOM
Defense Logistics Agency (DLA)
OMB
NIST
Defense Intelligence Agency
IDA
MITRE/Santa Maria
RAND
8


Revised Supply Chain Definitions
Supply Chain Resilience
Supply Chain Resilience (SCR) -The capability of supply chains to respond quickly, so as to ensure continuity of operations after a disruption, and to quickly adapt to change. Resilience is the expected outcome of proactive Supply Chain Risk Management and Supply Chain Security.
Supply Chain Security
Supply Chain Security (SCS) - The application of policies, procedures, processes, and technologies to ensure the security, integrity, and uninterrupted flow of products while moving through the supply chain. Examples include the ability to protect supply chains from cyber infiltrations and the introduction of counterfeit material.
Supply Chain Risk Mgmt
Supply Chain Risk Management (SCRM) The process of proactively identifying supply chain vulnerabilities, threats, and potential disruptions and implementing mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services as risks are found, or disruptions occur.
9


Supply Chain Risk Management Recommendations Phase 2
DMAG
Cross Functional Team (?)
Medical
Transportation
Climate
Training
Environment
Data Integration & Analytics
CCMDs
Metrics
Agriculture
Other TBD?
Framework Refined
Policy
Resourcing Strategy
Roles & Oversight
DAU
January 2023 Proposed IOC
10


Strategic SCRM Recommendation
Establish a SCRMCFT (led by OASD(S)) to develop and implement a DoD SCRM policy and governance framework.
• Publish fully coordinated DoD Supply Chain Risk Taxonomy and SCRM Framework.
• Establish enterprise SCRM roles and responsibilities and transition points; provide governance, oversight, and decisions on cross-functional and operational supply chain-related decisions.
• Prioritize, assess, monitor, and mitigate risk; identify vulnerabilities and derive strategies. Develop department priorities beyond the EO14017 5 key sectors (chemical, agriculture, transportation, REE, etc.)
• Create scalable resourcing model that can be replicated at echelon; identify recurring funding requirements, personnel, structure, and tools
• Establish a SCRM phase-in plan (maturity model)
• Define the additional LOEs not captured in phase 1; *revisit the infrastructure & installation management LOE*
• DAU led deliverable to develop a comprehensive curriculum and training roadmap
• Integration of supply chain activity into JCCL, JP4.0 and JP3.0
• Purposeful integration of SCRM within OPLANs
• Develop integrated data strategy with sponsorship of enterprise level supply chain tools and capabilities (Santa Maria/SCREEn, Advana, IDA, Commercial Tools) to procure supply chain data once and share across the enterprise.
Goal: Persistent, holistic, and comprehensive approach to risks across the DoDs supply chain eco-system, strengthen the DoD's integrated deterrence posture, and support warfighter operations.
11


Proposed Framework
• Revised Lines of Effort (1-8)
• Strategic Gaps
• Policy Gaps
• Process Gaps
• Key Policies
• Key Working Groups and Councils
• Challenges & Opportunities
• Supply Chain Data
12

Operational Lines of Effort

LOE1: Industrial Base Capabilities (Industrial Base Policy)

- Leverage industrial base analyses by sector, to identify capacity and resiliency, to meet DoD requirements; develop data and the applications needed to conduct robust industrial analysis
- Develop assessments of future industrial base capabilities; make investments to close gaps in defense capacity and capabilities and create and sustain reliable sources of supply
- Organize engagements with industrial base
- Conduct international engagement efforts including government-to-government dialogue with allies and partners on joint industrial base concerns and areas of potential collaboration
- Coordinate within the department to identify priority areas and develop mitigation strategies; leverage appropriate authorities.
- Collaborate with interagency partners to identify, mitigate, and monitor risks and issues across the Industrial base.
- Develop programs to increase participation of small, and medium, companies in the industrial base; maximize opportunities to ensure that the nation's small businesses remain responsive, resilient, secure, and diversified
- Inform the Committee on Foreign Investment in the United States (CFIUS) on national security concerns.
- Develop DoD policy and provide guidance, oversight, and technical assistance on assessing, or investing, in defense industrial capabilities to senior leadership.
- Coordinate with components on any proposal to use U.S. Government funds to preserve industrial capability
- Establishing workforce development programs to meet the skilled workforce needs of the DIB

13

Operational Lines of Effort

LOE2: Acquisition Supply Chain Security (Acquisition)

- Establish procurement policies, procedures, authorities, and guidance to mitigate supply chain risks; advocate for, and enable, DoD authority to waive requirements for accepting risk, when applicable
- Update / review contracting terms to support supply chain security to include information sharing and risk reduction strategies for the supply chain. In coordination with DoD Components, strengthen DFARS SCRM related clauses and other related acquisition guidance and policy
- Ensure compliance of supply chain dependability and financial reliability to include; Buy American Act, financial responsibility, criminality, FOCI, and subcontracts. Partner with industry to reduce supply chain risk across all sub-tiers in supply chain.
- Support supply quality and reliability, counterfeit/nonconformance, obsolescence, inspection, warranty, and safety related DFARS provisions/clauses
- Provide authority to the DHS, DoD, and the ODNI to issue exclusion orders, upon the recommendation of the FASC. These orders are issued to protect national security by excluding certain covered products, services, or sources from the Federal supply chain
- Establish policy, and assign responsibilities, to support the identification of beneficial ownership, and assessment and mitigation of foreign ownership, control, or influence (FOCI) of covered contractors and subcontractors to enhance supply chain resilience
- Improve supply chain security and protection efforts across all phases of acquisition, development, production, and sustainment; develop appropriate transition guidance and resourcing strategies for supply chain management of programs in sustainment
- Establish policies and procedures that address vendor supply chain threats and enable mitigation of risk associated with commercial support to DoD operations outside of the United States. Implement acquisition authorities that enable termination and restriction of vendors that pose a significant threat to US missions and forces
- Provide technology and cyber support to electronics and digital technologies supply chains, cyber and cloud standards, incident reporting, 3252 exclusionary authorities, S/W Maintenance and Patents/Tech Data. Ensure cyber standard compliance of the NIST 800.171 standards for information protection and cyber standards across the DIB
- Identify cyber vulnerabilities in our S/W supply chain through DIB reporting/testing and threat assessment when source code has been exposed to foreign governments. Establish and enhance cyber policies and procedures around weapon/control systems

14

Operational Lines of Effort (*cont.*)

LOE3: Supply Chain Sustainment (Logistics)

- Develop and implement supply chain risk management (SCRM) policies in coordination with the Under Secretary of Defense for Research and Engineering (USD(R&E)).
- Assist with the supply chain illumination and resolution of high visibility SCRM for enterprise level supply chain issues
- Develop and implement Diminishing Manufacturing Sources and Material Shortages (DMSMS) and Counterfeit Prevention Policies within the DoD to enhance supply chain resilience
- Develop and implement DoD materiel management and disposition policies; monitor the overall effectiveness and efficiency of the DoD materiel management systems and continually develop improvements
- Collect and monitor enterprise-wide supply chain performance metrics (e.g., customer wait time, non-mission capable rates, procurement lead-time)
- Review life cycle sustainment plans for major weapon system acquisitions (e.g., F-35); develops requirements for addressing SCRM within LCSPs
- Regular engagement, and ownership of, SCRM related audits and congressional inquiries
- Assess, monitor and mitigate vendor supply chain threats in support of COCOMs as part of Vendor Threat Mitigation (VTM) requirements
- Monitor and assess risk and the performance of organic industrial base and transportation industrial base to enhance supply chain resilience

15

Functional Lines of Effort

LOE4: Technology Protection (R&E)

- Serve as a collaboration hub and the DoD focal point for coordination, operational information-sharing, partnering proposals and assessments of supply chain risk related to technology protection
- Assess technology protection efforts, identify best practices, develop innovative methodologies, and propose concepts and tools for operational fielding, and make recommendations for supply chain security policy changes, that can be leveraged across the DoD security and intelligence enterprises, federal government, private sector, and academia
- Conduct continuous discovery of supply chains for indicators of risks to/from individual suppliers; provide timely and accurate assessments across the technology protection portfolio (Department and DIB partners, NSIB - PJL)
- Synchronize efforts across the DoD to create and support standard reporting thresholds of information that are needed in the application of security and protection activities of the supply chain
- Assess threats to the supply chain and how to make classified/CUI info/threat assessments available to the enterprise; optimize the use of data to improve mission and business effectiveness
- Address manufacturing needs of critical technology & acquisition system; develop and enhance technologies and manufacturing capabilities that are independent of sole source suppliers (PJL), prohibited suppliers, and potential adversarial nations to enhance supply chain resilience
- Build DoD and DIB advanced manufacturing workforce capabilities and capacity through systems analysis, design, and key investments in foundational and enabling capabilities
- Work with DCSA and other relevant stakeholders to ensure secure transfer of technologies within the supply chain throughout the acquisition process
- Ensure sustainability is considered as part of technology development

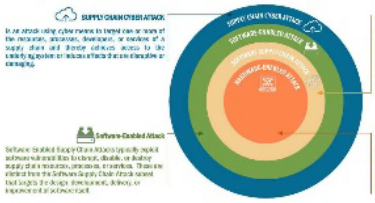
16

Functional Lines of Effort

***LOE5/6: Cyber & ICT (CIO)**

- Protect DOD network supply chains, issue policy for the protection of contractor networks and DOD systems
- Conduct and maintain CSCRM assessments and evaluations; responsible for advisories and coordination across the enterprise (IC-SCR). Conduct continuous discovery of dynamic supply chains for indicators of risks to/from individual suppliers
- Implementation of congressional requirements and lead for interagency coordination of cyber and ICT related supply chain equities or related activities
- Collaborate with enterprise stakeholders (CFIUS, Team Telecom, CMMC. DIB CS Program); share information (classified and unclassified) across the enterprise
- Lead cyber focused supply chain tool pilots, perform threat assessments of vendors, and conduct supply chain illuminations/deep dives. Provide assessment and analysis support to the Department in order to communicate strategic risk
- Establish and maintain an operational Cyber/ ICT SCRM program to enable acquisition risk owners to identify, assess, and manage Cyber/ICT supply chain risks.
- Establish basic Cyber/ICT supply chain risk due diligence capabilities for decision support and continual monitoring of suppliers for high-interest commodity Cyber/ ICT and critical acquisitions
- Co-chairs SMWG meetings- Principal to Federal Acquisition Security Council; participate in DSAWG/ISRMC
- Inform cyber security architecture SCRM section
- In coordination with Services and components, establish Cyber/ICT-SCRM metrics for the enterprise
- Inform cyber security architecture SCRM section

**LOE 5 & 6 combined*



17

Functional Lines of Effort

LOE7: Intelligence and Security (I&S)

- Understand the complex connections and dependencies across intelligence/CI organizations; improve WOG collaboration and develop communication/reporting processes
- Conduct supply chain threat and vulnerability assessments; recommend countermeasures and mitigating strategies
- Update policies, standard forms, and Systems Of Record Notification (SORN) to facilitate the collection, usage, storage, and sharing of information-PII related in support of acquisition, contracting, and supply chain monitoring
- Enhance the nation's supply chain and cyber security, leveraging multidisciplinary counterintelligence and security expertise to inform, guide, and coordinate integrated risk decisions and responses with strategic partners
- Secure US critical supply chains from foreign influence attempts to compromise the integrity, trustworthiness and authenticity of products and services; assess and mitigate the activities of foreign influence enterprise and other adversarial attempts aimed at compromising the global network of pathways-supply chains that provide mission-critical products, materials and services
- In coordination with R&E and CIO, develop policies, programs, and systems to safeguard critical technologies throughout the supply chain

18

Functional Lines of Effort

LOE8: Installation & Critical Infrastructure (DHS/CISA)

- Conduct supply chain threat and vulnerability assessments; recommend countermeasures and mitigation strategies
- Assess physical and digital risks associated with installations and critical infrastructure supply chains
- Perform mission analysis to identify components that can impact supply chain related missions, essential tasks and functions
- Continuously monitor real estate encroachment (in proximity to installations and key infrastructures)
- Implement SCRM strategies for military construction projects during the design phase
- Provide help to private sector owners and operators (state and local) to secure their supply chains in support of mission readiness
- Conduct vulnerability assessments and Identify alternative means of fulfilling the mission if key supply chains are disrupted; ensure Mission Assurance plans are in place and exercised regularly
- Share supply chain risks and threats across the enterprise

cisa.gov

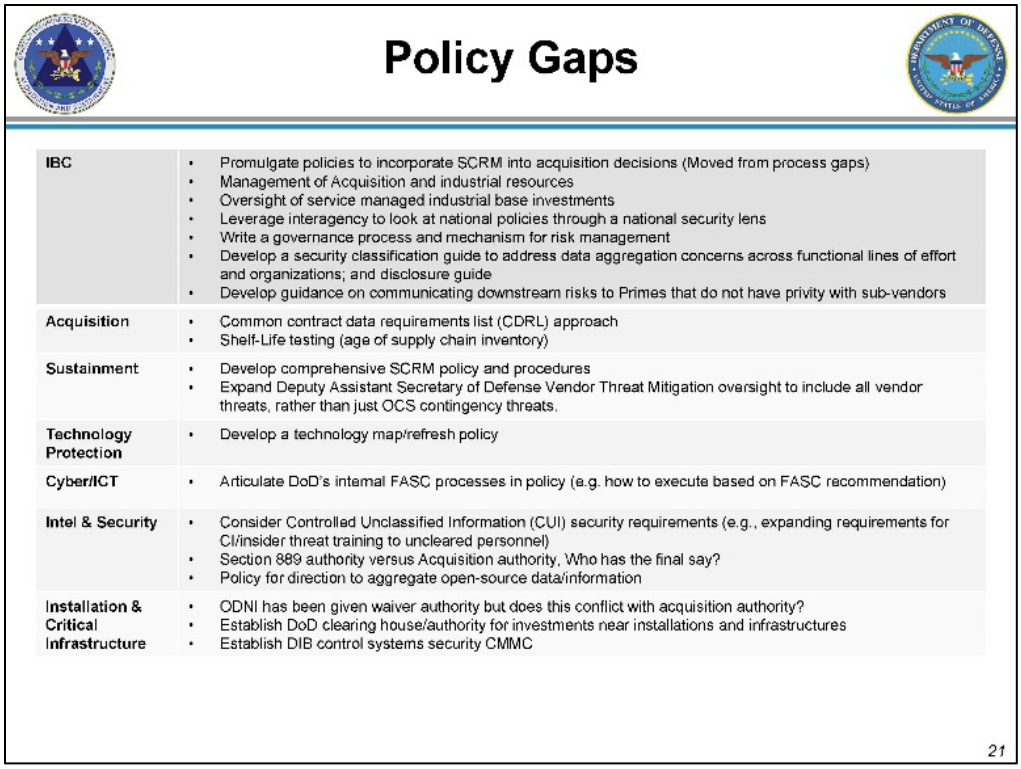
19

Strategic Gaps

Goal: Persistent, holistic, and comprehensive approach to risks across the DoDs supply chain eco-system, **strengthen the DoD's integrated deterrence posture**, and support warfighter operations.

- Establish common risk taxonomy and definitions to serve as the underpinning of a Department SCRM framework
- Increase end-to-end transparency and knowledge of DOD's multi-tier supply chain ecosystem(s)
- Develop a comprehensive industrial base resiliency strategy with proactive assessment of vulnerabilities. Establish vulnerability planning exercises from which mitigation strategies can be derived
- Resource and maintain enterprise level supply chain eco-system maps, supplier insight, risk scores, and continuous monitoring to identify systemic risks to DoD
- Establish a DoD supply chain risk strategy
- Resolve gaps in coordination with roles and responsibilities
- Create a DoD governance and oversight structure that can be replicated at echelon

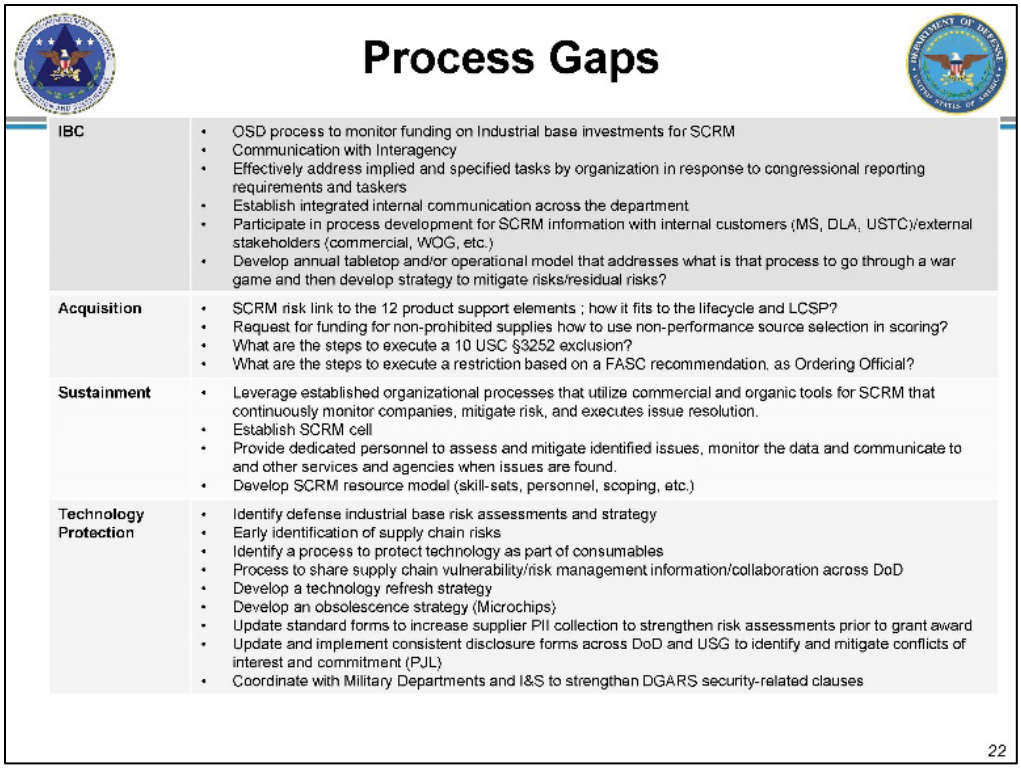
20



Policy Gaps

IBC	• Promulgate policies to incorporate SCRM into acquisition decisions (Moved from process gaps) • Management of Acquisition and industrial resources • Oversight of service managed industrial base investments • Leverage interagency to look at national policies through a national security lens • Write a governance process and mechanism for risk management • Develop a security classification guide to address data aggregation concerns across functional lines of effort and organizations; and disclosure guide • Develop guidance on communicating downstream risks to Primes that do not have privity with sub-vendors
Acquisition	• Common contract data requirements list (CDRL) approach • Shelf-Life testing (age of supply chain inventory)
Sustainment	• Develop comprehensive SCRM policy and procedures • Expand Deputy Assistant Secretary of Defense Vendor Threat Mitigation oversight to include all vendor threats, rather than just OCS contingency threats.
Technology Protection	• Develop a technology map/refresh policy
Cyber/ICT	• Articulate DoD's internal FASC processes in policy (e.g. how to execute based on FASC recommendation)
Intel & Security	• Consider Controlled Unclassified Information (CUI) security requirements (e.g., expanding requirements for CI/insider threat training to uncleared personnel) • Section 889 authority versus Acquisition authority, Who has the final say? • Policy for direction to aggregate open-source data/information
Installation & Critical Infrastructure	• ODNI has been given waiver authority but does this conflict with acquisition authority? • Establish DoD clearing house/authority for investments near installations and infrastructures • Establish DIB control systems security CMMC

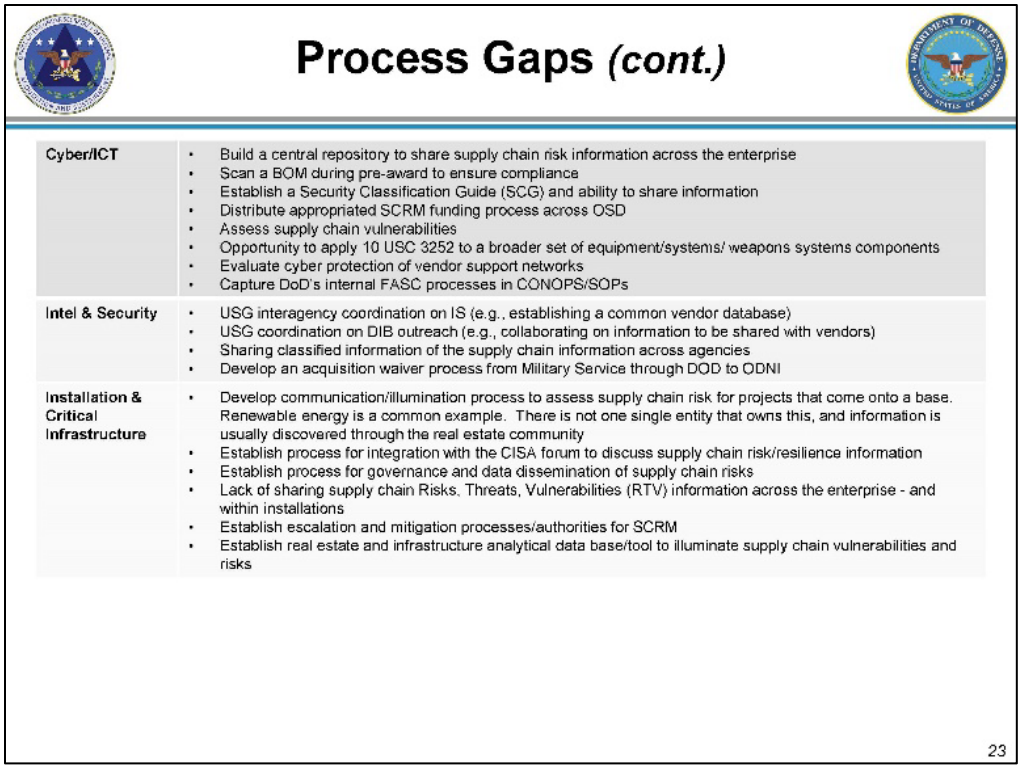
21



Process Gaps

IBC	• OSD process to monitor funding on Industrial base investments for SCRM • Communication with Interagency • Effectively address implied and specified tasks by organization in response to congressional reporting requirements and taskers • Establish integrated internal communication across the department • Participate in process development for SCRM information with internal customers (MS, DLA, USTC)/external stakeholders (commercial, WOG, etc.) • Develop annual tabletop and/or operational model that addresses what is that process to go through a war game and then develop strategy to mitigate risks/residual risks?
Acquisition	• SCRM risk link to the 12 product support elements ; how it fits to the lifecycle and LCSP? • Request for funding for non-prohibited supplies how to use non-performance source selection in scoring? • What are the steps to execute a 10 USC §3252 exclusion? • What are the steps to execute a restriction based on a FASC recommendation. as Ordering Official?
Sustainment	• Leverage established organizational processes that utilize commercial and organic tools for SCRM that continuously monitor companies, mitigate risk, and executes issue resolution. • Establish SCRM cell • Provide dedicated personnel to assess and mitigate identified issues, monitor the data and communicate to and other services and agencies when issues are found. • Develop SCRM resource model (skill-sets, personnel, scoping, etc.)
Technology Protection	• Identify defense industrial base risk assessments and strategy • Early identification of supply chain risks • Identify a process to protect technology as part of consumables • Process to share supply chain vulnerability/risk management information/collaboration across DoD • Develop a technology refresh strategy • Develop an obsolescence strategy (Microchips) • Update standard forms to increase supplier PII collection to strengthen risk assessments prior to grant award • Update and implement consistent disclosure forms across DoD and USG to identify and mitigate conflicts of interest and commitment (PJL) • Coordinate with Military Departments and I&S to strengthen DGARS security-related clauses

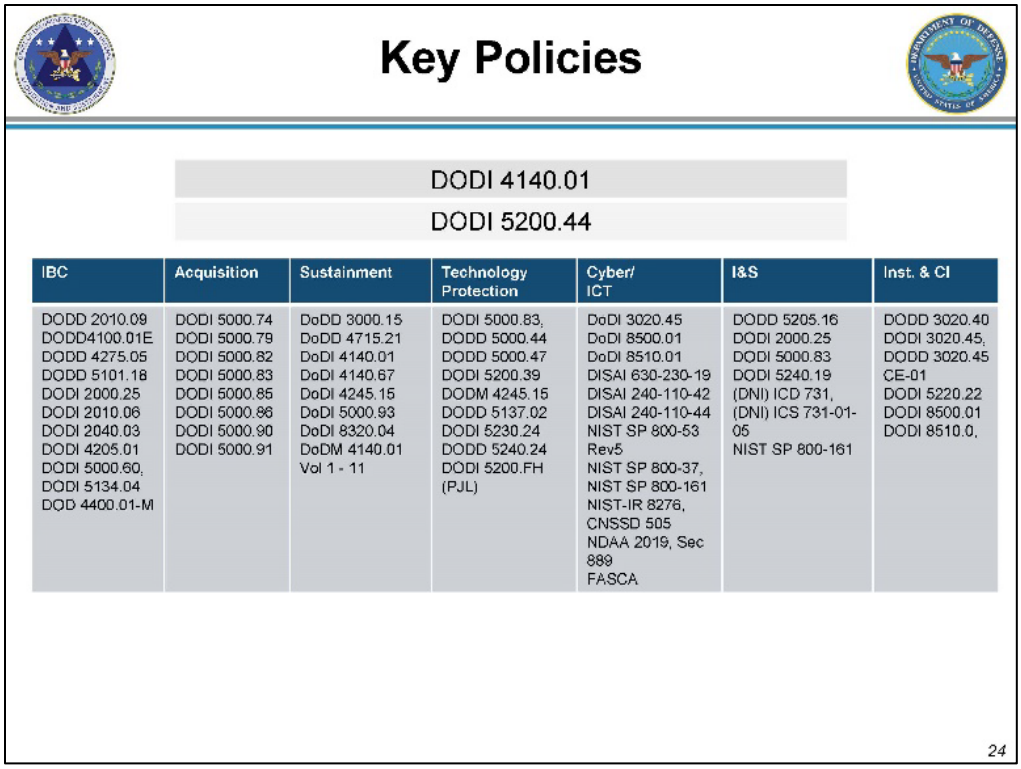
22



Process Gaps *(cont.)*

Cyber/ICT	• Build a central repository to share supply chain risk information across the enterprise • Scan a BOM during pre-award to ensure compliance • Establish a Security Classification Guide (SCG) and ability to share information • Distribute appropriated SCRM funding process across OSD • Assess supply chain vulnerabilities • Opportunity to apply 10 USC 3252 to a broader set of equipment/systems/ weapons systems components • Evaluate cyber protection of vendor support networks • Capture DoD's internal FASC processes in CONOPS/SOPs
Intel & Security	• USG interagency coordination on IS (e.g., establishing a common vendor database) • USG coordination on DIB outreach (e.g., collaborating on information to be shared with vendors) • Sharing classified information of the supply chain information across agencies • Develop an acquisition waiver process from Military Service through DOD to ODNI
Installation & Critical Infrastructure	• Develop communication/illumination process to assess supply chain risk for projects that come onto a base. Renewable energy is a common example. There is not one single entity that owns this, and information is usually discovered through the real estate community • Establish process for integration with the CISA forum to discuss supply chain risk/resilience information • Establish process for governance and data dissemination of supply chain risks • Lack of sharing supply chain Risks, Threats, Vulnerabilities (RTV) information across the enterprise - and within installations • Establish escalation and mitigation processes/authorities for SCRM • Establish real estate and infrastructure analytical data base/tool to illuminate supply chain vulnerabilities and risks

23



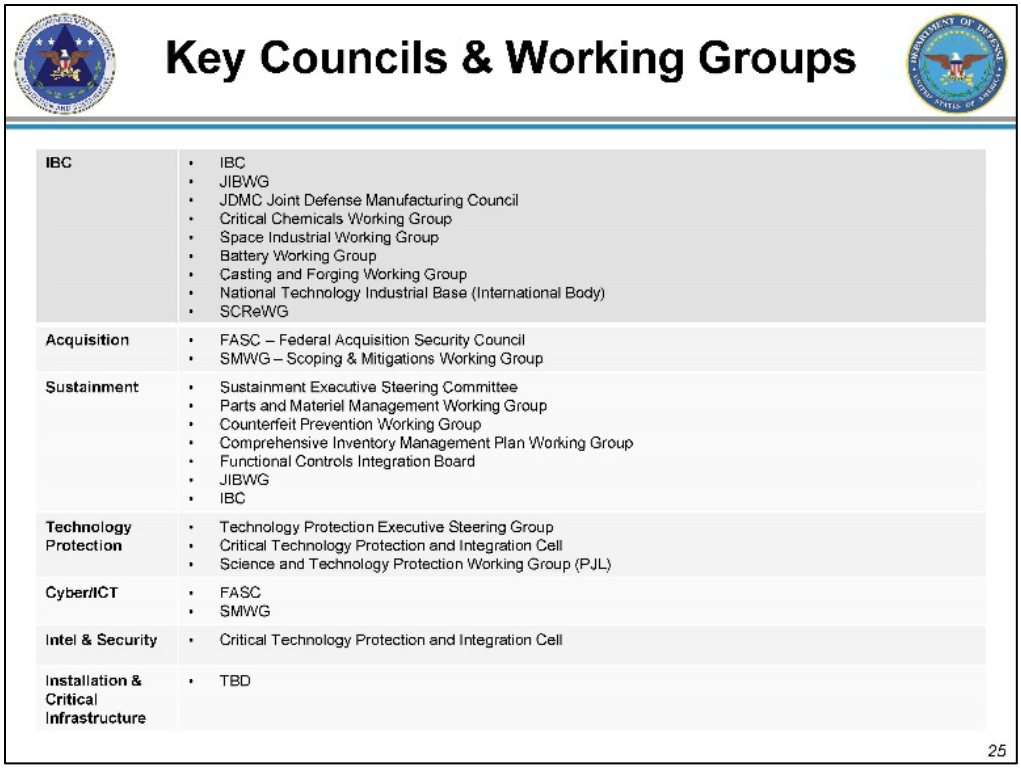
Key Policies

DODI 4140.01

DODI 5200.44

IBC	Acquisition	Sustainment	Technology Protection	Cyber/ ICT	I&S	Inst. & CI
DODD 2010.09 DODD4100.01E DODD 4275.05 DODD 5101.18 DODI 2000.25 DODI 2010.06 DODI 2040.03 DODI 4205.01 DODI 5000.60, DODI 5134.04 DOD 4400.01-M	DODI 5000.74 DODI 5000.79 DODI 5000.82 DODI 5000.83 DODI 5000.85 DODI 5000.86 DODI 5000.90 DODI 5000.91	DoDD 3000.15 DoDD 4715.21 DoDI 4140.01 DoDI 4140.67 DoDI 4245.15 DoDI 5000.93 DoDI 8320.04 DoDM 4140.01 Vol 1 - 11	DODI 5000.83, DODD 5000.44 DODD 5000.47 DODI 5200.39 DODM 4245.15 DODD 5137.02 DODI 5230.24 DODD 5240.24 DODI 5200.FH (PJL)	DoDI 3020.45 DoDI 8500.01 DoDI 8510.01 DISAI 630-230-19 DISAI 240-110-42 DISAI 240-110-44 NIST SP 800-53 Rev5 NIST SP 800-37, NIST SP 800-161 NIST-IR 8276, CNSSD 505 NDAA 2019, Sec 889 FASCA	DODD 5205.16 DODI 2000.25 DODI 5000.83 DODI 5240.19 (DNI) ICD 731, (DNI) ICS 731-01- 05 NIST SP 800-161	DODD 3020.40 DODI 3020.45; DODD 3020.45 CE-01 DODI 5220.22 DODI 8500.01 DODI 8510.0,

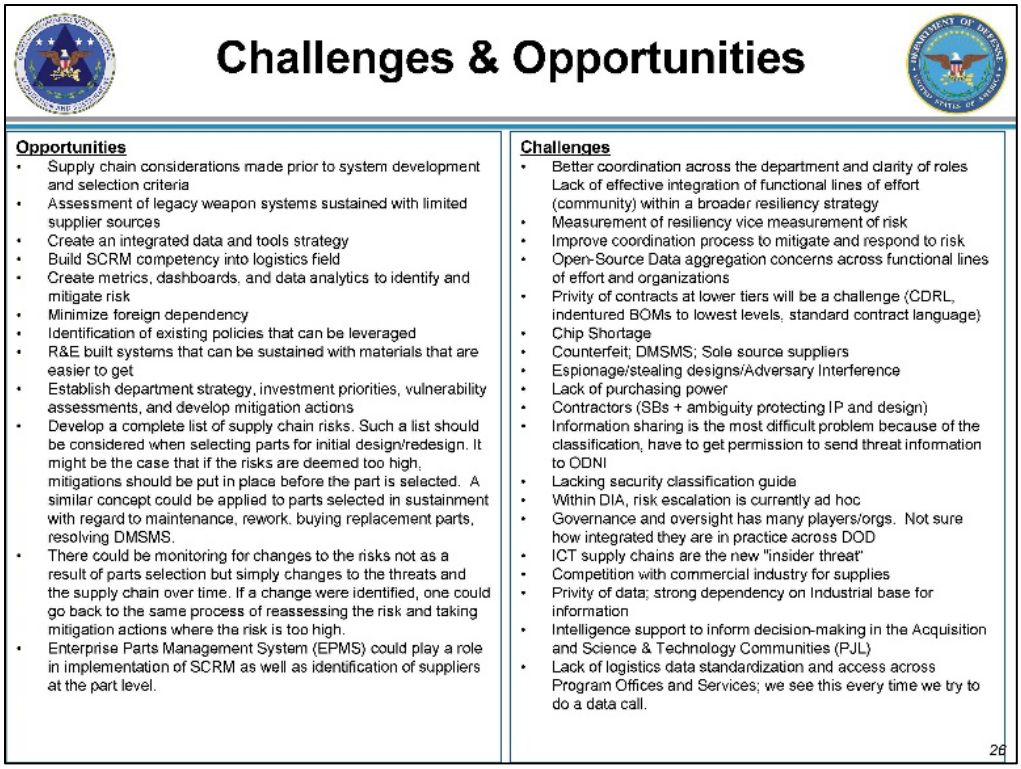
24



Key Councils & Working Groups

IBC	• IBC • JIBWG • JDMC Joint Defense Manufacturing Council • Critical Chemicals Working Group • Space Industrial Working Group • Battery Working Group • Casting and Forging Working Group • National Technology Industrial Base (International Body) • SCReWG
Acquisition	• FASC – Federal Acquisition Security Council • SMWG – Scoping & Mitigations Working Group
Sustainment	• Sustainment Executive Steering Committee • Parts and Materiel Management Working Group • Counterfeit Prevention Working Group • Comprehensive Inventory Management Plan Working Group • Functional Controls Integration Board • JIBWG • IBC
Technology Protection	• Technology Protection Executive Steering Group • Critical Technology Protection and Integration Cell • Science and Technology Protection Working Group (PJL)
Cyber/ICT	• FASC • SMWG
Intel & Security	• Critical Technology Protection and Integration Cell
Installation & Critical Infrastructure	• TBD

25



Challenges & Opportunities

Opportunities

- Supply chain considerations made prior to system development and selection criteria
- Assessment of legacy weapon systems sustained with limited supplier sources
- Create an integrated data and tools strategy
- Build SCRM competency into logistics field
- Create metrics, dashboards, and data analytics to identify and mitigate risk
- Minimize foreign dependency
- Identification of existing policies that can be leveraged
- R&E built systems that can be sustained with materials that are easier to get
- Establish department strategy, investment priorities, vulnerability assessments, and develop mitigation actions
- Develop a complete list of supply chain risks. Such a list should be considered when selecting parts for initial design/redesign. It might be the case that if the risks are deemed too high, mitigations should be put in place before the part is selected. A similar concept could be applied to parts selected in sustainment with regard to maintenance, rework, buying replacement parts, resolving DMSMS.
- There could be monitoring for changes to the risks not as a result of parts selection but simply changes to the threats and the supply chain over time. If a change were identified, one could go back to the same process of reassessing the risk and taking mitigation actions where the risk is too high.
- Enterprise Parts Management System (EPMS) could play a role in implementation of SCRM as well as identification of suppliers at the part level.

Challenges

- Better coordination across the department and clarity of roles Lack of effective integration of functional lines of effort (community) within a broader resiliency strategy
- Measurement of resiliency vice measurement of risk
- Improve coordination process to mitigate and respond to risk
- Open-Source Data aggregation concerns across functional lines of effort and organizations
- Privity of contracts at lower tiers will be a challenge (CDRL, indentured BOMs to lowest levels, standard contract language)
- Chip Shortage
- Counterfeit; DMSMS; Sole source suppliers
- Espionage/stealing designs/Adversary Interference
- Lack of purchasing power
- Contractors (SBs + ambiguity protecting IP and design)
- Information sharing is the most difficult problem because of the classification, have to get permission to send threat information to ODNI
- Lacking security classification guide
- Within DIA, risk escalation is currently ad hoc
- Governance and oversight has many players/orgs. Not sure how integrated they are in practice across DOD
- ICT supply chains are the new "insider threat"
- Competition with commercial industry for supplies
- Privity of data; strong dependency on Industrial base for information
- Intelligence support to inform decision-making in the Acquisition and Science & Technology Communities (PJL)
- Lack of logistics data standardization and access across Program Offices and Services; we see this every time we try to do a data call.

26

Supply Chain Data Integration

Problem Statement: The Department of Defense requires a persistent, holistic, and comprehensive means to assess supply chain risks

- **Unable to identify systemic risks across the Department, across the Defense Industrial Base, across the Services, and across Program Offices**
  - Sharing supply chain illumination data and supplier-risk data provide holistic visibility of vulnerabilities
- **Require a capability for both proactive (persistent, dynamically updated) and reactive (in response to exposures of critical risks) risk assessment**
  - Get "left of buy" with deeper acquisition due diligence
  - Respond to identified vulnerabilities by informing denial/mitigation courses of action
- **No single commercial Supply Chain Risk Management (SCRM) tool adequately responds to all DoD supply chain risk use cases**
  - Diverse risk categories include Compliance, Political/Regulatory, Environment, Economic, Foreign Influence, Cybersecurity, Production Quality, Financial, etc.

Goal: Create a platform to achieve **full spectrum supply chain risk evaluation** with common visibility across DOD

27

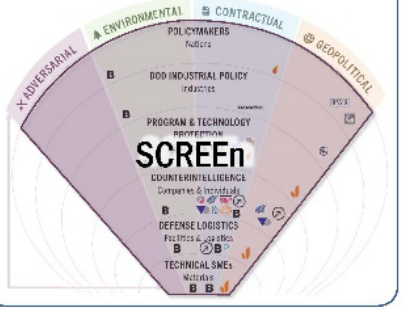
Supply Chain Risk Evaluation Environment (SCREEn)

DoD enterprise SCRM capability

Full Spectrum Risk Identification

Two risk assessment options:

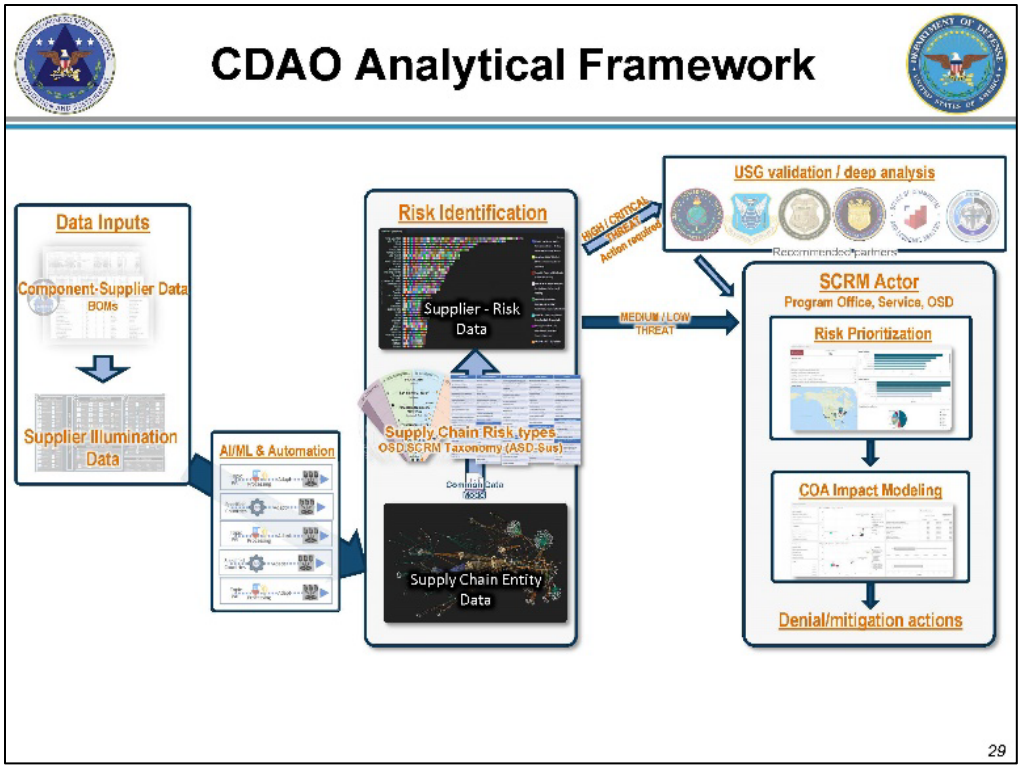
- Raw data analysis
- Commercial vendor analysis

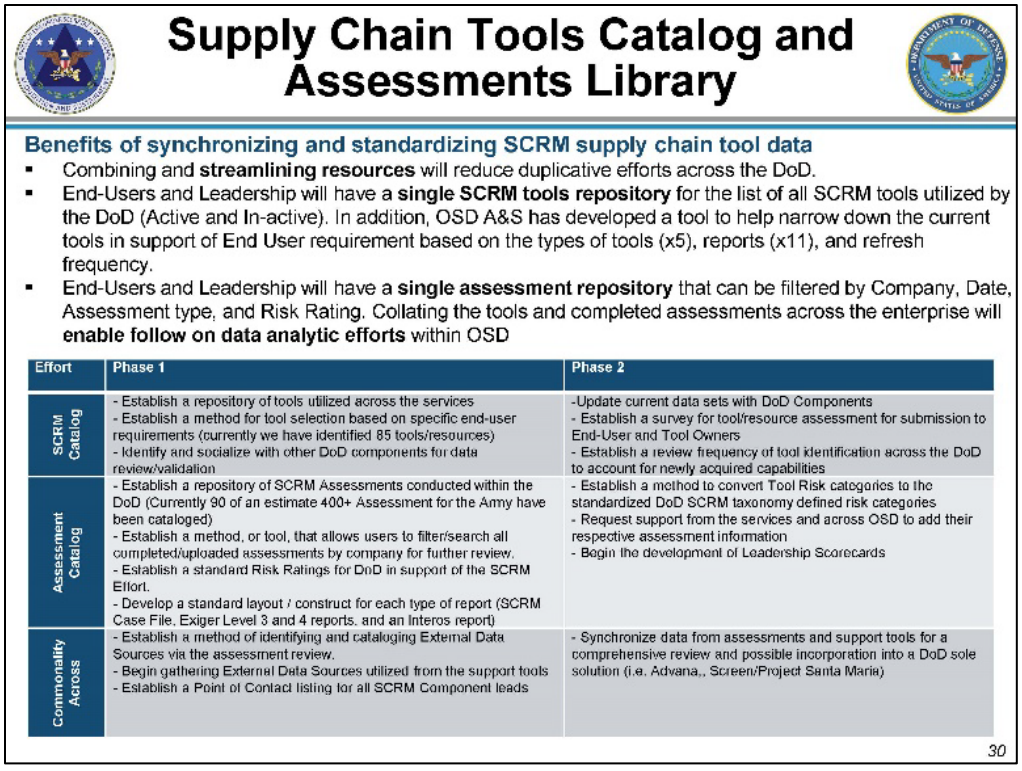


Program Offices, Services, OSD

- Bring Your Own Data (Common Data Models)
- Supply chain risk awareness across POs, Services, OSD
- All levels of classification: IL4/5 (CUI), IL6 (SECRET), JWICS (TOP SECRET)

28

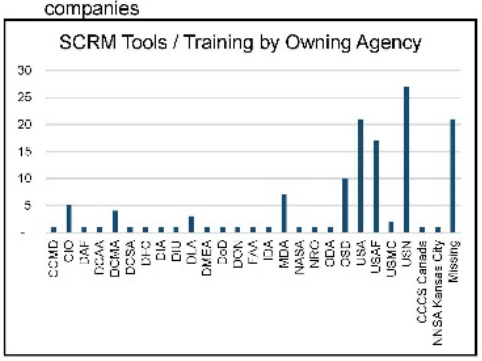

CDAO Analytical Framework
Data Inputs
Component-Supplier Data
BOMs
Supplier Illumination Data
AI/ML & Automation
Risk Identification
Supplier - Risk Data
Supply Chain Risk types
OSD SCRM Taxonomy (ASD:Sus)
Supply Chain Entity Data
HIGH / CRITICAL THREAT
Action Required
USG validation / deep analysis
Recommended partners
MEDIUM / LOW THREAT
SCRM Actor
Program Office, Service, OSD
Risk Prioritization
COA Impact Modeling
Denial/mitigation actions
29

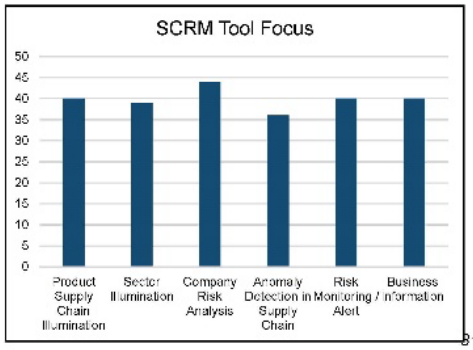

Supply Chain Tools Catalog and Assessments Library
Benefits of synchronizing and standardizing SCRM supply chain tool data
Combining and streamlining resources will reduce duplicative efforts across the DoD.
End-Users and Leadership will have a single SCRM tools repository for the list of all SCRM tools utilized by the DoD (Active and In-active). In addition, OSD A&S has developed a tool to help narrow down the current tools in support of End User requirement based on the types of tools (x5), reports (x11), and refresh frequency.
End-Users and Leadership will have a single assessment repository that can be filtered by Company, Date, Assessment type, and Risk Rating. Collating the tools and completed assessments across the enterprise will enable follow on data analytic efforts within OSD
Effort
Phase 1
Phase 2
SCRM Catalog
- Establish a repository of tools utilized across the services
- Establish a method for tool selection based on specific end-user requirements (currently we have identified 85 tools/resources)
- Identify and socialize with other DoD components for data review/validation
-Update current data sets with DoD Components
- Establish a survey for tool/resource assessment for submission to End-User and Tool Owners
- Establish a review frequency of tool identification across the DoD to account for newly acquired capabilities
Assessment Catalog
- Establish a repository of SCRM Assessments conducted within the DoD (Currently 90 of an estimate 400+ Assessment for the Army have been cataloged)
- Establish a method, or tool, that allows users to filter/search all completed/uploaded assessments by company for further review.
- Establish a standard Risk Ratings for DoD in support of the SCRM Effort.
- Develop a standard layout / construct for each type of report (SCRM Case File, Exiger Level 3 and 4 reports, and an Interos report)
- Establish a method to convert Tool Risk categories to the standardized DoD SCRM taxonomy defined risk categories
- Request support from the services and across OSD to add their respective assessment information
- Begin the development of Leadership Scorecards
Commonality Across
- Establish a method of identifying and cataloging External Data Sources via the assessment review.
- Begin gathering External Data Sources utilized from the support tools
- Establish a Point of Contact listing for all SCRM Component leads
- Synchronize data from assessments and support tools for a comprehensive review and possible incorporation into a DoD sole solution (i.e. Advana., Screen/Project Santa Maria)
30

Supply Chain Tools Status

Supply Chain Tools Catalog

- Utilized data calls conducted by Industrial Base Policy for review and standardization of tools information. Combined/compared multiple data calls from FY21 to FY22
- Established a catalog / repository for SCRM Tools used Agency wide – **86 tools with attribute data collected thus far**
  - Within the components there is an estimated 67 tools/training being utilized (Army: 21, Navy: 27, Air Force: 17, and Marines: 2)
  - Tool/training alignment are COCO: 28, GOCO: 13, and GOGO: 20
- Developed a portal-based repository to house all documentation pertaining to SCRM tools based on off the excel workbook. Working with agency leads to review, update, delete, and upload to the portal site
- Working with agency leads to develop a survey based on the tools for feedback from both end users and companies



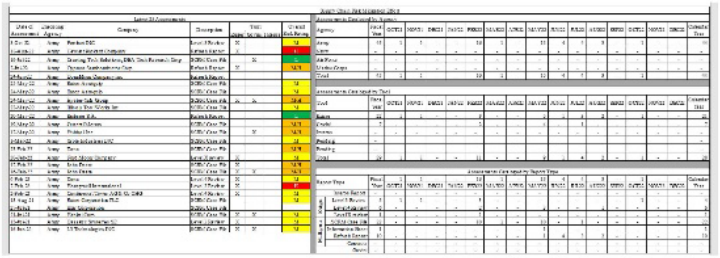


31

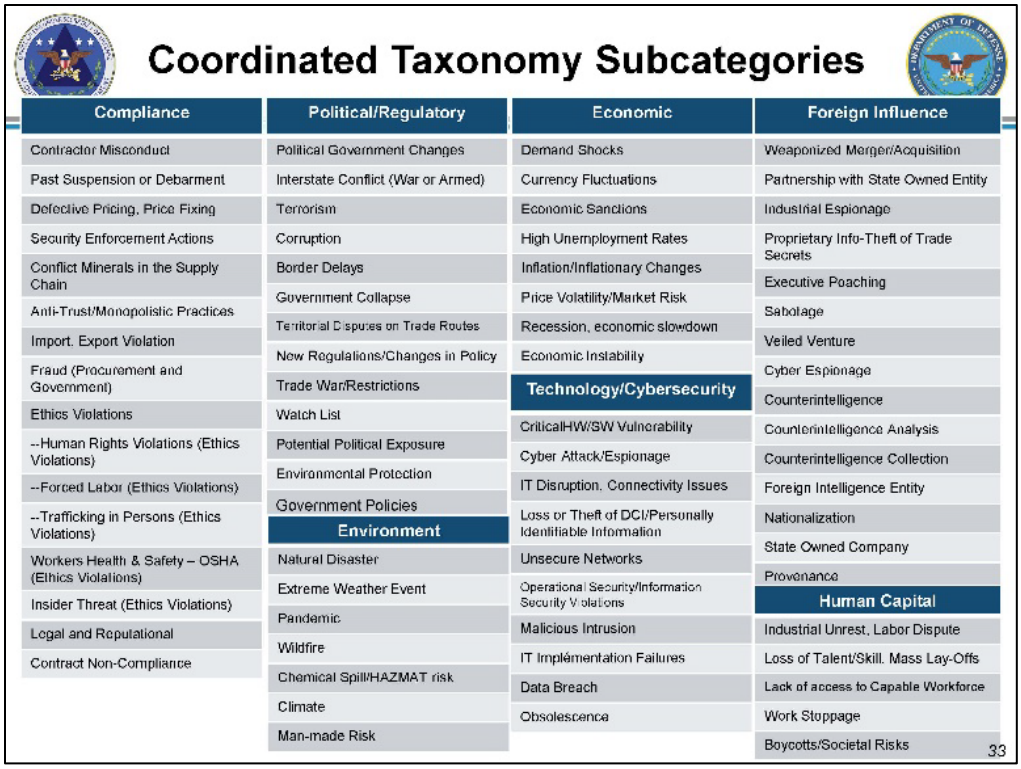
Supply Chain Assessments Status

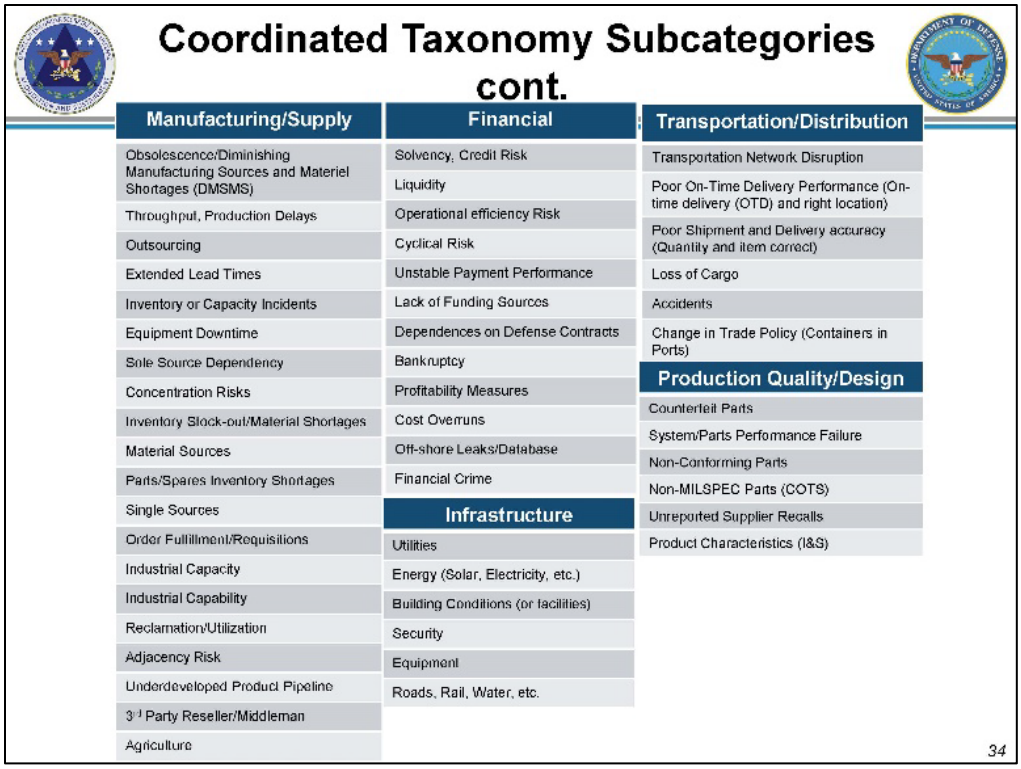
Supply Chain Assessments Library

- **Reviewed and cataloged an estimated 349 of 1,344 assessments** (est 2,503 pages)
- Developed tools within the excel workbook that allow end-users to search our cataloged assessments by: Company Name, Keyword, Country, Risk Level, FY, Report that searches the entirety of all entries, and OSD Risk alignment tool.
- Developed automated leadership score cards
- Developed an approach to analyze sources identified within the report
- Incorporated the draft OSD risk taxonomy; developed a cross reference logic that takes the results from assessments and aligns them to OSD Risk Categories (and sub)
- Working with the Army AVN DEVCOM to evaluate integration of their Industrial Base Entity Resolution Supply Chain Illumination (IBERSCI) tool to auto populate current specified fields of data; along with, possibly incorporating our logic into their tool
- **Goal is to hand off workbook, tools, and logic to the CDAO Advana team** for their review and integration into SCREEn



32


Coordinated Taxonomy Subcategories
Compliance
Contractor Misconduct
Past Suspension or Debarment
Defective Pricing, Price Fixing
Security Enforcement Actions
Conflict Minerals in the Supply Chain
Anti-Trust/Monopolistic Practices
Import, Export Violation
Fraud (Procurement and Government)
Ethics Violations
--Human Rights Violations (Ethics Violations)
--Forced Labor (Ethics Violations)
--Trafficking in Persons (Ethics Violations)
Workers Health & Safety – OSHA (Ethics Violations)
Insider Threat (Ethics Violations)
Legal and Reputational
Contract Non-Compliance
Political/Regulatory
Political Government Changes
Interstate Conflict (War or Armed)
Terrorism
Corruption
Border Delays
Government Collapse
Territorial Disputes on Trade Routes
New Regulations/Changes in Policy
Trade War/Restrictions
Watch List
Potential Political Exposure
Environmental Protection
Government Policies
Environment
Natural Disaster
Extreme Weather Event
Pandemic
Wildfire
Chemical Spill/HAZMAT risk
Climate
Man-made Risk
Economic
Demand Shocks
Currency Fluctuations
Economic Sanctions
High Unemployment Rates
Inflation/Inflationary Changes
Price Volatility/Market Risk
Recession, economic slowdown
Economic Instability
Technology/Cybersecurity
Critical HW/SW Vulnerability
Cyber Attack/Espionage
IT Disruption, Connectivity Issues
Loss or Theft of DCI/Personally Identifiable Information
Unsecure Networks
Operational Security/Information Security Violations
Malicious Intrusion
IT Implementation Failures
Data Breach
Obsolescence
Foreign Influence
Weaponized Merger/Acquisition
Partnership with State Owned Entity
Industrial Espionage
Proprietary Info-Theft of Trade Secrets
Executive Poaching
Sabotage
Veiled Venture
Cyber Espionage
Counterintelligence
Counterintelligence Analysis
Counterintelligence Collection
Foreign Intelligence Entity
Nationalization
State Owned Company
Provenance
Human Capital
Industrial Unrest, Labor Dispute
Loss of Talent/Skill, Mass Lay-Offs
Lack of access to Capable Workforce
Work Stoppage
Boycotts/Societal Risks
33


Coordinated Taxonomy Subcategories cont.
Manufacturing/Supply
Obsolescence/Diminishing Manufacturing Sources and Materiel Shortages (DMSMS)
Throughput, Production Delays
Outsourcing
Extended Lead Times
Inventory or Capacity Incidents
Equipment Downtime
Sole Source Dependency
Concentration Risks
Inventory Stock-out/Material Shortages
Material Sources
Parts/Spares Inventory Shortages
Single Sources
Order Fulfillment/Requisitions
Industrial Capacity
Industrial Capability
Reclamation/Utilization
Adjacency Risk
Underdeveloped Product Pipeline
3rd Party Reseller/Middleman
Agriculture
Financial
Solvency, Credit Risk
Liquidity
Operational efficiency Risk
Cyclical Risk
Unstable Payment Performance
Lack of Funding Sources
Dependences on Defense Contracts
Bankruptcy
Profitability Measures
Cost Overruns
Off-shore Leaks/Database
Financial Crime
Infrastructure
Utilities
Energy (Solar, Electricity, etc.)
Building Conditions (or facilities)
Security
Equipment
Roads, Rail, Water, etc.
Transportation/Distribution
Transportation Network Disruption
Poor On-Time Delivery Performance (On-time delivery (OTD) and right location)
Poor Shipment and Delivery accuracy (Quantity and item correct)
Loss of Cargo
Accidents
Change in Trade Policy (Containers in Ports)
Production Quality/Design
Counterfeit Parts
System/Parts Performance Failure
Non-Conforming Parts
Non-MILSPEC Parts (COTS)
Unreported Supplier Recalls
Product Characteristics (I&S)
34

Original Framework

Back-up

35

Operational Lines of Effort & End State

Goal: Develop cohesive framework to effectively manage supply chain risk across the DOD

LOE1: Supply Chain Resiliency (Industrial Policy)

- Leverage recently completed supply chain studies regarding critical capabilities to focus on developing US sources of manufacture and other critical US based technologies
- Develop budget/resources, manufacturing strategies and small business opportunities to increase domestic production in conjunction with US based private industry
- Improve information sharing regarding predatory investment. (Trusted Capital Program)
- Identify top technologies. or companies to monitor so as to avoid dilution of efforts and work with A&S and others to develop mechanisms to share information across the services and other agencies.
- Improve CFIUS reporting and FIR information sharing

LOE2: Acquisition Supply Chain Security (Acquisition)

- Update / Review contracting terms to support Supply Chain illumination and Security to include information sharing and risk reduction strategies for the Supply Chain.
- Partner with OEM's prior to contract award on transparency into Supply Chain with various illumination tools to reduce risk of security of all sub-tiers in Supply Chain.
- Work with IP. R&E and I&S and others to develop mechanisms to share information across the services/agencies
- Perform technology decomposition to identify essential technology elements (ETE) and enabling technologies crucial to creating and maintaining DoD warfighter advantage in order to prioritize SCRM resources (PJL)
- Ensure prior to contract award all vendors meet all requirements in FAR/DFAR and DoD contracting policy such as cyber and 889(b) and 2339(a).
- In coordination with CDSE, develop acquisition security curriculum
- Establish security as fourth pillar along with cost, schedule, and performance
- In coordination with Military Departments and I&S, strengthen DFARS security-related clauses

36

Lines of Effort & End State (*cont.*)

Goal: Develop cohesive framework to effectively manage supply chain risk across the DOD

LOE3: Supply Chain Sustainment (Logistics/Sustainment)

- **Establish and resource Service or DoD level SCRM cell** and expand Deputy Assistant Secretary of Defense Vendor Threat Mitigation oversight to include all vendor threats, rather than just OCS contingency threats.
- Leverage established organizational processes that utilize commercial and organic tools for SCRM that continuously monitor companies, mitigate risk, and executes issue resolution.
- Establish dedicated personnel to assess and mitigate identified issues. monitor the data and communicate to and other services and agencies when issues are found.
- Work with R&E and IP to source replacements for outdated or compromised technology or capabilities.
- Develop comprehensive SCRM policy/guidance that incorporates areas such as: DMSMS, Obsolescence, Counterfeit, Risk, etc.

37

Functional Lines of Effort & End State

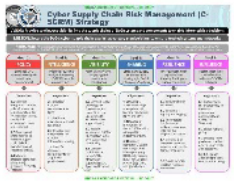
Goal: Develop cohesive framework to effectively manage supply chain risk across the DOD

LOE4: Technology Development (R&E)

- Develop Science & Technology protection, research security training, and due diligence training resources (PJL)
- Increase end-to-end transparency and knowledge of DOD's multi-tier supply chain ecosystem(s)
- Develop technology protection requirements and policies related to suppliers supporting technology development
- Assess supply chain risks related to technology development efforts such as: OTAs, SBIRs, CRADAs, Academia
- Conduct continuous discovery of supply chains for indicators of risks to/from individual suppliers
- Coordinate with SCRM Cell to develop and maintain supply chain eco-system Maps, Supplier Insights, Risk Scores, and Continuous Monitoring
- Update standard forms to increase PII collection to strengthen risk assessments prior to grant award
- Coordinate with Military Departments and I&S to strengthen DGARS security-related clauses

LOE5: ICT (CIO)

- Increase end-to-end transparency and knowledge of DOD's multi-tier supply chain ecosystem(s)
- Understand the complex connections and dependencies across ICT specific supply chain ecosystem
- Answer complex risk and resiliency questions impacting suppliers across the ICT ecosystem
- Conduct continuous discovery of dynamic supply chains for indicators of risks to/from individual suppliers
- Maintain supply chain eco-system Maps, Supplier Insights, Risk Scores, and Continuous Monitoring



LOE6: Cyber SW/HW (CIO) C-SCRM

- Increase end-to-end transparency and knowledge of DOD's multi-tier supply chain ecosystem(s)
- Understand the complex connections and dependencies across cyber HW/SW specific supply chain ecosystems
- Answer complex risk and resiliency questions impacting suppliers across the cyber ecosystem
- Conduct continuous discovery of dynamic supply chains for indicators of risks to/from individual suppliers
- Maintain supply chain eco-system Maps, Supplier Insights, Risk Scores, and Continuous Monitoring

38

Functional Lines of Effort & End State (*cont'd*)

Goal: Develop cohesive framework to effectively manage supply chain risk across the DOD

LOE7: Intelligence and Security (I&S)

- Increase end-to-end transparency and knowledge of DOD's multi-tier supply chain ecosystem(s)
- Understand the complex connections and dependencies across intelligence/CI organizations
- Improve WOG collaboration and develop communication/reporting processes
- Conduct continuous discovery of dynamic supply chains for indicators of risks to/from individual suppliers
- Maintain supply chain eco-system Maps, Supplier Insights, Risk Scores, and Continuous Monitoring
- Conduct threat and vulnerability assessments; recommend countermeasures and mitigating strategies
- Update policies, standard forms, and SORNs to facilitate the collection, usage, storage, and sharing of information
- **Develop strategy that focuses on the supply chain in great power competitions**

LOE8: Installation & Critical Infrastructure (DHS/CISA)

- Increase end-to-end transparency and knowledge of DOD's multi-tier supply chain ecosystem(s) and the connections and interdependencies between infrastructure elements and sectors
- Understand the complex interagency connections and dependencies: improve WOG collaboration
- Conduct continuous discovery of dynamic supply chains for indicators of risks to/from individual suppliers
- Maintain supply chain eco-system Maps, Supplier Insights, Risk Scores, and Continuous Monitoring
- Conduct threat and vulnerability assessments; recommend countermeasures and mitigating strategies
- Update policies, standard forms, and processes to facilitate the collection, usage, storage, and sharing of information

In the United States (U.S.), the Patriot Act of 2001 defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

39

Proposed Supply Chain Definitions

Supply Chain Resilience

Supply Chain Resilience (SCR) -The capability of supply chains to respond quickly to unexpected events, adapt to changes and ensure continuity of operations after a disruption. Resilience is the outcome of proactive Supply Chain Risk Management and Supply Chain Security.

Supply Chain Security

Supply Chain Security (SCS) - - The application of policies, procedures, processes, and technologies to ensure the security, integrity, and uninterrupted flow of products while moving through the supply chain. Examples include the ability to protect supply chains from cyber infiltrations and the introduction of counterfeit material.

Supply Chain Risk Mgmt

Supply Chain Risk Management (SCRM) - A process of proactively identifying supply chain vulnerabilities to potential disruptions and implementing mitigation strategies and actions to ensure the security, integrity, and uninterrupted flow of products as risks are found, or disruptions occur.

40

Appendix E. Abbreviations

AFRICOM	U.S. Africa Command
ANSI	American National Standards Institute
ASD(A)	Assistant Secretary of Defense for Acquisition
ASD(IBP)	Assistant Secretary of Defense for Industrial Base Policy
ASD(S)	Assistant Secretary of Defense for Sustainment
AWC	Army War College
CCMD	Combatant Command
CDAO	Chief Digital and Artificial Intelligence Office
CDRL	contract data requirements list
CENTCOM	U.S. Central Command
CFIUS	Committee on Foreign Investment in the United States
CI	Counter-intelligence
CIA	U.S. Central Intelligence Agency
CIO	DoD Chief Information Officer
CISA	Cybersecurity and Infrastructure and Security Agency
CMMC	Cybersecurity Maturity Model Certification
CNSSD	Committee on National Security Systems directive
CTPIC	Critical Technology Protection Integration Center
CUI	controlled unclassified information
CYBERCOM	U.S. Cyber Command
DARPA	Defense Advanced Research Project Agency
DASD	Deputy Assistant Secretary of Defense
DASD(IBR)	Deputy Assistant Secretary of Defense for Industrial Base Resilience
DASD(Log)	Deputy Assistant Secretary of Defense for Logistics

DAU	Defense Acquisition University
DC3	Defense Cyber Crime Center
DCMA	Defense Contract Management Agency
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense FAR Supplement
DFC	U.S. International Development Finance Corporation
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	defense industrial base
DISA	Defense Information Systems Agency
DISAM	DISA manual
DLA	Defense Logistics Agency
DMAG	Deputies Management Action Group
DMEA	Defense Microelectronics Agency
DMSMS	Diminishing Manufacture Sources and Material Shortages
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DPC	Defense Pricing & Contracting
DSAWG	Defense Information Assurance & Security Accreditation Working Group
DTS	Defense Transportation System
EO	executive order
EUCOM	U.S. European Command

FAR	Federal Acquisition Regulation
FASC	Federal Acquisition Security Council
FOCI	foreign ownership, control, or influence
GAO	Government Accounting Office
GDLS	General Dynamics Land Systems
GM	General Motors
GSA	General Services Administration
HASC	House Armed Services Committee
HII	Huntington Ingalls Industries
IBP	Industrial Base Policy
ICT	information communication technology
IDA	Institute of Defense Analysis
INDOPACOM	U.S. Indo-Pacific Command
ISO	International Organization for Standardization
ISRMC	International Security Risk Management Consortium
JAPEC	Joint Acquisition Protection & Integration Cell
JFAC	Joint Federated Assurance Center
J&J	Johnson & Johnson
LOE	line of effort
MDA	Missile Defense Agency
MIT	Massachusetts Institute of Technology
MITRE	Federally funded research and development center (FFRDC) founded in 1958
MSU	Michigan State University
NASA	National Aeronautics and Space Administration

NDAA	National Defense Authorization Act
NDIA	National Defense Industry Association
NDU	National Defense University
NGA	National Geospatial Intelligence Agency
NIST	National Institute of Standards and Technology
NIST-IR	NIST internal report
NIST-SP	NIST special publication
NIU	National Intelligence University
NORTHCOM	U.S. Northern Command
NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office
NSA	National Security Agency
NSIB	National Security Innovation Base
NTIB	National Technology and Industrial Base
NWC	Naval War College
OCS	operational contract support
ODNI	Office of Director of National Intelligence
OEM	Original Equipment Manufacturer
OIB	Organic Industrial Base
OIPB	Office of Planning and Budgeting
OMB	Office of Management and Budget
OPLAN	operations plan
OSD	Office of the Secretary of Defense
OT	operational technology

OUSD(A&S)	Office of the Under Secretary of Defense for Acquisition and Sustainment
PSU	Penn State University
RAND	FFRDC founded in 1948
R&E	Research and engineering
SASC	Senate Armed Services Committee
SBIR	Small Business Innovation Research
SCM	supply chain management
SCRLC	Supply Chain Risk Leadership Council
SCRM	supply chain risk management
SCRMC	Supply Chain Risk Management Consortium
SCS	supply chain security
SMWG	Systems Management Working Group
SOCOM	U.S. Special Operations Command
SOUTHCOM	U.S. Southern Command
SORN	System of Record Notification
SPACECOM	U.S. Space Command
STRATCOM	U.S. Strategic Command
STTR	Small Business Technology Transfer
TRANSCOM	U.S. Transportation Command
TSN	trusted systems network
U of M	University of Michigan
USAF	United States Air Force
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(R&E)	Under Secretary of Defense for Research & Engineering

USMC	U.S. Marine Corps
USN	U.S. Navy
USTC	U.S. Transportation Command
VTM	Vendor Threat Mitigation
WOG	whole of government

Appendix F. DoD Guidance

Name	Date of Publication	Title
(DNI) ICD 731	12/7/2013	Intelligence Community Directive Supply Chain Risk Management
(DNI) ICD 731-01-05	7/17/2019	Intelligence Community Supply Chain Risk Assessments
CNSSD 505	11/17/2021	Committee on National Security Systems Supply Chain Risk Management (SCRM)
DISAI 240-110-42	2/24/2014	DISA Program Protection
DISAI 240-110-44		Supply Chain Risk Management
DISAI 630-230-19	3/21/1988	Security Requirements for Automated Information Systems
DoD 4400.01-M	2/21/2002	Department of Defense priorities and Allocations Manuel
DoDD 2010.09	4/28/2003	Acquisition and Cross-Servicing Agreements
DoDD 3000.16	7/6/2022	Vendor Threat Mitigation
DoDD 3020.40	11/29/2016	Mission Assurance (MA)
DoDD 3020.45 CE-01	5/23/2017	Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP)
DoDD 4100.01E	3/6/2019	DoD Supply Chain Materiel Management Policy
DoDD 4275.05	8/31/2018	Acquisition and Management of Industrial Resources
DoDD 4715.21	1/14/2016	Climate Change Adaptation and Resilience
DoDD 5000.44	8/31/2018	Industrial Modernization Incentives Program
DoDD 5000.47	9/4/2015	Anti-Tamper (AT)
DoDD 5101.18	6/12/2018	DOD Executive Agent for Printed Circuit Board and Interconnect Technology
DoDD 5137.02	7/15/2020	Under Secretary of Defense for Research and Engineering (USD(R&E))
DoDD 5205.16	9/30/2014	The DoD Insider Threat Program
DoDD 5240.24	10/15/2013	Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)
DoDI 2000.25	12/16/2021	DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States
DoDI 2010.06	7/29/2009	Materiel Interoperability and Standardization with Allies and Coalition Partners
DoDI 2040.03	7/15/2020	End Use Certificates (EUCs)
DoDI 3020.45	8/14/2018	Mission Assurance Construct
DoDI 4140.01	3/6/2019	DoD Supply Chain Materiel Management Policy
DoDI 4140.67	4/26/2013	DoD Counterfeit Prevention Policy
DoDI 4205.01	6/8/2016	DoD Small Business Programs (SBP)
DoDI 4245.15	11/5/2020	Diminishing Manufacturing Sources and Material Shortages Management
DoDI 5000.60	7/18/2014	Defense Industrial Base Assessments
DoDI 5000.74	1/10/2020	Defense Acquisition of Services
DoDI 5000.79	10/15/2019	Defense-Wide Sharing and Use of Supplier and Product Performance Information (PI)
DoDI 5000.82	4/21/2020	Acquisition of Information Technology (IT)

Name	Date of Publication	Title
DoDI 5000.83	7/20/2020	Technology and Program Protection to Maintain Technological Advantage
DoDI 5000.83	7/20/2020	Technology and Program Protection to Maintain Technological Advantage
DoDI 5000.85	8/6/2020	Major Capability Acquisition
DoDI 5000.86	9/11/2020	Acquisition Intelligence
DoDI 5000.90	12/31/2020	Cybersecurity for Acquisition Decision Authorities and Program Managers
DoDI 5000.91	11/4/2021	Product Support Management for the Adaptive Acquisition Framework
DoDI 5000.93	6/10/2021	Use of Additive Manufacturing in the DoD
DoDI 5134.04	12/4/2017	Director of Small Business Programs
DoDI 5200.39	5/28/2015	Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)
DoDI 5200.44	11/5/2012	Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)
DoDI 5200.FH	4/21/2016	DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)
DoDI 5220.22	3/18/2011	National Industrial Security Program (NISP)
DoDI 5230.24	1/10/2023	Distribution Statements on DoD Technical Information
DoDI 5240.19	1/31/2014	Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)
DoDI 8320.04	9/3/2015	Item Unique Identification (IUID) Standards for Tangible Personal Property
DoDI 8500.01	3/14/2014	Cybersecurity
DoDI 8510.01	7/19/2022	Risk Management Framework for DoD Systems
DoDM 4140.01 Vol 1-11	3/8/2017	DOD Supply Chain Materiel Management Procedures: Inventory Accountability and Special Management And Handling
DoDM 4245.15	10/26/2022	Management of Diminishing Manufacturing Sources and Material Shortages
NDAA 2019, Sec 889	8/13/2019	Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment
NIST SP 800-161	5/5/2022	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
NIST SP 800-37	12/20/2018	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
NIST SP 800-53 Rev5	12/10/2020	Security and Privacy Controls for Information Systems and Organizations
NIST-IR 8276	2/11/2021	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry