SYM-AM-25-365

Excerpt from the Proceedings of the Twenty-Second Annual Acquisition Research Symposium and Innovation Summit

Volume III

Supplier Chain Visibility—A Contracting Necessity

Published: May 5, 2025

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

Supplier Chain Visibility—A Contracting Necessity

Rafaela Kovacs—is the Chief of Contracts at Air Force Operational Test and Evaluation Center, responsible for a contract portfolio providing relevant, credible, and timely test and evaluation to more than 90 major acquisition programs. Kovacs is also the Air Force Operational Test and Evaluation Center Director of Small Business Programs and responsible for managing the small business program on behalf of the commander. She holds an unlimited contracting officer's warrant, agreements officer under 10 USC 4022, and is a certified professional contracts manager. Kovacs earned her Master of Business Administration at the University of New Mexico. [Rafaela.a.kovacs.civ@mail.mil]

Tamie Haines—is a Supervisory Price and Cost Analyst with the Department of Contract Management Agency, having held various acquisition roles, including contract administrator and specialist, as well as a warranted Administrative Contracting Officer for prominent defense weapons systems. Haines served in the United States Air Force, commissioned through the Air National Guard in 2017, and is currently an A-Staff Officer. She previously served as a Space Control Officer and Contracting Officer with Flight Commander and Contingency experience. Haines holds a Master in Business Administration degree and is pursuing a doctorate in public administration. [Tamie.n.haines.civ@mail.mil]

Peter Guinto—Mentor

Abstract

This paper investigates the weaknesses present in federal procurement supply chains, emphasizing cost analysis, cybersecurity, and risk mitigation within defense contracts. Utilizing data from more than 200 Contractor Cost Data Reports and 87 Price Negotiation Memorandums (2015–2025), the analysis shows that subcontracting, materials, and inter-company transfers constitute more than 80% of direct costs, emphasizing the necessity for increased transparency and accountability in government acquisitions. The study points out significant threats, including dependence on foreign sources, cybersecurity vulnerabilities, and inadequate oversight of single-source suppliers. It assesses private-sector frameworks like IBM's cognitive supply chain and Starbucks' enterprise risk management to pinpoint best practices applicable to defense procurement.

This paper also considers unsuccessful legislative attempts to enforce supply chain compliance, highlighting the significance of flexible policies, contractor involvement, and financial incentives. Key recommendations include improving bill of materials transparency, widening the oversight of DCMA and DCAA, and bolstering domestic manufacturing efforts. Case studies from the F-35 and C-17 programs demonstrate the repercussions of insufficient oversight and the benefits of responsible sourcing practices. Ultimately, the paper promotes a forward-thinking, technology-focused, and risk-managed procurement approach that enhances national security and fortifies the resilience of the defense industrial base.

Introduction

Cost analysis in government contracting is essential for ensuring financial accountability, identifying inefficiencies, and optimizing expenditures. An analysis examining 212 Contractor Cost Data Reports (CCDRs) from 2015 through March 2025 revealed $974 million in subcontracting, material, and inter-company work transfers (IWT) expenses, with these categories comprising 83% of total direct costs (DoD, 2025a). Similarly, a review of 87 Defense Pricing and Contracting, Acquisition Policy (DPCAP) Price Negotiation Memorandums (PNMs) from 2022 to 2025 resulted in $120.7 billion in subcontracting, material, and IWT expenses, accounting for 81% of total direct costs (DoD, 2025b). The alignment between CCDR and PNM data highlights consistent cost distributions across programs, allowing a deeper examination of cost drivers and potential efficiencies within government acquisition.

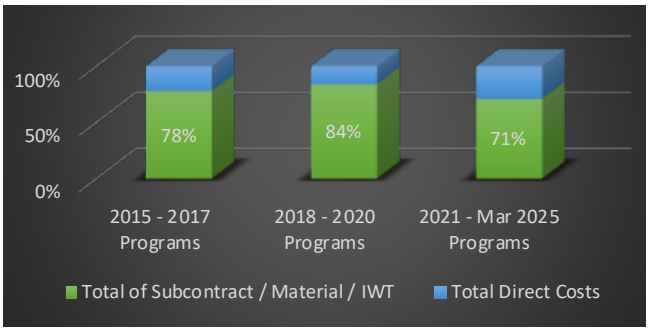

Figure 1. CCDRs 2022–2025

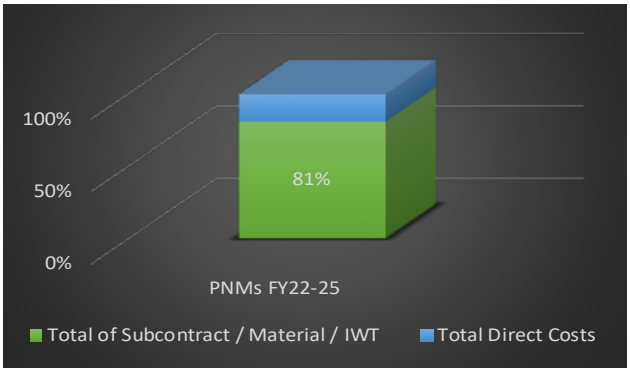

Figure 2. DPCAP PNMs Peer Reviews 2022–2025

Supply Chain Vulnerabilities and Cybersecurity Threats In Federal Procurement

The security of the federal supply chain is a critical concern in defense contracting, where reliance on foreign sources and cybersecurity threats create serious vulnerabilities. The Government Accountability Office (GAO) has identified weaknesses in managing risks, particularly concerning single-source suppliers and critical material dependencies. Rare earth elements essential for defense systems are largely sourced from foreign suppliers—especially China—raising concerns about supply disruptions and adversarial influence (GAO, 2024a).

The Department of Defense (DoD) also depends heavily on sole-source contractors for essential components. A GAO report found that the DoD does not consistently assess risks related to these suppliers, limiting its ability to prepare for disruptions (GAO, 2017). The report recommends more robust frameworks for tracking and mitigating supply chain dependencies.

Cybersecurity presents another major risk to federal procurement systems. Proposed amendments to the Federal Acquisition Regulation (FAR) would require vendors to report incidents within eight hours and disclose vulnerabilities in supply chain software (DoD et al., 2023). The Cybersecurity and Infrastructure Security Agency (CISA) further emphasizes the need for Software Bills of Materials (SBOMs) to identify and manage risks in third-party software (CISA, 2023).

Finally, the waiver process for domestic preference laws lacks consistent oversight and data accuracy. Although agencies are required to report when foreign goods are purchased, the GAO found errors and gaps in reporting that weaken transparency (GAO, 2024b). Improving this process would enhance accountability and help reinforce domestic sourcing in federal procurement.

Supply Chain Resilience and Disruption Mitigation

The Evolving Landscape Of Supply Chain Disruptions

The complexities of modern supply chains have increased vulnerabilities to disruptions, requiring strengthening mitigation strategies. Recent research identifies the severity of supply chain interruptions and examines frameworks organizations can adopt to enhance resilience. Blackhurst et al. (2005) recommend critical research areas in managing disruptions and identifying the need for proactive risk assessment and rapid recovery strategies. They contend that firms must develop a deeper understanding of supply chain vulnerabilities to effectively mitigate operational and financial risks. Additionally, Craighead et al. (2007) expand on this perspective, stating that the severity of supply chain disruptions is affected by design characteristics such as density, complexity, and node criticality. Their study emphasizes that supply chains with high node interdependence are more vulnerable to cascading failures, making it essential for companies to cultivate reactive and proactive mitigation capabilities.

Centers of Excellence as a Strategic Response

The idea of Supply Management Centers of Excellence (SM COEs) has surfaced as a systematic method for enhancing supply chain resilience (Handfield, 2024). A CAPS Research study outlines optimal practices for building COEs focused on supply market intelligence, risk management, and advanced analytics. Evidence indicates that organizations with dedicated COEs are more likely to standardize procurement procedures, improve category management insights, and employ data-driven decision-making models that foresee and address supply chain risks. The findings show that 59% of surveyed companies have at least one SM COE, with another 10% in the process of establishing one. These centers play a vital role in promoting best practices in supply management, disseminating intelligence, and encouraging a forward-thinking approach to risk management. Additionally, the research points to the growing incorporation of predictive analytics and digital twins in COEs to facilitate real-time monitoring and forecasting of supply chain disruptions.

Dynamic Stress Testing for Supply Chain Resilience

Stress testing is an emerging approach aimed at enhancing supply chain resilience, drawing parallels with established financial risk assessment techniques. Handfield et al. (n.d.) advocate for dynamic stress testing, which incorporates artificial intelligence (AI) and machine learning (ML) to deliver real-time scenario evaluations and predictive disruption notifications. Their research highlights the value of AI-powered simulations that consistently adjust risk assessments in response to changing global conditions. Through stress testing, organizations can proactively identify weaknesses by simulating possible supply chain shocks like geopolitical tensions, trade limitations, and resource scarcity. For instance, Honeywell has implemented dynamic stress testing to address risks associated with tariffs, international conflicts, and supply chain interruptions due to climate change. This methodology has enabled firms to bounce back more swiftly from disturbances, maintain supply continuity, and enhance supplier relationships through proactive oversight.

Build Resilience into the Procurement Process

Building a resilient supply chain requires a strategic approach focused on both downstream management and upstream vision. It is more than mere component acquisition. A procurement center can most effectively collaborate with risk management functions and other business units to manage supply chain risk (Schnellbacher et al., 2023). In one survey, only 10% of respondents indicated that their companies utilized a full range of capabilities to build a resilient supply chain.

Supply resilience can be achieved by combining human and technological resources. Three main activities can mitigate supply chain security threats from foreign dependencies and cyber vulnerabilities. Identifying hidden risks involves examining tier-2 suppliers for critical material sources, particularly rare earth elements, to reduce reliance on single foreign sources. Upon completing this analysis, AI systems can provide early warnings, recommend alternative sources, and strategize for strategic reserves while addressing vulnerabilities through strategic buffering, alternative supplier development, and stricter security standards. Enhancing cybersecurity during procurement through third-party security ratings or cybersecurity questionnaires enables proactive risk management and boosts the chain's overall resilience.

Lessons from the COVID-19 Supply Chain Crisis

The COVID-19 pandemic acted as a crucial examination of global supply chains, revealing critical gaps in visibility and responsiveness. Finkenstadt and Handfield (2021) investigate the visibility challenges faced in supply chains during the pandemic, particularly in sourcing personal protective equipment (PPE). Their findings show that dependence on low-cost suppliers from various regions exacerbated shortages and delays. The research highlights the need for supply chain mapping, diversified inventory, and investments in digital tracking technologies to improve visibility and readiness for future disruptions. The changing landscape of supply chain interruptions requires a strategic and layered approach to resilience. By integrating SM COEs, conducting dynamic stress tests, and employing AI-driven analytics, organizations can create an effective risk management framework. The lessons from the COVID-19 pandemic highlight the critical need for investment in tools for supply chain visibility and the establishment of strong mitigation strategies. As supply chains become more intricate, organizations must take proactive steps to implement these strategies, ensuring operational continuity and boosting their competitive edge.

F-35 Supply Chain Challenges and Security Risks

The F-35 Joint Strike Fighter program, the DoD's most expensive weapon system, has encountered ongoing supply chain issues, such as production delays, semiconductor shortages, and security risks linked to foreign-sourced materials (GAO, 2024c). One of the most concerning vulnerabilities was the discovery of a Chinese-sourced magnet within the aircraft's power system, raising alarms about adversarial infiltration and potential national security threats (Magnuson, 2022). The existence of foreign-manufactured components in critical defense systems highlights the necessity for tighter supply chain oversight and stronger sourcing policies to reduce security risks. A review of seven F-35 Lightning II and Air Vehicle Production acquisitions valuing $33.48 billion in total direct costs highlighted a significant 92% expenditure profile of subcontracting, material, and inter-company work transfers (IWT) expenses (DoD, 2025a, 2025b).

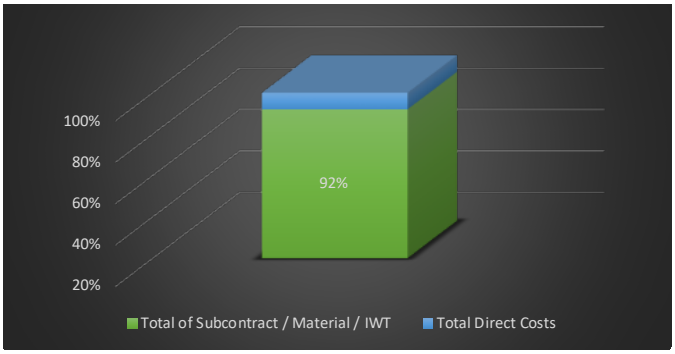

Figure 3. F-35 Expenditure Profile Review

Additionally, disruptions in the semiconductor supply chain have hindered F-35 production, worsening modernization delays and raising program costs (Fulco, 2023). The program's dependency on global semiconductor suppliers, mainly from geopolitically sensitive regions, has made it susceptible to supply shocks. Shivakumar and Wessner (2022) emphasize that semiconductors are crucial for national defense, and reliance on foreign sources poses operational risks that may affect military readiness.

A 2024 GAO report revealed that contractors deliver engines and aircraft late due to ongoing manufacturing issues and parts shortages. Technology Refresh 3 (TR-3), a $1.8 billion upgrade for the F-35's Block 4 modernization, faces delays from supply chain disruptions, including software and hardware shortages (GAO, 2024c). These delays impact cost efficiency and the DoD's ability to maintain a competitive technological edge. To address these challenges, the DoD must implement stronger supply chain visibility mechanisms, enforce stricter sourcing transparency requirements, and explore domestic semiconductor production to reduce foreign dependency. By adopting best practices from private sector supply chain management, such as blockchain tracking and AI-driven procurement monitoring, the DoD can improve oversight and mitigate F-35 supply chain risks.

C-17 Supply Chain Challenges

The C-17 Globemaster III, a critical aircraft for tactical airlift and airdrop missions and aeromedical evacuations, highlights the DoD's need to better manage supply chains for defense systems and platforms. A DoD Inspector General (IG) audit of its performance-based logistics (PBL) contracts exposed significant vulnerabilities in acquiring spare parts at fair and reasonable prices, stemming from the Department's handling of the bill of materials (BOM). A review of two C-17 Globemaster III acquisitions of $942 million in total direct costs highlighted a 57% expenditure profile of subcontracting, material, and IWT expenses.

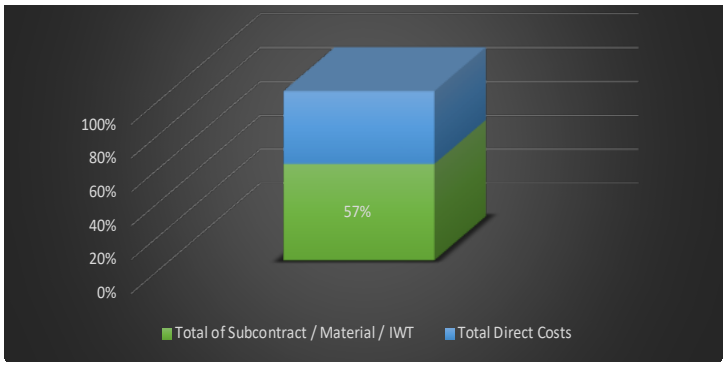

Figure 4. C-17 Globemaster III Expenditure Profile Review

Sole-source contracts like the C-17 PBL create an uneven playing field for negotiating prices. The vendor creates information asymmetry by the details it chooses to include in the BOM and cost data; thus, the government relies on the vendor's data to create its negotiation position. The lack of transparency and limited negotiation leverage increases the risk of inflated pricing.

Furthermore, the DoD does not require BOMs to be incorporated into the contract, which can create a disparity between proposed and actual materials. The audit found that 46.5% of the items delivered under the contract were included in the proposed BOM. Allowing vendors the discretion to provide materials of their choice undermines the initial determination of fair and price reasonableness, makes it difficult to anticipate and mitigate risks associated with

diminishing manufacturing sources and material shortages (DoD, Office of Inspector General, 2024), and introduces potential quality control issues that affect readiness and safety.

Two approaches can be utilized in efforts to resolve audit findings. First, clear requirements for submitting complete and accurate BOMs would enhance total supply chain visibility. Second, strategies to reduce reliance on sole-source contracts could strengthen the negotiation position, such as incentivizing competition through dual sourcing or an open bidding process or proactively developing alternative sources for critical components or materials. Ultimately, improved data transparency would provide the Government with visibility into vendor pricing data and subcontractor relationships.

Lastly, retaining the Design Control Authority (DCA) is another targeted approach that could be applied in specific situations to mitigate challenges. The DCA is most appropriate for aircraft or weapons system programs where changes significantly affect components, manufacturing, and overall supply chain stability. It assists in managing obsolescence and mitigating supply chain risks that threaten the mission or national security. Regardless of the mechanism, addressing these supply chain vulnerabilities will position the DoDto ensure that the C-17 and other critical assets remain mission-ready while maintaining responsible stewardship of taxpayer resources.

Raytheon Settlement: A Cautionary Case for Subcontractor Oversight

The recent $950 million settlement between Raytheon Company and the U.S. Department of Justice (DOJ) highlights the risks of managing subcontractors and suppliers in federal procurement. The DOJ reported that Raytheon's subsidiary, RTX Corporation (previously known as Raytheon Technologies), admitted to participating in a bribery and fraud scheme that lasted a decade, which involved its jet engine manufacturer, Pratt & Whitney. This scheme included the establishment of fake subcontracts that funneled more than $55 million in bribes to government officials across various foreign nations to obtain defense contracts. Additionally, there were instances where Raytheon employees submitted false or misleading certifications, leading to the export of sensitive military hardware and technology of U.S. origin to unauthorized entities, thus breaching the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR; U.S. Department of Justice, 2024).

Using false subcontracts to disguise bribery payments highlights significant internal controls, subcontractor evaluation, and export compliance failures. Additionally, it raises serious doubts about supplier oversight within the defense industrial sector, particularly concerning high-risk components such as jet engines and aerospace technologies. In instances like the C-17 program, where sole-source vendors prevail, and prime contractors maintain information imbalances, this situation emphasizes strong oversight systems that authenticate subcontractor credibility, promote transparent billing practices, and reduce the risk of corruption and export violations. Enhancing these controls during the acquisition phase, instead of relying exclusively on subsequent sustainment audits, would allow for earlier identification and prevention of such misconduct.

Failed Legislative Attempts to Incentivize Supply Chain Compliance

Several legislative efforts to enhance transparency in defense contracting supply chains have faced obstacles linked to feasibility, cost, and enforcement. For example, the Supply Chain Illumination provision was initially framed for defense contractors to implement supply chain monitoring technologies and gave a short period for the Secretary of Defense to create incentives and minimum technical standards, including cybersecurity requirements. Objections to specific tool mandates on the grounds of possible security threats and small business compliance strains resulted in a requirement to incentive contractors to assess and monitor the

entire supply chain for potential vulnerabilities and noncompliance risks (H. R. 5009, § 849). Another initiative to reimburse contractors for unforeseen disruptions and introduced a quick waiver process stalled due to budgetary issues and worries that contractors might pass costs onto the government. Additionally, a proposal to expedite supply chain reviews, referencing 10 U.S.C. § 4863 and 4872, aimed to improve risk disclosures concerning specialty metals and restricted foreign materials by providing a temporary National Security Waiver (NSW) as a corrective measure. Contractor hesitancy to self-report non-compliance due to risk of penalties, and conflicts with existing procurement regulations halted proposal consideration. Lastly, a proposal for safe harbor encouraged contractor transparency (report supply chain weakness and non-compliant materials) by protecting the disclosures from penalties and accepting non-compliant materials during NSW reviews. Critics contended this would weaken enforcement by shifting liability to the government and diminishing contractor accountability. These unsuccessful legislative attempts highlight the complexity needed to balance effective and enforceable supply chain reform with compliance requirements, cost implications, and contractor responsibility.

Compliance requirements such as mandating specific tools encountered substantial industry pushback, especially from small enterprises. Objections to the initial Supply Chain Illumination draft voiced vendor dependency and that inflexible standards and tight deadlines offered limited flexibility for scalable implementation. There would likely be inconsistent implementation across the defense industrial sector. Waiver-based compliance model initiatives, like expedited supply chain review, frequently clash with procurement regulations, leading to procedural delays and reduced contractor involvement. Further, the potential repercussions of voluntary disclosures created hesitancy towards transparency, undermining the purpose of the interim waiver system, which aimed to promote corrective actions and accountability.

Cost considerations hampered several of proposed legislation efforts. Hefty costs associated with compliance was another protest to the first draft of Supply Chain Illumination. The Department's budget constraints hindered ability to provide financial incentives intended to promote stronger supply chain management. Uncertainty about cost responsibilities discourages contractors from committing to strong risk management strategies.

Contractor responsibility is paramount in supply chain management. Although liability protections like a safe harbor encourage transparency, they often appear to reduce contractor accountability. From a broader industrial viewpoint, the decline of domestic capabilities, particularly in rare earth magnet manufacturing, poses challenges for compliance, sometimes placing it beyond a contractor's immediate influence. Consequently, many companies are reluctant to divulge proprietary information to potential rivals or "competimates," worried about losing their competitive edge or facing disintermediation. Additionally, cash flow is a vital consideration in these decisions, as disruptions in network flow significantly impact compliance and performance results. Ultimately, it is crucial for the government to respond promptly, not just to control costs and ensure taxpayer responsibility but also to foster the operational stability contractors require to sustain profitability.

Restoring Freedom's Forge Act: A Path Toward Supply Chain Modernization

The Restoring Freedom's Forge Act represents a legislative effort to revitalize defense procurement and enhance supply chain resilience (Restoring Freedom's Forge Act, 2024) by streamlining procurement processes, eliminating bureaucratic barriers, and strengthening domestic manufacturing capabilities. It attempts to resolve DoD procurement challenges like inadequate supply chain transparency and excessive dependence on foreign materials through mandates for better tracking and reporting methods to improve supply chain transparency.

Issues highlighted in recent GAO reports (2024a, 2024b, 2024c) include single-source reliance, cybersecurity risks, and uneven enforcement of domestic sourcing regulations. To

tackle these shortcomings, the legislation outlines a three-part strategy. First, it aims to eliminate bureaucratic hurdles that hinder procurement and limit competition, thus speeding up the acquisition process and expanding the supplier pool (Restoring Freedom's Forge Act, 2024). Second, it intends to boost supply chain visibility by requiring enhanced tracking and reporting systems, enabling government agencies to pinpoint vulnerabilities sooner and respond more accurately. Finally, the act encourages domestic production by providing incentives for the onshoring of essential materials and components, thereby reducing U.S. dependence on potentially hostile nations for crucial defense supplies. Together, these actions represent a concerted effort to modernize federal procurement and strengthen national security through more robust and accountable supply chains.

One of the act's key provisions focuses on streamlining acquisition regulations, aligning with previous reports' recommendations highlighting the adverse effects of excessive oversight and slow procurement cycles (Restoring Freedom's Forge Act, 2024). By simplifying the approval process for new defense suppliers, the legislation aims to diversify the DoD's supply base, reducing the risks associated with single-source suppliers (GAO, 2017). Additionally, the act encourages companies to produce critical materials onshore, especially in sectors such as rare earth elements and semiconductors, which are essential for national security (GAO, 2024a).

Another important aspect of the act is incorporating modern technology into procurement oversight. By utilizing blockchain, AI-driven supply chain monitoring, and digital ledger tracking, the act seeks to enhance supply chain transparency (Restoring Freedom's Forge Act, 2024). These tools can help reduce cybersecurity threats and improve real-time tracking of subcontractor performance, strengthening recent amendments to the FAR (DoD et al., 2023).

The Act is likely to face similar challenges as the failed legislative attempts especially with contractors' full compliance with enhanced supply chain reporting requirements. There is industry resistance to increased regulatory burdens. Additionally, critics contend that excessive procurement deregulation could lessen accountability, and raise the risks of fraud, cost overruns, and security vulnerabilities. While the act promotes domestic manufacturing, enhancing U.S. production capacity for critical materials will demand time and significant investment (Shivakumar & Wessner, 2022). To ensure effectiveness, streamlining procurement and maintaining adequate oversight must be balanced with adequate measures to prevent supply chain vulnerabilities.

The Restoring Freedom's Forge Act represents a forward-thinking approach to defense procurement reform, tackling supply chain inefficiencies and bolstering domestic manufacturing (Restoring Freedom's Forge Act, 2024).While the act can potentially improve the DoD's supply chain resilience, its success will hinge on practical implementation, industry compliance, and consistent investment in domestic production capabilities. Future research should analyze how effectively the act meets its objectives and whether additional safeguards are required to mitigate potential risks in a less regulated procurement environment.

Private Industries' Success in Supply Chain Management

IBM's Supply Chain Management: A Model For Government Adoption

IBM has established itself as a leader in supply chain management by leveraging AI, predictive analytics, and sustainability-driven strategies. By implementing a cognitive supply chain, IBM has achieved 100% order fulfillment and cost savings of $160 million, demonstrating the effectiveness of AI-powered decision-making and risk mitigation (Martinez, 2023). The federal government, particularly the DoD and procurement agencies, could adopt IBM's methodologies to enhance supply chain visibility, resilience, and efficiency.

IBM's cognitive supply chain incorporates AI, ML, and real-time data analytics to optimize logistics and procurement. This system enables IBM to proactively address disruptions by predicting demand, optimizing inventory, and mitigating supplier risks (Martinez, 2023). The federal government, facing challenges with supply chain transparency, could benefit from a similar AI-based approach to tracking spending, identifying supply vulnerabilities, and improving contract management.

IBM incorporates sustainability into its supply chain by utilizing responsible sourcing and conducting environmental impact assessments. This structure ensures compliance with international regulations while enhancing operational efficiency (McGrath & Jonker, 2024). The DoD and other agencies responsible for managing critical materials could adopt IBM's sustainable supply chain model to improve resilience and security, especially in overseeing semiconductor and rare-earth element supplies.

One of IBM's key innovations is its ability to consolidate diverse legacy systems into a unified, transparent supply chain platform (IBM, n.d.). This cohesive approach allows all stakeholders to access the same real-time data, enhancing coordination between suppliers, logistics providers, and procurement teams. The government could adopt a similar digital infrastructure to increase visibility at the subcontractor level, mitigating risks associated with unverified foreign suppliers.

Starbucks Supply Chain Management: Valuable Lessons for Government

Starbucks stands out in supply chain management, evolving with the global environment. From a single store in Seattle in 1971, it now boasts 40,000 locations. Over the past 17 years, Starbucks has reduced its footprint, cut logistics costs, improved logistics quality, and embraced new technology (Tabansi, 2023). It implemented enterprise resource management (ERM) to analyze macro trends related to materials, geopolitical events, and environmental changes, allowing for effective risk mitigation. These efforts provide the DoD insights to enhance transparency, expand the supplier base, and integrate new technologies.

One of Starbucks' initial supply chain efforts was investigating the cause of rising costs. The company discovered that outsourcing decisions had not been reassessed during the growth period, leading to an unnecessarily complex supply chain and a critical reorganization needed (O'Byrne, 2020). The DoD could adopt a similar strategy by requiring contractors to provide a detailed supply chain map, including all sub-tiers, to understand better the risks hidden within it.

Starbucks' supply chain management has incorporated updated technology as new capabilities have become available. In 2014, the company began utilizing enterprise resource management to identify macro trends that could potentially disrupt supply chain operations (Supply Chain Quarterly, 2014). Post-COVID, Starbucks integrated a new system that actively tracks risks in the supply chain and mitigates them to the extent that is within the company's control (SFK Inc. et al., 2024). The DoD could replicate this approach by investing in a platform that centralizes supply chain data across all its programs to aggregate, monitor, and analyze risks using predictive analytics.

Part of Starbucks' supply chain reorganization involved terminating ineffective partnerships and requiring weekly scorecards on service quality. Over two years, these efforts saved the company more than $500 million (O'Byrne, 2020). The DoD cannot dictate which prime or sub-tier contractors to include in its supply chain. However, it could adopt a similar approach by collaborating with the industry to develop standard quality levels that can be tracked in the aforementioned supply chain platform. This would be a public-private partnership to standardize data, necessitating cybersecurity measures to protect the supply chain information. The DoD could use the data to incentivize its prime contractors to reward sub-tier contractors that exceed quality levels or proactively manage risks down the supply chain.

AI in the Modern Supply Chain

AI is transforming all business sectors with its ability to analyze large data sets and identify complex patterns, creating the potential for enhanced decision-making, process optimization, and mitigating risks in an intricate global supply chain. The move towards AI supply chain management appears to be a strong operational decision backed by financial outcomes. In 2022, companies reported that costs decreased by more than 10% and revenue increased by more than 5% after their first year of AI adoption for supply chain management (Chui et al., 2022).

Benefits

Georgetown University's Walsh School of Foreign Service investigated AI's ability to develop a resilient supply chain and concluded its use has three advantages (Cohen & Tang, 2024). The capability to process vast amounts of data can predict fluctuations in demand with higher accuracy than historical methods, resulting in rightsized inventory levels. Data integration from diverse sources (supplier databases, news feeds, and social media analysis) builds a comprehensive view of the supply chain. The enhanced visibility allows for early identification of potential disruptions (supplier-related issues, geopolitical instability, or natural disasters). It equips decision-makers with time to develop and implement mitigation strategies to minimize chain disruptions and facilitates the evaluation of multiple scenario responses through simulations. By modeling the impact of different decisions, identifying the most effective solution becomes more transparent.

Limitations

While AI offers significant advantages in supply chain management, it is crucial to recognize its limitations. The efficacy of AI depends on the quality and accuracy of data inputs; as noted by an academic expert with extensive experience in Federal procurements and acquisitions, commercially available supply chain analytics utilize AI and ML to analyze publicly accessible information, which can result in inaccurate predictions and poor decision-making. These adverse outcomes may stem from the platform's inability to differentiate between outsourced and subcontracted relationships or between headquarters and plant locations. These limitations underscore the necessity of human oversight, especially in complex supply chain relationships (R. Handfield, personal communication, March 5, 2025).

Proposed Solutions to Enhance Supply Chain Oversight

A comprehensive set of policy, technological, and structural reforms must be adopted to address the persistent challenges in defense procurement and supply chain vulnerabilities. In addition to the lessons learned noted in previous sections, the recommendations aim to enhance transparency, mitigate risks, and strengthen domestic manufacturing capabilities, ensuring that national security interests are prioritized in the supply chain.

Recommendation 1: Strengthening Policy and Regulatory Frameworks

A major issue in defense procurement is the lack of visibility into lower-tier suppliers, heightening risks of foreign infiltration and counterfeit materials (GAO, 2024a). Revisions to the FAR and DFARS should ensure full transparency of lower-tier suppliers, especially for contracts involving critical components. Expanding DFARS 252.244-7001 to mandate disclosures from Tier 2+ suppliers would compel prime contractors to report subcontractor sources, preventing reliance on unverified foreign entities (Restoring Freedom's Forge Act, 2024). Annual supply chain reports from prime contractors should also be required to assess compliance and procurement integrity.

Another key policy reform seeks to limit exceptions for foreign sourcing by tightening waivers under the Berry Amendment and establishing domestic sourcing requirements for

defense materials. The Defense Production Act (DPA) Title III should be managed proactively rather than reactively, with strategic long-term investments informed by forward-looking data mapping. While DPA Title III offers tools such as loan guarantees, direct purchases, and grants to expand domestic capacity (Office of the Assistant Secretary of Defense for Industrial Base Policy, n.d.), its full potential remains underutilized when implemented solely in response to crises.

For instance, China's 2023 export restrictions on gallium and germanium, a decision that sparked concern across the defense, energy, and electronics sectors, demonstrate how supply disruptions can emerge suddenly and at scale, affecting critical defense programs (Holderness et al., 2023). Increased use of predictive analytics and industrial base mapping could aid in identifying and addressing supply chain vulnerabilities sooner, ensuring funding is directed to stabilize domestic production before strategic materials become unavailable. These strategies would help lessen reliance on foreign-made materials while bolstering domestic industrial capacity and resilience.

Recommendation 2: Expanding Oversight and Workforce Training

Expanding the authority of the Defense Contract Management Agency (DCMA) and the Defense Contract Audit Agency (DCAA) for auditing will enhance oversight of subcontractors and ensure compliance with supply chain security policies. The 2024 GAO report highlights that inadequate auditing has led to supply chain inefficiencies and security vulnerabilities (GAO, 2024c). Strengthening DCMA's role in contract execution will provide greater enforcement capabilities to ensure that suppliers adhere to domestic sourcing and cybersecurity standards. Additionally, acquisition professionals need specialized training in supply chain risk management. Mandating training in supply chain security for contracting officers and program managers will enhance their ability to assess contractor compliance and mitigate risks related to foreign dependencies (Restoring Freedom's Forge Act, 2024).

Building on this, DCMA should also act as a central arbitrator to manage shared supplier resources across the defense industrial base. Without centralized coordination, prime contractors function like independent herders in the "tragedy of the commons" scenario, exhausting shared supplier capacity without insight into each other's activities (Broga, 2006; Investopedia, 2023). This absence of communication results in overbooking of suppliers, delayed deliveries, and inflated costs, burdens that ultimately fall on the government to absorb. The government assumes full system risk when subcontractors are overextended across multiple primes, and their limitations go unrecognized. To prevent this, supply chain oversight should take place within acquisition, rather than sustainment, to influence contract decisions before a crisis point. In this model, DCMA would enforce compliance and manage capacity transparency, ensuring sustainable use of industrial resources for national defense.

Recommendation 3: Enhance Bom Transparency and Responsible Sourcing Oversight

One of the most overlooked yet critical tools in supply chain risk management is the BOM. According to a Fortune 500 Chief Procurement Officer (CPO), BOMs are foundational to world-class supply chain management, and even executive-level leaders regularly review them due to their strategic importance (CPO, personal communication, March 7, 2025). Oversight of BOMs enables early identification of sourcing risks, particularly when the government has visibility into all levels of sub-tier suppliers, not just direct contractors.

The government must ensure that BOM reviews include a comprehensive understanding of the original sources of parts, particularly for critical components. Integrating emerging technologies into BOM and inventory analysis would improve visibility, integrity, and real-time tracking throughout the supply chain (CPO, personal communication, March 7, 2025). These

tools can help prevent counterfeit parts, identify foreign vulnerabilities, and support proactive rather than reactive supply chain decisions.

The mutual dependency between government agencies and suppliers requires a collaborative and secure oversight model. Experienced supply chain subject matter experts (SMEs) could be engaged under non-disclosure agreements (NDAs) to guide BOM assessments, engineering change management, and overall procurement strategy to enable effective governance while maintaining confidentiality. This approach would protect proprietary information while ensuring expert insights inform acquisition decisions (CPO, personal communication, March 7, 2025).

Additionally, utilizing impartial third-party organizations, such as those following the Electronic Industry Citizenship Coalition (EICC) structure and the Responsible Business Alliance (RBA), can support ethical sourcing and help establish fair and reasonable pricing in contract negotiations. These entities already provide responsible sourcing verification and pricing analytics to the private sector, and their neutrality could enhance credibility and consistency in federal acquisition processes (CPO, personal communication, March 7, 2025). Integrating their capabilities would align defense procurement with commercial best practices while reinforcing transparency and sustainability across the defense industrial base.

Conclusion

An in-depth analysis of contractor cost data and procurement records reveals a pressing concern: the federal government lacks the necessary visibility into the subcontracting and material flows that comprise the backbone of our national defense supply chain. This systemic blind spot undermines strategic oversight, impedes proactive risk management, and jeopardizes fiscal responsibility and mission readiness. With subcontracting, material costs, and transfers between companies accounting for more than 80% of total direct costs, the lack of transparent oversight threatens taxpayer money and mission preparedness. Additionally, ongoing vulnerabilities discussed further jeopardize the integrity and resilience of the supply chain.

Insights gained from legislative missteps, successful private sector examples from companies like IBM and Starbucks, and notable defense projects, including the F-35 and C-17, indicate that the government's predominant emphasis on sustainment is inadequate. It is crucial to integrate risk management, data analytics, and supplier accountability much earlier in the life cycle to enhance procurement processes. For effective modernization and security of federal supply chains, the government must shift its focus to visibility during the acquisition stage, utilizing methods such as dynamic stress testing, predictive analytics, and AI-driven mapping to identify and mitigate threats proactively.

Moving forward requires more than just temporary solutions. It calls for a fundamental change in culture and operations regarding acquisition, policy, and oversight. This shift must focus on real-time transparency, enforce ethical sourcing standards, and encourage proactive teamwork within the defense industrial sector. Only then will the government be able to guarantee sturdy, efficient, and secure supply chains that address the changing needs of national security and fiscal accountability.

Disclaimer

The views expressed are those of the author(s) and do not reflect the official policy or position of the Naval Postgraduate School, US Navy, Department of Defense, or the US Government.

List of Acronyms and Abbreviations

3PL	Third-Party Logistics
AECA	Arms Export Control Act (AECA)
AI	Artificial Intelligence
BOM	Bill of Material
CCDR	Contractor Cost Data Report
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
COE	Centers of Excellence
CPO	Chief Product Officer
DCAA	Defense Contract Accounting Agency
DCMA	Defense Contract Management Agency
DoD	Department of Defense
DOJ	Department of Justice
DPA	Defense Production Act
EICC	Electronic Industry Citizenship Coalition
ERM	Enterprise Resource Management
FAR	Federal Acquisition Regulations
GAO	Government Accountability Office
DCA	Design Control Authority
DFAR	Defense Federal Acquisition Regulations
DPCAP	Defense Pricing Contracts and Acquisition Policy
IG	Inspector General
IoT	Internet of Things
ITAR	International Traffic in Arms Regulations
IWT	Inter-Work Transfers
ML	Machine Learning
NDA	Non-Disclosure Statement
NSW	National Security Waiver
PBL	Performance-Based Logistics
PNM	Price Negotiation Memorandum
PPE	Personal Protective Equipment
RBA	Responsible Business Alliance
RFID	Radio-Frequency Identification
SBOM	Software Bill of Materials
SM	Supply Management
SME	Subject Matter Expert
TR-3	Technology Refresh 3

List of References

Blackhurst, J., Craighead, C. W., Elkins, D., & Handfield, R. B. (2005). An empirically derived agenda of critical research issues for managing supply-chain disruptions. *International Journal of Production Research, 43*(19), 4067–4081. https://doi.org/10.1080/00207540500151549

Broga, C. (2006, Fall). *Jargon alert: Tragedy of the commons*. Region Focus. Federal Reserve Bank of Richmond. https://www.richmondfed.org/-/media/richmondfedorg/publications/research/econ_focus/2006/fall/pdf/jargon_alert.pdf

Chui, M., Hall, B., Mayhew, H., Singla, A., & Sukharevsky, A. (2022). *The state of AI in 2022—and a half-decade in review.* McKinsey & Company. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review

Cohen, M. C., & Tang, C. S. (2024, February 5). The role of AI in developing resilient supply chains. *Georgetown Journal of International Affairs.* https://gjia.georgetown.edu/2024/02/05/the-role-of-ai-in-developing-resilient-supply-chains/

Cybersecurity and Infrastructure Security Agency. (2023). *2023 top routinely exploited vulnerabilities.* https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a

Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007, February). The severity of supply chain disruptions: Design characteristics and mitigation capabilities. *Decision Sciences, 38*(1), 131–156. https://doi.org/10.1111/j.1540-5915.2007.00151.x

Finkenstadt, D. J., & Handfield, R. (2021). Blurry vision: Supply chain visibility for personal protective equipment during COVID-19. *Journal of Purchasing and Supply Management, 27*(3), 100689. https://doi.org/10.1016/j.pursup.2021.100689

DoD. (2025a). *Contractor Acquired Data Entry (CADE) system dataset* [Unpublished internal database].

DoD. (2025b). *Defense Contracting Pricing and Acquisition Policy, Price Negotiation Memorandums dataset* [Unpublished internal database].

DoD, GSA, & NASA. (2023). *Federal acquisition regulation: Cyber threat and incident reporting and information sharing.* https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing

Department of Defense, Office of Inspector General. (2024). *Audit of C-17 spare parts pricing* (Report No. DODIG-2025-009) [Audit report]. Department of Defense.

Fulco, M. (2023, June 13). How aerospace can improve its supply of semiconductors. *Aviation Week Network.* https://aviationweek.com/shownews/paris-air-show/how-aerospace-can-improve-its-supply-semiconductors

GAO. (2017). *Defense supply chain: DOD needs complete information on single sources of supply to proactively manage the risks* (GAO-17-768). https://www.gao.gov/products/GAO-17-768

GAO. (2024a). *Critical materials: Action needed to implement requirements that reduce supply chain risks* (GAO-24-107176). https://www.gao.gov/products/GAO-24-107176

GAO. (2024b). *Federal contracting: Opportunities exist to improve the reporting of waivers to domestic preference laws* (GAO-24-106166). https://www.gao.gov/products/GAO-24-106166

GAO. (2024c). *F-35 Joint strike fighter: Program continues to encounter production issues and modernization delays.* https://www.gao.gov/products/gao-24-106909

Handfield, R. (2024, January 23). *Best practices in forming centers of excellence*. CAPS Research. https://www.capsresearch.org/blog/posts/2024/january/caps-research-best-practices-in-forming-centers-of-excellence/

Handfield, R., Retherford, B., & DeGrange, W. (n.d.). *Why dynamic stress testing is critical for supply chain resilience.* NC State Poole College of Management. [Manuscript in preparation].

Holderness, A., Velazquez, N., Carroll, H. H., & Cook, C. (2023, July 7). *Understanding China's gallium sanctions*. Center for Strategic & International Studies. https://www.csis.org/analysis/understanding-chinas-gallium-sanctions

IBM. (n.d.). *IBM supply chain solutions.* https://www.ibm.com/supply-chain

Investopedia. (2023, September 25). *What is the tragedy of the commons in economics?* https://www.investopedia.com/terms/t/tragedy-of-the-commons.asp

Magnuson, S. (2022, September 20). AFA news: Chinese-sourced magnet in F-35 prompts supply chain concerns. *National Defense.* https://www.nationaldefensemagazine.org/articles/2022/9/20/chinese-sourced-magnet-in-f-35-prompts-supply-chain-concerns

Martinez, J. (2023, October 25). *IBM saves $160 million, achieves 100% order fulfillment with cognitive supply chain*. Cloud Wars. https://cloudwars.com/cloud/how-ibm-achieved-100-order-fulfillment-and-160-million-cost-savings-with-cognitive-supply-chain/

McGrath, A., & Jonker, A. (2024, March 14). *What is sustainable supply chain management?* IBM. https://www.ibm.com/think/topics/sustainable-supply-chain-management

O'Byrne, R. (2020, February 4). *7 mini case studies: Successful supply chain cost reduction and management*. https://www.linkedin.com/pulse/7-mini-case-studies-successful-supply-chain-cost-rob-o-byrne

Office of the Assistant Secretary of Defense for Industrial Base Policy. (n.d.). *Defense production act title III overview*. Retrieved from https://www.businessdefense.gov/ibr/mceip/dpai/dpat3/docs/DPA-TitleIII-Overview.pdf

SFK Inc., SKK Marine, & SFK SecCon. (2024, July 19). *Starbucks supply chain management: Optimizing global coffee distribution through risk mitigation and sustainable practices.* https://sfkcorp.com/starbucks-supply-chain-management-optimizing-global-coffee-distribution-through-risk-mitigation-and-sustainable-practices/

Shivakumar, S., & Wessner, C. (2022, June 8). *Semiconductors and national defense: What are the stakes?* Center for Strategic & International Studies. https://www.csis.org/analysis/semiconductors-and-national-defense-what-are-stakes

Supply Chain Quarterly. (2014, February 25). Starbucks adds risk management program to help protect its supply chain. https://www.thescxchange.com/finance-strategy/plan/risk-management-starbucks

Tabansi, O. (2023, December 1). *Starbucks's supply chain challenges and how it overcame them*. https://supplychainnuggets.com/starbuckss-supply-chain-challenges-and-how-it-overcame-them/

U.S. Department of Justice. (2024, October 16). *Raytheon company to pay over $950 million in connection with foreign bribery, export control, and fraud schemes*. https://www.justice.gov/usao-edny/pr/raytheon-company-pay-over-950-million-connection-foreign-bribery-export-control-and

U.S. Senate. (2024). *Restoring freedom's forge act.* Wicker Senate Office. https://www.wicker.senate.gov/services/files/4396C3A9-DA26-4BD6-A655-9E0910B83DA8

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net