MITRE | Center for Data-Driven Policy

MOTIVATING A SUPPLY CHAIN ENTERPRISE APPROACH TO PROTECT THE DEFENSE INDUSTRIAL BASE

The global network of materials, manufacturing, and services that make up the U.S. defense industrial base (DIB) is vulnerable to potential disruptions by adversaries seeking to exploit the Department of Defense's (DoD) supply chain dependencies. The creation of a comprehensive Protect the DIB program offers a pragmatic and cost-efficient solution to safeguard DoD's access and sustainment of critical systems and technologies.

The Case for Action

The U.S. DIB has become increasingly global, with worldwide dependencies ranging from foreign-manufactured equipment and components to foreign investment in research and development (R&D) for critical technologies. This creates significant risk for the DIB where those dependencies intersect with competitor or adversary nations that could weaponize supply chain dependencies. To counter these risks, DoD requires an enterprise-level analytic capability for identifying and mitigating risks to defense systems at scale, including a practical, cost-effective means for verifying the provenance, trustworthiness, accessibility, and non-maliciousness of suppliers that are at risk of influence by adversary nations.

This concept is supported by the objectives outlined in the 2024 National Defense Industrial Strategy (NDIS)[1] by leveraging expanded supply chain visibility to "proactively, aggressively, and systematically" mitigate risks, manage disruptions, and fulfill the requirements of the FY24 National Defense Authorization Act (NDAA).[2] For example, Section 856 of the NDAA calls on DoD to "analyze, map, and monitor supply chains" and identify key risks and vulnerabilities within these supply chains.

Key Challenges and Opportunities

To meet the goals outlined in the 2024 NDIS, a thorough Protect the DIB program is essential. This program requires access to, funding for, and a contractual method to procure a wide range of regularly updated data from both commercial and governmental sources. Utilizing this data necessitates a continuous investment in automation development to comprehensively map DIB supply chains beyond program silos, thereby identifying potential risks and vulnerabilities. The data should be stored in a repository that can be easily queried, allowing information from the Services and Program Offices to be readily stored. The program also requires

DoD requires an enterprise-level analytic capability for identifying and mitigating risks to defense systems at scale.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®
mitre.org

a modeling component to evaluate the effects of certain courses of action (COAs) on cost, schedule, performance, and operational risk. Furthermore, the program must devise a method to share approved risk information with industry, allies, and partners to ensure the security and resilience of the supply chain across public-private interfaces.

However, the establishment of such a comprehensive program presents challenges. Currently, multiple organizations within DoD have a role in supply chain risk and resilience, leading to a lack of centralized or dedicated funding. There remain challenges with how contracts for supply chain data, e.g., bills of material and supplier information, are managed and limitations on data sharing within DoD and across the government. There are also obstacles to sharing information with industry and allied partners to enable risk mitigation COAs. This process is impeded due to concerns regarding industry proprietary information or inadvertently violating contract privity. Legal ambiguity exists regarding who bears potential legal risks and liabilities if information sharing leads to adverse contract actions or if the underlying information is proven outdated or incorrect. Without the ability to share DoD risk information with its partners (industry and international), the government cannot depend on its contractor base and supply chain to adequately mitigate risks, which could ultimately compromise the defense programs themselves. To succeed, an enterprise program will need to ensure it has the necessary policies or legislation to address these challenges, along with appropriate incentives or penalties to foster an effective partnership between the government, partners, and industry for supply chain security.

Data-Driven Recommendations

The following recommendations provide next steps for implementing a Protect the DIB program, agnostic to the specific sources of funding and stakeholders.

1. EFFICIENTLY ACQUIRE AND USE SUPPLY CHAIN DATA.

Contracting methods such as a data consortium can streamline the collection and use of supply chain data by consolidating contracts with supply chain illumination and data vendors and providing efficient access to commercial supply chain capabilities to DoD users. To fully utilize this data for rapid vulnerability discovery, new automated algorithms and software solutions will need to be developed.

2. ENABLE CONTINUOUS RISK ALERTING.

To continuously identify supply chain risks, DoD should consider creating a comprehensive data repository where identified risks can be stored in a secure, accessible database. Authorized DoD users could query the database to understand risks, subscribe to alerts, or report new findings and suggest mitigation strategies, creating a beneficial feedback cycle.

3. IMPLEMENT COA MODELING CAPABILITIES FOR DATA-DRIVEN DECISION MAKING.

The establishment of a quantitative framework for COA modeling is critical to effective supply chain risk management because it provides the capability to assess COA impact to cost, schedule, and performance, allowing decision makers to assess tradeoffs.

4. ESTABLISH FUNDING AND AUTHORITIES.

There is a clear need for a materiel solution that enables users to rapidly assess vulnerabilities across defense supply chains. This includes the development, integration, and hosting of data, as well as the development of automation to accelerate risk identification, requiring funding and clearly delineated authorities within DoD in order to create a robust system.

5. BALANCE MISSION WITH PRIVACY AND CIVIL LIBERTIES.

Update and/or create new policies to ensure adherence to and protection of privacy and civil liberties, while allowing for monitoring and assessment of U.S. companies to determine supply chain risks and promote transparency on DIB supply chains.

6. ESTABLISH MECHANISMS TO SELECTIVELY RELEASE VULNERABILITIES TO INDUSTRY, ALLIES, AND PARTNERS, WHILE MINIMIZING LEGAL RISKS.

New or updated legislation and/or policy guidance is needed to empower DoD to disseminate information to industry and key allies and partners. A potential model that could be adapted is Cybersecurity and Infrastructure Security Agency's (CISA) process for sharing cybersecurity risk information with industry, ensuring that industry, allies, and partners can take mitigating actions while protecting DoD from legal liability.

Implementation Considerations

A comprehensive Protect the DIB program would require a diverse set of regularly updated data, significant focus on automation, and a shift from a program-centric to a supplier-centric approach. Implementing such a program presents several challenges, including the lack of a central authority managing supply chain risk and resilience across the DoD enterprise, lack of dedicated resourcing, and limitations on data sharing across the government and with industry. Changes to DoD policy are likely needed, including updates to the Federal Acquisition Regulation (FAR) to allow for data aggregation and requiring contract primes to share sub-tier supplier information, policy outlining data standardization across services and program offices, and policy updates that allow sharing of information across agency authorities.

MITRE Resources and Support

MITRE has several experts, efforts, and papers related to DIB supply chains. These include:

- Non-Traditional Data Employment for Competition Cross-Cutting Priority (NTD XCP), which seeks to identify economic, supply chain, and cyber links between U.S., adversary, and allied countries using publicly and commercially available data to enable whole-of-nation courses of action. The NTD XCP is partnered with DoD to prototype a capability to detect foreign ownership, control, and influence risks in DIB supply chains at scale.
- System of Trust framework, which provides a taxonomy for supply chain risk management.

Endnotes

1 https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf

2 https://www.congress.gov/bill/118th-congress/house-bill/2670/text

About the Center for Data-Driven Policy

The Center for Data-Driven Policy, bolstered by the extensive expertise of MITRE's approximately 10,000 employees, provides impartial, evidence-based, and nonpartisan insights to inform government policy decisions. MITRE, which operates several federally funded research and development centers, is prohibited from lobbying. Furthermore, we do not develop products, have no owners or shareholders, and do not compete with industry. This unique position, combined with MITRE's unwavering commitment to scientific integrity and to work in the public interest, empowers the Center to conduct thorough policy analyses free from political or commercial pressures that could influence our decision-making process, technical findings, or policy recommendations. This ensures our approach and recommendations remain genuinely objective and data-driven.

Connect with us at policy@mitre.org.