NATIONAL SUPPLY CHAIN INTEGRITY MONTH

A SPOTLIGHT ON

DEFENSE

Fortifying the Defense Industrial Base (DIB) Supply Chains

"Securing Defense-Critical Supply Chains" is the Department of Defense (DoD) response to Executive Order 14017, which directs an assessment of supply chains for the DIB. The study examines vulnerabilities within DIB supply chains that threaten the development and sustainment of critical capabilities essential to national security. While the DoD report focuses on risk to critical capabilities impacting the DIB supply chains, this National Counterintelligence and Security Center (NCSC) Supply Chain Spotlight emphasizes the counterintelligence and security risks highlighted in the DoD report.

Counterintelligence Risks

- **Decreased Supply Chain Visibility**
    - Inability to identify sub-tier suppliers subject to the jurisdiction or direction of a foreign government
    - Difficulty identifying threats, vulnerabilities, and risks in sub-tier supply chains enables the insertion of counterfeit or compromised components into the DIB supply chains
- **Antiquated Acquisition Policies and Procedures**
    - Deterrence of domestic investment due to high capital investment requirements
    - Inconsistent DoD procurement practices create instability in sub-tier suppliers and hinders investment into newer technologies
- **Foreign Ownership, Control, or Influence**
    - DoD market shares are not significant enough to drive commercial/industrial change towards common standards and modernized technologies
    - Heavy reliance on foreign nations and sole source suppliers for critical mission components due to eroded domestic supply chains
- **Cyber Posture of DoD Networks**
    - Cyber actors increasingly targeting the DIB with sophisticated and well-resourced cyberattacks
    - The insufficient cybersecurity postures of DIB software development and distribution channels expose DIB networks to both conventional cyberattacks as well as software supply chain attacks

The counterintelligence risks identified above outline the myriad of risks that the DIB faces. However, the DIB also recognizes the importance of the Information Communications Technology (ICT) supply chain to mission critical goods and services. The ICT supply chain supporting the DIB must be secure to enable mission critical operations around the global. Thus, protecting the ICT supply chain becomes a force multiplier for protecting other critical supply chains, including the DIB supply chains.

NOTE: This NCSC Supply Chain Spotlight summarizes relevant information from the subject report to highlight counterintelligence and security issues. Please review the report in full to understand all supply chain risks identified by the authoring department. **https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF**