Fortifying the U.S. Transportation Supply Chain

The Department of Transportation (DOT) recently published its "Supply Chain Assessment of the Transportation Industrial Base: Freight and Logistics" for its one-year review required by Executive Order 14017, America's Supply Chains. The DOT supply chain analysis focuses on risks from the declining infrastructure supporting the logistics of transporting goods within the country. The report categorizes transportation infrastructure risks by sea, land, air, storage capacity, and availability of trained personnel. DOT proposes ways to keep this dynamic system of transporting goods operational into the far future. While the focus of this report emphasizes organizational, fiscal, and employment risks, this National Counterintelligence and Security Center (NCSC) Supply Chain Spotlight concentrates on counterintelligence threats highlighted in the DOT report's stated risks.

Counterintelligence Risks

According to the DOT report, the American Merchant Marine is in decline and U.S. supply chains rely on ten large foreign-owned ocean carrier companies responsible for 80 percent of the world's shipping capacity. Having no domestic merchant fleet means the U.S. Armed Forces will have to entrust foreign crews to ship weapons and supplies. This increases the risk of sabotage, foreign intelligence collection, and disruption of logistical support to U.S. troops in hazardous situations.

Bottlenecks are increasing at U.S. ports and warehouses, as new space for storage is becoming more difficult to acquire. DOT recommends a new common automation software for all U.S. ports to optimize space, report movement of goods, reduce redundancy, and increase the speed of delivery. The recommended software solution meets the definition of "critical software" developed by the National Institute of Standards and Technology (NIST). Therefore, DOT should follow the NIST security recommendations for protecting critical software to thwart potential risks in the software development process. If such security protocols are not followed, malicious code or activity could be introduced into the software supply chain amplifying bottlenecks or disrupting delivery of critical goods.

DOT recommends a smart automated transportation system to collect data on commodity, product, and raw material flows within the U.S. to help anticipate future points of disruption. Foreign threat malware is a critical supply chain risk to this system, which identifies competitor shipments, prices, and quantities to gain insider advantage against U.S. firms in future trade.

To ensure the successful implementation of DOT's supply chain recommendations, DOT will need to promote secure practices for the Information Communications Technology (ICT) supply chain as well. The ICT supply chain is essential to protecting the transportation innovations needed to mitigate the potential vulnerabilities in a global transportation supply chain.

NOTE: This NCSC Supply Chain Spotlight summarizes relevant information from the subject report to highlight counterintelligence and security issues. Please see the report in full to understand all supply chain risks identified by the department. https://www.transportation.gov/supplychains/EO14017/fullreport