CONTRIBUTED CONTENT & PRESENTATIONS

Supply Chain Security Is National Security: Cyber, Physical, and Personnel Protections

OCTOBER 29, 2024

Authors: Jonathan R. Todd, Vanessa I. Gomez, Megan K. MacCallum

U.S. supply chain security is increasingly under threat. The White House's National Security Strategy describes this moment as an inflection point. Many federal agencies have taken charge in elevating the very concept of "supply chain security" to a subject matter expertise with serious national security implications. The geopolitical basis for this change in tone are ever present. In this year alone, Russia's attack on Ukraine dragged on as an enduring cross-border war, U.S. tensions with China have grown from a trade war to tensions in the South China Sea, and conflict in the Middle East escalates with little sign of resolution, including Houthi attacks on cargo ships. In many ways supply chain professionals now work on the front lines of U.S. national security.

Threat Assessments for Supply Chains

Company supply chain security efforts target three types of risks: Cyber Threats, Physical Security Threats, and Personnel Threats. This article surveys certain federal programs targeting historic and emerging threats within these risk categories together with the corresponding regulatory requirements. This simple three-part construct for assessing categories of threat applies to all asset and non-asset operations. It helps to manage risk assessments, deployment of resources, incident response, and corrective actions in the context of national security. Its value extends well beyond minimum regulatory compliance.

CyberSecurity Controls

Cyber threats are reported with such great frequency they are now fixed in the national consciousness. Supply chains are no different. Two federal agencies that have increased attention on this vulnerability in supply chains are the U.S. Cybersecurity and Infrastructure Agency (CISA) and the Transportation Security Administration (TSA). The theme of these efforts is a need for steadfast awareness and reporting of activities by potential threat actors.

CISA Incident Reporting - The ransomware cyberattack on Colonial Pipeline in 2021 resulted in a multimillion-dollar loss paid to the hackers and nearly a weeklong shutdown of the company's operating systems. The shutdown impacted the U.S. fuel supply, causing localized gasoline, diesel fuel, and jet fuel shortages. This impact was exacerbated by panicked individuals rushing to buy and stockpile fuel for fear of a national shortage. In 2022, President Biden signed into law the Cyber Incident Reporting Critical Infrastructure Act, which requires covered entities, including a number of supply chain participants, to develop a cybersecurity incident reporting plan with near-immediate escalation to CISA. Incidents must be reported within 72 hours and ransomware payments within 24 hours.

TSA Security Directives - The TSA published Security Directives aimed at the rail industries and pipeline operators shortly after the Colonial Pipeline incident. The rail Security Directive targeted freight and passenger rail transportation and public bus transportation. The Directive requires operators to: (1) report actual and potential cybersecurity incidents to CISA; (2) designate a round-the-clock available Cybersecurity Coordinator to serve as a point of contact between the TSA; (3) review current cybersecurity risks; (4) identify vulnerabilities in cybersecurity and develop a plan to address those risks; (5) implement mitigation measures to protect against ransomware and IT attacks; (6) implement a cybersecurity contingency and recovery plan; and (7) conduct a cybersecurity architecture design review. Later in 2023 the TSA issued similar measures for TSA-regulated airport and aircraft operators. Those measures include access control limits for critical cyber systems, and continuous monitoring and detection policies for cybersecurity threats and anomalies.

Physical Security Controls

Physical threats are more traditional in their risk profile, although they remain significant. The protection of cargoes, transportation movements, and facilities has long been a point of concern. National security threats of terrorism, espionage, and even theft are appreciable throughout the supply chain. A wide range of federal agencies have long maintained programs and regulatory requirements to mitigate risk exposure from physical threats. New efforts are emerging for specific geopolitical concerns.

CBP C-TPAT Program - U.S. Customs and Border Protection (CBP) has collaborated with industry under the Customs-Trade Partnership Against Terrorism (C-TPAT) program since 2006, although the roots of the program extend to the immediate post-9/11 era. The program seeks to strengthen the integrity of international supply chains and, more importantly, the importer and service provider relationships throughout those supply chains. Today there are approximately 11,400 certified program participants across the trade community. Those private companies have entered agreements with CBP to bolster supply chain security, including by identifying security gaps in the chain and implementing specific security measures and best practices. In return, the partners receive benefits, including a reduced number of CBP examinations, front of line inspections, shorter wait times at the border, and access to Free and Secure Trade (FAST) Lanes, among others.

TWIC Cards and FCLs - Credentialing and requirements for escorted access to certain facilities, and for those performing certain services, are a widespread tool supporting supply chain security. For example, security clearances and access cards can protect against terrorist violence, theft, and espionage. The Maritime Transportation Security Act requires that workers who access secure areas of maritime facilities and secure vessels are screened and credentialed. The TSA developed and implemented the Transportation Worker Identification Credential (TWIC) card to help meet this need as well as others. These physical security measures protect the U.S. ports as well as carriers and goods that move through them by requiring personnel to pass Security Threat Assessments (STAs). Similar programs exist for other fact patterns, such as the Department of State's facility security clearance (FCL) program that manages levels of access to classified information for Government contractors.

TSA Security Programs - The TSA is also on the front lines of managing physical security for passenger and all-cargo air carrier operations. Public security program requirements for air carriers,

indirect air carriers, and certified cargo screening facilities include stringent STAs, facility security, chain of custody, cargo screening standards, and known shipper requirements. These protocols aim to prohibit introduction of explosives and incendiaries in air traffic while also guarding against violence and air privacy.

PHMSA Security Plan - The U.S. Department of Pipeline and Hazardous Materials Safety Administration (PHMSA) regulates transportation of hazardous materials over U.S. rail, highways, and waters. One of the ways that PHMSA addresses the risk of terrorist threats on hazardous materials in transportation is the requirement for certain parties to develop and maintain a security plan. Movements of explosives, flammable or poisonous gases, flammable liquids, and spontaneously combustible materials, as well as certain toxins and chemicals, require the security plan. It must include an assessment of transportation security risks associated with facilities, such as unauthorized access, and must provide appropriate measures to address those risks. The security plan must also address security of active shipments and of shipments stored incidental to those movements.

BIS Export Controls and OFAC Economic Sanctions - The concept of physical security also extends to export controls and economic sanctions, particularly from a national security perspective. Many of these restrictions were aimed at stifling the economic power and weapons development potential of government, military, and leaders. For example, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) has addressed tensions with China through export controls, along with other agencies including the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC). BIS and OFAC use export controls and trade sanctions respectively to advance national security interests by preventing receipt of sensitive items, such as semiconductor technology, and "blocking" high-risk individuals and entities from transactions. Additionally, BIS maintains a Military End Use List of high-risk entities prohibited from receiving U.S. exports to China. The agencies have also implemented a series of broad-based trade restrictions applicable to dealings with Russia following the invasion of Ukraine.

Personnel Security Controls

Personnel threats are another long-standing risk receiving attention throughout the supply chain. These extend well beyond screenings for who may have access to certain facilities, such as TWIC cards or certain domestic technologies such as deemed export restrictions. Most fundamentally the question of personnel security is seen in restrictions around who may hold certain roles, and responsibility for important functions, with high-impact significance for supply chain security and national security.

TSA Security Coordinator - TSA requires regulated functions, including Indirect Air Carriers (IACs), to appoint both a Cybersecurity Coordinator and a Security Coordinator. The Security Coordinator is a management-level employee who undergoes an STA, which amounts to an FBI background check, and who must be on call 24 hours as the primary point of contact for security-related activities and communications with the TSA.

FMC Qualified Individual - The U.S. Federal Maritime Commission (FMC) similarly requires appointment and scrutiny of a specified individual responsible for compliance of international shipping conducted by Non-Vessel Operating Common Carriers (NVOCCs). Those persons are referred to in regulation as the Qualifying Individuals (QIs). NVOCCs must appoint a QI to be

responsible for compliance and to be accountable to the FMC as a condition to receiving and maintaining their FMC license. The QI must hold an officer-level role at the company, must have at least three years' experience in the ocean transportation intermediary space, must provide employment and professional experience references, and must pass a background check.

CBP Customs Broker - CBP similarly establishes strict requirements for a person to become a licensed U.S. Customs Broker and, importantly from an enterprise perspective, to serve as the Broker-Officer securing a company's license. Brokers hold responsibility for lawfully entering goods into the U.S. for their importer clients, including the financial aspects of calculating and remitting customs duties. The sensitive nature of this role for our supply chain is seen in the need to pass a rigid license examination and post a bond to perform as a broker. An entity seeking license must appoint an individual broker as an officer and must be empowered under its formation documents to conduct customs business, and individuals must undergo background checks including fingerprinting.

Risk-Appropriate Supply Chain Security Programs

Now is the time to take supply chain security seriously. The federal government's approach to these issues has been largely decentralized to date. Collectively these regulatory requirements and their enforcement serve to fortify the supply chain against threats to domestic commercial interests and national security.

As the risk environment grows in response to geopolitical pressures, the need for companies to remain vigilant also grows in importance. Effective supply chain security efforts begin with minimal regulatory requirements but necessarily require tailored focus. No supply chain is exactly like another due to complexities of operational needs, global footprint, and unique relationships. There is no one-size-fits-all solution to Cyber Threats, Physical Security Threats, and Personnel Threats. Each company is free to assess its own risks and programmatic solutions to those vulnerabilities that extend beyond minimum requirements. Enterprise performance, public reputation, and national security are at stake.

Jonathan R. Todd is Vice Chair of Benesch's Transportation & Logistics Practice Group. He may be reached at 216.363.4658 and jtodd@beneschlaw.

Vanessa I. Gomez is an associate with the Practice Group and may be reached at 216.363.4482 and vgomez@beneschlaw.

Megan K. MacCallum is an associate with the Practice Group and may be reached at 216.363.4185 and mmaccallum@beneschlaw.com.