NATIONAL SUPPLY CHAIN INTEGRITY MONTH

A SPOTLIGHT ON

AGRICULTURE

Fortifying the Agri-Food Supply Chain

The Department of Agriculture's (USDA) one-year report, *"USDA Agri-Food Supply Chain Assessment: Program and Policy Options for Strengthening Resilience"* as required by Executive Order 14017, *America's Supply Chains*, highlighted four supply chain vulnerabilities: Pesticides; Farm Machinery parts, products dependent on low labor costs, and cyber attacks. USDA's supply chain analysis was specific to China due to concerns regarding China's retaliation against U.S. trade actions and tariffs imposed in the last several years. This NCSC Supply Chain Spotlight focuses on counterintelligence risks highlighted by the stated vulnerabilities in the USDA Report.

Counterintelligence Risks

The USDA analysis illuminated that active ingredients of pesticides are the most essential U.S. imports from China, valued at more than $2 billion annually. These include the primary ingredients in some commonly used pesticides, such as glyphosate. China provides more than 70 percent of imports of several pesticide ingredients, and many of these are not available domestically. Greater geographic concentration and interdependence of such critical ingredients may create bottlenecks that can result in interruptions and opportunities for foreign adversaries to limit access to these critical ingredients.

In addition, cyberattack temporary shutdowns at supply chain "choke points" in food production, manufacturing, and distribution can produce significant disruption. For example, a May 2021 cyberattack on the second largest U.S. meat processing firm forced a three-day closure of 25 percent of beef and 20 percent of pork processing national capacity, respectively.

The USDA report states that to be most effective, the federal government needs an interconnected dynamic food supply chain monitoring platform to bolster protection against cyberattacks, and ensure data integrity and confidentiality across agency partners. In addition to informing real-time response, use of an interconnected dynamic platform could also be used for longer-term assessments of supply chain vulnerabilities and metrics.

For this platform to be fully successful, strong software supply chain integrity best practices will need to be employed. Employing a software bill of materials (SBOM), for example, will offer rapid identification of significant vulnerabilities such as the Log4shell exploit or the SolarWinds Orion software supply chain attack that could disrupt the food supply chain. Thus, protecting the ICT supply chain is essential to protecting all other critical supply chains, including the food supply chain.

NOTE: This 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://www.ams.usda.gov/sites/default/files/media/USDAAgriFoodSupplyChainReport.pdf