NATIONAL SUPPLY CHAIN INTEGRITY MONTH

MANUFACTURING AND PRODUCTION

National Counterintelligence and Security Center Factsheet
April 2021

THREATS

The manufacturing and production industry must address physical, human, and cyber threats in order to secure their supply chains. Physical threats include climate change/natural disasters that may reduce the supply of raw materials and disrupt production of final products. Facility flaws – "guards and gates" – also present a physical threat that may allow penetration points at manufacturing sites. Malicious human actions (e.g., crime, sabotage, and terrorism) and non-malicious human actions (e.g., accidents and negligence) also threaten "just in time" manufacturing schedules. Finally, cyber threats including ransomware attacks, software supply chain exploits a means by which threat actors may compromise industrial control systems as well as corporate networks and information systems bringing production to a standstill.

BEST PRACTICES

- **Fortify Facility & Utility Information Systems**: Fortify any utility penetration point that operates Emergency Communication Systems, Building Access Systems, and/or other resources: commercial power, telecommunications, water, natural gas, etc. When such systems are connected to the internet, vulnerabilities can be introduced allowing for cyber-enabled remote intrusions.
- **Institute Full Product Integrity Tracking**: Track all products coming in and out using unique IDs or digital markers. Utilize barcodes, RFIDs, GPS, when possible. Ensure and document traceability for everything that passes through the supply chain.
- **Maintain Physical Backups**: Ensure redundancy in all parts of the manufacturing supply chain, both physical and digital. Implement backup generators, emergency stockpiles, fail-safes, and "golden copies" (master versions) of data.
- **Practice Due Diligence**: Be active in maintaining cyber hygiene. Routinely audit all elements of critical infrastructure— physical, cyber, and human. Utilize DHS cyber & vulnerability assessments, reviews, the National Vulnerability Database, and National 304 Checklist Program.
- **Protect Commercial Consumer Account Data**: Protect consumer personal identifiable information (PII) with the same level of protection as company proprietary data.
- **Participate in Public-Private Partnerships**: Communicate with stakeholders in the manufacturing sector to provide a coordinated front against supply chain threats. Attend "information-sharing venues" such as conferences, forums, workshops, threat briefing, tabletop exercises, working groups, as well as the Annual Critical Manufacturing Sector Security Conference.
- **Check for Vendor SCRM Programs:** Contract with vendors, suppliers and subcontractors that have supply chain risk management (SCRM) programs and uphold federal NIST ICT standards.

NOTE: Information contained herein was gathered from the most reliable sources found in the public domain on supply chain risk management, including information from the Department of Homeland Security, the National Institute of Science and Technology, the Federal Bureau of Investigation, and the National Counterintelligence and Security Center.

The information in this product was prepared with the assistance of the 2021 Federal Virtual Intern Service