



NATIONAL SUPPLY CHAIN
INTEGRITY MONTH



A SPOTLIGHT ON

HEALTH & HUMAN SERVICES

Fortifying the U.S. Public Health Supply Chain and Industrial Base

In response to Executive Order 14017, the Department of Health and Human Services (HHS) released its “[Public Health Supply Chain and Industrial Base One-Year Report](#),” which outlines HHS’s initiatives to help make our public health supply chain and industrial base more resilient, diverse, and secure. The report also identifies key weaknesses to this crucial supply chain. HHS efforts to enhance visibility into this critical supply chain supports our nation’s counterintelligence and security community. While the focus of this report emphasizes resiliency risks, this National Counterintelligence and Security Center (NCSC) Supply Chain Spotlight focuses on counterintelligence risks based on the supply chain threats identified in the HHS report.

HHS-Identified Counterintelligence Risks

- Foreign dependencies
- Single source for supplies
- U.S. access to raw materials
- Lack of visibility and coordination between federal state, local, and tribal governments
- Counterfeit products entering the U.S.
- Reliance on semiconductors for medical devices

Whether the public health supply chain or industrial base is disrupted by another global pandemic, a weather event, foreign intelligence entities, or economic disruption, strengthening how the U.S. anticipates and manages challenges will make the nation more resilient and better prepared for future public health emergencies.

The majority of recommendations identified in the HHS report focus on improving information and communications technologies (ICT), thus a heavy reliance on the ICT supply chain. Specifically, software improvements are needed to better manage the public health supply within the industrial base. Mitigating the activities of foreign intelligence entities and other adversaries who attempt to compromise the ICT supply chain to target or misuse health supply or industrial base support is critical to the nation’s preparation. Foreign adversaries targeting the ICT supply chain may gain access to the healthcare industrial base in order to collect private, medical, genomic, biometric, economic, and financial information that is processed or stored on systems in the public health supply chain and industrial base. Thus, protecting the ICT supply chain is just as important as protecting the health supply chain and industrial base.

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://aspr.hhs.gov/MCM/IBx/2022Report/Pages/default.aspx>