Cyberspace Solarium Commission Calls for Cohesive IT Supply Chain

DHS will be a key leader for IT supply chain security efforts, according to a new report.

Kate Macri
Thu, 10/22/2020 - 14:03

The Cyberspace Solarium Commission wants the Department of Homeland Security to work with other federal agencies and Congress to address significant vulnerabilities in the IT supply chain by reshoring manufacturing of some critical parts, integrating supply chain risk management intelligence efforts, and shifting the supply chain away from China and overall Chinese influence.
In a new report, the commission calls for the agency-specific supply chain risk management task forces to consolidate under “a single vision and strategy” to better address supply chain risk and eliminate risk management blind spots. It also asks DHS to lead the creation of technology security centers to test and evaluate information and communications technologies (ICT) to better secure the supply chain.

The commission names China as a notable source of risk for the ICT supply chain and wants the White House and Congress to draft their own version of “Made in China 2025.”

The U.S. relies heavily on China for the mining of key raw materials — like silicon and germanium for semiconductor chips and rare earth materials (REE) for improving hardware performance. The U.S. also relies on countries susceptible to Chinese influence (including Taiwan, Japan and South Korea) for various stages of semiconductor development, like fabrication.

“In July 2020, Intel, which has traditionally produced its own semiconductors, placed a multibillion-dollar order with Taiwan Semiconductor Manufacturing Company (TSMC) to outsource a portion of wafer fabrication,” the report said.

One reason the report details for a largely offshore ICT supply chain is the ICT market’s high barriers to entry. Information and communications technologies are industries heavy in capital expenditures, requiring large amounts of investment upfront. The industry is also deeply consolidated with very little market competition.

China developed a competitive edge in the ICT market due to government subsidies and an aggressive, government-led prerogative to make China the world leader in ICT manufacturing and services.

To limit overreliance on China and other southeast Asian countries susceptible to Chinese influence, the commission wants DHS and other agencies like the Defense Department and the departments of State and Commerce to identify and catalogue a complete roster of key ICT parts and components, then help identify states, municipalities and localities as prime places to resshore manufacturing and development of some of those parts and components.
“Through DHS, the executive branch should identify five suitable candidates for establishing critical technology clusters and work with relevant state and local government and private stakeholders to facilitate their launch through Foreign Trade Zone designations, tax incentives, and government investment in research and development,” the report said.

By reshoring some critical segments of the U.S. ICT supply chain, like chip manufacturing, the U.S. can build an “ICT industrial base” and won’t face an IT catastrophe if nation-state actors try to disrupt or compromise the supply chain.

The biggest ask of the commission is a National Supply Chain Intelligence Center, which would “integrate and consolidate” other agency-specific task forces, like DHS’ ICT Supply Chain Risk Management Task Force.

“The Center, which could take the form of either a new or existing structure, should be designed to integrate supply chain intelligence efforts from across the federal government with those of other public and private partners and should serve as the central and shared knowledge resource for threats to supply chain activities or supply chain integrity,” the report said.

This request builds off of the wish list in the commission’s March 2020 white paper, which called for a National Cyber Director to bring cohesion to the nation’s cybersecurity posture.

The commission also wants DHS to lead the selection of three Critical Technology Security Centers to continuously test and evaluate ICT for commercial and government use. These centers could be another line of defense against vulnerabilities and compromises in the ICT supply chain, especially within imported components or finished products.

The three centers should focus on network technology security, connected industrial control systems security and open-source software security, especially as software supply chains become increasingly critical to ICT infrastructure, the report said.
Other notable recommendations listed by the commission include Congress-funded research and development for critical technologies and ensure a strong domestic market for telecommunications equipment by tying 5G infrastructure investment to interoperable standards.

National security concerns over the U.S. ICT supply chain continue to grow as the U.S. and other highly developed countries increasingly rely on ICT infrastructure for all aspects of societal functioning, including businesses, schools and local governments. Mass telework due to the COVID-19 pandemic has only increased this reliance on ICT infrastructure.

“The imperative is clear,” said the commission in the report. “Chinese government interventions in its own domestic industry, in global trade and in standard-setting bodies has created an uneven playing field on which companies in the United States and partner countries struggle to compete. ... Now is the time for strategic cohesion.”

View printer friendly version
Department of Homeland Security
5G
IT infrastructure
Cybersecurity Solarium Commission
Federal Cybersecurity
DOD
IT supply chain
Standard