IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry

DEFEND TODAY,
SECURE TOMORROW

OVERVIEW OF EXECUTIVE ORDER 14017 – AMERICA'S SUPPLY CHAINS

On February 24, 2021, President Biden signed Executive Order 14017, "America's Supply Chains" to strengthen the resilience of U.S. supply chains. The Executive Order directed the Secretary of Commerce and the Secretary of Homeland Security to submit a one-year report on supply chains for critical sectors of the information and communications technology (ICT) industrial base. The scope of the assessment includes a study of the supply chains supporting communications hardware, computing and data storage hardware, end-user devices, as well as critical software including open-source software and firmware. The Departments of Commerce and Homeland Security (DHS) have provided the report titled, Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry, to the President.

BACKGROUND

The ICT industry produces the technologies that individuals, companies, and governments alike rely on to connect and protect our society. The reliance on ICT products across all critical infrastructure sectors of the economy underscores the critical importance of this industry to U.S. economic growth and national security. While U.S. companies continue to lead on design innovation for products including communications equipment, computer and data storage, and end-user devices, manufacturing for these products has largely shifted to Asia, and China in particular.

The risks of ceding much of the ICT manufacturing supply chain to Asia has become apparent during the COVID-19 pandemic, when the U.S. ICT industry experienced supply chain disruptions that reduced the availability and timeliness of critical ICT components and products. The report analyzes the impact of this loss of domestic manufacturing and also evaluates the current supply chain conditions for select hardware and software products, key risks that threaten to disrupt those supply chains, the robustness of the domestic ICT workforce, as well as impacts from climate related issues. To address issues and risks, the report recommends a whole-of-government strategy to strengthen ICT supply chain resiliency.

RECOMMENDATIONS

Building a more secure and resilient ICT supply chain will require significant effort from the government as well as industry stakeholders to implement the long-term strategy detailed in the assessment. To supplement this comprehensive approach, DHS is taking the following immediate actions to support and secure this vital industry:

Revitalize the U.S. ICT Manufacturing Base

Over the past 30 years, the U.S. ICT industrial base has evolved into a highly globalized industry with U.S. companies leading on design innovation for products in key end-use markets including communications equipment, computer and data storage, and end-user devices. However, during this time, manufacturing for these products has largely shifted to Asia, and China in particular. As a result of the decades-long shift to Asia, the U.S. ICT manufacturing base represents a small percentage of the domestic ICT industry and one that produces low-volume, highly specialized products. To address the current dependency on a single region, nation, or manufacturer to produce U.S. ICT goods, efforts must be made to revitalize the domestic manufacturing ecosystem. DHS, in consultation with industry stakeholders, is committed to investing in a long-term solution that strengthens U.S. manufacturing capabilities and builds resilience throughout the U.S. ICT supply chains.

Support the private sector in expanding manufacturing capacity through financial incentives and procurement preference:

- Incentivize the U.S. government's purchase of ICT products, services, and components to be made by domestic producers and service providers, particularly small to mid-size manufacturers. In addition, implement enhanced Buy American Act provisions that incentivize the production of ICT products and services which bring significant revenue to the U.S. economy, including design contribution, and with tolerances for assembly in allied or partner nations.

Build Resilience through Secure and Transparent Supply Chains

The U.S. ICT industry relies on globalized and complex supply chains which complicates industry's ability to elucidate all suppliers and ensure product integrity and security throughout the supply chain. The lack of supply chain transparency and security assurance presents several risks, such as the insertion of counterfeit or used parts into critical hardware components and the injection of malicious software code. While the private sector must take the lead on building more transparency and security into their supply chains, the U.S. Government should promote such practices through the following actions:

Promote supply chain risk management practices through procurement and monitoring efforts:

- Continue to support the supply chain transparency and resilience work of the Cybersecurity and Infrastructure Security Agency's (CISA) ICT Supply Chain Risk Management (SCRM) Task Force as it focuses on key issues such as identifying appropriate information for the development of a baseline hardware bill of materials template that organizations can use when procuring or deploying ICT products as well as identifying ways in which small and medium-sized ICT businesses can strengthen their supply chain resilience.
- In support of the *National Strategy to Secure 5G*, CISA will continue to lead 5G risk management efforts so the U.S. can fully benefit from all the advantages 5G connectivity promises to bring. The *CISA 5G Strategy* establishes five strategic initiatives that stem from the four lines of effort defined in the *National Strategy to Secure 5G*. Guided by three core competencies: Risk Management, Stakeholder Engagement, and Technical Assistance, these initiatives include associated objectives to ensure there are policy, legal, security, and safety frameworks in place to fully leverage 5G technology while managing its significant risks.
- Continue to advance the work of CISA's Joint Cyber Defense Collaborative (JCDC). Established in August 2021, the JCDC leverages new authorities provided by the National Defense Authorization Act (NDAA) of 2021 to bring partners—including those in federal and state, local, tribal, and territorial governments and the public and private sectors—together to unify defensive actions and drive down risk in advance of cyber incidents occurring. This collaboration is designed to strengthen the nation's cyber defenses through planning, preparation, and information sharing. As a community, the JCDC deploys innovation, collaboration, and imagination to protect American businesses, government agencies, and the American people against malicious cyber activity. CISA and its partners, through the JCDC, responded to the widespread exploitation of a critical remote executive vulnerability in Apache's Log4j software library.
- Advance the work of the Federal Acquisition Security Council (FASC)—the interagency body tasked with enhancing the security, resiliency, and reliability of federal ICT by developing uniform criteria for programs across federal agencies; improving information sharing on supply chain risk, including government to government, government to industry, and industry to industry; and setting forth procedures for making exclusion and removal determinations for any ICT considered to represent a security risk. Additionally, the FASC has appointed DHS, acting through CISA, as the executive agency for overseeing information sharing guidance that it sets forth.

Collaborate with International Partners to Improve Supply Chain Resiliency

The globalized nature of the ICT supply chain necessitates solutions to enhance supply chain resilience, must include collaboration with U.S. ally and partner nations. Through international engagements, the U.S. can work to diversify the ICT manufacturing base, develop standards that enhance security, and strengthen trade mechanisms to counter unfair practices.

Improve international collaboration to advance shared interests:

- Enhance federal government participation in global ICT standards development activities and encourage U.S. companies to also increase participation in such activities. This includes promoting awareness and adoption of existing international standards, risk mitigation techniques, and best practices used for securing the ICT supply chain with subject-matter experts and foreign partners.
- DHS will continue to participate and advance the work of the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an interagency committee authorized to review certain transactions involving foreign investment in the U.S. to determine the effect of such transactions on the national security of the U.S. On February 13, 2020, regulations implementing the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) took effect to expand the jurisdiction of CFIUS. FIRRMA now requires investors to file mandatory declarations for transactions in certain critical technologies, critical infrastructure, or the personal data of U.S. nationals. These businesses are known as TID businesses (technology, infrastructure, and data).
- Through the Committee for the Assessment of Foreign Participation in the United States Telecommunications Sector or "Team Telecom," DHS will continue to assist the Federal Communications Commission (FCC) in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the U.S. telecommunications sector.

Invest in Future ICT Technologies

Innovation through research and development efforts is the foundation for a thriving ICT industry. While the U.S. remains the global leader in the research and development of cutting-edge technologies, continued investment is needed to sustain a prosperous R&D ecosystem and remain globally competitive.

Sustain the R&D ecosystem through federal programs and legislation:

- DHS will continue to invest in early stage R&D projects and products, including those in the ICT space, through several of its programs including the Silicon Valley Innovation Program, the Small Business Innovation Research Program, and the National Urban Security Technology Laboratory.

Engage with Industry Stakeholders on Resiliency Efforts

Ongoing engagement with U.S. ICT companies will be critical to share information, address needs, and mitigate risks.

Strengthen public-private engagements:

- Continue to build and leverage existing public-private partnerships through fora such as CISA's ICT Supply Chain Risk Management (SCRM) Task Force. These partnerships are crucial to developing and incentivizing an information sharing community among industry players that will help to inform industry, the public, and the government about risks facing ICT supply chains. Over the past two years, the Task Force has produced groundbreaking studies and developed resources to assess the trustworthiness of vendors and suppliers, and analyze and mitigate threat scenarios for ICT products and services. The Task Force has also developed recommendations to improve the sharing of supply chain risk information between government and industry, and guidance on how to build more resilient ICT supply chains.

RESOURCES

- CISA's Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry: www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry
- CISA's Executive Order 14017 webpage: CISA.gov/eo14017
- ICT Supply Chain Risk Management: CISA.gov/supply-chain
- NRMC Resources: CISA.gov/nrmc-resources