CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAINS

Christopher Kincaid
June 20, 2022

Purpose and Outcomes

Purpose: Review the U.S. effort to evaluate the supply chain conditions and disruption risks for hardware and software products and develop strategies to strengthen supply chain resiliency.

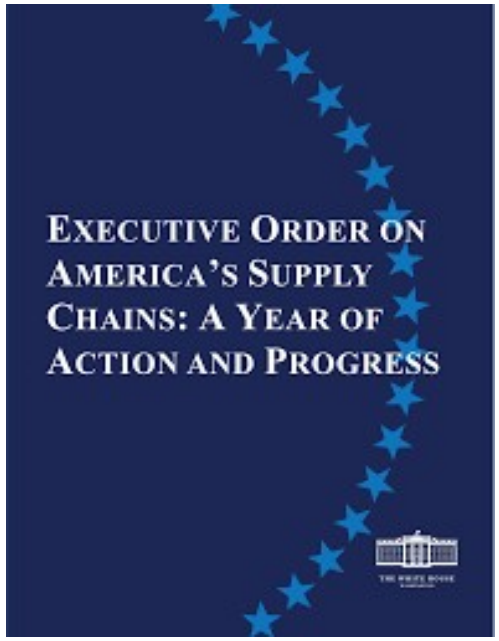
Outcomes:

- Review of report findings on the information and communications technology (ICT) supply chains.
- Understand interconnectivity as a driver of vulnerability and risk to supply chains.
- Consideration of risk management recommendations to limit future supply chain disruptions.

America's Supply Chains Effort

In 2021, President Joe Biden issued Executive Order 14017: *Securing America's Supply Chains*, mandating one-year government-led supply-chain reviews.

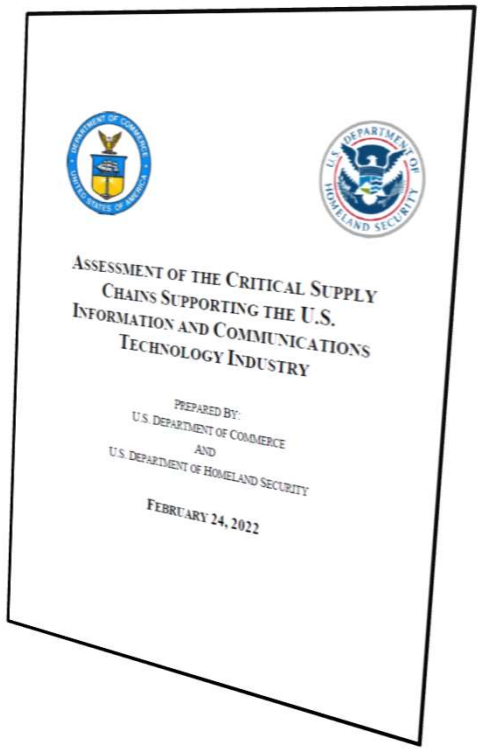
- The reviews were focused on the need for resilient, diverse, and secure supply chains to ensure U.S. economic prosperity and national secure
- The Departments of Commerce and Homeland Security conducted a one-year assessment of the supply chains for the U.S. ICT industrial base.



ICT Supply Chain Assessment

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

- Studied supply chains for communications hardware, computing and data storage hardware, end-user devices as well as critical software including open-source software and firmware.
- Identified key risks to ICT supply chain.
- Assessed the ICT workforce.
- Provided recommendations on ICT supply chain transparency, resiliency, and security.



Assessment Key Findings

State of ICT Manufacturing and Related Challenges

- The U.S. continues to lead in ICT development and innovation in many product categories.
- However, production and assembly of many products is increasingly concentrated in China.

State of the ICT Software Sector and Related Risks

- The nature of the current ICT software ecosystem creates several security risks.

State of the ICT Workforce and Related Risks

- The domestic manufacturing and software development industry struggles to find qualified employees.

Cross-Cutting Supply Chain Vulnerabilities Impacting the ICT Industrial Base

- Structural vulnerabilities across the ICT supply chains present several disruption risks.

External Risks to the ICT Industrial Base Supply Chain

- The U.S. is overexposed to externally derived risks stemming from intellectual property theft, economic dependencies, weak labor standards and climate concerns.

Supply Chain Vulnerabilities

- Pandemic related supply and demand shifts and bottlenecks
- Lack of ecosystem for electronics production
- Single source and single region suppliers
- Lack of visibility of junior tier suppliers
- Inventory management
- Maintaining supply chain hardware and software integrity
- Extended supply chains

External Risks to ICT Supply Chain

- Theft of intellectual property and cyber intrusions
- Economic risks
- Forced labor risks
- Climate risks

Assessment Recommendations

Revitalize the U.S. ICT Manufacturing Base

Build Resilience through Secure and Transparent Supply Chains

Collaborate with International Partners to Improve Supply Chain Security and Resiliency

Invest in Future ICT Technologies

Strengthen the ICT Workforce Pipeline

Ensure Sustainability Remains a Cornerstone of ICT Development

Engage with Industry Stakeholders on Resiliency Efforts

Continue to Study the ICT Industrial Base

Actions Taken

ICT Manufacturing

- Investments in Manufacturing Ecosystem, such as the $1 billion Build Back Better Regional Challenge, and the Economic Development Administration.
- Funding programs to advance long-term competitiveness of U.S. manufacturing.
- The America COMPETES Act, authorizing Commerce to monitor and map gaps in domestic supply chains, and make investments to rebuild essential capacity.

Advisory Committee on Supply Chain Competitiveness

- Commerce launched a reconstituted federal advisory committee within the International Trade Administration called the *Advisory Committee on Supply Chain Competitiveness*.

Security

- The National Institute of Standards and Technology (NIST) released a Secure Software Development Framework – a set of secure software development practices for each software development lifecycle.
- The NIST is updating the NIST Cybersecurity Framework, including how to integrate best practices on supply chain security.

International Summits

- Ministerial-level convening of international partners, private sector and other stakeholders, to discuss securing global supply chain resilience in October 2022.

Actions Taken

ICT Manufacturing and Workforce

- Incentivize the U.S. government's purchase of domestic ICT products, services, and components,

Secure and Transparent Supply Chains

- Continue to support the supply chain transparency and resilience work of CISA's ICT Supply Chain Risk Management Task Force.
- Developing templates for ICT businesses procuring or deploying ICT products.
- Continue to lead 5G risk management efforts so the U.S. can fully benefit from 5G connectivity.

Collaborate with International Partners

- Enhance and encourage federal government participation in global ICT standards development activities.
- Continue to advance the work of the Committee on Foreign Investment in the United States.

Invest in Future ICT Technologies

- Continue to invest in early-stage R&D projects and products, including those in the ICT space.

Engage with Industry Stakeholders

- Continue to build and leverage public-private partnerships such as CISA's ICT SCRM Task Force.

Conclusion

"Promoting a more secure and resilient ICT supply chain is going to take a whole-of-government approach, working together to protect and strengthen the very supply chains that keep our economy running and our communities safe. However, ***government cannot accomplish this goal alone*** *- there is also important work to be done by the private sector and other non-governmental partners."* - Secretary of Commerce Gina M. Raimondo and Secretary of Homeland Security Alejandro Mayorkas

Excerpt from Introductory Note to *Assessment Of The Critical Supply Chains Supporting The U.S. Information And Communications Technology Industry*

For more information:

www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry

Questions?

Email:
christopher.kincaid@cisa.dhs.gov
Phone: 202.309.0923