

**MAY 24, 2022**

For more information,
contact:

Stephen J. Orava
+1 202 661 7937
sorava@kslaw.com

Christine E. Savage
+1 202 626 5541
csavage@kslaw.com

J. Michael Taylor
+1 202 626 2385
jmtaylor@kslaw.com

Jamieson L. Greer
+1 202 626 5509
jgreer@kslaw.com

Patrick J. Togni
+1 202 626 2958
ptogni@kslaw.com

Adam Harper
+1 202 393 3799
arharper@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue,
NW
Suite 900
Washington, D.C. 20006
Tel: +1 202 737 0500

Departments of Commerce and Homeland Security Release Report on Information and Communications Technology Supply Chain

EVALUATES INFORMATION AND COMMUNICATIONS TECHNOLOGY INDUSTRY AND PROPOSES RECOMMENDATIONS FOR INCREASED DOMESTIC PRODUCTION

This is the third in a series of client alerts regarding intensive assessments of six key supply chains – including supply chains supporting the U.S. information and communications technology (“ICT”) industry – that President Biden ordered last year pursuant to Executive Order on America’s Supply Chains (the “American’s Supply Chains E.O.” or “E.O. 14017”). As we previously reported, E.O. 14017 required relevant agencies to conduct comprehensive, “whole-of-government” reviews of identified critical supply chains. These reviews were to be undertaken in two steps. The first step required an immediate analysis (within 100 days of the executive order) concerning four key supply chains. The second step required more intensive, sectoral-specific supply chain assessments to be completed within one year of E.O. 14017 — including a report on the domestic ICT industrial base. Pursuant to the second step, the Department of Commerce (“DoC”) and Department of Homeland Security (“DHS”) jointly issued a report on February 24, 2022 entitled “Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry” (the “One-Year ICT Report”).

The One-Year ICT Report examines critical sectors and subsectors of the ICT industrial base. For purposes of the One-Year ICT Report, the ICT industrial base consists of communications equipment, data storage, and end-user devices, as well as critical software including firmware and open-source software. A list of twenty-seven North American Industry



Classification System (“NAICS”) codes used to define the ICT industrial base is included as Appendix B to the One-Year ICT Report. The One-Year ICT Report “evaluates the current supply chain conditions for [the selected] hardware and software products, identifies key risks that threaten to disrupt those supply chains, and proposes a strategy to mitigate risk and strengthen supply chain resiliency.”

CURRENT STATE OF U.S. INDUSTRIAL BASE AND RELATED RISKS

The One-Year ICT Report addresses the following areas of concern regarding the current state of the U.S. ICT industrial base: (1) ICT manufacturing; (2) ICT software; (3) ICT workforce; (4) cross-cutting ICT industrial base supply chain vulnerabilities; and (5) external risks to the ICT industrial base supply chain.

1. ICT MANUFACTURING

DoC and DHS conclude that “manufacturing for a wide range of critical ICT hardware products is currently concentrated in Asia” from components to final products. Key examples that were examined in the report include: (1) printed circuit boards; (2) fiber optic cables; (3) printed circuit board assemblies and electronic assemblies; (4) routers, switches, and servers; and (5) LCDs/displays.

The report determined that China’s share of production is increasing across all five product categories. For example, China holds 52.4 percent of global printed circuit manufacturing sales (\$32.7 billion) while the United States holds an estimated four percent (\$2.88 billion). The One-Year ICT Report describes some of the causes for the shift to China, including China’s market-distorting trade practices, provision of subsidies, and significant state ownership in ICT manufacturing operations.

2. ICT SOFTWARE

The One-Year ICT Report examines the software and firmware used in ICT products, which enable “the underlying ICT hardware to function, directs flows and processing of information, and facilitates a user’s interaction with a technology product.” The report describes the increasing use of open-source software (“OOS”) in software development, stating that “75 percent of all audited codebases in 2020 contain[ed] at least one open-source component and open source compris[ed] 70 percent of the overall code.” While OOS “has accelerated innovation and provides economic and societal benefits,” the report also expressed concerns about security vulnerabilities that are embedded into OOS and incorporated into finished software.

The One-Year ICT Report also noted that the firmware level of software is “a large and ever-expanding attack surface” and that “hackers have increasingly targeted firmware to launch devastating attacks.”

3. ICT WORKFORCE

DoC and DHS identify an urgent need to expand domestic training and educational opportunities in order to create the workforce that is necessary to increase domestic production of ICT products.

4. CROSS-CUTTING ICT INDUSTRIAL BASE SUPPLY CHAIN VULNERABILITIES

The One-Year ICT Report identifies several “cross-cutting vulnerabilities impacting the U.S. ICT industrial base,” including ongoing challenges due to the COVID-19 pandemic, systemic disadvantages caused by a decades-long lack of sufficient domestic investment in ICT manufacturing, overreliance on single-source and single-region suppliers, insufficient transparency at all tiers of the ICT supply chain, threats to supply chain resiliency that are caused by “just-in-time” inventory management planning, and how bad actors (e.g., insider threats or counterfeit components) can cause harm to an ICT organization’s business.



5. EXTERNAL RISKS TO THE ICT INDUSTRIAL BASE SUPPLY CHAIN

The One-Year ICT Report notes that the ICT sector “is also vulnerable to external risks attributable to geopolitical tensions, economic dependencies, labor, and climate concerns” and notes that the ICT Industry “is particularly vulnerable to supply chain shocks.” Examples include intellectual property theft and cyber intrusions, overreliance on offshoring, the presence of forced labor in the ICT supply chain, and supply chain vulnerability due to climate change.

RECOMMENDATIONS

DoC and DHS recommend several policy and legislative actions to address the threats to the ICT supply chain, including the following:

1. REVITALIZE THE U.S. ICT MANUFACTURING BASE THROUGH GOVERNMENT FUNDING AND INCREASED USE OF BUY AMERICAN PROVISIONS

As a result of the large shift in ICT production 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.” The One-Year ICT Report recommends providing support for expanding manufacturing capacity by: (1) utilizing U.S. government procurement and funding incentives such as Title III of the Defense Production Act and the Creating Helpful Incentives to Produce Semiconductors for America (“CHIPS”) Act; (2) providing incentives through the National Institute of Standards and Technology’s (“NIST”) Manufacturing Extension Partnership (“MEP”); (3) implementing strong Buy America provisions; (4) encouraging the inclusion of ICT manufacturing supply chains in DoC’s Comprehensive Economic Development Strategies; and (5) increasing minority participation in the ICT supply chain.

2. BUILD RESILIENCE THROUGH SECURE AND TRANSPARENT SUPPLY CHAINS

Several steps may be taken in ICT supply chains to address risks, such as the insertion of counterfeit or used parts into critical hardware components and the injection of malicious software code. The One-Year ICT Report recommends the implementation of supply chain risk management practices through U.S. procurement requirements and monitoring efforts. The report also recommends building upon Executive Order 14028 ([Improving the Nation’s Cybersecurity](#)) to create “pilot programs for consumer software and [Internet of Things] labeling; developing minimum elements for a Software Bill of Materials (“SBOM”); and prioritizing security initiatives for open-source software.”

To this end, the report recommends the creation of an Assured Supplier Program for ICT purchases by the federal government and the establishment of a Critical Supply Chain Resilience Program at DoC to “identify, monitor, and address supply chain vulnerabilities and partner with industry, labor, and other public and private stakeholders to strengthen resilience throughout the ICT industry,” including in the critical infrastructure sector.

3. COLLABORATE WITH INTERNATIONAL PARTNERS

DoC and DHS recommend improving international collaboration to advance shared interests in key areas such as joint investment opportunities, information-sharing, and cooperation on sustainability, labor, and security standards.

4. INVEST IN FUTURE ICT TECHNOLOGIES

The report indicates that robust research and development (“R&D”) spending is required for the United States to remain competitive. Other funding proposals would target manufacturing technology enhancements, job training, R&D tax credits and funding the CHIPS Act, and investing in institutions that serve minorities “to expand the participation of underserved communities into public and private R&D ICT ecosystems.”



5. STRENGTHEN THE ICT WORKFORCE PIPELINE

The One-Year ICT Report recommends intensive use of federal funds to expand access to computer science and science, technology, engineering, and mathematics (“STEM”) programs while also encouraging states to “develop and fund programs through their allocation of the \$42.5 billion Broadband Equity, Access, and Deployment program funded in the Bipartisan Infrastructure Law.”

6. ENGAGE WITH INDUSTRY STAKEHOLDERS ON RESILIENCY EFFORTS

The One-Year ICT Report recommends strengthening public-private engagement on supply chain and ICT domestic manufacturing projects. In particular, the report urges the Office of Management and Budget Made in America Office (“MIAO”) and Made in America Council to “promote domestic sourcing and communicate best practices used across agencies facing similar challenges for both procurement and financial assistance projects.”

CONCLUSION

The One-Year ICT Report lays out a blueprint for intensive investment by the United States in the ICT industrial base in order to mitigate risks and to spark innovation in this critically important supply chain. Affected stakeholders should take steps now to determine how best to participate as the process unfolds in the near future.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 23 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.” View our [Privacy Notice](#).

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MIAMI	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	