ASSESSMENT OF THE CRITICAL SUPPLY CHAINS SUPPORTING THE U.S. INFORMATION AND COMMUNICATIONS TECHNOLOGY INDUSTRY

PREPARED BY:

U.S. DEPARTMENT OF COMMERCE

AND

U.S. DEPARTMENT OF HOMELAND SECURITY

FEBRUARY 24, 2022

Introductory Note

From Secretary of Commerce Gina M. Raimondo and Secretary of Homeland Security Alejandro Mayorkas

Over the past year, the Departments of Commerce and Homeland Security have worked in concert to evaluate the strength and resilience of the information and communications technology (ICT) supply chains pursuant to Executive Order 14017, on "America's Supply Chains." The resulting report, *Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry*, was drafted by our departments after consulting with hundreds of stakeholders from across the ICT industry, the Federal Government, and the academic community. We would like to thank those who have contributed to this report through public comments, briefings, and consultations.

The enclosed report evaluates the current supply chain conditions facing the ICT industry, identifies key risks that threaten to disrupt those supply chains, and proposes a strategy to mitigate risk and strengthen supply chain resiliency.

The importance of having resilient and secure supply chains supporting the U.S. ICT industry cannot be overstated. The unprecedented disruptions brought on by the COVID-19 pandemic have emphasized the need to take immediate action. The Departments of Commerce and Homeland Security have already begun to take steps aimed at mitigating risks identified in the report. These actions include investing in domestic manufacturing capacity and workforce development, developing supply chain security frameworks, collaborating with international partners to improve resiliency, investing in ICT research and development efforts as well as reducing cyber risks.

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.

We look forward to working with the ICT industry and other domestic and international partners to take actionable steps in implementing measures identified in the assessment that build resilience and security throughout the ICT supply chain and across our nation.

Gina M. Raimondo

Secretary of Commerce

Alejandro N. Mayorkas

Secretary of Homeland Security

Executive Summary

On February 24, 2021, President Biden issued Executive Order (E.O) 14017 on *America's Supply Chains*, which directed a whole-of-government approach to reviewing risks in, and strengthening the resilience of, supply chains supporting six industries that are critical to U.S. economic prosperity and national security.[1] As part of this comprehensive review, E.O. 14017 directed the Departments of Commerce and Homeland Security to conduct a one-year assessment of the supply chains for critical sectors and subsectors of the U.S. information and communications technology (ICT) industrial base as defined by the respective agencies. In response, the Departments of Commerce (DOC) and Homeland Security (DHS) have prepared the following assessment of the supply chains supporting communications hardware, computing and data storage hardware, end-user devices, and critical software including open-source software and firmware.

The U.S. ICT industry serves an important role in our economic and national security, producing the technologies relied on by individuals, industries, and governments to connect, innovate, and protect our society. However, the COVID-19 pandemic and related disruptions have exposed structural vulnerabilities in both domestic and global supply chains that resulted in the reduced availability of critical ICT products and tested the resiliency of the ICT industry.

The following assessment evaluates the current supply chain conditions for select 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. A summary of these findings is detailed below.

Summary of Key Findings

- C*urrent State of ICT Manufacturing and Related Challenge*s: The United States continues to lead in ICT development and innovation in many product categories. However, the production of many products such as printed circuit boards (PCBs) and displays has become increasingly concentrated in China, along with electronics assemblies. For a limited number of products studied such as fiber optic cables, the United States still maintains a domestic manufacturing base.
- *Current State of the ICT Software Sector and Related Risks:* The nature of the current ICT software ecosystem creates several security risks. The ubiquitous use of open-source software can threaten the security of the software supply chain given its vulnerability to exploitation. Furthermore, the complexity of the ICT supply chain has led many Original Equipment Manufacturers (OEMs) to outsource firmware development to third party suppliers, which introduces risks related to the lack of transparency into suppliers' programming and cybersecurity standards.
- *Current State of the ICT Workforce and Related Risks*: The outsourcing of ICT manufacturing has resulted in a significant reduction in the domestic ICT production and manufacturing workforce. Comparatively, the domestic software developer and

[1] U.S. President. Executive Order. "On America's Supply Chains, Executive Order 14017 of February 24, 2021," 86 Fed. Reg., 11849, (March 1, 2021): 11849-11854.

engineering workforce, which makes up 40 percent of the U.S. ICT workforce, is expected to grow significantly based on current hiring trends. However, in both segments –manufacturing and software development – industry stakeholders reportedly struggle to find qualified employees across occupations.

- *Cross-Cutting Supply Chain Vulnerabilities Impacting the U.S. ICT Industrial Base*: Structural vulnerabilities across the ICT supply chains have presented several risks that have become more apparent as a result of disruptions caused by the COVID-19 pandemic. These include the lack of a domestic ecosystem for many segments of ICT production, overreliance on single-source and single-region suppliers, and the difficulty in maintaining product integrity due to complex supply chains. These vulnerabilities increase the potential for supply chain disruptions and complicate product and supply chain security efforts.
- *External Risks to the ICT Industrial Base Supply Chain*: The current state of the ICT industrial base supply chain leaves the United States overexposed to a variety of externally derived risks stemming from intellectual property theft, economic dependencies, weak labor standards and climate concerns.

Recommendations to Strengthen ICT Supply Chain Resiliency

To address these and other risks identified in the assessment, and to strengthen supply chain resiliency, the Secretaries of Commerce and Homeland Security recommend implementation of the following comprehensive strategy.

1. *Revitalize the U.S. ICT Manufacturing Base*: Support domestic investment and production of key ICT products, potentially including printed circuit boards (PCBs) and semiconductors, through appropriate federal procurement incentives and funding of programs like Title III of the Defense Production Act and the Creating Helpful Incentives to Produce Semiconductors for America Act.
2. *Build Resilience through Secure and Transparent Supply Chains:* Promote supply chain risk management practices through procurement and monitoring efforts such as implementing an Assured Supplier Program for PCBs for Federal Government and establishing a Critical Supply Chain Resilience Program at the Department of Commerce.
3. *Collaborate with International Partners to Improve Supply Chain Security and Resiliency:* Improve international engagements through existing fora to advance shared interests in the ICT industry. These interests include bolstering supply chain security and diversity for critical products, strengthening trade enforcement, and enhancing participation in international standards development.
4. *Invest in Future ICT Technologies:* Sustain the research and development (R&D) ecosystem through federal programs and legislation by supporting and expanding programs aimed at bringing nascent technologies to market as well as advancing manufacturing technologies.
5. *Strengthen the ICT Workforce Pipeline***:** Support and expand programs that attract, educate, and train the ICT workforce by enhancing computer science curricula and

investing in multiple secondary and post-secondary pathways, including through registered apprenticeships, career and technical education programs, and community college programs. Grant investments should be aligned with employer-led sectoral partnerships that ensure training is linked to real-world job opportunities.

6. *Ensure Sustainability Remains a Cornerstone of ICT Development*: Promote adoption of enhanced labor and environmental standards and the adoption of more sustainable ICT production facilities through financial incentives and government programs.
7. *Engage with Industry Stakeholders on Resiliency Efforts:* Strengthen public-private engagements to promote awareness and adoption of risk mitigation techniques and best practices for securing the ICT supply chain.
8. *Continue to Study the ICT Industrial Base*: Conduct further industrial base studies on critical ICT products such as PCBs and related microelectronics to monitor industry developments and guide long-term policy planning.

Table of Contents

Executive Summary 2
1. Introduction 8
2. Methodology 11
2.1 Scope of Work 11
2.2 Research Methodology 12
2.3 Stakeholder Engagements 13
3. Overview of the ICT Industrial Base 15
3.1 Evolution of the ICT Industrial Base Market Structure 15
3.2 Overview of Critical End-Uses of ICT Products 17
4. Current State of ICT Manufacturing and Related Challenges 21
4.1 Upstream Components: Printed Circuit Boards 21
4.2 Upstream Components: Fiber Optic Cable 24
4.3 Upstream Assembly: Printed Circuit Board Assemblies and Electronics Assemblies 27
4.4 Downstream Products: Routers, Switches, and Servers 28
4.5 Downstream Products: LCDs/Displays 31
5. Current State of the ICT Software Sector and Related Risks 33
5.1 Background on the Software Supply Chain 34
5.2 Overview of Open-Source Software 36
5.3 Open-Source Software Supply Chain Risks 38
5.4 Firmware Overview 40
5.5 Firmware Risks 41
6. Current State of the ICT Workforce and Related Risks 44
6.1 ICT Hardware Manufacturing Workforce 44
6.2 ICT Software Workforce 47
6.3 Human Capital-Related Risks 50
7. Cross-Cutting Supply Chain Vulnerabilities Impacting the U.S. ICT Industrial Base 54
7.1 Ongoing COVID-19-Related Supply and Demand Shifts and Bottlenecks 54
7.2 Lack of Ecosystem for Electronics Production 55
7.3 Single Source and Single Region Suppliers 57
7.4 Lack of Visibility of Junior Tier Suppliers 59

7.5 Inventory Management 62
7.6 Maintaining Hardware and Software Integrity along the ICT Supply Chain 63
7.7 Extended Supply Chains 68
8. External Risks to the ICT Industrial Base Supply Chain 69
8.1 Theft of Intellectual Property and Cyber Intrusions 70
8.2 Economic Risks 71
8.3 Forced Labor Risks 73
8.4: Climate Risks 74
9. Recommendations to Strengthen ICT Supply Chain Resiliency 76
Appendix A 83
Appendix B 85
Appendix C 86

1. Introduction

The Information and Communications Technology (ICT) industry produces the technologies that individuals, companies, and governments alike rely on to connect, develop, and protect our society. The reliance on ICT products across all sectors of the economy makes the industry of critical importance to U.S. economic growth and national security. However, over the past few decades, the United States has ceded manufacturing of much of the ICT supply chain to Asia. The disadvantage of off shoring manufacturing has become apparent during the COVID-19 pandemic when the U.S. ICT industry experienced severe supply chain disruptions. The COVID-19 pandemic as well as other conditions have reduced the availability of critical ICT products. In response to these and supply chain disruptions in other industries, on February 24, 2021, President Biden issued an Executive Order (E.O. 14017) on *America's Supply Chains*, which aims to build resilient, diverse, and secure supply chains supporting six critical industries to ensure U.S. economic prosperity and national security.[2] E.O. 14017 directs the Departments of Commerce and Homeland Security to conduct a one-year assessment on the supply chains for critical sectors and subsectors of the U.S. ICT industrial base, as determined by the Secretary of Commerce and the Secretary of Homeland Security. Pursuant to E.O. 14017, the scope of the following 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 ICT industry is a key contributor to the U.S. economy and domestic employment. While economic measurements of the ICT industry vary, the Bureau of Economic Analysis (BEA) estimates that in 2019 the digital economy accounted for $2,051.6 billion or 9.6 percent of gross domestic product (GDP). The digital economy has increased its contribution to the U.S. economy since 2005, when it represented 7.8 percent of GDP, with real value-added averaging 6.5 percent annual growth compared to only 1.8 percent for the overall economy. [3][4] While significant, these figures may underrepresent the importance of the ICT industry for the U.S. economy. For example, enterprise software systems can have a compounding effect on economic growth through the substantial benefits and economies of scale that they provide to small businesses.

In addition to its contribution to the economy, the ICT industry is a major provider of high-quality domestic employment. In 2019, over 2.1 million people were employed in the computer systems design and related services sector, or about 1.3 percent of total employment, up from 1.1 million in 2005.[5][6] ICT-related occupations such as computer and information technology (IT)

---

[2] U.S. President, Executive Order, "On America's Supply Chains, Executive Order 14017 of February 24, 2021," 86 Fed. Reg., 11849, (March 1, 2021): 11849-11854.

[3] Bureau of Economic Analysis, "Updated Digital Economy Estimates – June 2021," U.S. Department of Commerce, June 28, 2021, https://www.bea.gov/system/files/2021-06/DE%20June%202021%20update%20for%20web%20v3.pdf.

[4] In its definition of the digital economy, the BEA includes 1) infrastructure, or the basic physical materials and organizational arrangements that support the existence and use of computer networks and the digital economy, primarily information and communications technology (ICT) goods and services; 2) E-commerce, or the remote sale of goods and services over computer networks; and 3) priced digital services, or services related to computing and communication that are performed for a fee charged to the consumer. While these categories do not map precisely to this report's ICT focus, there is significant overlap. *See* https://www.bea.gov/data/special-topics/digital-economy.

[5] Bureau of Economic Analysis, "Updated Digital Economy Estimates – June 2021," U.S. Department of Commerce, June 28, 2021. https://www.bea.gov/system/files/2021-06/DE%20June%202021%20update%20for%20web%20v3.pdf.

[6] Bureau of Labor Statistics, "Household Data Annual Averages," U.S. Department of Labor, accessed November 19, 2021, https://www.bls.gov/cps/aa2019/cpsaat01.pdf.

positions also tend to pay higher salaries. In May 2020, the median annual wage for this occupation category was $91,250, more than twice the median annual wage of $41,950 for all occupations.[7] Employment rates in computer and IT occupations are also projected to grow by 13 percent from 2020 to 2030, faster than the average for all occupations.[8] However, the ICT industry currently faces a significant need of qualified workers to meet expected increases in demand. The ICT industry is an important employer of Americans, and the industry will require significant investment in workforce education and training to remain globally competitive.

Resilient and secure ICT supply chains are critical to U.S. economic and national security because ICT products and services are widely used across the economy, including in systems used by the government and critical infrastructure sectors.[9] Without secure sourcing and technologically advanced systems, systems supporting critical infrastructure, such as electric power grids, gas lines, and industrial control systems, will face greater risks of disruption and compromise. In addition, ICT products are subject to a range of inherent and introduced risks due to the numerous critical components inside each product.[10]

The ICT sector is also vulnerable to a variety of external shocks which risk disrupting supply chains and impact U.S. economic and national security. Supply chain shocks threaten employees and firms at all stages of production. In fact, across the economy companies can expect losses equal to almost 45 percent of one year's profits over the course of a decade due to supply chain disruptions.[11] Disruptions that originate at the firm-level can propagate through supply chain networks to impact suppliers and customers, affecting not only direct affiliates but indirectly linked firms.[12] In 2016, after earthquakes struck a part of Japan central to silicon production, closely linked Chinese companies suffered abnormal negative stock market returns.[13] These firm-level effects can have substantial country-level consequences: by one estimate, the Great East Japan Earthquake of 2011 led to a 0.47 percent decline in Japanese GDP as a result of input-output linkages.[14] These disruptions can impact not only the affected companies but also employees, as companies seek to cut costs by reducing their workforces or limiting wage increases.

The impact from the COVID-19 pandemic and the resulting global shortages of critical ICT components have highlighted the weaknesses of long and globally concentrated supply chains

---

[7] Bureau of Labor Statistics, "Computer and Information Technology Occupations," U.S. Department of Labor, accessed November 19, 2021, https://www.bls.gov/ooh/computer-and-information-technology/home.htm.
[8] Ibid.
[9] ICT is also a growing and critical component of the global and domestic transportation industries. ICT provides logistical efficiencies, greater transparency of goods movement, and, increasingly, greater safety and mobility for travelers who benefit from the integration of GPS-assisted navigation systems, emergency response applications, or advanced crash-avoidance systems such as vehicle-to-everything (V2X) communications.
[10] Carl McCants of Defense Advanced Research Projects Agency, Meeting with U.S. Departments of Commerce and Homeland Security, (Virtual Meeting, October 15, 2021).
[11] Susan Lund et al., "Risk, resilience, and rebalancing in global value chains," McKinsey Global Institute, August 6, 2020, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/Risk%20resilience%20and%20rebalancing%20in%20global%20value%20chains/Risk-resilience-and-rebalancing-in-global-value-chains-full-report-vH.pdf.
[12] Christoph E. Boehm, Aaron Flaaen, and Nitya Pandalai-Nayar, "Input Linkages and the Transmission of Shocks: Firm-Level Evidence from the 2011 Tohoku Earthquake," *The Review of Economics and Statistics* 101 (1): 60-75, https://doi.org/10.1162/rest_a_00750.
[13] Li Ding et al., "The contagion and competition effects across national borders: Evidence from the 2016 Kumamoto earthquakes," *International Journal of Production Economics* 235 (2021): 108-115. https://doi.org/10.1016/j.ijpe.2021.108115.
[14] Vasco M. Carvalho et al., "Supply Chain Disruptions: Evidence from the Great East Japan Earthquake," *The Quarterly Journal of Economics* 136 No. 2 (2021): 1255-1321. https://doi.org/10.1093/qje/qjaa044.

and the consequences of their disruption. A variety of factors have coincided to produce unprecedented shortages: pandemic recovery and economic stimulus in parts of the world increased demand; factory shutdowns in key production locations constricted supply; and global labor shortages strained production and distribution networks. Supply shortages and shipping constraints are expected to continue through 2022, with negative consequences for GDP growth in the United States and the rest of the world.[15] While ICT firms recognize the risks posed by their supply chains, one 2021 survey indicated that only 16.7 percent of firms in the IT/Tech/Electronics industry were interested in completely transforming their supply chain strategy, the smallest share of any industry. Despite the difficulties of shifting and otherwise enhancing the resiliency of firm production networks, it remains clear that action needs to be taken to better insulate the ICT industry from future disruptions.

In accordance with E.O. 14017, this assessment defines critical sectors and subsectors supporting the ICT industry, evaluates the current supply chain conditions, identifies key risks that threaten to disrupt those supply chains, and proposes a strategy to mitigate risk and strengthen supply chain resiliency. This report is organized into nine sections. The next section describes the methodology employed to research and prepare this industrial base assessment. The third section provides an overview of the ICT industrial base and defines critical end-use markets for ICT industrial base products. The fourth section reviews the current state of the ICT manufacturing base and supporting supply chains and identifies associated risks. The fifth section analyzes the current state of the ICT software sector and related risks. The sixth section assesses the composition of the U.S. ICT workforce and its ability to meet the needs of the industry and broader economy. The seventh section identifies the supply chain vulnerabilities that exist across the industry and the eighth section details other external risks that threaten to disrupt, constrain, or eliminate the critical supply chains that support the ICT industrial base. The final section provides recommendations to mitigate identified vulnerabilities and risks and strengthen the resiliency and security of the supply chains supporting the U.S. ICT industrial base.

[15] Sara Johnson, "Supply imbalances bring higher inflation and lower growth," IHS Markit, October 21, 2021. https://ihsmarkit.com/research-analysis/supply-imbalances-bring-higher-inflation-lower-global-growth.html.

2. Methodology

2.1 Scope of Work

This report provides an assessment of the supply chains for critical sectors and subsectors of the ICT industrial base, as determined by the Secretary of Commerce and the Secretary of Homeland Security. For this assessment, the scope of 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. These products were identified in part based on the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's (CISA) National Critical Function criteria which describes the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public health or safety.[16] Within this defined scope, this assessment focuses on the supply chains of a select number of components, devices, and software foundational to multiple facets of the nation's ICT industrial base. In addition to criticality, these components, devices, and software were selected to exemplify broader trends impacting the U.S. ICT supply chains and to identify opportunities for the U.S Government and industry to build resilience.

This assessment primarily focuses on the manufacturing needs, challenges, and risks inherent to the supply chains of key hardware products and inputs and evaluates the footprint of the U.S. manufacturing base within the ICT supply chain. The supply chain assessment also evaluates the human capital needs and challenges required to produce or develop critical hardware and software.

This report provides an actionable strategy for the Federal Government and industry to begin implementing measures that build resilience and security within the supply chains for critical sectors of the ICT industry. The recommendations are intended to complement recent and ongoing studies conducted in this industry by Federal agencies. Accordingly, this report does not assess the supply chains for semiconductors, critical minerals and batteries as these studies were completed through the 100-day reviews as directed by Executive Order 14017.[17] In addition, while information and communications technology and services (ICTS) security is an important issue within the ICT industry, there are other ongoing efforts to improve the security of such technology and service transactions and to address cybersecurity measures. These efforts include work being done pursuant to E.O. 13873, *Securing the Information and Communications Technology and Services Supply Chain,* and E.O. 14028, *Improving the Nation's Cybersecurity,* respectively.[18] Given this report's focus on manufacturing issues, cyber risks will be addressed

---

[16] Cybersecurity and Infrastructure Security Agency, "Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services", U.S. Department of Homeland Security, April 2020, https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf.

[17] Executive Office of the President, *Building Resilience Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017,* June 2021, https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

[18] U.S. President, Executive Order, "Securing the Information and Communications Technology and Services Supply Chain," Executive Order 13873 of May 15, 2019," 84 Fed. Reg., 22689, (May 17, 2019): 22689-22692; U.S. President, Executive Order, "Improving the Nation's Cybersecurity," Executive Order 14028 of May 12, 2021," 86 Fed. Reg., 26633, (May 17, 2021): 26633-26647.

primarily in the context of product integrity across the supply chain. Other relevant topics that are excluded to avoid duplicative actions include ICT-related services such as cloud services and the protection of personal and sensitive data which are being addressed in the E.O. efforts mentioned above.

2.2 Research Methodology

Literature Review and Collation Scorecard

The assessment of the U.S. ICT supply chain conditions is supported by a review of 74 reports and articles from academic, industry, and government sources. To collate the research, the working group drafting this assessment developed a rubric or "scorecard" comprised of ten categories of distinct elements of the ICT industrial base. The categories are listed below, and further defined in Appendix A.

1. Essential Goods, Materials and Services
2. Financials/Business Practices
3. Supply Chain Capacity and Procurement
4. Policy and Legal
5. Manufacturing and Logistics
6. Cybersecurity Risks
7. Risks to the Supply Chain and Impacts on the Nation
8. Research & Development and Innovation
9. Initiatives and Recommendations
10. Human Capital and STEM Education

Each research input was analyzed using this scorecard framework and collated based on relevance to each of the ten analysis fields. This organizational approach enabled the prioritization of internal research activities and facilitated the drafting of the report based on topical references.

Federal Register Notice of Inquiry Comments

On September 20, 2021, the Department of Commerce's Bureau of Industry and Security (BIS) published a Federal Register Notice of Inquiry soliciting comments from the public on the overall health of the supply chains for critical sectors and subsectors of the ICT industrial base and recommendations for policies and actions to strengthen supply chain resilience. BIS received a total of 35 comments from U.S. and foreign businesses, industry associations, private individuals, and U.S. and foreign government entities. The comments covered the identification of: 1) critical goods and materials that underlie the ICT supply chain, 2) manufacturing or other capabilities necessary to produce or supply these materials, 3) risks that threaten to disrupt, strain or eliminate the supply chain, 4) resilience within manufacturing and distribution of the ICT industrial base, allied and partner approach to the prioritization of critical ICT goods and services, and 5) specific policy recommendations that would strengthen supply chain resiliency for the ICT industrial base. Each comment was reviewed and incorporated where appropriate into this assessment to ensure adequate representation of stakeholder perspectives.

Data Collection

The interagency body collected data from a variety of sources including survey data and statistical figures from the Bureau of Industry and Security, the Bureau of Economic Analysis (BEA), the Census Bureau, the Economic Development Administration, and the International Trade Administration. Each database was queried using 27 North American Industry Classification System (NAICS) codes, provided in Appendix B, that represent the previously defined scope of the ICT industry. To establish this scope, the DOC and DHS developed a list of NAICS codes based on the defined scope of the ICT industry and cross-referenced this list with BEA's 2021 *Digital Economy* taxonomy. Additional data were provided by the U.S. Patent and Trademark Office and international organizations such as the Organization for Economic Cooperation and Development and the International Telecommunication Union. This data highlighted recurring themes such as labor skill shortages, domestic innovation and competitiveness, the relative strength of manufacturing exports, and ICT's significance within the larger digital economy.

2.3 Stakeholder Engagements

Stakeholder engagements were held with U.S. government and private sector partners to garner input to further inform the report and aid in the assessment process.

U.S. Government Stakeholders

To ensure adequate representation of crucial ICT government stakeholders and leverage specialized expertise and perspectives, an interagency body was established with members from:

- Department of Homeland Security (DHS)
    - CISA's National Risk Management Center (NRMC)
    - Office of Strategy, Policy and Plans (PLCY)
- Department of Commerce (DOC)
    - Bureau of Industry and Security (BIS)
    - International Trade Administration (ITA)
    - National Institute of Standards and Technology (NIST)
    - National Telecommunications and Information Administration (NTIA)
    - U.S. Patent and Trademark Office (USPTO)
    - Economic Development Administration (EDA)

The core body met regularly to coordinate each office's contributions to this report. Furthermore, the working group sought the advice of a small council of representatives from across the U.S. government to inform the analysis and recommendations of this report.

Industry Stakeholders

In preparation for the drafting of this report, members of the interagency body consulted with representatives from ICT companies and industry associations to adequately assess the critical supply chains supporting the ICT industrial base. Industry representatives provided insights on the scope of critical sectors and subsectors and the current supply chain challenges impacting the ICT industrial base. In addition, all members of the ICT industry were invited to participate in a virtual public forum held on October 29, 2021; over 350 people registered for the forum. During

the event, five speakers from U.S. businesses, industry associations, and an academic institution presented proposals to mitigate the risks facing critical supply chains supporting the ICT industrial base.[19]

[19] More information on the ICT Forum including a transcript can be found here: https://bis.doc.gov/ictforum.

3. Overview of the ICT Industrial Base

The U.S. ICT industrial base is highly specialized and depends on complex, global supply chains that are geographically concentrated. Evaluation of the current conditions of the ICT industry requires context and an understanding of the evolution of this market as well as an understanding the criticality and widespread applications of ICT products. This section details how the ICT industrial base has evolved over time followed by descriptions of select ICT products and their critical applications which reflect the importance of ensuring ICT supply chains are secure and resilient.

3.1 Evolution of the ICT Industrial Base Market Structure

Over the past 30 years, the ICT industrial base has evolved from being vertically integrated to being one that is highly outsourced, with most major brand companies outsourcing nearly every step of and input into the manufacturing process. Beginning in the mid-1980s, original equipment manufacturers (OEMs) in the computer industry, such as IBM and Cisco, that traditionally managed end-to-production services, began outsourcing manufacturing and software development to specialized technology companies, such as Intel (microprocessor chips) and Microsoft (operating software), and to contract manufacturers.[20] Contract manufacturers are companies that perform manufacturing services for other companies on a contractual basis. To produce a computer, these OEM companies could no longer design and manufacture their own computer chips or develop operating system software, but instead, so that their equipment was compatible with everyone else's, outsourced these needs to companies specializing in those products, such as Intel and Microsoft. This process, called vertical specialization, led ICT OEMs to focus on design and innovation of new and improved technologies.[21] Over time, OEMs have increasingly adopted this business model with many companies eliminating all manufacturing capabilities. These OEMs now add value primarily through research and development, product design, and marketing new technologies to their customer base. By 2006, leading computer companies, including Dell, HP Inc. (formerly Hewlett Packard), Acer, and Apple, had completely outsourced their notebook manufacturing operations.[22] The U.S. ICT industry reflects this evolution of the OEMs. The United States is the world's leader in technology innovation, but most hardware manufacturing takes place in other countries.

During the 1990s, as ICT OEMs shed manufacturing capabilities, contract manufacturing companies acquired these production facilities and began consolidating the market to offer the full suite of production services, including specialized design manufacturing for components and software.[23] Today, 43 percent of the electronics assembly market is outsourced to contract

---

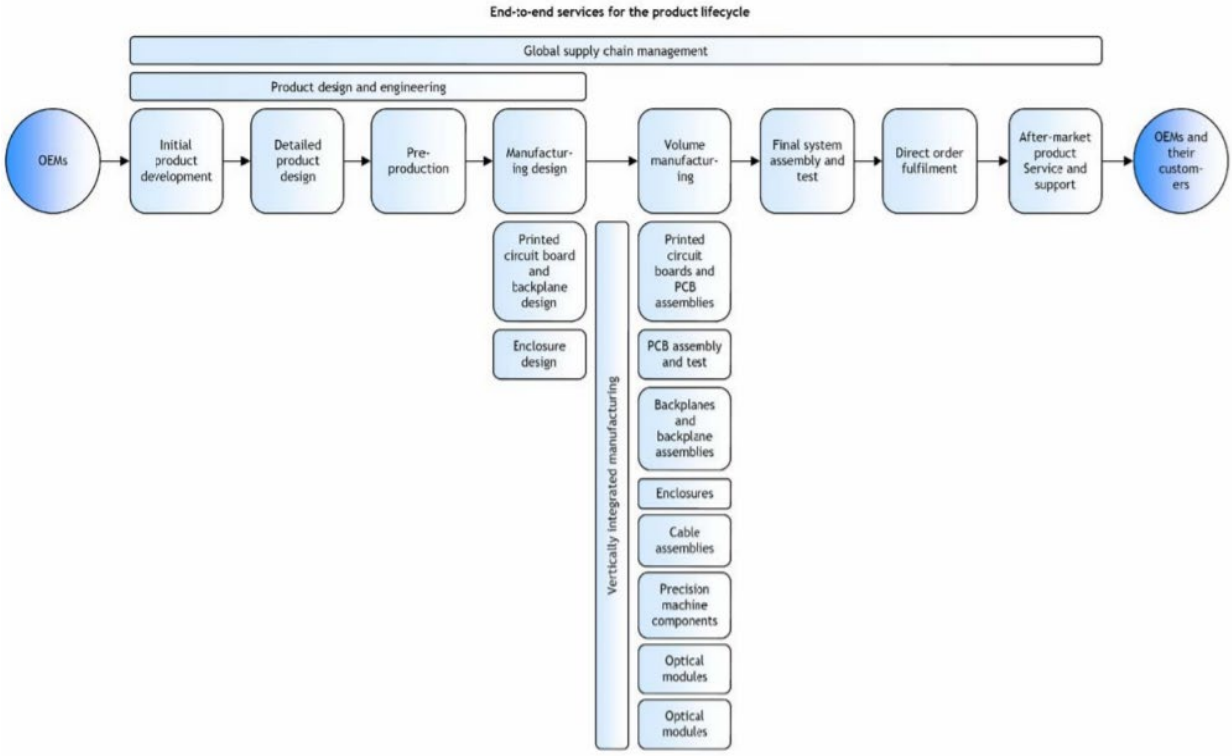
[20]Annelie Evermann, "The ICT Sector in the spotlight: Leverage of public procurement decision on working conditions in the supply chain," Electronics Watch Consortium, (2014), https://electronicswatch.org/the-ict-sector-in-the-spotlight_723519.pdf.
[21] Esther de Haan and Irene Schipper, "CSR Issues in the ICT Hardware Manufacturing Sector", Centre for Research on Multinational Corporations (SOMO), September 1, 2005, https://www.somo.nl/csr-issues-in-the-ict-hardware-manufacturing-sector/.
[22]Annelie Evermann, "The ICT Sector in the spotlight: Leverage of public procurement decision on working conditions in the supply chain".
[23] Esther de Haan and Irene Schipper, "CSR Issues in the ICT Hardware Manufacturing Sector".

manufacturers. The remainder is assembled by OEMs for their brand products.[24] Within the ICT contract manufacturing industry, two distinct models emerged – the electronics manufacturing service (EMS) model and the original design manufacturer (ODM) model. The EMS pertains to contract manufactures that oversee the entire production process on behalf of the OEM while the OEM maintains control over the product development process. The ODM model involves contract manufacturers managing both the product design and manufacturing processes while the OEM controls marketing and brand development.[25]

The figure below details the end-to-end services involved in the typical ICT hardware product life cycle. In the current OEM-EMS model that dominates the ICT industry, brand-name companies may only oversee production design and preferred suppliers and the final connection to their customers. The bulk of the manufacturing and actual procurement is managed by EMS or ODM companies.

Figure 1: End-to-End Services for the Product Lifecycle

Source: Centre for Research on Multinational Organizations[26]



One of the primary reasons that ICT OEMs have eliminated manufacturing capabilities is low profit margins and the need for mass production to make a profit, so instead they concentrate on

[24] Randall Sherman, "*Now Available!* The Worldwide OEM Electronics Assembly Market – 2021 Edition,". Nevada City: New Venture Research, July 2021, https://newventureresearch.com/wp-content/uploads/OEM2021-RS.pdf.OEM2021-RS.ppp (newventureresearch.com).

[25] Esther de Haan and Irene Schipper, "CSR Issues in the ICT Hardware Manufacturing Sector".

[26] Ibid.

product design, especially for consumer and legacy technology goods. To overcome these margins, contract manufacturers set up production in Taiwan, China and other Asian economies to provide manufacturing services for many products at once, which limits downtime. In particular, factors such as lower labor costs, subsidies, infrastructure benefits, availability of capital and land, and a central location in Asia lured high volume consumer product EMS assembly to China. For example, Foxconn increased its employment from 47,000 people to 1.1 million from 2004 to 2014, with 99 percent of those employees located in mainland China.[27]

Also, the vertical specialization and segmentation of the ICT industrial base has led to a geographic specialization whereby certain products and services are sourced from single regions or countries.[28] EMS and ODMs source components, subsystems, and parts from other suppliers, and any one product may contain thousands of components. This has led to economies of scale where an ICT manufacturer may mass produce and specialize in one component. Today, many components are manufactured in Asia, and in particular China, Japan, and Taiwan. Production of low-value component production followed assembly production to China, as low value component producers were pressured to provide just-in-time product and low-cost delivery to the assembly plants. However, some specialized components that require more advanced technical processes are still produced outside of Asia. Section 4 provides an in-depth analysis of the supply chains of selected components.

While the United States remains the leader in the design and innovation for the ICT sector, China leads in manufacturing. This shift is evident in the U.S. share of global electronics manufacturing, which has declined from 30 percent to five percent over the past 25 years.[29] The current market structure, with its geographic concentration of manufacturing in Asia, bears significant risk. To fully capture the implications that the current market structure has on the ICT hardware supply chains, section 3.2 provides an in-depth assessment of three major end-use markets.

3.2 Overview of Critical End-Uses of ICT Products

The intent of this section is to outline the breadth and importance of the ICT sector by providing descriptions of selected products and product categories, their importance to the U.S. industrial base, and the subsequent need to assess the supply chain. The products covered in this section are divided into three general categories: communications hardware, computing and data storage hardware, and end-user devices. Many ICT products could fall into more than one of the three categories, but these broad categories cover many critical ICT products. This section does not provide an exhaustive list of ICT products; instead, it is meant to include illustrative examples, and the inclusion or exclusion of a specific product does not signify whether it is a priority.

Communications Equipment

---

[27] Guillaume Delautre, "The distribution of value added among firms and countries: The case of the ICT manufacturing sector," International Labour Organization, January 2017, https://www.ilo.org/wcmsp5/groups/public/---dgreports/---inst/documents/publication/wcms_544190.pdf.

[28] Timothy Sturgeon, Presentation on "Supply chain resilience and smart reshoring in massively modular industries: The case of ICT," Virtual Forum for Risks in the Information Communication Technology Supply Chain, (Bureau of Industry and Security, October 29, 2021).

[29] Comments of IPC and USPAE (the U.S,. Partnership for Assured Electronics) to Request for Information, "Risks in the Information and Communications Technology Supply Chain," 86 Fed. Reg. 52127, (Sept. (September 20, 2021), (IPC and U.S, Partnership for Assured Electronics USPAE, November 45, 2021) .

Communications equipment enables instant connection with people and information worldwide. This vast category includes broadcasting equipment (i.e., radio and television studio equipment, transmitting and receiving antennas, satellites, cable television equipment, and GPS equipment), as well as telecommunications equipment (i.e., goods that facilitate wireless and wireline networks such as undersea cables, modems, fiber optic cables, bridges, routers, and gateways).[30] Telecommunications equipment enables digital communication, expands access to data, and transforms the way enterprises and consumers work, learn, and interact.[31]

Communications equipment holds strategic importance to the United States as the backbone of U.S. critical communications infrastructure. For example, emergency services depend on broadcasting and telecommunications equipment such as portable radios used by first responders, as well as equipment used by FirstNet, the emergency wireless broadband network.[32] Communications equipment also allows for the smooth operation of many other vital sectors, including the transmission of financial transactions by banks and the management of mass transit and air traffic control.[33] Importantly, telecommunications equipment provides the foundation for next-generation networks, including fifth generation wireless networks (5G). As 5G deployment continues, expected benefits include enhanced connectivity that will spur innovation across various vertical sectors, such as healthcare, energy, and transportation.

The United States was a leader in telecommunications equipment manufacturing, producing one-third of the world's telecommunications equipment, until the late 1990s.[34] Industry consolidation through mergers and acquisitions reduced the number of U.S. firms, and business miscalculations by some U.S. equipment producers caused major players to exit the telecommunications infrastructure market.[35] These trends were exacerbated by Chinese state support for its domestic producers through non-market policies and practices such as forced technology transfer, intellectual property theft, market distorting subsidies, and other types of state support which stifled innovation and competition in the industry.[36] These practices accelerated a decline in U.S. manufacturing for communications hardware. Today, while U.S. firms are not absent from the communications hardware market, the amount of manufacturing in the United States has decreased significantly.

Computing and Data Storage

Computing equipment includes widely used items like personal computers, servers, and ATMs. These devices are often paired with data storage products ranging from hard disk drives (HDDs)

---

[30] NAICS Manual 2017 *North American Industry Classification [NAICS] System, United States, 2017,* (Executive Office of the President, Office of Management and Budget, 2017.
[31] IBM Cloud Education, "Networking," IBM, March 17, 2021, https://www.ibm.com/cloud/learn/networking-a-complete-guide.
[32] "Power of FirstNet," FirstNet, Accessed February 2, 2022, https://www.firstnet.com/power-of-firstnet.html; Mark Wilson, "Inside the High-Stakes World of Designing for 911 Operators," Fast Company, March 22, 2021, https://www.fastcompany.com/90617212/inside-the-high-stakes-world-of-designing-for-911-operators.
[33] "Communications Sector Specific Plan," CISA, 2015, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf
[34] Robert D. Atkinson, "Who Lost Lucent?: The Decline of America's Telecom Equipment Industry," American Affairs Journal, August 20, 2020, https://americanaffairsjournal.org/2020/08/who-lost-lucent-the-decline-of-americas-telecom-equipment-industry/.
[35] Ibid.
[36]Robert D. Atkinson, "How China's Mercantilist Policies Have Undermined Global Innovation in the Telecom Equipment Industry," Information Technology and Innovation Foundation, June 22, 2020, https://itif.org/publications/2020/06/22/how-chinas-mercantilist-policies-have-undermined-global-innovation-telecom.

and solid-state drives (SSDs) to magnetic tape and USB sticks. Together, computing and storage devices allow businesses to manage the growing quantities of data that are produced each year.[37]

The computing and data storage industries are vital to the U.S. economy. Today, high-performance computing can track financial services and aid in the development of cures for diseases, while quantum computers will eventually support many sectors including banking and logistics.[38] Computer servers are also gaining importance as more organizations rely on cloud storage powered by server equipment.[39]

Although U.S. companies are leaders in computing and data storage, much of the manufacturing process now takes place in Asia.[40] One example is the 2021 HDD market: the first and second positions of market share by global revenue were occupied by two U.S. companies, Seagate and Western Digital; however, Southeast Asia has been a top manufacturing location for HDDs in recent years.[41] Southeast Asia recently replaced China as the top location for HDD manufacturing because U.S. tariffs and increasing labor costs in China make production less appealing.[42] While the U.S. remains crucial for R&D activities in these sectors, limited U.S. manufacturing capabilities are a cause for concern.

End-User Devices

End-user devices include a range of ubiquitous products, including laptops, tablets, handsets, and displays. These devices enable employees to work virtually, connect students to remote learning, and provide access to emergency services. From hospitals to small businesses, all facets of the economy are dependent on end-user ICT devices to operate. In 2018, it was estimated that 84 percent of U.S. households owned a smartphone and 78 percent owned a desktop or laptop computer.[43]

The COVID-19 pandemic has only increased demand for end-user devices. Shipments of desktops, notebooks, and tablets increased dramatically in 2020 as workers and students made a rapid shift to virtual operations.[44] The U.S. personal computer market, for example, experienced

---

[37] Tom Coughlin, "175 Zettabytes By 2025," *Forbes*, November 27, 2018, https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/?sh=2dae086c5459.

[38] "What is high performance computing," NetApp, accessed January 27, 2022, https://www.netapp.com/data-storage/high-performance-computing/what-is-hpc/; "How quantum computing could change financial services," McKinsey & Company, last modified December 18, 2020, https://www.mckinsey.com/industries/financial-services/our-insights/how-quantum-computing-could-change-financial-services; "Quantum computing could transform the logistics industry within the next decade," DHL, last modified September 24, 2020, https://lot.dhl.com/quantum-computing-could-transform-the-logistics-industry-within-the-next-decade/.

[39] Sai Vennam, "What is cloud computing," last modified August 18, 2020, https://www.ibm.com/cloud/learn/cloud-computing.

[40] Sascha Segan, "Silicon, USA: Technology That's Actually Made in America," *PC Magazine*, September 2, 2021, https://www.pcmag.com/news/silicon-usa-technology-made-in-america; Cade Metz, "Where in the World Is Google Building Servers?," *Wired*, July 6, 2012, https://www.wired.com/2012/07/google-server-manufacturing/.

[41] "Nearly 68 Million HDDs Shipping in 3Q21," Storage Newsletter, October 12, 2021, https://www.storagenewsletter.com/2021/10/12/nearly-68-million-hdds-shipped-in-3q21/; Pairat Temphairojana, "Seagate to invest $470mln in Thailand over next 5 years," Reuters, February 10, 2015, https://www.reuters.com/article/us-thailand-seagate-technolo/seagate-to-invest-470-mln-in-thailand-over-next-5-years-idUSKBN0LE15720150210.

[42] Aaron Lee and Willis Ke, "HDD manufacturing cluster formed in Thailand," Digitimes Asia, March 12, 2020, https://www.digitimes.com/news/a20200312PD207.html?mod=3&q=hdd.

[43] U.S. Census Bureau, "Computer and Internet Use in the United States: 2018," Census.gov, October 8, 2021, https://www.census.gov/newsroom/press-releases/2021/computer-internet-use.html.

[44] IDC, "Personal Computing Devices - Market Share," December 13, 2021, https://www.idc.com/promo/pcdforecast.

its fastest growth in 20 years during the pandemic.[45] This unprecedented demand, along with supply chain disruptions for components, has led to production backlogs and delays.[46]

Historically, technological innovation has led to lower prices and more advanced devices, resulting in greater convenience and innovation for consumers. U.S. companies remain global leaders across many product categories for end-user devices, and U.S.-branded products are sold worldwide. However, many end-user devices are low-cost, high-volume products that use established technology, and, to the extent some of these devices were produced in the United States at one time, most of that production shifted out of the United States beginning in the 1980s. Given that consumer hardware production is generally a low-margin business, it is difficult for new entrants to succeed in the market without relying on a software or services portfolio to make money. Further, as explained later in this report, it is often not cost-competitive to manufacture in the United States.[47] This has created an environment where many U.S. companies are leaders in designing end-user devices, and those devices are necessary for the economy to function, but current U.S. manufacturing of many of those devices is limited or nonexistent.

In conclusion, the U.S. ICT hardware industrial base has evolved to be a highly globalized industry with complex supply chains. U.S. companies continue to lead in design innovation and represent premier, global brands for products in key end-use markets, including communications equipment, computer and data storage, and end-user devices. However, ICT manufacturing has largely shifted to Asia, and to China in particular. The next section will review the current state of manufacturing for many of these products and highlight specific, associated risks.

---

[45] "Gartner Says Worldwide PC Shipments Grew 10.7% in Fourth Quarter of 2020 and 4.8% for the Year," Gartner, January 11, 2021, https://www.gartner.com/en/newsroom/press-releases/2021-01-11-gartner-says-worldwide-pc-shipments-grew-10-point-7-percent-in-the-fourth-quarter-of-2020-and-4-point-8-percent-for-the-year.

[46] Jon Swartz, "HP's PC Sales Hit a Wall, but CEO Says 'We Are Selling Everything We Can Produce'," MarketWatch (MarketWatch, August 26, 2021), https://www.marketwatch.com/story/hp-shares-slip-2-on-flat-personal-systems-sales-due-to-supply-chain-constraints-11630008791.

[47] Christina Bonnington, "Why Hardware Makers Rarely Make Their Money from Hardware," Slate Magazine (Slate, August 5, 2018), https://slate.com/technology/2018/08/why-hardware-makers-like-roku-rarely-make-their-money-from-hardware.html.

4. Current State of ICT Manufacturing and Related Challenges

U.S. ICT OEMs remain on the leading edge of innovation, but manufacturing for a wide range of critical ICT hardware products is currently concentrated in Asia. This section analyzes the current state of production for several key products to demonstrate opportunities and challenges for building supply chain resilience throughout the ICT industrial base.

The following subsections highlight examples from each stage of the ICT manufacturing process, including upstream components, assembly, and final products. The analysis provides an overview of the manufacturing process, where global production is concentrated, and market barriers to supply chain diversification. The list of selected components and devices is by no means exhaustive, and the exclusion of a specific component should not be considered an indication that this technology is insignificant or lacks supply chain vulnerabilities. Instead, the intent of this section is to further demonstrate how the broader ICT hardware supply chain functions and highlight product-specific risks that need to be considered when addressing supply chain resiliency. The discrete risks identified in this section build on broader, cross-cutting vulnerabilities that will be addressed in section 7 of this report.

4.1 Upstream Components: Printed Circuit Boards

Unassembled (bare) printed circuit boards (PCBs) are the map for the placement and interconnection of semiconductors, passive components, and electronic connectors[48] that enable the electronic functions of an end product. Semiconductors and other components do not work until they are assembled onto a PCB. PCBs are in all ICT hardware, including in telecommunications hardware and end-user devices, and are also widely used in many other sectors, such as automotive, defense, and medical technology.

The interconnect and component placement pattern of each PCB is unique to that board. Some PCBs have a standard footprint, such as PCBs for computer motherboards, memory modules, and certain display modules; and after assembly they can be used in different brands and types of equipment. However, most PCBs are customized for a specific product.

Different environments and end-uses require different specifications for optimal performance so there are many different types of PCBs, including flexible, rigid for lead-free solder (widely used in consumer devices), rigid for lead solder (used for harsh environments such as automotive and defense/aerospace), and boards combining flexible and rigid sections (which are often used in medical and defense/aerospace as flexible sections are used on curved surfaces while rigid sections accommodate key components and input devices). In addition, boards can be made with one or multiple layers. Just as PCBs come in a wide range of types and designs, PCB makers vary in their specialization. For instance, only some companies can manufacture flexible boards, high layer count boards, or specialty PCB-type products for semiconductor packaging.

Taiwan is home to half of the ten largest PCB companies. Only one U.S. firm, TTM Technologies, is in the top ten globally; the remainder are located in Japan and China. Europe

[48] E.g., Board to board connectors

also has PCB companies, though none of them are as large as the Asian and U.S. firms.[49] However, much of the manufacturing of PCBs takes place in China.

Manufacturing Footprint. PCB production in the United States is primarily for low-volume, high-mix specialty boards, such as those used in industrial, medical, defense, and aerospace products. Large scale PCB manufacturing is concentrated in Asia, particularly in China, Japan, Taiwan, and South Korea.

In recent decades, U.S. manufacturing of PCBs declined as China and other Asian countries increased production. According to the trade association IPC International and the U.S. Partnership for Assured Electronics (USPAE), approximately $11 billion worth of PCBs were produced annually in the United States prior to the shift in production to Asia in 2000-2001.[50] In 2000, North America had the largest number of PCB facilities globally, with approximately 780. By March 2020, that number had fallen to an estimated 230, while the number of facilities in China increased to 1,480 over that time. Approximately 150 of those facilities in China were owned by companies headquartered outside China.[51]

Figure 2: March PCB companies and Factories estimated in 2020[52]

	China**	N. America	Europe	Japan	Taiwan	S. Korea	S.E.A.	India	S. America	ROW*	World
No. Companies	1,250	190	170	110	80	70	80	130	37	130	2,247
No. Factories	1,480	230	190	190	120	90	90	130	37	130	2,687

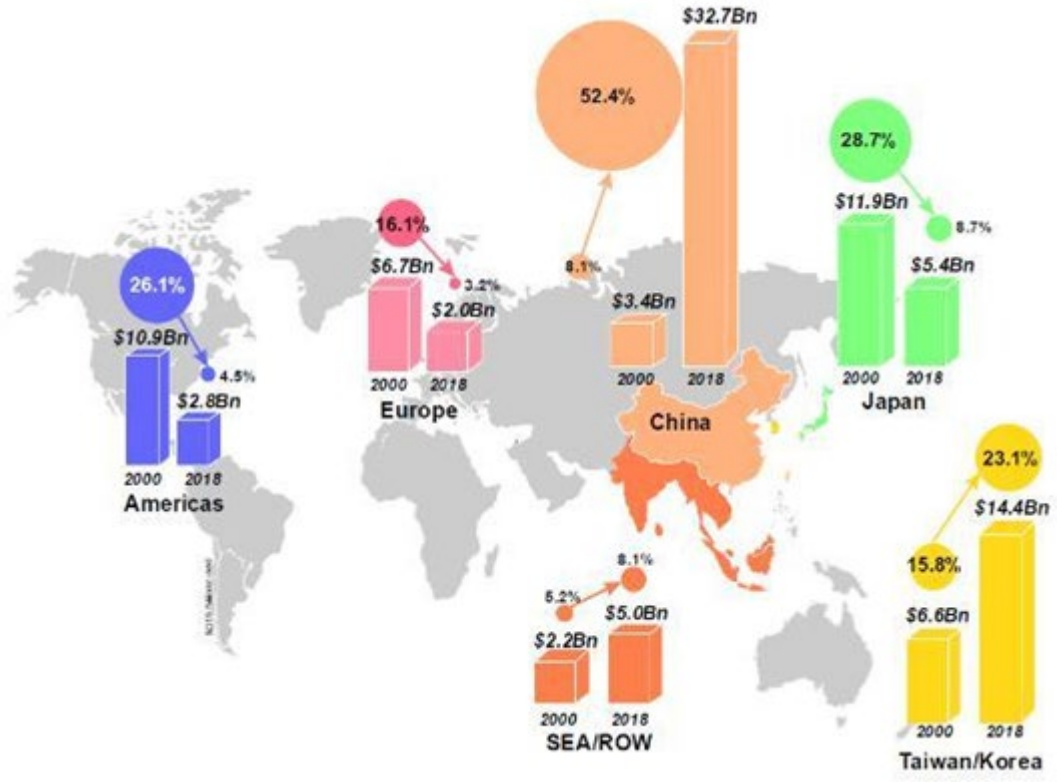
Source: N.T. Information Ltd. *Includes Africa, Middle East and Russia (rough estimate) **As of May 2021, about 70 new plants are under construction and under plan

China leads the world in global sales of PCB manufacturing, with a 52.4 percent share ($32.7 billion) of the market in 2018. In contrast, approximately $2.88 billion worth of PCBs are produced in the United States, and the current U.S. global production share of PCBs is at an estimated four percent.[53] In the past two decades, China overtook Japan and the United States, which were the global leaders in 2000, as seen in Figure 3. Taiwan, Korea, and Southeast Asia are also growing manufacturing locations.[54]

[49] Dr. Hayao Nakamura, "Big Gets Bigger and Faster: The Annual NT-100 Largest PCB Manufacturers", *Circuits Assembly,* July 23, 2021, https://circuitsassembly.com/ca/editorial/menu-features/35946-big-gets-bigger-and-faster-the-annual-nt1-100-largest-pcb-fabricators.html.
[50] *Comments of IPC and USPAE to Request for Information, 86 Fed. Reg 52127.*IPC and the U.S. Partnership for Assured Electronics (USPAE) Comments.
[51] Nakamura, "Big Gets Bigger."
[52] Nakamura, "Big Gets Bigger."
[53] "Global PCB output value will reach US $66.1 billion in 2020, and China will account for half of the global market" *Eolane,* 2019.
[54] Ibid.

Figure 3: Relocation of PCB Manufacturing 2000-2018[55]

Source: Eolane



China's rapid rise as the leader of PCB manufacturing was due to a variety of factors. The Chinese government subsidized the construction and equipment of PCB manufacturing plants. In addition, while there is some U.S. production of PCB laminate, most of the chemicals required for PCB manufacture is produced overseas, and PCB manufacturing equipment and materials are easily available in China.[56] Clustering of input materials, PCB manufacturing, and associated assembly in East Asia reduces production costs and transportation time. However, China is less competitive in leading-edge PCB technologies, and most Chinese-based PCB production is destined for low-end, high-volume consumer electronics.

The key risks facing the U.S. PCB supply chain include:

- **Facility inefficiencies**. U.S. plants are often older than their Asian counterparts, meaning they lack automation and rely on costly manual labor, which inhibits their ability to increase production. The facilities face a catch-22 situation where inefficiencies prevent them from winning significant projects, yet the plants cannot upgrade for efficiency without more capital from significant projects. According to IPC and USPAE, "{e}lectronics manufacturing is a notoriously thin-margin business, making it difficult to…upgrade costly manufacturing equipment." Such upgrades are necessary to perform

[55] Ibid.

[56] "Bringing Back PCB Manufacturing is Easier Said than Done" *Printed Circuit Design and Fab, March 2021, Vol. 38. No. 3,* Circuits Assembly, 16.

sophisticated work, to meet customer needs, and to achieve "the capabilities, quality standards, and cost-efficiencies necessary to compete in the global economy."[57]

- **Heavy dependence on U.S. defense contracts**. U.S. PCB manufacturing companies often are small and medium sized businesses that do not have the capacity for large scale production, nor do they have the capital to purchase additional equipment, so they concentrate on specialty PCBs for defense, medical, or industrial use. While U.S. manufacturers have an advantage in quality, performance, and lead time, they struggle to complete on price. Many U.S. producers say they would not survive without defense contracts.[58] Thus, beginning in 2023, Section 808 of the National Defense Authorization Act (FY 2021) prohibits the Department of Defense (DoD) from sourcing PCBs from China and other covered nations without a waiver.[59] However, focusing solely on PCB production for DoD will not create the economies of scale to re-develop a significant PCB industrial base for commercial uses in the United States.

In summary, PCBs are essential for the electronic functions of ICT hardware as well as for a wide array of automotive, defense, and medical devices. In the past 20 years China has overtaken the U.S. as the global leader in PCB manufacturing and sales. The small PCB industry left in the U.S. leads in quality and performance, but lack efficiencies created by automation technologies. Thus, the market has become specialized and dependent on government and defense procurement and limited production for highly regulated specialty electronics for medical and industrial use. U.S. PCB facilities must overcome these risks for long-term viability.

4.2 Upstream Components: Fiber Optic Cable

Fiber optic cable is a transmission medium that sends large amounts of data through strands of glass using light beams. It is the core technology behind subsea cable networks that transfer 99 percent of all international data. Fiber optic cable also supports connectivity at both the national and local levels. Nationally, it carries long-haul traffic across the country, including data that originates on wireless networks. Locally, it can serve as "middle-mile" transport to carry data between neighborhoods, and it is increasingly used for "last-mile" transport to deliver high speed broadband services to community anchor institutions, businesses, and consumers' homes. Demand for fiber optic cable has grown significantly in recent years as the use of fiber has increased in our nation's telecommunications networks. The Fiber Broadband Association estimates that 43 percent of Americans have access to fiber infrastructure today.[60]

Manufacturing fiber optic cable involves three primary steps. First is the production of glass preform: glass rods are treated with chemicals that prevent light from escaping. Next, the glass preform is heated to "draw" the melted glass into ultrathin strands, known as "bare fiber," that maintain the same chemical properties as their source rods. Finally, the bare fiber is covered in a

---

[57] IPC and USPAE Comments; see also Flex comments

[58] BIS report, article https://www.bis.doc.gov/index.php/documents/technology-evaluation/2378-u-s-bare-printed-circuit-board-industry-assessment-2017/file BIS report, article https://www.bis.doc.gov/index.php/documents/technology-evaluation/2378-u-s-bare-printed-circuit-board-industry-assessment-2017/file

[59] U.S. Congress, "H.R.6395 - 116th Congress (2019-2020): William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," January 1, 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395.

[60] "Fiber Broadband Enters Largest Investment Cycle Ever," Fiber Broadband Association, last modified January 5, 2022, https://www.fiberbroadband.org/blog/fiber-broadband-enters-largest-investment-cycle-ever.

protective coating (plastic resin, woven textiles, braided metals, or any combination thereof, depending on the end-use of the cable). Some manufacturers perform all three steps, while others specialize in just one of these production steps.

Manufacturing Footprint. The major global producers of fiber optic cable include Corning, Yangtze Optical Fiber and Cable (YOFC), Furukawa, Hengtong Group, and FiberHome.[61] Corning is a U.S.-headquartered firm, and the others are headquartered in China or Japan, suggesting that while the United States maintains an industrial base a large share of fiber optic cable manufacturing also takes place in Asia.[62]

Against this backdrop, the global supply chain for fiber optic cable is increasingly centered in China. In 2000, China supplied 3 percent of global imports of bare fiber and 3 percent of the world's final optical cable imports. By 2017, the country supplied 12 percent of the world's raw fiber imports and 31 percent of global optical cable imports.[63] This dominance has come from rapid growth in Chinese production capacity during that time period.

China's market-distorting trade practices, provision of subsidies, and significant state ownership of optical fiber companies have also been central to this transformation. In 2019 alone, the Chinese government provided subsidies ranging from 350 million RMB to 511 million RMB (approximately $50-73 million USD per company) to the Chinese optical fiber cable producers FiberHome, ZTT, and Hengtong.[64] FiberHome is fully controlled by a Chinese state-owned entity, as are several major China-headquartered producers of raw materials needed for optical fiber cable, such as aramid fiber.[65]

While U.S. exports of optical cable have grown in dollar value, the U.S. share of global exports has diminished as China has outpaced the United States in capacity. In 2000, the United States represented 26 percent of global exports in optical cable. By 2017, that share reduced by half to 13 percent.[66] After China and the United States, Mexico, Japan, and Germany were the next three leading exporters of fiber optic cables to the world in 2017.[67] The United States maintained a positive trade balance in optical fiber cable with the rest of the world for nearly 70 percent of the period from 2002-2020.[68]

---

[61] "Top 10 US and International Fiber Optics Suppliers," Thomas Publishing Company, accessed January 27, 2022, https://www.thomasnet.com/articles/top-suppliers/fiber-optics-manufacturers-suppliers/.

[62] "Company Profile," Corning Incorporated, accessed January 27, 2022, https://www.corning.com/worldwide/en/about-us/company-profile.html; "Contact Us," YOFC, accessed January 27, 2022, https://en.yofc.com/list/259.html; "Company Profile," Furukawa Electric, accessed January 27, 2022, https://www.furukawa.co.jp/en/company/outline.html; "Our Company," Hengtong Group, accessed January 27, 2022, http://www.hengtonggroup.com/en/home/company/index.html; "FiberHome Contact," FiberHome, accessed January 27, 2022, https://en.fiberhome.com/contact/Default.aspx.

[63] United Nations, UN Comtrade Database, https://comtrade.un.org/, cited as the source by International Trade Administration, U.N. Trade—Top Partners (HS Codes 900110 and 85447000, China optical cable and raw fiber imports to the world), Trade Policy Information System (TPIS), https://tpis1.trade.gov/cgi-bin/wtpis/prod/tpis.cgi.

[64] "Commission Implementing Regulation (EU) 2021/2011," European Union, last modified November 18, 2021, https://eur-lex.europa.eu/eli/reg_impl/2021/2011/oj (exchange rate as of December 31, 2019).

[65] Ibid.

[66] United Nations, UN Comtrade Database, https://comtrade.un.org/, cited as the source by International Trade Administration, U.N. Trade—Top Partners (HS Code 85447000, U.S. optical cable imports to the world), Trade Policy Information System (TPIS), https://tpis1.trade.gov/cgi-bin/wtpis/prod/tpis.cgi.

[67] Ibid.;. (top 5 import suppliers of fiber optic cables to the world).

[68] U.S. Census Bureau, Foreign Trade Division, https://www.census.gov/foreign-trade/index.html, cited as the source by International Trade Administration, TradeStats Express (HS Code 854470), https://www.trade.gov/tradestats-express-national-and-state-trade-data.

U.S. demand for fiber optics is expected to grow significantly, driven by the Biden-Harris Administration's priorities to support high speed broadband deployment through various programs funded through the American Rescue Plan and the Infrastructure Investment and Jobs Act (IIJA), as well as the Federal Communications Commission's Rural Digital Opportunity Fund (RDOF). In anticipation of increased demand, companies have publicly announced new investments in domestic capacity totaling $275 million in 2021. These include Corning's $150 million investment in North Carolina,[69] Prysmian Group's $50 million investment in North Carolina,[70] CommScope's $50 million investment in North Carolina,[71] and Sterlite's $25 million investment in South Carolina.[72] While fiber optic cable supply is expected to increase in the near future, the industry is currently facing challenges related to supply and demand shifts and bottlenecks, which are discussed in Section 7.

Key risks facing the U.S. fiber optic cable supply chains include:

- **Impact of China's excess capacity**. According to viaPhoton, a U.S.-based fiber optic solutions provider, China currently has over 300 million kilometers of excess fiber capacity and "estimates suggest that capacity will grow to nearly 600 million kilometers by 2024, 300 million kilometers of which will outpace China's internal demands."[73] By comparison, the world's total production of optical fiber in 2020 was close to 500 million kilometers.[74] When Chinese firms export their surplus production to other countries, prices often fall and competitors may struggle to stay in business. In this context, industry observers have closely followed the European Commission's recent anti-dumping decision on single-mode optical fiber cables from China, which are now facing tariffs of up to 44 percent.[75] Applicants successfully argued that increased low-cost imports from China had prevented European Union (EU) firms from benefiting from the 2016-2019 demand growth, despite increases in production and sales. EU producers added that these profitability barriers prevented them from investing in emerging technologies such as 5G.[76] In the United States, by contrast, the fiber optic industry is expected to benefit from domestic stimulus measures, but it will remain important to monitor China's excess capacity moving forward.

In summary, the U.S. manufacturing base for bare fiber and optical cable is expected to grow steadily as demand increases with the deployment of 5G and the expansion of broadband access.

---

[69] "Corning and AT&T Expand Collaboration as Corning Works to Meet Record Broadband Deman and Support Growth of U.S. Manufacturing,", Corning Incorporated, September 28, 2022, https://www.corning.com/worldwide/en/about-us/news-events/news-releases/2021/09/corning-and-att-expand-collaboration-as-corning-works-to-meet-record-broadband-demand-and-support-growth-of-us-manufacturing.html.

[70] "Prysmian Group to invest $50 million to expand production technologies and create 50 jobs in Claremont," Catawba County Economic Development Corporation, September 7, 2021, https://www.catawbaedc.org/news/Prysmian_September_2021.

[71] Virginia Annable, "CommScope revamping, investing in plants," *Hickory Daily Record,* June 16, 2021, https://hickoryrecord.com/news/local/commscope-revamping-investing-in-plants/article_8d7c8be0-cec8-11eb-8f3c-d7c82de4f8d4.html.

[72] "STL establishing operations in Kershaw Country," South Carolina Office of the Governor, June 23, 2021, https://governor.sc.gov/news/2021-06/stl-establishing-operations-kershaw-county.

[73] Comments of viaPhoton, to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (viaPhoton, November 4, 2021).

[74] Mitch Jacoby, "As telecom demands grow, optical fibers will need to level up," *Chemical & Engineering News,* March 16, 2020, https://cen.acs.org/materials/photonics/telecom-demands-grow-optical-fibers/98/i10.

[75] Wei Shi, "Chinese optical-fibre cables face punitive EU tariff," *Informa Tech*, November 19, 2021, https://telecoms.com/512242/chinese-optical-fibre-cables-face-punitive-eu-tariff/.

[76] "Case AD669 - Optical fibre cables (OFC)," European Commission, last modified January 27, 2022, https://trade.ec.europa.eu/tdi/case_details.cfm?id=2479.

However, the supply chain is currently impacted by supply and demand shifts and bottlenecks. Globally, U.S. share of the world's imports has diminished as China's companies continue to flood the market with excess supply that is largely enabled by Chinese government subsidies. While the United States is still a key producer of fiber optics manufacturing, China's excess capacity remains a global problem that will likely require coordinated actions to address.

4.3 Upstream Assembly: Printed Circuit Board Assemblies and Electronics Assemblies

Semiconductors, connecting components and passive components are placed on, or connected to, the printed circuit board to create a PCB assembly (PCA). PCAs are the parts that run the electronic functions in ICT, consumer, automotive, industrial, medical, and defense/aerospace goods.

According to Census, in 2019, U.S. company sales of PCAs (NAICS 334418) were $22.2 billion. However, most of the sales price for PCA's is for the cost of inputs, not from the PCA manufacturing process. The value-added for the PCA manufacturing process itself was only $6.2 billion (30 percent of sales). Semiconductors are the highest value inputs into the assembly process, with other inputs such as other components assembled on and to the printed circuit board, the PCB itself, and materials used in the assembly process (solder, aluminum, etc.) making up the balance of inputs.[77]

Both PCA and final product assembly are done either by the brand name manufacturers (OEM) for their own use, or by EMS companies who assemble electronics on contract, as previously discussed. Globally, 43 percent of all electronic goods assembly is done by EMS companies rather than the OEMs.[78] In 2018, the end-use markets for EMS assembly were communications (36 percent share), computer (23 percent share), consumer (17 percent share), industrial (9 percent), medical (3 percent), automotive (7 percent), and defense/aviation/other transport/other (5 percent).[79]

Manufacturing Footprint. China is the leading location for EMS production, especially for cell phones, laptops, and other high-volume ICT and consumer electronic goods. In addition, EMS and ODM companies are mainly headquartered in Asia, and Taiwan in particular. As shown in Appendix C, among the top 20 EMS and ODM companies in 2020, 14 companies are headquartered in Asia, with 11 of these companies located in Taiwan and Taiwanese-based EMS and ODM companies comprise nearly 82 percent of the global market.[80] The largest EMS firm, Taiwanese company Foxconn/Hon Hai, reported revenues of $160 billion in 2020, three times that of second-ranked Pegatron (Taiwan).[81]

---

[77] 2017-2019 Annual Survey of Manufacturers, 2019 (ASM): Summary Statistics for Industry Groups and Industries in the U.S.: 2017-2019, *United States Census Bureau*.

[78] *Now Available! The Worldwide OEM Electronics Assembly Market.*

[79] "Global EMS Market Grew 15% in 2018 to nearly $542 Billion," *EPS News,* July 24, 2019, https://epsnews.com/2019/07/24/global-ems-market-grew-15-in-2018-to-nearly-542-billion/.

[80] Bloomberg L.P., "Market share graph for global EMS/ODM companies 2017 to 2020," accessed December 2021. See Appendix C.

[81] Michael Buetow, "How M&A and India Will Reshape the Electronics Manufacturing Landscape", *Circuits Assembly Online,* May 26, 2021, https://circuitsassembly.com/ca/editorial/menu-features/35673-how-m-a-and-india-will-reshape-the-electronics-manufacturing-landscape.html.

Despite China's dominance, worldwide growth is occurring in many locations. Mexico, which was once the hub for assembly for the North American market prior to China's rise, has started to restore EMS production, especially for ready to ship items like televisions and displays. [82] Eastern Europe is a hub for the European assembly industry, though assembly for European companies also takes place in China and Southeast Asia. India is growing as an EMS hub; however, infrastructure issues and the general business climate have hindered its growth.[83] Southeast Asian countries, including Thailand, Malaysia, and Vietnam, are also budding locations for EMS.[84] Lastly, the United States leads in EMS production for low volume high mix products like medical/industrial and defense/aerospace electronics.

Key risks facing the U.S. PCA and Electronic Assemblies supply chain include:

Counterfeit or used parts. More awareness of counterfeit or used parts surfacing from China's board and product assembly industry came during the dot-com boom in the 2000s. Reportedly, Chinese workers in assembly plants secretly produced extra products and sold the products themselves, or sold rejected components disguised as new products.[85] Recent shortages of needed components on an unpredictable basis has led to use of third-rate suppliers, and a revival of counterfeit, substandard, and parts not to specification from China through alternate distribution channels.[86] For example, Japanese manufacturer Jenesis ordered chips from the Chinese e-commerce site Alibaba that failed in testing, and were proven to be counterfeit.[87]

In summary, PCAs and electronic assembly production is heavily dependent on EMS companies dominated by Chinese production. U.S. production is limited to low volume specialized products like medical/industrial and defense/aerospace electronics. The concentration of production assembly in China has increased the risk of counterfeit or used components being inserted into products, potentially damaging product integrity and brand reputation and creating a possible security risk. China's centralized supply chains are an advantage that pose a threat to the U.S.'s ability to compete in the PCAs and electronics assembly industry.

4.4 Downstream Products: Routers, Switches, and Servers

Networking equipment such as routers, switches, and servers are critical for transmitting data, distributing data processing and applications, communicating across devices, and connecting networks. Different types of networking equipment are used by consumers, enterprises, network operators, and communications service providers. Routers, switches, and servers consist of various components such as the motherboard, central processing unit (CPU), power supply, hard

---

[82] Doug Donahue, "Mexico: A new Hub for Electronics Manufacturing", *I Connect007*, September 28, 2018, https://smt.iconnect007.com/index.php/article/112848/mexico-a-new-hub-for-electronics-manufacturing/112851/

[83] "'India Can Make $300-bn electronics by 2026,'" *The Hindu*, January 20, 2022, https://www.thehindu.com/business/india-can-make-300-bn-electronics-by-2026/article38320653.ece.

[84] Michael Buetow, "How M&A and India Will Reshape the Electronics Manufacturing Landscape."

[85] Robb Hammond, "China's New Export Laws are Placing Lives in Jeopardy," AERI, Accessed February 2, 2022, https://www.aeri.com/chinese-counterfeit-parts/.

[86] Computing U.K., "Counterfeit, Substandard Chips are Penetrating the Supply Chain, Industry Insiders Warn," Communications of the ACM, September 20, 2021, https://cacm.acm.org/news/255667-counterfeit-substandard-chips-are-penetrating-the-supply-chain-industry-insiders-warn/fulltext.

[87] Dev Kundaliya, "Counterfeit and Substandard Chips are penetrating the supply chain, industry insiders warn" Computing.co.uk, Sept 20, 2021 https://www.computing.co.uk/news/4037363/counterfeit-substandard-chips-penetrating-supply-chain-industry-insiders-warn.

drives, random access memory (RAM), PCBs, and many others. As a result, the final products can be very complex, with a single server containing between 3,500 to 4,000 components.[88]

While the United States has several leading companies that supply networking equipment (i.e., Dell, HPE, IBM), most production is concentrated in Asia through EMS companies, which Taiwanese headquartered companies dominate (i.e. Foxconn, Inventec, Wistron). The supply chain for networking hardware, like the broader ICT industry, is global and generally follows the OEM-EMS model described in Section 3. Figure 4 portrays a typical production process that, while varied, may involve thousands of steps with the networking hardware products passing through many borders before reaching their final destination.[89]

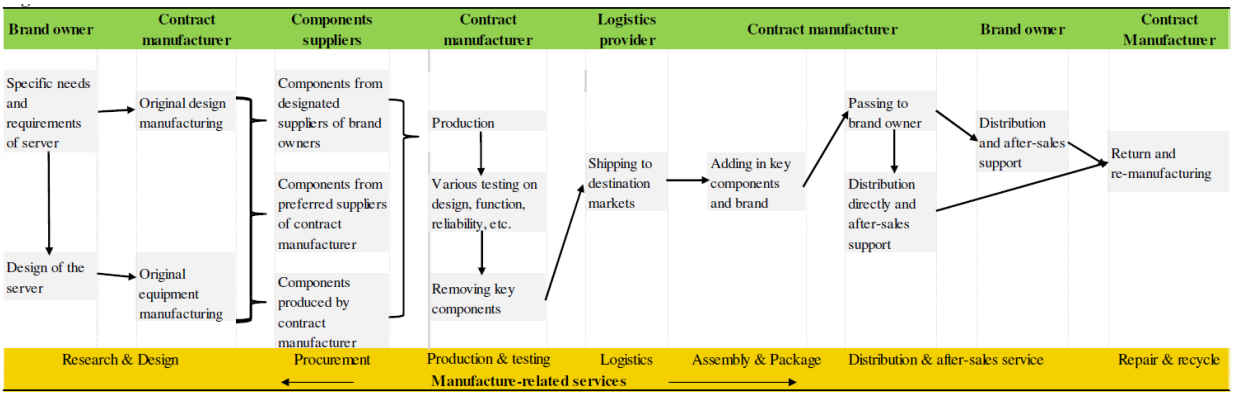


Figure 4: A Server Global Value Chain

Source: APEC Services in Global Value Chains: Manufacturing-Related Services [90]

Manufacturing Footprint. Geographically, Asia, and, in particular China, leads globally in the final assembly of networking equipment manufacturing. Taiwanese EMS or ODM companies account for 90 percent of global server manufacturing and approximately two-thirds of their final assembly for servers is in China.[91] China has developed an ecosystem for electronics system manufacturing through decades of targeted investments, which has conferred advantages with respect to capital, labor, and supplier and demand base.[92] These manufacturing clusters are evolving in East and Southeast Asia for various components in networking hardware. In addition to cost efficiencies, the production and assembly cluster ecosystems allow for faster product upgrades and customization implementation. Consequently, there is no significant capacity

[88] Matt Kimball, "Do You Know Where Your Servers Come from? Here's Why Securing the Supply Chain Matters," Forbes (Forbes Magazine, May 19, 2020), https://www.forbes.com/sites/moorinsights/2020/05/19/do-you-know-where-your-servers-come-from-heres-why-securing-the-supply-chain-matters/?sh=5dd5101ae150.
[89] Comments of Telecommunications Industry Association to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (TIA, November 4, 2021).
[90] "Services in Global Value Chains: Manufacturing-Related Services," APEC, https://www.apec.org/publications/2015/11/services-in-global-value-chains-manufacturing-related-services.
[91] Colley Hwang, "Views from Taiwan (10): The Structure of the Server Sector," DIGITIMES (DIGITIMES Inc., August 9, 2021), https://www.digitimes.com/news/a20210806VL205.html?mod=3&q=server%2Bmanufacturing.
[92] Comments of Flex to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (Flex, November 4, 2021); Comments of HP to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (HP, November 3, 2021).

outside of China for key components of the networking hardware manufacturing supply chain such as power supplies.

Fortunately, networking equipment manufacturers have recently taken steps to shift to a more geographically dispersed supply chain. This could be due to increased demand in the United States and Europe for key end uses, such as datacenters. For some companies, the COVID-19 pandemic has demonstrated that single-market mass production is not sustainable in the long term. Various ICT manufacturing facilities shut down in China at the onset of the pandemic, causing disruptions to the supply chain.[93] Major Taiwanese companies including Inventec, Quanta, Wistron, Foxconn, and Mitac, have also moved factories back to Taiwan or expanded factories in other countries, including the United States, Mexico, the Czech Republic and Germany.

Recently, some U.S. companies have increased final assembly of networking equipment in the United States to provide for the U.S. market.[94] U.S. companies have acknowledged that tariffs and cybersecurity concerns are leading to the shift away from Asia. Contracts with the U.S. government may also act as a positive incentive to increase production domestically.[95] Because of increasing transportation costs, EMS providers also see opportunities to increase the final assembly of larger products like switches and server racks in the United States.[96]

Key risks facing the U.S. networking hardware equipment supply chain include:

- **Increasing competition and price pressures on U.S. companies**. Demand for networking equipment is expected to grow in the coming years due to increased demand for cloud computing and other internet services. While there are still many sources of U.S.-branded networking equipment, Chinese companies such as Huawei and Inspur are gaining global market share in routers, servers, and other networking technology. As a result, there is increasing competition and price pressure for U.S. companies, especially in foreign markets.

In summary, networking hardware, like much of the ICT industrial base, is largely produced by Taiwanese EMS companies with production concentrated in China. Recent supply chain disruptions and transportation costs have motivated some firms to diversify production and assembly locations, including moving production facilities to the United States. However, because significant capacity for key portions of the networking hardware supply chain do not currently exist outside of China, efforts to relocate facilities will require significant time and investment.

---

[93] Vipul Kumar, "China plus One – an Emerging Supply Chain Diversification Strategy," Supply and Demand Chain Executive, October 4, 2021, https://www.sdcexec.com/sourcing-procurement/sourcing-solutions/article/21747630/aranca-china-plus-one-an-emerging-supply-chain-diversification-strategy.

[94] "Hewlett Packard Enterprise Becomes the Only Major Server Manufacturer to Ship the World's Most Secure Industry-Standard Servers with U.S. Country of Origin," HPE (Hewlett Packard Enterprise, December 9, 2021), https://www.hpe.com/us/en/newsroom/press-release/2020/10/hewlett-packard-enterprise-becomes-the-only-major-server-manufacturer-to-ship-worlds-most-secure-industry-standard-made-in-usa-servers.html.

[95] Barclay Ballard, "Foxconn's Wisconsin Plant Wins Google Server Contract," TechRadar (TechRadar, November 24, 2020), https://www.techradar.com/news/foxconns-wisconsin-plant-wins-google-server-contract.

[96] Comments of Flex to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (Flex, November 4, 2021).

4.5 Downstream Products: LCDs/Displays

Liquid Crystal Displays (LCDs) are used in a variety of devices including smartphones, computer monitors, and televisions. By layering upstream components such as glass substrate, electrodes, liquid crystal, PCBs, and a light source, LCDs can produce visual images on screen. Many products outside the ICT industry are increasingly dependent on LCD panels as well, especially within the automotive, healthcare, and education sectors. There are a variety of sizes and types of LCDs ranging from large flat panel displays to smaller LCD panels used for smartphones.

Manufacturing Footprint. Historically, the LCD panel supply chain has been concentrated in East Asia, though it has shifted between various countries. Over the past decade, China has become the largest location for LCD manufacturing followed by Taiwan, South Korea, and Japan. China supported the growth of its LCD industry by providing government subsidies and reduced taxes to domestic display manufacturers.[97] As a result, most Chinese LCDs are sold below cost and there is no cost-effective way to diversify production out of China. Because of the concentration in China, any disruptions in the region will have an oversized effect on the display supply chain, as demonstrated by China's 2021 power supply shortages which reduced display production.[98] There is almost no LCD production outside of East Asia, but other countries in the Americas and Asia may be positioned to emerge as potential alternative locations with significant engagement from industry and governments.[99]

Unlike other product categories, China leads in both LCD manufacturing and sales activities among its domestically headquartered firms. China's BOE Technology and China Star Optoelectronics Technology (owned by TCL Group) are leaders in large LCDs while Tianma Microelectronics leads in smaller panels. Chinese companies' share of global flat panel display production capacity increased from approximately 0 percent in 2011 to 46 percent in 2019 and is forecasted to reach 62 percent by 2023.[100] Korean headquartered firms LG Display and Samsung were former leaders that have lost market share to their Chinese rivals. However, Korean firms still hold an advantage in manufacturing newer display technologies such as organic light-emitting diode (OLED) panels.[101] There are no major U.S. companies involved in LCD production nor is there significant LCD manufacturing in the United States.

---

[97] Shuhei Ochiai, "Subsidized Chinese Makers Squeeze Asia's LCD Industry," Nikkei Asia (Nikkei Asia, April 21, 2019), https://asia.nikkei.com/Business/Business-trends/Subsidized-Chinese-makers-squeeze-Asia-s-LCD-industry.

[98] Adam Hwang and Rebecca Kuo, "Output of Panel Components, LCD Modules in China Falls 30% Due to Power Restrictions," DIGITIMES (DIGITIMES Inc., October 18, 2021), https://www.digitimes.com/news/a20211015PD204.html?mod=3&q=lcd.

[99] Steve Shen and Jingyue Hsiao, "India Reportedly to Invest US$20 Billion to Develop LCD Panel Industry," DIGITIMES (DIGITIMES Inc., May 31, 2021), https://www.digitimes.com/news/a20210528PD210.html.

[100] Charles Annis, "Boe Becomes World's Largest Flat-Panel Display Manufacturer in 2019 as China Continues Rise to Global Market Dominance," Omdia, June 4, 2021, https://omdia.tech.informa.com/OM003804/BOE-Becomes-Worlds-Largest-Flat-Panel-Display-Manufacturer-in-2019-as-China-Continues-Rise-to-Global-Market-Dominance.

[101] Kotaro Hosokawa, "LG and Samsung in Full Retreat before Chinese Flat-Panel Onslaught," Financial Times, April 28, 2020, https://www.ft.com/content/945ee1ce-7031-4670-ad25-df6f04a30d23.

Key risks facing the U.S. LCDs/Displays supply chain include:

- **Supply Chain Consolidation in China**. As noted above, China has provided targeted support to its domestic display manufacturers, and competition among suppliers within China is intensifying with the emergence of new domestic suppliers. These factors have led to sharp increases in the global supply of liquid crystal display panels made in China and made by China-based brands, while production in other countries such as South Korea has decreased.[102]

In summary, Chinese companies hold a significant share of the global production of LCDs. Buttressed by Chinese government non-market policies and practices, Chinese firms dominate the industry while their competitors struggle to compete with their artificially low-priced products. Since displays are important in other sectors, lack of manufacturing diversity may increase supply chain risks in other product areas outside of ICT.

[102] Adam Hwang and Rebecca Kuo, "Panels to Be in Oversupply in 2022, Says Hannstar Display VP," DIGITIMES (DIGITIMES Inc., November 12, 2021), https://www.digitimes.com/news/a20211112PD211.html?mod=3&q=lcd.

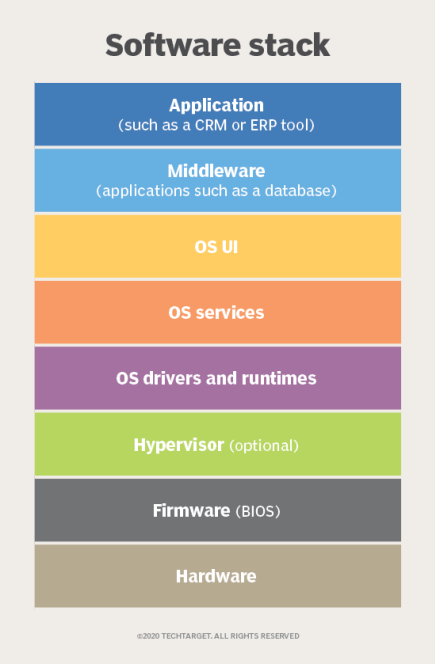
5. Current State of the ICT Software Sector and Related Risks

Software can be defined as the set of instructions that tell a computer how to work. It is a dynamic product: it undergoes changes from its point of inception to the end of its use. Updates are required to improve functionality, accommodate changes to the operating environment, and to apply patches to resolve bugs or vulnerabilities. Software is rarely built from scratch today. Rather, it is typically compiled from existing code libraries, both open source and proprietary, with new software code developed to provide specific capabilities on top of the sourced code.

Software is ubiquitous and found in all information and communications technology. It enables the underlying hardware to function, directs flows and processing of information, and facilitates a user's interaction with a technology product.

The type and purpose of software varies. Pursuant to Figure 5, a stack of software is a group of programs that work to enable a technology product to function as intended:

Figure 5: Software Stack[103]



- **Applications software** is the most familiar type of software as it performs functions for an end-user.
- **Middleware software** helps to enable communications and connectivity between applications and is typically found in complex system environments. Examples where middleware software is used include web servers and extract, transform and load tools.
- **The operating system (OS)** performs critical functions as it manages both computer hardware, software resources, and provides the common services needed to load computer programs into memory and then execute them. The OS is the enabling interface between middleware and application software and the hardware. It performs boot functions, device drivers control specific devices that are connected to the computer, like a printer or mouse, and provides utilities that assist the user in performing tasks, like running back ups or anti-virus scans.
- A product may also include **hypervisor software** which creates and runs a virtual machine. This can allow for multiple instances of an operating system to share the virtualized hardware resources.
- At the lowest level of this stack is **firmware**, which provides the necessary instructions for how the device communicates with the computer hardware.[104]

While there are various types and purposes of software in the software stack, the focus of this section is on open-source software and firmware, as they are ubiquitous across the sector and

[103]Margie Semilof and James Montgomery, "Software Stack," TechTarget, updated November 2020, https://www.techtarget.com/searchapparchitecture/definition/software-stack.
[104] "Glossary: firmware", Computer Security Resource Center, National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/firmware.

present unique supply chain security issues. Open-source software (OSS) is "software that can be accessed, used, modified, and shared by anyone. OSS is often distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative and/or that meet the definition of "Free Software" provided by the Free Software Foundation." [105] A feature of OSS is that anyone can inspect, modify, and enhance the source code and it is usually obtained by accessing a publicly available software library. Firmware is software which provides the necessary instructions for how the device communicates with the computer hardware.[106]

The following subsections provide background on the software supply chain, an overview of open-source software and firmware, and a review of risks pertaining to open-source software and firmware.

5.1 Background on the Software Supply Chain

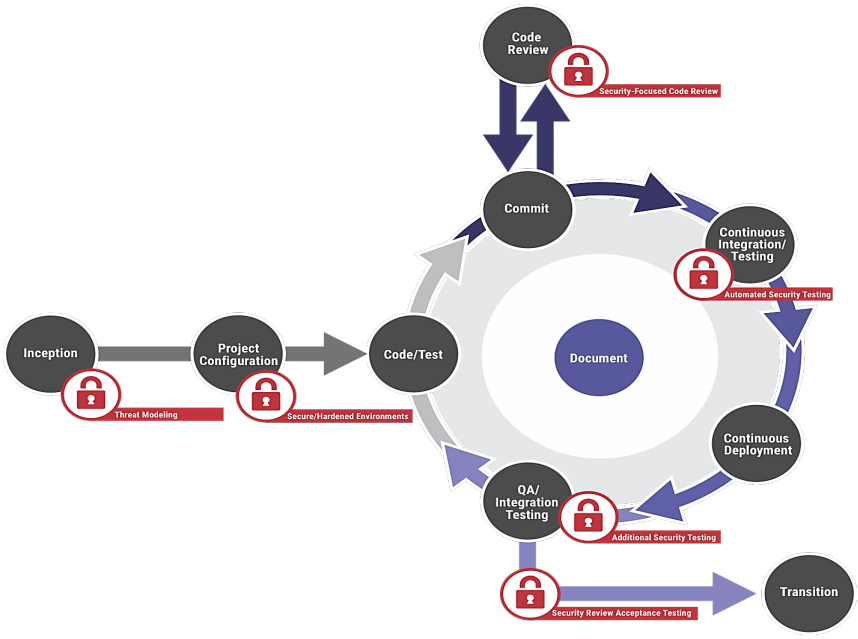
Regardless of the type, "software is an enduring capability that must be supported and continuously improved through its life cycle."[107] The graphic portrayed in Figure 6 provides a high-level depiction of these life cycle steps. [108] The cycle begins with a concept that is shaped into requirements associated with a given software project. Software is then built and compiled to produce a viable component that is tested and then integrated into hardware and other software.

A software supply chain is the entire sequence of events that impacts software from the point of origin where it is designed and developed, to the point of end-use. Each sequence and element in this chain affects the software in some manner and can contribute to its assurance level or introduce a weakness that can be exploited. The supply chain includes the software code itself as well as the systems and tools used by developers, proprietary and open-source software repositories, signing keys, compilers, and download portals. The entities that comprise the software supply chain can include multiples of developers and technology providers. In many instances, the author of a given open-source software component is unknown. It is also unusual to find a single company responsible for the entirety of a software code base.

---

[105] Open Source Code, NIST S 6106.01, December 6, 2018, https://www.nist.gov/document/finals610601ver1pdf
[106] "Glossary: open source software", Computer Security Resource Center, National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/firmware.
[107] J. Michael McQuade and Richard M. Murray (co-chairs) Gilman Louie, et al., "Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage," Defense Innovation Board, March 21, 2019, https://media.defense.gov/2019/Mar/26/2002105909/-1/-1/0/SWAP.REPORT_MAIN.BODY.3.21.19.PDF.
[108] Dr. William R Nichols and Scanlon, Dr. Thomas, "DoD Developers Guidebook for Software Assurance," Software Engineering Institute Carnegie Melon University December 2018, p. 16.

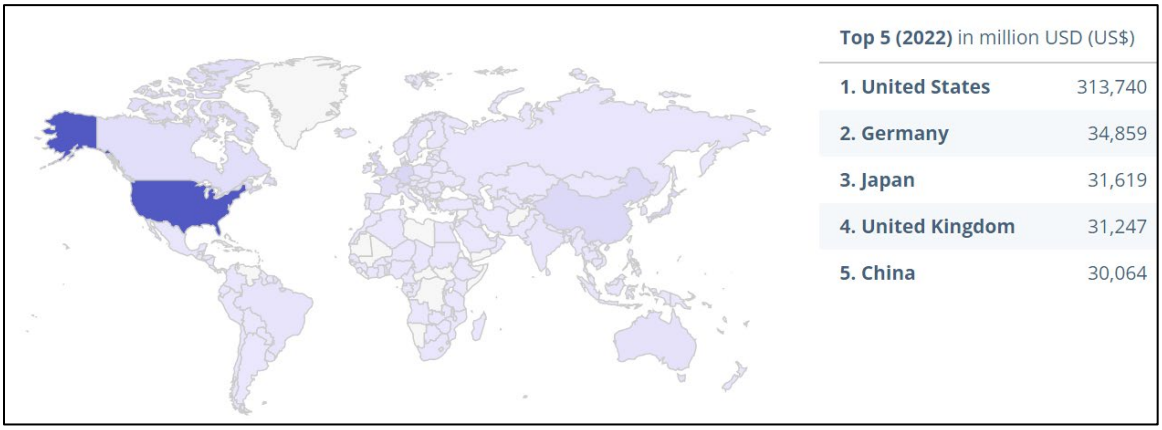
Figure 6: The Software Life Cycle[109]



Software is developed on a global scale. The United States dominates the global marketplace for software in terms of revenue (see Figure 7 below) with $313.7 billion in revenue anticipated in 2022, growing to $409.9 billion by 2026.[110] As detailed in Section 6, currently, the United States has the largest software developer labor force; however, the Asia Pacific region has the highest growth rate for software developers. To that end, forecasters believe that, by 2024, India will overtake the United States as the largest software developer population center. Latin America has the second largest growth behind the Asia Pacific region. Eastern Europe also is a global hotspot for software development.[111]

[109] Dr. William R Nichols and Scanlon, Dr. Thomas, "DoD Developers Guidebook for Software Assurance," Software Engineering Institute Carnegie Melon University December 2018, 16.
[110] "Technology Markets, Software," Statista, August 2021, https://www.statista.com/outlook/tmo/software/united-states.
[111] "How Many Software Developers Are There in the World," *Daxx*, September 23, 2021, https://www.daxx.com/blog/development-trends/number-software-developers-world.

Figure 7: Projected 2022 Global Software Revenue Comparison[112]



5.2 Overview of Open-Source Software

Open-Source Software (OSS) plays a critical role in today's software ecosystem, with 75 percent of all audited codebases in 2020 containing at least one open-source component and open source comprising 70 percent of the overall code.[113] OSS is found throughout the software stack. The universal desire for faster innovation fundamentally requires that software developers reuse code frequently and efficiently. This, in turn, has led to a critical dependence on OSS libraries borrowed from third-party ecosystems. These third-party components and packages represent the building blocks of modern software development.[114] Unlike proprietary or "closed" software which restricts who can access, use, and change the source code, open-source software is source code that anyone can inspect, modify, and enhance, and is obtained by accessing a software library. This library contains prewritten code that is available for reuse by a developer to create software programs and applications.

A 2020 industrial base assessment conducted by the Bureau of Industry and Security at the U.S. Department of Commerce, which was completed by 389 U.S. ICT participants that develop security-related products, provides insight into the use of OSS in the U.S. ICT industry. More than 50 percent of respondents indicated the use of open-source software in 24 of the 55 product types that were detailed in the assessment. Well-known software and cybersecurity companies were among the most frequent users of OSS, reporting that 100 percent of the products they identified in the survey contain OSS. This finding demonstrates the ubiquitous nature of OSS in hardware and software technologies developed by large firms within the U.S. ICT industrial base.

Respondents identified network security devices such as deep packet inspection (DPI) appliances, firewalls, security information and event management tools, network infrastructure

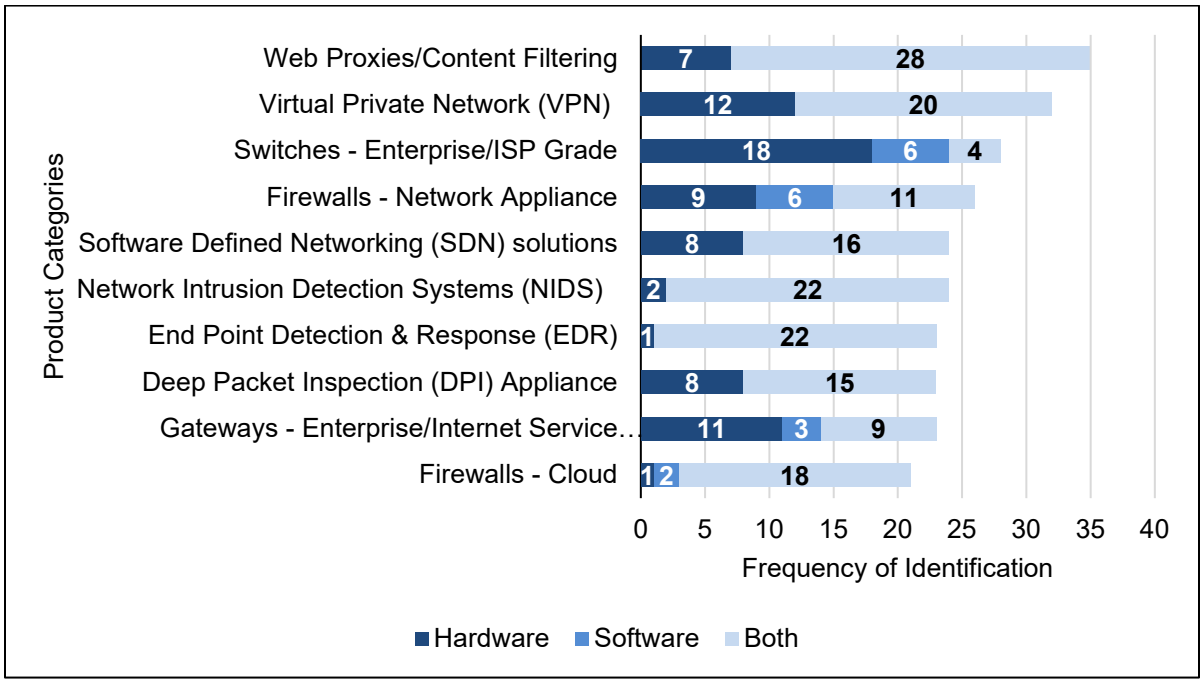
---

[112] "Technology Markets, Software," Statista.
[113] "2021 Open Source Security Risk Analysis Report," Synopsys, Accessed October 2021, https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html.
[114] "2021 State of the Software Supply Chain," Sonatype, https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021.

devices such as routers and gateways, and other products such as printers, scanners, and supervisory control and data acquisition (SCADA) systems as the types of products for which they frequently used OSS.

Figure 8 below portrays specific hardware and software technologies with the highest percent of OSS integration as reported by respondents. Web proxy and content filtering technology was the most frequently identified product, with 65 percent of respondents who design, manufacture and/or sell web proxies integrating their hardware and software technologies with OSS. Similarly, 62 percent and 60 percent of respondents supporting networked SCADA systems and networked connected health systems or devices identified use of OSS, respectively.

Figure 8: Frequency of Respondents Indicating Use of Open-Source Software by Hardware/Software Technology[115]



The global supply of open-source libraries continues to grow exponentially, fueled by new versions of existing projects constantly being released, and by the creation of new projects. Currently, the four largest revenue producing open-source ecosystems contain a combined 37,451,682 components and packages. These same communities released a combined 6,302,733 new versions of components/packages over the last year and have commenced723,570 new projects in support of 27 million developers worldwide.[116] Microsoft's GitHub, the world's largest repository for open-source code with 40 million users and 206 million code repositories,

[115] Note: Excludes "Other – Other Products." *National Security Assessment: Use of Select Software in Information and Communications Technology*, Bureau of Industry and Security, U.S. Department of Commerce, July 2021.

[116] Ibid.

reported that over 10 million new developers joined and over 44 million new projects were created in 2019 alone."[117]

Chinese software developers rely heavily on GitHub, the world's largest open-source code repository with 40 million users and 206 million code repositories. China has been one of the fastest growing users outside of the United States. China's Ministry of Industry and Information Technology (MIIT), one of China's most prominent technology policymakers, has championed the importance of the country having its own domestic open-source alternatives. To build its own version of GitHub, MIIT picked Gitee to construct an "independent, open-source code hosting platform for China."[118] The project will be headed by a consortium led by Open-Source China, a Shenzhen-based firm and Gitee. This new hosting service is considered to be a government-led effort with support from research universities and participation from the private sector, and includes a group of ten organizations, including Huawei. Gitee claims to have "hosted more than ten million open-source repositories and provided services to over five million developers so far."[119] In the coming years, it will be worth watching the potential growth of the Gitee platform given the backing of the Chinese government and several large private sector firms.

5.3 Open-Source Software Supply Chain Risks

The availability of open-source software has accelerated innovation and provides economic and societal benefits, but it can also pose risks, especially if it is implemented in organizations without robust cybersecurity practices. The most basic challenge with OSS security can be the lack of a single responsible entity to help organizations find or fix a security issue. There is no responsible entity to make a "fix" and often there is not an immediate release of an alert identifying the security issue. Instead, organizations submit a "pull request" in an open-source repository or one of the developers would review the reporting and resolve the security issues. Given the already vast and growing use of OSS, the urgency and importance of ensuring that OSS is secure and can be trusted cannot be overstated. In 2021, there was a 650 percent global increase in software supply chain compromises aimed at exploiting weaknesses in upstream open-source ecosystems. Comparatively, the same statistic was 430 percent in 2020.[120] Bad actors are no longer waiting for public vulnerability disclosures to pursue an exploit. Instead, they are seizing the initiative to insert new vulnerabilities into open-source projects that support the global software supply chain and then exploit these vulnerabilities.

A recent example of an OSS security vulnerability is a flaw in Apache's Log4Shell software library. Log4Shell has become an internet vulnerability that has affected millions of computers and involves an obscure but nearly ubiquitous piece of software, Log4j. According to the Wall Street Journal, "software developers use the Log4j framework to record user activity and the behavior of applications. Distributed free by the nonprofit Apache Software Foundation, Log4j has been downloaded millions of times and is among the most widely used tools to collect information across corporate computer networks, websites, and applications. An Apache

---

[117] "The 2021 State of the Octoverse," GitHub, Inc., 2021, https://octoverse.github.com/.
[118] Rita Liao, "China is Building a GitHub Alternative called Gitee," *TechCrunch+*, August 21, 2020, https://techcrunch.com/2020/08/21/china-is-building-its-github-alternative-gitee/.
[119] Ibid.
[120] "2021 State of the Software Supply Chain," Sonatype.

spokeswoman said the way Log4j is inserted into different pieces of software makes it impossible to track the tool's reach."[121]

Because of the Log4j security flaw, hundreds of millions of devices are at risk and the flaw allows attackers to execute code remotely on a target computer, which could let them steal data, install malware, or take control of the affected system. Cybersecurity company Akamai Technologies, Inc. has tracked ten million attempts to exploit the Log4j vulnerability per hour in the United States.[122] In addition, foreign governments are taking advantage of the flaw, as security company Mandiant Inc and Microsoft Corporation have traced attempted compromises that exploit the flaw to hackers with suspected links to China and Iran. DHS's Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly says that the Log4j security flaw is the "most serious" vulnerability she's seen in her decades-long career, and it could take years to address.[123] To remediate against the flaw, CISA suggests organizations immediately identify internet-facing devices that have Log4j and ensure that security teams respond to alerts related to these devices. Organizations should also install a web application firewall with rules that automatically update.[124] The Log4j incident highlights the importance of prioritizing patches when they become available, conducting security reviews, and immediately reporting compromises to authorities.

The utilization of software libraries can provide avenues for supply chain compromises. Three common compromise methods are Package Typo Squatting, Dependency Confusion, and Malicious Injects, described below.

- **Typo Squatting** involves a malicious actor that names a tainted software component something similar to the name of a well-known component and uploads the software package into a registry that can then be downloaded from the Internet.
- A **Dependency Confusion** attack or supply chain substitution attack occurs when a software installer script is tricked into pulling from a public repository a malicious code file, typically using the same name but a newer version, instead of the intended file of the same name from an internal repository. This technique takes advantage of weaknesses in an automated process inherent in certain software build tools since the tool is designed to find and fetch the latest version of any package.
- **Taint/Malware attacks** involve threat actors inserting malicious code into publicly available code libraries, which developers then add (often unwittingly) to their own third-party code.[125] These attacks can also include insertion of counterfeit components during system design and development across the supply chain.

---

[121] David Uberti, James Rundle, and Catherine Stupp, "The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw," *The Wall Street Journal*, December 21, 2021, https://www.wsj.com/articles/what-is-the-log4j-vulnerability-11639446180.
[122] Ibid.
[123] Jen Easterly, "CISA Director Says The LOG4J Security Flaw Is The 'Most Serious' She's Seen In Her Career," interview by Eamon Javers, *CNBC*, December 16, 2021, https://www.cnbc.com/video/2021/12/16/cisa-director-says-the-log4j-security-flaw-is-the-most-serious-shes-seen-in-her-career.html.
[124] "Apache Log4j Vulnerability Guidance," Department of Homeland Security Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance.
[125] Dr. Trey Herr, William Loomis, Stewart Scott, et al., "Breaking Trust: Shades of Crisis Across An Insecure Software Supply Chain," *Atlantic Council*, July 26, 2020,https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/

5.4 Firmware Overview

Firmware is a set of programs and data embedded into hardware, typically stored in non-volatile memory such as read-only memory (ROM), erasable programmable read-only memory (EPROM), or flash memory. Firmware is crucial to system operation, providing instructions and guidance for the device to communicate with other devices or perform a set of basic tasks and functions as the software intended. Firmware is tailor-made for each model or product and enables the operation of both simple and complex ICT devices and systems such as medical devices, manufacturing systems, data centers, power plants, mass transit systems, and telecommunications. To that end, because it connects hardware to software, firmware is necessary for a wide range of electronics such as traffic lights, digital watches, printers, remote controls, mobile phones, network routers and switches, and servers.

In addition, individual devices attached to personal computers (PCs) have firmware that directs hardware actions, including drives, network adaptors, processors, memory, peripheral devices (e.g., Wi-Fi adapter, router, webcam, keyboard, battery, sound card, USB stick). The basic input/output system (BIOS) is a notable example of firmware. The BIOS facilitates the hardware initialization process and then hands control to the Operating System (OS) in a PC. BIOS is often used interchangeably with unified extensible firmware interface (UEFI), a newer version of host processer boot firmware. Although UEFI has become the new standard boot firmware in PCs, many use BIOS and UEFI interchangeably, and BIOS are still found across devices today.

Firmware Supply Chain

While firmware is effectively low-level software, or the command function level of software, it has very little to do with modern programming languages. At its core are instructions that define how a device operates and how it communicates with other hardware and peripherals. Firmware does not have previously designed code libraries or packages that software developers typically use. Instead, firmware development must be started from scratch and writing firmware requires deep hardware knowledge and masterful coding skills.[126] In 2019, there were 5,041 firmware engineers employed in the United States[127]

The entities involved in the firmware supply chain generally fall into four groups: Reference implementers such as U.S.-based firms Intel and AMD, and open-source platform TianoCore; Independent BIOS vendors (IFVs) such as U.S.-based firms American Megatrends and Phoenix Technologies, and Taiwan-based firm Insyde; Original device manufacturers (ODMs) such as Taiwan-based firms Foxconn, Wiwynn, Compal, and Quanta Computer; and Original electronic manufacturers (OEMs) such as U.S.-based firms Dell and HP, and Hong Kong-based firm Lenovo.[128] Typically, ODMs and OEMs have their own firmware teams, creating a firmware image tailored to each platform's hardware configuration. The teams can create their own custom solution, but often they license a UEFI development codebase from an IFV. These IFV solutions

[126] Ronni Shendar, "Firmware Runs the World, But Who Will Write It?" *Western Digital Blog*, June 21, 2021, https://blog.westerndigital.com/firmware-runs-the-world.
[127] "Hardware/Firmware Engineer Statistics and Facts in the US," Zippia, https://www.zippia.com/hardware-firmware-engineer-jobs/demographics/.
[128] Alex Tereshkin, Alex Matrosov, Adam 'pi3' Zabrocki, "Safeguarding UEFI Ecosystem: Firmware Supply Chain is Hard(coded)," Blackhat USA 2021, August 4-5, 2021 Briefings.

are based on reference designs from silicon manufacturers, which the ODM and OEM use as the basis for end-user products.[129]

5.5 Firmware Risks

Firmware presents a large and ever-expanding attack surface, as the population of electronic devices grows. Securing the firmware layer is often overlooked, but it is a single point of failure in devices and is one of the stealthiest methods in which an attacker can compromise devices at scale. Over the past few years, hackers have increasingly targeted firmware to launch devastating attacks.

Attacker advantages. Due to firmware's privileged position within the device, attacks conducted via firmware grant malicious actors unique advantages. Attackers can subvert OS and hypervisor visibility and bypass most security systems, hide, and persist in networks and devices for extended periods of time while conducting attack operations, and inflict irrevocable damage. Firmware can also be a lucrative target with a relatively low cost of attack. Despite its essential role in electronic devices, firmware security has not traditionally been a high priority for manufacturers or users and is not always well protected. The National Vulnerability Database has tracked a five-fold increase in reported vulnerabilities subject to exploitation over the last four years. In a 2021 study commissioned by Microsoft interviewing over 1,000 enterprise security professionals, 80 percent of enterprises reported that they had been the victim of a firmware compromise at least once in the last two years.[130] Furthermore, 21 percent of security decision-makers in the survey admit their firmware data goes unmonitored and only 29 percent of security budgets are allocated to protect firmware.[131] Although this trend is changing in PCs as manufacturers and customers have realized the need for built-in protection, many devices still have firmware that is not well secured. Firmware on items such as network cards, Wi-Fi adapters, and USB hubs are often not properly signed with public or private keys. These devices have no way to verify that the operating firmware is authentic and can be trusted.

Complex Supply Chains. As discussed in Sections 3, 4, and 6, device manufacturers rely on a complex chain of component suppliers which may present organizational risks for firmware security. In PC production, for example, the OEMs are typically responsible for firmware and the rest of the PC platform elements. However, many OEMs outsource firmware development to third-party suppliers where OEMs may not have visibility into their cybersecurity hygiene. Even if OEMs establish security standards, they may not be able to enforce supplier security protocols across a wide range of components and sub-suppliers. Furthermore, individual OEM vendors may modify the firmware based on device needs once the firmware has been delivered to the OEM. This can lead to confusion about what party is ultimately responsible for firmware integrity and who is to supply customer updates. In addition, as devices and firmware change, OEMs often contract with different firmware developers, which can lead to delays or a lack of any update when older devices require updating and the original developer is not available. All of these factors can leave firmware open to malicious attacks.

---

[129] "Understanding UEFI and the Firmware Ecosystem," UEFI Forum, February 25, 2020, https://uefi.org/node/4046.
[130] "Security Signals," Microsoft, March 2021, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWPStZ.
[131] George Hulme, "Your Firmware is a Wide Open Back Door," *Endpoint.,* April 30, 2021, https://endpoint.tanium.com/your-firmware-is-a-wide-open-back-door/.

Updates. Pre-existing, unidentified, or inherent vulnerabilities are compounded by updating firmware, which varies widely across devices. A firmware's update process and capability vary by device. Some devices receive regular firmware updates. Some may only receive one update over their lifetimes, while others may never receive an update. Device firmware may be updated wirelessly or require a physical connection to another device (e.g., USB, CD/DVD drive, etc.). Even for devices that are designed to update regularly, manufacturers do not always provide clear and readily available information on how to update the firmware.

In addition, the process to update is not simple, and therefore not always done. For example, it may not be clear what the latest firmware update is for a particular device. As a result, users may not be able to quickly determine whether the device's firmware is up to date. For devices with firmware that is not cryptographically signed and secure, devices may be updated with unsigned code, meaning firmware could be rewritten without needing any verification from the user. A once-trusted device may no longer be trusted as secure after an unencrypted update.

Firmware updates present a major logistical challenge for many enterprises. In many instances, device firmware is never updated or may only be updated in an emergency. In addition, vendors may only supply firmware updates if driven by an incident or identified vulnerability. Because users cannot always identify the latest firmware or determine if a device is running the latest version, IT security professionals may not be able to independently verify critical security information and must rely on information provided by vendors. In addition, even if an organization wanted to upgrade security to a specific standard across devices, the age and variety of devices and their individual firmware make this extremely challenging.

Ransomware. Finally, while some malicious actors have exploited firmware to launch ransomware attacks, spreading malicious code and accessing sensitive information, others target firmware itself with ransomware. Historically hackers have used boot kits to target the Master Boot Record (MBR), altering the MBR on the hard drive. For instance, the hackers behind the 2016 Petya attack initially moved to control the MBR and, more recently, the Thanos ransomware actors have used this method.[132] One of the more alarming trends in attacks on firmware is the threat actor focus on Unified Extensible Firmware Interface (UEFI). Suspected state actors have carried out attacks that were previously only theoretical. In one instance of this attack, dubbed MosaicRegressor, hackers repurposed Vector EDK UEFI rootkit components that were leaked in 2015 and created a multi-stage, modular framework for data gathering and espionage. Researchers believe hackers inserted modified UEFI either remotely or using a USB flash drive and were then able to connect to victims' command and control servers, download modules, and use the modules to steal data. These types of implants are almost impossible to extract and can only be removed by flashing the motherboard.[133]

Compromised firmware in today's devices, which are almost always connected to networks, can result in catastrophic effects. Devices with unprotected firmware can lead to system-wide damage. Malicious code in the firmware of products such as USBs and network interface cards,

---

[132] Robert Falcone, "Thanos Ransomware: Destructive Variant Targeting State-Run Organizations in the Middle East and North Africa," Palo Alto Networks, September 4, 2020, https://unit42.paloaltonetworks.com/thanos-ransomware/, and "The Top 5 Firmware Attack Vectors," Eclypsium, December 28, 2018, https://eclypsium.com/2018/12/28/the-top-5-firmware-and-hardware-attack-vectors/.

[133] Mark Lechtick et al., "MosaicRegressor: Lurking in the Shadows of UEFI," SecureList, October 5, 2020, https://securelist.com/mosaicregressor/98849/, and Pavel Shosin, "Malware Delivery through UEFI Bootkit with MosaicRegressor," Kaspersky Daily, October 7, 2020, https://usa.kaspersky.com/blog/mosaicregressor-uefi-malware/23419/.

can not only give attackers control over the device itself but may allow attackers to bypass OS security measures to access high levels of privilege on a PC or an entire network. As the population of devices expands, particularly interconnected IoT devices, issues in firmware security will be magnified exponentially. As attacks have increased, government and industry have begun to address firmware vulnerabilities to protect against and mitigate the impacts of future attacks.

In summary, open-source software and firmware are integral to the ICT industrial base, enabling the development and functionality of nearly all types of ICT software and hardware products. However, the nature of these products in addition to the software supply chain itself present several risks. First, the dynamic nature of software development exposes the supply chain to countless sources of both known and unknown vulnerabilities, from insecure open-source software to zero-day exploits. Second, the growing reliance on open-source software increases the risk and potential impact of software supply chain attacks through methods such as package typo squatting and malicious injects. Finally, firmware presents a large and ever-expanding attack surface as the number of electronic devices grows and the ICT supply chain increases in complexity. Product integrity assurance throughout the ICT industry is important to ensure secure and reliable products.

6. Current State of the ICT Workforce and Related Risks

The resiliency of the ICT supply chain is contingent upon a stable and developed workforce. This section reviews the state of the current U.S. ICT hardware manufacturing and software engineering workforce and related workforce risks.

6.1 ICT Hardware Manufacturing Workforce

As mentioned in section 4, a significant portion of ICT manufacturing has relocated to Asia. This has contributed to a downturn in domestic production capabilities. From January 1997 to June 2009, advanced manufacturing in the United States lost over 2 million jobs, of which 36 percent or 720,000 jobs were computer and electronics manufacturing roles. During this time, the share of U.S. advanced manufacturing jobs across all industries in the private sector fell from 7.5 percent to 4.9 percent."[134] Today there are approximately 274,000 ICT manufacturing or production-related occupation jobs in the United States, representing approximately five percent of the domestic ICT workforce, according to the most recent data from the Bureau of Labor Statistics (BLS).

The largest of these employment groups is *Semiconductor and Other Electronic Component Manufacturing*, which accounts for approximately 147,000 jobs or about 54 percent of the ICT manufacturing workforce. The manufacturing workforce in this group specialized in the production of semiconductors, printed circuit boards, connectors, passive components, and printed circuit board assemblies.

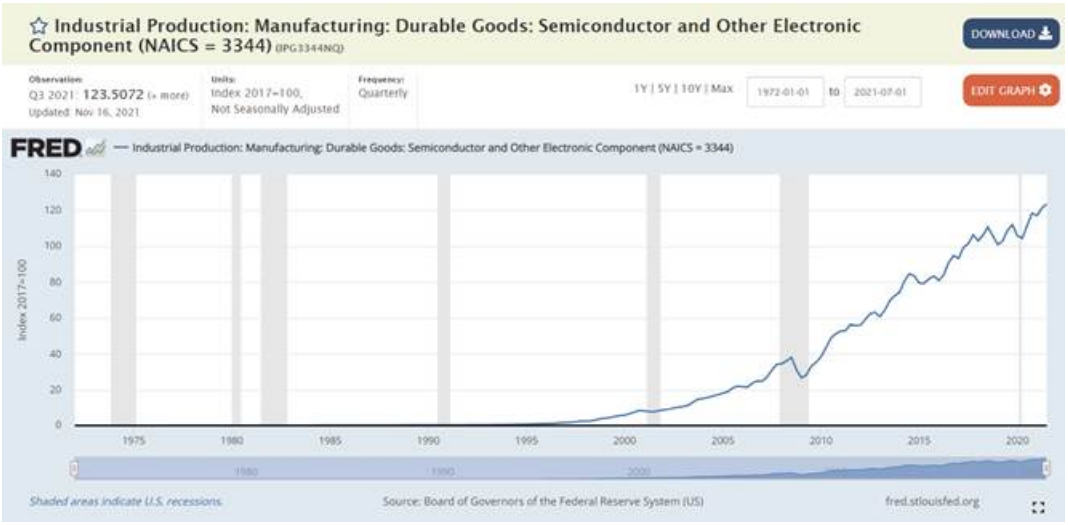


Figure 9: Industrial Production: Manufacturing: Durable Goods: Semiconductor and Other Electronic Components (NAICS =3344)[135]

[134] "Advanced Manufacturing Is a Key Cog in U.S. Economy," Saint Louis Fed (Federal Reserve Bank of St. Louis, March 29, 2018), https://www.stlouisfed.org/on-the-economy/2018/march/advanced-manufacturing-key-cog.
[135] "Industrial Production: Manufacturing: Durable Goods: Other Electrical Equipment and Component (NAICS = 3344)," FRED (Saint Louis Fed, January 14, 2022), https://fred.stlouisfed.org/series/IPG3344SQ.

Another crucial part of the domestic ICT workforce is any occupation that falls under *Other Electrical Equipment and Component Manufacturing.* This employment group covers approximately 71,000 Americans and is responsible for the production of critical ICT products like fiber optic cable as well as other electrical products like batteries and current carrying wired devices. Despite modest gains in this group's industrial production over the past decade, industry participants have cited excess fiber capacity as one of the reasons that American companies are poised to take advantage of an expected surge in global demand. The global fiber optic market is expected to reach USD 5,384.6 million by 2027, compared to a market size of USD 2,589.5 million in 2020.[136] Provisions in the Bipartisan Infrastructure Law, particularly the $65 billion investment to ensure every American has access to high-speed internet, is expected to contribute to an increase in demand in this employment category.[137]

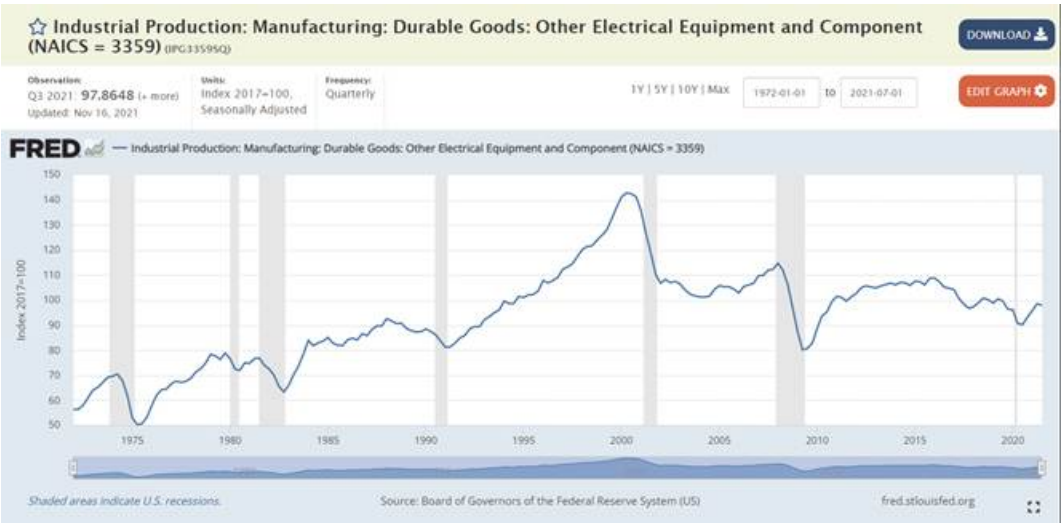


Figure 10: Industrial Production: Manufacturing: Durable Goods: Other Electrical Equipment and Component (NAICS =3359)[138]

Skills, training, and education required for ICT manufacturing jobs are wide-ranging, spanning from trade or vocational schools to advanced degrees. The required skills include technical skills for line workers, and operations, project and systems management, supply chain planning and procurement skills for higher-level manufacturing roles.[139] Job functions include material handling, equipment maintenance and general product assembly. In an average American ICT manufacturing operation, industry experts estimate that approximately 50 percent of employees fall under the *unskilled labor* category when they are hired and thus require training for their role

[136] "The Worldwide Ribbon Fiber Optic Industry Is Expected to Reach $5.3+ Billion by 2027," The Worldwide Ribbon Fiber Optic Industry is Expected to Reach $5.3+ Billion by 2027, September 3, 2021, https://www.prnewswire.com/news-releases/the-worldwide-ribbon-fiber-optic-industry-is-expected-to-reach-5-3-billion-by-2027--301369077.html.
[137] "President Biden's Bipartisan Infrastructure Law," The White House (The United States Government, December 2, 2021), https://www.whitehouse.gov/bipartisan-infrastructure-law/.
[138] "Industrial Production: Manufacturing: Durable Goods: Other Electrical Equipment and Component (NAICS = 3359)," FRED (Saint Louis Fed, January 14, 2022), https://fred.stlouisfed.org/series/IPG3359SQ.
[139] "Summary Report for: 51-2022.00 - Electrical and Electronic Equipment Assemblers," O*NET OnLine (Department of Labor, 2021), https://www.onetonline.org/link/summary/51-2022.00.

throughout the first year. Alternatively, only 25 percent of employees are hired onto the job with previously acquired skills that can immediately be put to use on the factory floor. The remaining 25 percent are generally hired for skilled management-type functions.[140]

The following examples illustrate some of the gaps and challenges in strengthening U.S. employment in ICT manufacturing for outlines several segments on the supply chain reviewed in Section 4.

PCB Manufacturing. While design and engineering roles play a crucial role in the value chain, not all PCB-related occupations require an advanced degree. Of the 21,000 U.S. workers in the PCB industry, 16,000 are in manufacturing roles.[141] One of the most significant challenges for U.S. PCB manufacturers is finding qualified workers, and for many, it is the primary reason PCB manufacturing has been outsourced. There are some certification and training programs in the United States, but in most cases, workers only receive on the job training. In contrast, China offers a degree in PCB manufacturing, and the Chinese government has prioritized creating a skilled labor force.[142]

Component Manufacturing. Nearly all production of low-cost upstream components such as integrated connector modules (ICMs) and power supplies is concentrated in China.[143] Many of these components are labor intensive and production has not been automated, making it difficult to diversify production locations. For example, ICM manufacturing still involves manually wrapping copper wire and the main source of skilled labor to perform this task is in China. It can take years to train a new labor force and requires significant investment by industry. While it is not cost efficient to move this type of production back to the United States without a change in technology, creating a geographically diversified manufacturing base will require capacity building and training in other countries.

Printed Circuit Assembly. Some of the jobs in a PCA factory are repetitive: insertion of large components and other parts, inspection, and shipping. In the United States, employees are taught welding and similar skills but can often not fill higher roles due to a lack of management training. According to Singapore/U.S. EMS company, Flextronics, the skills, training, and education required for manufacturing jobs are wide-ranging from trade school to advanced degrees. The majority of employees in these production roles maintain a high school diploma or equivalent and one year or less in an apprenticeship that will allow them to develop skills such as operations monitoring and technical drafting of machinery.[144] The required skills include technical skills for line workers, and operations, project and systems management, supply chain planning and procurement skills for higher-level manufacturing roles.[145] Additionally,

---

[140] Flex Ltd., Briefing to the Department of Commerce, (Virtual Meeting, January 11, 2022).
[141] "Annual Survey of Manufactures (ASM)," Census.gov (United States Census Bureau, October 8, 2021), https://www.census.gov/programs-surveys/asm.html.
[142] Bringing Back PCB Manufacturing is Easier Said than Done", *Printed Circuit Design and Fab,* February 10, 2021, https://pcdandf.com/pcdesign/index.php/current-issue/270-board-buying/15418-bringing-pcb-manufacturing-back-is-easier-said-than-done.
[143] John MacWilliams, "The Electronics Industry Starts to Ease Out of China," Connector Supplier, November 3, 2020, https://connectorsupplier.com/the-electronics-industry-starts-to-ease-out-of-china/. [144] "Details Report for: 51-2022.00 - Electrical and Electronic Equipment Assemblers," O*NET OnLine (Department of Labor, 2021), https://www.onetonline.org/link/details/51-2022.00.
[144] "Details Report for: 51-2022.00 - Electrical and Electronic Equipment Assemblers," O*NET OnLine (Department of Labor, 2021), https://www.onetonline.org/link/details/51-2022.00.
[145] Flex Ltd., Briefing to the Department of Commerce, (Virtual Meeting, January 11, 2022).

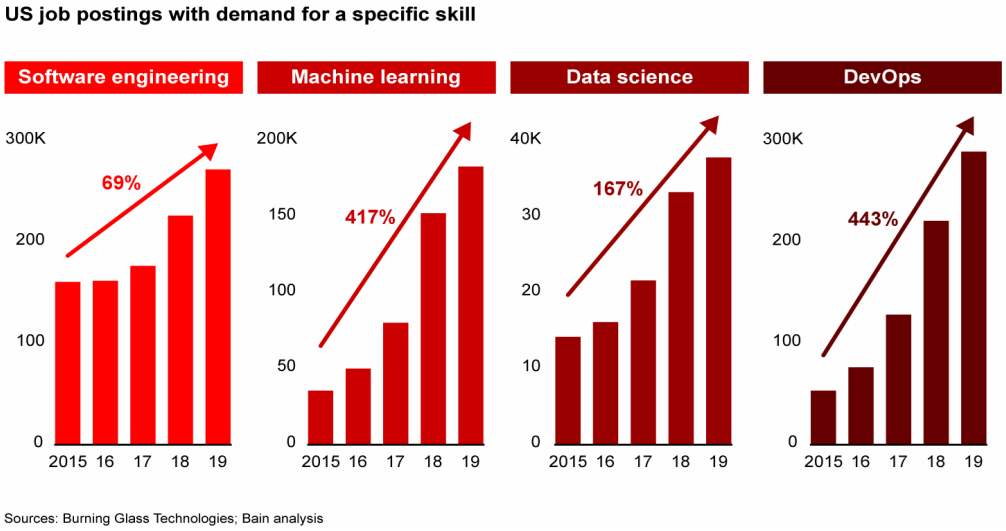
companies operating modern manufacturing facilities require different skills, such as project management, logistics, and procurement. In Germany, for instance, companies are incentivized to send their workers for further education a few days a week while working at the factory to increase their workers' skill sets.

6.2 ICT Software Workforce

In comparison to ICT production, which as stated above, employs just under 300,000 workers, software programming, design and engineering occupations employ two million Americans, accounting for more than 40 percent of domestic ICT employment.[146] The median salary for U.S. software developers in 2020 was $110,140,[147] well above the median *household* income of $67,521 in the same year.[148]

As ICT has become essential for businesses throughout the economy, the competition for technology talent has become more intense and widespread. The tight market for talent includes the well-known need for data scientists, software engineers, and other technical roles (Figure 11).

Figure 11: U.S. Job Postings with Demand for a Specific Skill[149]



The COVID-19 pandemic has created an unparalleled adoption of technology for businesses and organization across all industry sectors given that employees worked remotely. In addition, hiring by U.S. technology companies in August 2021 achieved a near two-year high, while payroll growth and tech employment in other sectors of the economy dropped. Technology companies added an estimated 26,800 workers in September 2021 in both technical and non-

---

[146] "Occupational Employment and Wage Statistics," U.S. Bureau of Labor Statistics, October 18, 2021, https://www.bls.gov/oes/tables.htm.
[147] "Software Developer Salary | US News Best Jobs," *U.S. News & World Report*, 2021, https://money.usnews.com/careers/best-jobs/software-developer/salary.
[148] Emily A. Shrider et al., "Income and Poverty in the United States: 2020," United States Census Bureau, September 14, 2021, https://www.census.gov/library/publications/2021/demo/p60-273.html.
[149] Jonathan Frick, KC George, and Julie Coffman, "The Tech Talent War Is Global, Cross-Industry, and a Matter of Survival," Bain, September 20, 2021.

technical positions, according to the Employment Situation report released by BLS[150] It was the greatest monthly gain in tech industry jobs since November 2018. Industry hiring increased by more than 120,000 positions from January to August 2021. In the meantime, the unemployment rate for technology jobs is 1.5 percent compared to the national rate of 4.2 percent.[151]

Within the technology sector, all five employment categories were robust in August 2021, supported by new hiring in data processing, hosting and related services (+11,900) and IT services and custom software development (+9,800). Other information services, including search engines (+3,500) and computer and electronic products manufacturing (+1,400) also showed solid job growth, while telecommunications had a modest gain (+200).[152] In addition, employer job postings for vacant technology jobs continued to increase in August 2021, surpassing 321,000. Three in 10 job postings were for positions in emerging technologies or jobs that require emerging technology skills.[153]

In the coming years, demand for software developers is expected to increase significantly in the United States and around the world. According to market research company, Evans Data Corporation Data's Global Developer Population and Demographic Study, there are 24.5 million software developers worldwide.[154] Forecasters predict that the number of software developers will increase to 27.7 million in 2023, 28.7 million in 2024, and 45 million by 2030.[155] The United States has the largest number of software developers, accounting for 4.3 million software positions across all industries, with the ICT industry representing nearly 50 percent of those positions.[156] Demand for software developer positions including web developers, full-stack developers, and cloud engineers grew nearly 25 percent from April-October 2019 to April-October 2020, according to an analysis by LinkedIn.[157] Furthermore, demand for machine learning engineers and artificial intelligence specialists was robust in 2020 as well, increasing 32 percent over the same period.[158] In addition, developers with proficiency with both front-end and back-end technologies are in high demand. According to HackerRank's 2020 Developer Skills Report, hiring managers at companies of various sizes "agree that full-stack developers are top priority."[159] To that end, 38 percent of these hiring managers indicated that full-stack developers were their number one priority for roles to fill in 2020.[160]

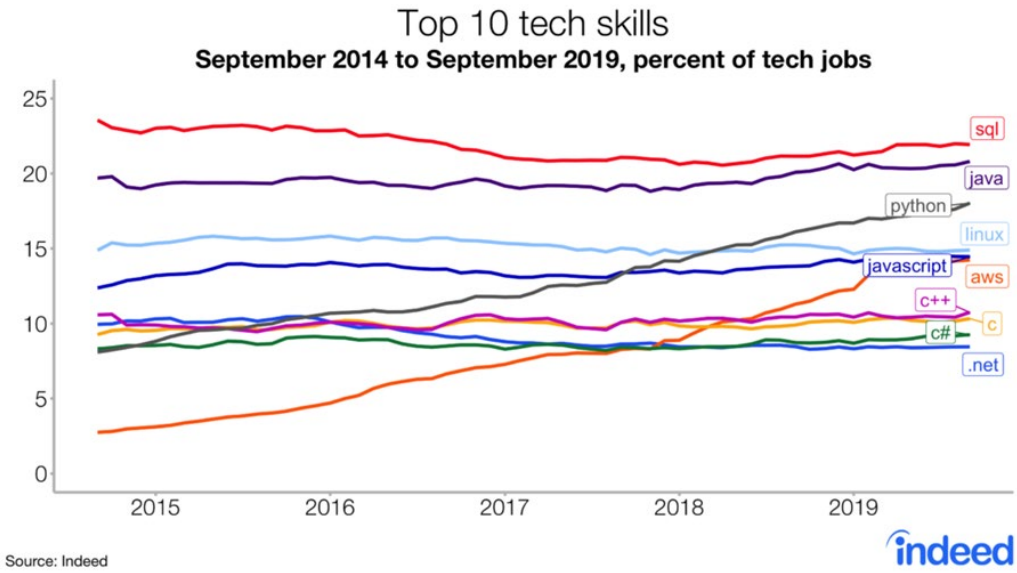
According to analysis conducted by the job employment website Indeed, SQL and Java are the top two skills that employers desired, according to millions of jobs posted on the Indeed website

---

[150] "Employment Situation News Release," U.S. Bureau of Labor Statistics, October 8, 2021, https://www.bls.gov/news.release/archives/empsit_10082021.htm.
[151] "Steven Ostrowski, "Tech Companies Accelerate Hiring as Other Industries Slow Employment Growth, CompTIA Analysis Finds," CompTIA, September 23, 2021, https://www.comptia.org/newsroom/2021/09/03/tech-companies-accelerate-hiring-as-other-industries-slow-employment-growth-comptia-analysis-finds.
[152] Ibid.
[153] Ibid.
[154] Scott Carey, "Software Developer Jobs Outlook for 2021," InfoWorld, January 20, 2021, https://www.infoworld.com/article/3604054/software-developer-jobs-outlook-for-2021.html.
[155] "How Many Developers Are in US and in the World [Updated]," Daxx, September 23, 2021, https://www.daxx.com/blog/development-trends/number-software-developers-world#:~:text=According%20to%20Evans%20Data%20Corporation,and%2028.7%20million%20in%202024.
[156] Ibid.
[157] Scott Carey, "Software Developer Jobs Outlook for 2021".
[158] Ibid.
[159] Ibid.
[160] Ibid.

platform between 2014 and 2019. Python was the third most common skill, followed by Linux, JavaScript and Amazon Web Services,[161] per Figure 12 below.

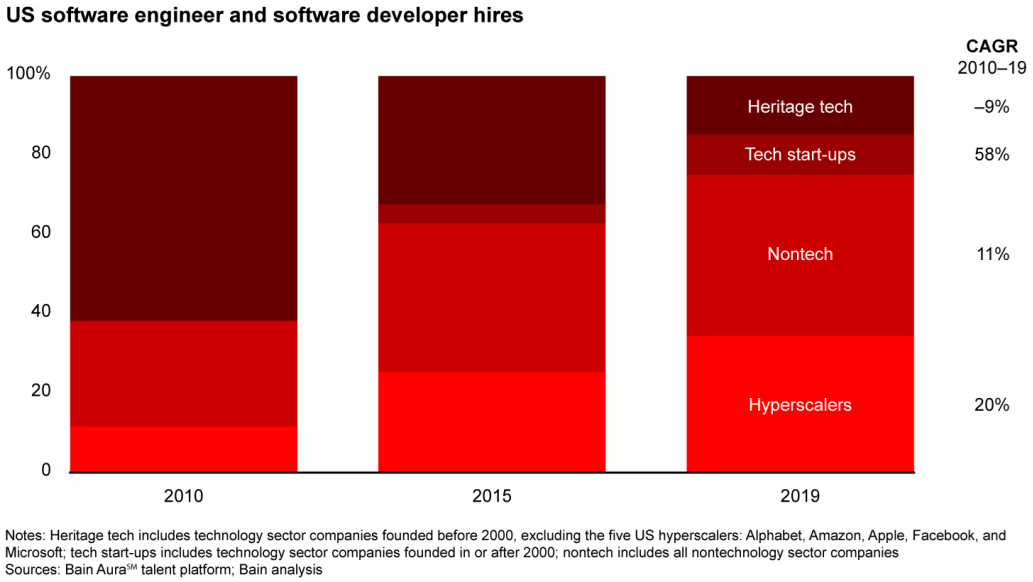
Figure 12: Top 10 Tech Skills, September 2014 to September 2019, Percent of Tech Jobs[162]



While the scope of in-demand technology roles is widening, companies are having to compete for employees with relevant skills. In addition, the competition for technology employees is not just among technology companies themselves. Other industries that are not typically associated with the ICT industry are now entering the fray. In 2019, before the COVID-19 pandemic disrupted hiring for most companies, more than 40 percent of software engineer and developer hires were made by non-technology companies, up from about a third in 2010, as detailed in Figure 13.[163]

[161] Andrew Flowers, "Indeed Tech Skills Explorer: Today's Top Tech Skills," Indeed, November 19, 2019, https://www.hiringlab.org/2019/11/19/todays-top-tech-skills/.
[162] Ibid.
[163] Ibid.

Figure 13: U.S. Software Engineer and Software Developer



6.3 Human Capital-Related Risks

The following section outlines key risks facing the U.S. ICT workforce.

Need for Qualified Workers

One of the primary risks facing the ICT workforce is the need to ensure that a robust pipeline exists to develop qualified workers for occupations in hardware manufacturing, installation and maintenance services, and software development. For example, with extensive new broadband deployments well underway and continued network scaling, technicians who can properly and efficiently install fiber, power, and radio equipment for telecommunications sites are in high demand across the country. A March 2021 report[164] from the Brookings Institution on federal infrastructure investment estimates that an $80 billion federal program for broadband would directly create nearly 200,000 job-years across 130 occupations, primarily for the installation, maintenance, and repair of this new infrastructure.[165] For example, the Communications Infrastructure Contractors Association (NATE), a South Dakota-based trade association that represents nearly 1,100 member companies estimates that, without critical investments in communications infrastructure training programs, its member companies will not have enough workers to carry out the mandates in federal and state broadband programs.[166] NATE estimates that there are only about 100 job-ready tower technicians graduating from public technical institutes and community colleges every year while approximately more than 14,000 technicians

[164] Marcela Escobari, Dhruv Gandhi, and Sebastian Strauss, "How federal infrastructure investment can put America to work," The Brookings Institution, March 2021, https://www.brookings.edu/wp-content/uploads/2021/03/Federal-infrastructure-investment.pdf.
[165] Alvaro Sanchez and Adam Scavette, "Broadband Subscription, Computer Access, and Labor Market Attachment Across U.S. Metros" (Federal Reserve Bank of Philadelphia, June 2021), https://www.philadelphiafed.org/-/media/frbp/assets/community-development/reports/broadband-subscription-computer-access-and-labor-market-attachment-across-us-metros.pdf.
[166] "2020 Workforce Survey Results," NATE - The Communications Infrastructure Contractors Association, November 2020, https://natehome.com/wp-content/uploads/2020/11/NATE-2020-Employer-Workforce-Survey-Final-Results-Document-1.pdf.

are needed to complete the current workload that exists today. With the additional tens of billions of dollars in new federal investments for broadband expansion in the recently passed Bipartisan Infrastructure Law, the prolonged demand for trained technicians is likely to increase even more.

The software workforce faces similar challenges. According to a September 2021 Gartner survey, IT executives believe the technology talent shortage is the "most significant adoption barrier to 64 percent of emerging technologies,"[167] compared with just 4 percent in 2020. A lack of talent availability was cited far more often than other barriers in 2021, such as implementation cost (29 percent) or security risk (7 percent). The survey cites talent availability as a leading factor inhibiting "adoption among all six technology domains included in the survey – compute infrastructure and platform services, network, security, digital workplace, IT automation and storage and database. IT executives cited talent availability as the main adoption risk factor for the majority of IT automation technologies (75 percent) and nearly half of digital workplace technologies (41 percent)."[168]

According to *Forbes*, "in the last few years, there has been a sharp increase in demand for software engineers who provide solutions to different software problems as more and more organizations undergo digital transformation. The IT industry is rapidly changing, which has led to a shortage of software engineers to help manage workloads, new technologies and new ways of working."[169] Indeed, the *Wall Street Journal,* citing CompTIA, an IT trade group, notes that there were approximately 920,000 unfilled IT positions in the U.S. from August to October 2019. [170] The technology job vacancies are partly the result of companies investing more in technology to increase their business initiatives. As Mehul Patel, CEO of tech recruiting site Hired, said to *CNBC Make It,* "every company is a tech company now."

Detailed analysis of applicant data reveals additional insights. The "iCIMS Benchmark Report on Hiring Tech Talent" analyzed 25 million technology applicants representing a large portion of the U.S. economy from January 1, 2016, to May 31, 2019, and found that companies are confronted with a deep technology talent deficit:

- **Employers hired only six for every 10 open tech positions in the United States:** In stark contrast, U.S. companies made 12 hires per 10 job openings for <u>all</u> positions (employers often post one opening to hire multiple candidates for the same role) over the same time period.
- **There is no shortage of technology applicants:** Despite the large number of unfilled positions, there were, on average, 43 tech applicants per hire in 2018 (up from 36 in 2016) compared to 21 applicants for all hires. The central problem is that employers find it increasingly difficult to find ***<u>qualified</u>*** tech candidates.

---

[167] "Gartner Survey Reveals Talent Shortages as Biggest Barrier to Emerging Technologies Adoption: 2021-2023 Emerging Technology Roadmap for Large Enterprises;" Gartner, September 13, 2021.
[168] Ibid.
[169] Thanh Pham, "Analyzing the Software Engineer Shortage," Forbes (Forbes Magazine, April 13, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/04/13/analyzing-the-software-engineer-shortage/?sh=7b0752e9321c.
[170] Jennifer Liu, "The US Has Nearly 1 Million Open IT Jobs - Here's How Much It Can Pay Off to Switch Industries into Tech," CNBC, November 6, 2019, https://www.cnbc.com/2019/11/06/how-switching-careers-to-tech-could-solve-the-us-talent-shortage.html.

- **It took 50 percent longer to hire tech positions than all other roles:** In the first five months of 2019, U.S. employers spent an average of 66 days to hire a new tech employee, which is 23 days longer for all other types of hires (43 days-to-hire on average). Days-to-hire jumped to 81 days from 66 in 2016 for software application developers, which is the most sought-after tech position. In comparison, employers are able to fill all of their openings for user support technicians, more commonly known as help desk, in an average of just 40 days.

Absent significant increases in qualified workers, the human capital gaps are likely to persist in the face of increasing demand. According to CompTIA, "[a]ccounting for the 60,300 people who graduate with a computer science degree every year, 20,000 developers who complete coding bootcamps, and even maxing out the 85,000 available H-1B visas to fill tech roles with international workers, that still leaves a major gap in talent."[171] In order to fill this gap, companies may need to commence or enhance their on-the-job training programs in order to upgrade employee skill sets.

Challenges for Workforce Development and Education Programs

The increase in workforce demand can in part be attributed to antecedent risks that include the inadequate development of ICT-tracked educational programs, the lack of inclusive access and awareness of training and opportunities within the ICT sector, and limited capacity and development of broadband infrastructure, particularly in rural and underrepresented communities.

Increasing ICT-related education and training programs is a prerequisite to developing a stronger ICT workforce within the U.S. hardware manufacturing and software development ecosystem. Such trainings can include various forms of work-based learning programs that link paid work experience to the attainment of relevant credentials and degrees, through proven workforce models in the ICT sector such as Registered Apprenticeship programs. To scale these efforts and to bring underrepresented communities into the workforce, programs could include workplace mentors that can provide the support and training to new entrants as well as community engagement partnerships with schools, college, community-based organization to build more inclusive pipelines. As stated in a July 2020 report by the Austrian Federal Ministry for Digital and Economic Affairs, "by voluntarily providing apprenticeship training, companies show that they accept social responsibility and make an important contribution to reducing youth unemployment while at the same time securing their future need for qualified skilled labor."[172]

At the high school level, only 51 percent of schools offer a foundational computer science course and only 4.7 percent of students are enrolled in such a course at any given time. Rural schools, urban schools, and schools with high percentages of economically disadvantaged students continue to be less likely to offer computer science classes.[173] For students who do not advance beyond high school, options become much more limited to enter the ICT workforce. Ninety percent of the ICT occupation groups identified by BLS require a bachelor's degree or higher to

[171] Ibid.
[172] "Apprenticeship System: The Dual System of Vocational Education and Training in Austria" (Republic of Austria - Federal Ministry for Digital and Economic Affairs, July 2020), https://www.bmdw.gv.at/dam/jcr:8dbc03d8-45b2-4fc8-b087-95725065f27e/Die%20Lehre_Englisch_Barrierefrei%20(002).pdf.
[173] "2021 State of Computer Science Education: Accelerating Action Through Advocacy" (Code Advocacy Coalition, November 2021), https://advocacy.code.org/2021_state_of_cs.pdf.

enter,[174] whereas less than half of American high school students enroll in a four-year college program after high school graduation.[175]

Barriers to Diversity in the Workforce

Registered Apprenticeship programs can be structured in a way to address gender and racial diversity issues in the ICT workforce. According to a 2020 report published by the National Center for Women & Information Technology (NCWIT), women comprise 57 percent of the overall professional workforce, but the percentage of women employed in computing and mathematical occupations has remained approximately 25 percent since 2007.[176] While the number of women earning degrees in Computer Information Systems is increasing, they are disproportionately white.[177] In addition, research indicates that approximately 56 percent of women leave the technology workforce, with evidence suggesting that high levels of attrition are fueled by workplace conditions, a lack of access to key roles, and dissatisfaction with career prospects.[178] The last factor is especially prevalent among women of color.[179] Apprenticeship programs can help address these issues by reducing barriers to diversity in the ICT workforce by providing tailored mentoring and sponsorship opportunities for diverse groups and by specifically targeting underrepresented population in recruiting and selection processes.[180]

In summary, a significant portion – 40 percent – of the U.S. ICT workforce consists of software employees, while manufacturing employees represent only five percent of the domestic ICT workforce. ICT companies and trade groups believe that critical investments are needed in training, apprenticeship, public education programs, and in STEM education, in order to meet future demand and remain technologically and economically competitive. If left unaddressed, this could have significant impact of ICT companies' ability to fulfill increased demand for key ICT products, impacting implementation of federal and state broadband programs as well as measures to increase manufacturing in the United States and advance technological capabilities of companies. Furthermore, the development of skills adjacency in ICT-specific education and apprenticeship programs is a collective effort that is necessary to meet current workforce needs and to introduce equitable ICT development programs that will provide opportunity for all Americans. These efforts should include a focus on addressing gender and racial diversity shortcomings by developing programs that reduce barriers to entry for underrepresented groups.

---

[174] "Computer and Information Technology Occupations: Occupational Outlook Handbook," U.S. Bureau of Labor Statistics, September 8, 2021, https://www.bls.gov/ooh/computer-and-information-technology/home.htm.
[175] "The NCES Fast Facts Tool: Immediate Transition to College," National Center for Education Statistics (NCES) (U.S. Department of Education), accessed January 25, 2022, https://nces.ed.gov/fastfacts/display.asp?id=51.
[176] "Highlights from the NCWIT Scorecard: Indicator Data Showing the Participation of Girls and Women in Computing," (National Center for Women in Technology, 2020), https://wpassets.ncwit.org/wp-content/uploads/2021/05/20221741/ncwit_scorecard_data_highlights_10082020.pdf.
[177] Ibid.
[178] Catherine Ashcraft, Brad McLain, and Elizabeth Eger, "Women in Tech: The Facts", National Center for Women in Information Technology, 2016, https://wpassets.ncwit.org/wp-content/uploads/2021/05/13193304/ncwit_women-in-it_2016-full-report_final-web06012016.pdf.
[179] Ibid.
[180] "Women in IT: The Facts Infographic [2016 Update]," National Center for Women, June 4, 2021, https://ncwit.org/women-in-it-the-facts-infographic-2016-update/.

7. Cross-Cutting Supply Chain Vulnerabilities Impacting the U.S. ICT Industrial Base

The ICT industry encompasses a diverse array of hardware and software technologies, with each product market facing discrete supply chain challenges as discussed in sections 4 and 5. However, there are also several key cross-cutting vulnerabilities impacting the U.S. ICT industrial base that threaten supply chain resilience and security. These include vulnerabilities related to the supply chain shifts and constraints due to the COVID-19 pandemic, the lack of a robust U.S. ecosystem for electronics production and emerging technologies, a reliance on single source and single region suppliers, a lack of junior tier supplier transparency, inventory management issues, a dependence on China for revenue generation, the difficulties maintaining hardware and software integrity along the entire supply chain, 5G security issues, and extended supply chains.

7.1 Ongoing COVID-19-Related Supply and Demand Shifts and Bottlenecks

The rapid shift to a work-from-home economy driven by the pandemic dramatically increased demand for electronic devices, including computers, laptops, and other electronics, as well as demand for the digital infrastructure and storage to support increased on-line activity. In addition, pandemic-related work restrictions led to cuts in production in various countries, including in Southeast Asia.[181] These factors have led to supply and demand mismatches impacting various products that are part of the ICT industrial base or supporting supply chains. These include semiconductors and related components.

As discussed in the Department of Commerce's 100-day review of the semiconductor supply chain, in late 2020, a global chip shortage began to emerge when automakers warned that relatively inexpensive semiconductors used in automobiles were becoming scarce and that this would potentially disrupt vehicle production. At the same time, as noted above, demand for electronic devices increased significantly. Based on buyer demand and orders, semiconductor suppliers shifted production and foundry orders away from chips used in various other industries (including, for example, automotive, medical devices, household appliances) automotive-grade chips where demand was falling to business and consumer electronics chips where demand was spiking.

The semiconductor challenges have impacted PCB manufacturing. Some advanced semiconductor packaging uses specialized versions of printed circuit boards as the base.[182] In 2020, producers of specialty boards saw increased sales while producers of PCBs for other applications, such as autos, experienced business declines due to a fall in demand as auto production slowed in the second quarter of 2020.[183] In 2020, sales of automotive boards contracted by 11.6 percent over 2019.[184] However, similar to the case with semiconductors,

---

[181] "Chip Shortage Set to Worsen as COVID Rampages through Malaysia," *Bloomberg News,* August 23, 2021, https://www.bloomberg.com/news/articles/2021-08-23/chip-shortage-set-to-worsen-as-covid-rampages-through-malaysia

[182] Executive Office of the President, *Building Resilience Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017.*

[183] Ibid.

[184] "PCB Market Grew 4.4% in 2020 led by chip package," *TheElec: Korea Industry Media*, March 16, 2021.

rapid supply and demand changes created a mismatch between demand for automotive use PCBs and available supply for such products.

The semiconductor challenges have also had ripple effects on other ICT products that rely on semiconductors and related components. According to a December 2021 USTelecom survey of 227 respondents in the communications sector, respondents reported supply chain challenges and increased lead times increases in various products including components, routers, switches, and servers.[185]

Supply chain bottlenecks have also impacted fiber optic cables. According to the same survey, 74 percent of respondents reported fiber optic supply challenges and 62 percent reported delivery lead times of more than six months.[186] Corning has indicated that lead times have lately extended far beyond the one-month standard for this industry.[187] Wireline service providers are also experiencing supply chain bottlenecks and labor shortages, with an industry survey finding that nearly half of company respondents faced fiber optics lead times of between nine months and two years.[188] Production cannot move forward if there is a delay or shortage of any one component. These delays have ripple effects throughout the U.S. economy as companies face barriers to growing their businesses and consumers experience longer wait times for upgraded connectivity.

7.2 Lack of Ecosystem for Electronics Production

As discussed in Section 3, ICT OEMs shed manufacturing capabilities in the 1990s and outsourced production. Around the same time, countries in Asia, in particular China, built an ecosystem for electronics system manufacturing through targeted investments in advanced manufacturing capabilities and associated infrastructure.[189] Government-sponsored funding and prioritization of the ICT sector has been underway for decades in China, and recent policy directives sought to further secure the country's role in advanced manufacturing. Additionally, the government of China has systematically implemented non-market policies and practices, including protectionist trade practices to further induce the localization of technology development and production in China for key sectors. Indeed, "the Chinese government has earmarked the ICT sector as crucial for its next economic development stage, and subsequently enacted policies to support the development of…advanced manufacturing."[190] Furthermore, the $300 billion Made in China 2025 strategy, aimed at transforming China into an advanced manufacturing leader through the localization of R&D, replacement of foreign suppliers for domestic alternatives, and the capture of domestic and foreign market shares, represents a clear

[185] Comments of United States Telecom to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (United States Telecom, November 4, 2021).
[186] Comments of United States Telecom to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (United States Telecom, November 4, 2021).
[187] Linda Hardesty, "Corning GM says fiber lead times are 'much longer' than a month," Fierce Telecom, December 3, 2021, https://www.fiercetelecom.com/broadband/corning-gm-says-fiber-lead-times-are-much-longer-month.
[188] Comments of United States Telecom to Request for Information.
[189] Yoko Kubota, "China's New $21 Billion High-Tech Manufacturing Fund Likely to Rankle U.S.," *The Wall Street Journal*, November 20, 2019, https://www.wsj.com/articles/chinas-new-21-billion-high-tech-manufacturing-fund-likely-to-rankle-u-s-11574250074; https://www.bloomberg.com/news/articles/2021-12-13/intel-to-invest-7-billion-on-manufacturing-plant-in-malaysia.
[190] "Market Monitor ICT China 2019," Atradius, June 18, 2019, https://atradius.us/reports/market-monitor-ict-china-2019.html.

effort to establish a one-way dependency in which the United States and other countries occupy a downstream, position in the ICT supply chain.

These policies have conferred advantages with respect to capital, labor, and supplier and demand base, facilitating efficiencies needed to compete globally.[191] For example, according to Flextronics, 90 percent of macro radio components are manufactured in Asia.[192] Macro radios are a critical piece of equipment used in telecommunications networks, including 5G networks.[193] Given this situation, establishing a material source outside of Asia would require significant capital investments for the vast majority of such components.[194] The 2017 case of Foxconn, the world's largest electronics contract manufacturer, provides an illustrative example of the difficulties inherent in reestablishing a robust manufacturing ecosystem in the United States. In 2017, Foxconn announced plans to build a $10 billion production facility in Mount Pleasant, Wisconsin. The facility was expected to be the Taiwanese company's main U.S. operation for producing and distributing LCD display screens used to manufacture large flat-screen televisions. Despite significant tax breaks, subsidies, and environmental exemptions from the State of Wisconsin, the project did not materialize as originally envisioned due to a lack of critical materials suppliers (e.g., glass-makers) in the geographic vicinity, a global glut in LCD production, and local labor costs making production unprofitable.[195] Investment in the plant was subsequently scaled down from $10 billion to $672 million.[196] The Foxconn endeavor highlights the difficulties that companies face when attempting to establish manufacturing in the United States including the need to be targeted and realistic in location selection, workforce availability, and government incentives.

Many American firms, including those in the technology and communications space, derive robust, recurring, and new growth revenue from sales in China that account for a substantial amount of their overall corporate revenue. The size of China's market and the surrounding region will continue to attract global businesses as companies seek to manufacture close to consumers. For example, in April 2020, at the very moment that the Japanese government announced plans to pay Japanese companies to leave China, 22 percent of Japanese companies surveyed by the Japan External Trade Organization indicated that they planned to expand their business in China, up 7 percent from the previous month.[197]

In addition to the lack of geographic proximity to key components, the high cost of capital in the United States poses another barrier for investing in high volume production. As noted earlier, PCB production and assembly in the United States is limited to low volume production for specialized end-uses. The leap to high-volume assembly in the United States would require

---

[191] Comments of Flex Ltd. to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (Flex Ltd., November 4, 2021); Comments of HP Inc., to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (HP Inc., November 4, 2021).
[192] Comments of Flex Ltd. to Request for Information.
[193] "Macro Cells," Altiostar, Accessed February 10, 2022, https://www.altiostar.com/products/radio/macro/.
[194] Ibid.
[195] Josh Dzieza, "The 8th Wonder of the World," *The Verge,* October 19, 2020, https://www.theverge.com/21507966/foxconn-empty-factories-wisconsin-jobs-loophole-trump.
[196] David Shepardson and Kevin Pierog, "Foxconn mostly abandons $10 billion Wisconsin project touted by Trump," *Reuters*, April 20, 2021, https://www.reuters.com/business/foxconn-sharply-scales-back-wisconsin-investment-2021-04-20/.
[197] Jamie Gorelick and Stephen Preston "U.S. Decoupling from China and the Onshoring of Critical Supply Chains: Implications for Private Sector Businesses," WilmerHale, August 26, 2020.

significant capital investment, particularly because EMS companies tend to operate on tight margins.[198]

7.3 Single Source and Single Region Suppliers

ICT supply chains are long and complex. This includes the production of mobile phones and communication equipment, which according to a study by the McKinsey Global Institute has become more concentrated in recent years.

A single end user product, such as a computer, comprises numerous components, each of which may be designed, manufactured, and assembled in a different country. The manufacturing of many of these components is geographically and sometimes organizationally concentrated. For example, Thailand is the source for 68 percent of imports into the Computer Storage Device Manufacturing industry.

In many cases, ICT companies struggle with their reliance on a single source for products that they purchase directly. While supply chain managers recognize the risk of an over-reliance on a single source, they often adopt this strategy to secure the necessary supply or due to the unique qualities of that product, or to control costs. This lack of flexibility can have devastating effects when a company's sole supplier is unable to provide components. There are often limited options from which a firm can choose, and many times, those options are sourced from a single region, continent, or company. As demonstrated in Figure 14, a large number of commodities for U.S. and European high tech, semiconductor and consumer electronics companies are sourced from areas in China that were quarantined during the pandemic. When extraction and production are so concentrated, alternative workarounds are difficult to find.

[198] Comments of Flex Ltd. to Request for Information.

Figure 14: Number of Commodities Source from Quarantined Areas of China for U.S. and European Companies in High-Tech, Semiconductor, and Consumer Electronics Industries[199]

Commodity	Total Number
Resistors	590
Capacitors	199
Thermal	60
Printed circuit board assemblies	53
Plastics and resins	50
Integrated circuits	44
Sheet metal	32
Audio devices	30
Memory	25
Hardware	20
Battery components	22
Cables	16
Electrical components	10
Crystals and oscillators	7
Switches	4
Paints	3

The lack of supplier diversity also has impacts on fifth generation (5G) wireless networks. Fourth generation (4G) and 5G infrastructure consists of software and ICT hardware (including a radio base station, user equipment, and wired communications infrastructure such as fiber optic cables, servers, and routers), which, as noted above, relies on single source and single region suppliers. Currently, the market for 4G and 5G infrastructure suppliers is heavily concentrated in five non-U.S. firms: China-based Huawei and ZTE, Sweden-based Ericsson, Finland-based Nokia, and South Korea-based Samsung. The network core provides numerous services to network users such as authentication, call switching, and routing. Increasingly, network core functions are being "virtualized" - moving from specialized hardware to software on "commercial off-the-shelf" (COTS) servers, including in the cloud. For radio access network (RAN) products, suppliers have traditionally used proprietary interfaces that effectively lock the mobile network operator into the use of a supplier's integrated solution for the entire RAN, making interoperability between RAN components from different suppliers difficult if not impossible.

A global range of operators are supporting an initiative to develop open, interoperable interfaces that could allow operators to disaggregate their networks across multiple software and hardware suppliers known as Open Radio Access Networks or Open RAN. The greater interoperability inherent in Open RAN would allow operators to use hardware and software within their radio access networks from a wider range of suppliers. However, to create a fully disaggregated network ecosystem, industry players are working to agree to "open" interfaces at specific junctures in the network, allowing this plug-and-play approach with different software and

[199] Tom Linton, Bindiya Vakil, "Coronavirus Is Proving We Need More Resilient Supply Chains," *Harvard Business Review*, March 5, 2020, https://hbr.org/2020/03/coronavirus-is-proving-that-we-need-more-resilient-supply-chains.

hardware suppliers. This effort could increase competition in the marketplace and reduce single supplier dependencies in the telecommunications supply chain.

While O-RAN can help increase the number of firms in the market, due to the concentration of production in Asia (particularly China), absent incentives, it is challenging to diversify locations of production. Making changes to the structure of the ICT supply chain is challenging and costly. Indeed, in a survey of 175 global supply-chain managers across six primary industries [200] conducted in February and March 2021, the IT/Tech/Electronics industry had the smallest share, at 16.7 percent, of companies seeking a complete transformation of their supply chain strategy, compared with the study average of 32.6 percent. In fact, the IT and electronics sector has seen less change in supply-chain strategy than other sectors in the past 18 months. Forty percent of supply-chain managers in the sector said they have not made or are not planning to make any material changes to their supply-chain strategies (compared with the average of 22.9 percent and higher than in all other sectors). According to the study, "this is to be expected, given manufacturing in this sector is highly specialized, often requiring specialized production facilities, and the colocation of suppliers, for example. In other words, specialized technology manufacturing supply chains cannot shift easily because of their sophistication relative to other industries, which necessitates a completely new production ecosystem be established in a new location."[201]

Despite the challenges in diversifying production locations, there is some evidence that companies are taking measures to diversify supply chains out of China. For example, Meiloon Industrial Co, which makes speakers and counts Harman International Industries among its clients, said it is seeking alternatives to China-based production and was speeding up its move of capacity to places like Taiwan and Indonesia. As discussed in Section 4, major ODMs have taken steps to expand capacity in other countries, including the United States, Mexico, the Czech Republic, and Germany. In addition, O-RAN solutions, which incentivize diversification of suppliers, can have the secondary effect of diversifying production locations.

Some U.S. companies are pursuing a "China-plus-one" model in an effort to reduce their dependency on Chinese suppliers. For example, Apple reportedly has investigated the possibility of moving one-third of its production for some devices out of China. Dell and HP were both making plans in 2018 to relocate up to 30 percent of their notebook production outside of China, according to news reports.[202]

7.4 Lack of Visibility of Junior Tier Suppliers

Following two events in 2011 - the earthquake and tsunami that devastated the Tohoku region of Japan, and extensive flooding in Thailand, many multinationals learned difficult lessons about the unseen weaknesses in their supply chains — weaknesses that resulted in loss of revenue, and in some cases, market capitalization. While most companies could quickly assess the impacts

[200] "Disruption, Digitisation, Resilience: The future of Asia-Pacific supply chains," The Economist Intelligence Unit; Citibank, March/February 2021.
[201] Ibid.
[202] Cheng Ting-Fang et al., "HP, Dell and Microsoft look to join electronics exodus from China," *Nikkei Asia,* July 3, 2019, https://asia.nikkei.com/Economy/Trade-war/HP-Dell-and-Microsoft-look-to-join-electronics-exodus-from-China.

that the disasters in Fukushima had on their direct suppliers, they were blindsided by the impacts on second- and third-tier suppliers in the affected region.

Less than a decade after the Tohoku disasters, however, many companies again experienced disruptions created by the COVID-19 pandemic. Global supply chain operators rushed to ascertain which of their upstream suppliers — those with whom they do not deal directly — were based in the affected regions that experienced shutdowns, disruptions to work and transportation, and access to supplies.

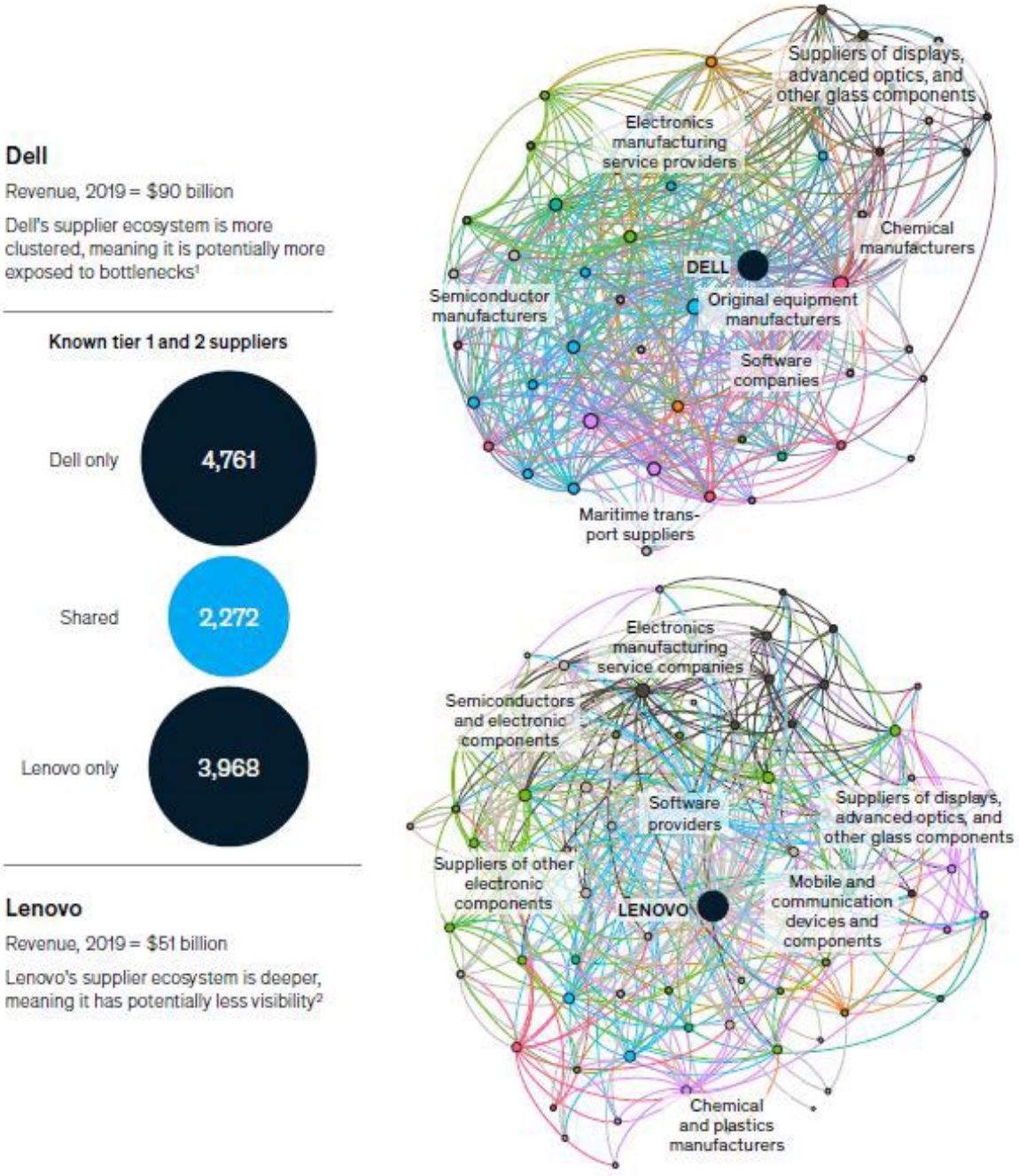
Complex and vast networks can make it difficult to identify vulnerabilities and interdependencies and present challenges to the development of effective strategies to provide redundancy and flexibility. A large multinational organization can have hundreds of tier one suppliers from which it purchases components directly. In turn, each of those tier one suppliers relies on hundreds of tier two suppliers. The whole supplier network for a large company can include tens of thousands of companies around the world when the deepest tiers are included in the network. For many companies, especially small -and medium-sized businesses, it is very difficult, if not impossible, and costly to obtain an accurate and complete picture of an organization's entire supplier network. Making this effort even more difficult is the fact that a company's suppliers can change on very frequent basis. Communications Equipment companies are one of the industries that have the largest number of tier one suppliers, with 2.2 times the industry median.[203]

According to the "Risk, Resilience, and Rebalancing in Global Value Chains" study by the McKinsey Global Institute, "companies often assess their supply chain vulnerabilities exclusively based on cost, focusing on the most expensive inputs or suppliers to which they direct the largest share of spending. But a cost-only lens may miss hidden vulnerabilities in the network. Network analysis can reveal some of the hidden dependencies lurking within supply chains." The study created a visual representation (see Exhibit 15 below) of the first- and second-tier supply chain ecosystems attached to two major ICT firms, Dell and Lenovo. Each company has a small "universe" inhabited by thousands of suppliers. The illustration demonstrates how "complex, multitiered, and multinational these networks are—and it dispels the notion that supply chains can move and reconfigure easily."

The analysis finds that "75 percent of Dell's 20 most connected suppliers are shared with Lenovo, and 70 percent of Lenovo's 20 most connected suppliers are shared with Dell. Foxconn, IBM, and Microsoft are hardware and software suppliers to both companies—and are highly connected in both networks. Should one become disrupted, it would not only affect Dell and Lenovo's existing operations but also limit their ability to secure alternative sourcing."

[203] Susan Lund, James Manyika, Jonathan Woetzel, et al., "Risk, Resilience, and Rebalancing in Global Value Chains."

Figure 15: Visual of Supply Chain Complexity[204]



[204] Ibid.

7.5 Inventory Management

The typical approach to supply chain management emphasizes the need to strike a balance between efficiency and resiliency. Increased competition and compressed profit margins have often driven supply chain managers to emphasize cost reduction, just-in-time deliverables (JIT), and days of supply inventory management.[205]

JIT allows manufacturing companies to cut costs by reducing the amounts of good and materials a firm needs to hold in stock. Production is for specific customer orders and the production cycle commences only after a customer has placed an order with the producer, thereby eliminating the need to hold a large inventory.[206] "By keeping inventories thin, major retailers have been able to use more of their space to display a wider array of goods. JIT has enabled manufacturers to customize their wares. And lean production has significantly cut costs while allowing companies to pivot quickly to new products."[207] To that end, waste should be driven from the system and purchases should only be placed when they are absolutely required. Furthermore, upstream suppliers should be kept on short notice to supply inventory only as it is necessary.

Each industry carries varying amounts of inventory. The ICT industry typically carries about three to 12 weeks of inventory, while the auto industry has about 2 to 10 weeks' worth. While lean supply chains may work in times of normalcy, the pandemic has demonstrated that JIT inventory works well only when there is flawless production and execution. When there are unexpected disruptions, such as lockdowns, transportation issues, quarantines, vastly increased demand, or staffing shortages, the system breaks down. The pandemic exposed that JIT lacks flexibility and agility when the supply chain comes under strain, especially if that supply chain is concentrated in a handful of geographic areas.

According to the McKinsey Global Institute, the trend is already underway for many sectors to hold more inventory, including the ICT sector. From 2017 to 2019, most value chains had lower inventory turnover than they did in the period from 2010 to 2012, per Exhibit 16 below.[208] This practice of buying products ahead as a means to increase inventory is favorable to larger firms with excess capital on-hand and places small and medium sized enterprises at a disadvantage.[209]

---

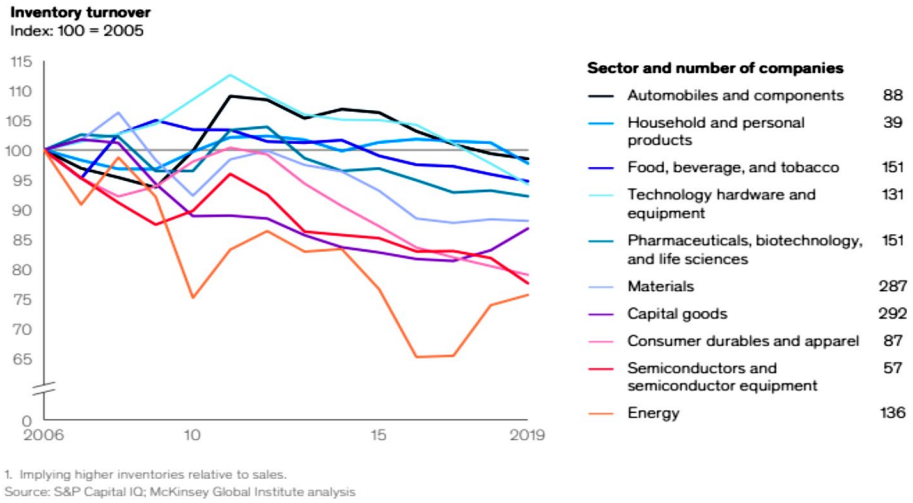
[205] Ushasri T.S. and Jitamitra Desai, "COVID-19 Era: How Supply Chains Are Adapting to Coronavirus Lockdowns," *Business Today,* June 26, 2020, https://www.businesstoday.in/opinion/columns/story/covid-19-how-supply-chain-industry-is-adapting-to-coronavirus-lockdowns-e-commerce-retail-sector-262322-2020-06-26.

[206] Emilia Ashton, "Our Current Supply Chain is Failing: Why Change Has Got to Come in 2020," *All Things Supply Chain*, June 29, 2020. https://www.allthingssupplychain.com/our-current-supply-chain-concept-is-failing-why-change-has-got-to-come-in-2020/.

[207] Peter Goodman and Niraj Chokski, "How the World Ran Out of Everything," *The New York Times*, October 13, 2021, https://www.nytimes.com/2021/06/01/business/coronavirus-global-shortages.html.

[208] Susan Lund, James Manyika, Jonathan Woetzel, et al., "Risk, Resilience, and Rebalancing in Global Value Chains."

Figure 16: Inventory Turnover[210]



1. Implying higher inventories relative to sales.
Source: S&P Capital IQ; McKinsey Global Institute analysis

7.6 Maintaining Hardware and Software Integrity along the ICT Supply Chain

Every company, organization, and individual that relies on ICT products is part a of a global supply chain. The evolving threat landscape, coupled with today's digitized world, provides a large attack surface for adversaries to launch sophisticated and stealthy supply chain compromises to steal, compromise, alter, or destroy sensitive information. Adversaries behind malicious code compromises can include national governments, terrorists, industrial spies, organized crime groups, or hackers. Their goals include, or combine, espionage, hacking, identity theft, crime, and terrorism.[211]

Threats can encompass insider threats, threats from extended supply chains, and threats from counterfeit parts. All of these jeopardize the ability to provide secure devices and data.

Insider Threats

DHS's Cybersecurity and Infrastructure Security Agency (CISA) defines an "insider threat" as the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to an organization's mission, resources, personnel, facilities, information, equipment, networks, or systems.[212] According to DHS, "insider threats include sabotage, theft, espionage, fraud, and competitive advantage, and are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware they are aiding a threat actor. It is vital that organizations understand normal employee baseline behaviors and ensure employees recognize how they may be used as a conduit for others to obtain information. An insider threat can be either unintentional or intentional and can impact the integrity of both the hardware and software ICT supply chains."

---

[210] Ibid.
[211] "Cyber Threat Source Descriptions," Cybersecurity & Infrastructure Security Agency, https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions.
[212] "Defining Insider Threats," Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/defining-insider-threats.

Hardware Supply Chain Integrity

The ICT hardware supply chain is complex and challenging to secure given the many different layers and supply tiers involved, which makes issues like the proliferation of counterfeit components and parts more difficult to detect. A counterfeit part is an unauthorized copy, imitation, substitute or modified component that has been knowingly misrepresented as a legitimate component from an authorized manufacturer. This issue has become a matter of increasing concern in relation to products within the ICT sector. Beyond the revenue loss experienced by the victims of counterfeits—estimated at $100 billion annually for the entire electronics sector—systems and end users can experience early or catastrophic failure as a result of counterfeit semiconductors.[213] In addition, the U.S. Semiconductor Industry Association testified in 2011 that it estimated that counterfeiting costs U.S.-based semiconductor companies more than $7.5 billion per year, translating into nearly 11,000 American jobs lost.[214]

To date, many of the security methods to check for counterfeit parts or sabotage are typically subjective and regularly depend on human intervention, such as visual inspections. This can include checking the alignment or placement of labels, looking for incorrect color, verifying the size or shape of markings, validating the authenticity of serial numbers, and the use of X-ray imaging. These steps are time consuming and expensive to conduct at volume and they often cannot catch all of the counterfeiting. In addition, it is difficult to verify that all of these steps are being taken throughout the entire supply chain, end-to-end. As a result, potentially malicious or counterfeit hardware is difficult to identify, a process that also requires robust resources and expertise to complete.

Hardware security technologies can help protect against these risks. These include the highly reliable hardware roots of trust technologies which can be used to verify, protect or restore system, data or code integrity, and attest identity for components in a hardware system. Government and private sector-led initiatives are underway to advance trust and security in the hardware supply chain using hardware roots of trust. These include the following:

- DOC's National Institute of Science and Technology's (NIST) has a Supply Chain Assurance initiative at the National Cybersecurity Center of Excellence to "produce example implementations to demonstrate how organizations can verify that the internal components of their purchased computing devices are genuine and have not been altered during the manufacturing and distribution processes." [215]
- Dell's 2020 "A Partnership of Trust: Dell Supply Chain Security", which provides insights into the company's levels of effort to increase their hardware supply chain integrity and resiliency. According to the company, the standards cover Sourcing Security, which includes requirements for counterfeit mitigation related to suppliers prior to acquisition, testing and verification processes post-acquisition, and placement of unique labels on parts for tracking and monitoring purposes.[216]

---

[213] Guin et al. "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", (IEEE, August 2014).
[214] "Detecting and Removing Counterfeit Semiconductors in the U.S. Supply Chain," Semiconductor Industry Association.
[215] "Supply Chain Assurance," National Cybersecurity Center of Excellence, National Institute for Standards and Technology, https://www.nccoe.nist.gov/supply-chain-assurance.
[216] "A Partnership of Trust: Dell Supply Chain Security," Dell Inc, 2021, https://i.dell.com/sites/csdocuments/CorpComm_Docs/en/supply-chain-assurance.pdf?newtab=true.

- Intel's Transparent Supply Chain framework, which, according to Intel "helps create visibility for product owners into hardware device composition and provenance, across the lifecycle of the device. The approach Intel developed has already led to a joint collaboration among Intel, Goldman Sachs, and Microsoft to make it easier for enterprise IT organizations to adopt such approaches."[217]
- A Microsoft-led industry initiative, Project Cerberus, is focused on developing and standardizing hardware building blocks that can serve as a foundation for building enhanced firmware and data protection, exploit/vulnerability detection, and reliable, centrally managed recovery across a range of devices.[218]

Software Supply Chain Integrity

Increasingly, the political, economic, and cultural functioning of society is dependent on software. Software itself is reliant on regular evolution and maintenance, including new version development and releases, patches, and updates, all of which present opportunities to compromise the software supply chain.[219] Software acquired through the supply chain may contain both known and unknown vulnerabilities associated with the quality, security, and integrity of the source code itself as well as the people, processes, and tools involved in the software development life cycle management. Thus, for software to be trusted, it is important that security is a prominent consideration throughout the entirety of the software life cycle and the trustworthiness of all the elements and processes within the supply chain must be considered. All computer software is susceptible to malicious code inserted into a software system, usually covertly, with intent of compromising the confidentiality, integrity, or availability of data, applications, or the operating system.[220] Software is particularly vulnerable within the ICT supply chain framework, involving retailers, distributors, and suppliers for the sale, delivery, and production of hardware, software, and managed services.[221]

From cradle to grave, software supply chain compromises are a threat in any phase of the ICT Supply Chain Lifecycle (Design, Development and Production, Distribution, Acquisition and Deployment, Maintenance, and Disposal). That span of vulnerability means a software's security is dependent upon employees, contractors, suppliers, resellers, cloud partners, and even customers, all of whom could include bad actors compromising software code.[222] Software developers often have complete access to the source code of critical systems to do their job. This very access can be exploited to insert logic bombs, flaws, or malware. When these malicious vectors are inserted early in the software development phases, they are more challenging to detect and discover. As a result, this could lead the developer to mark the component as

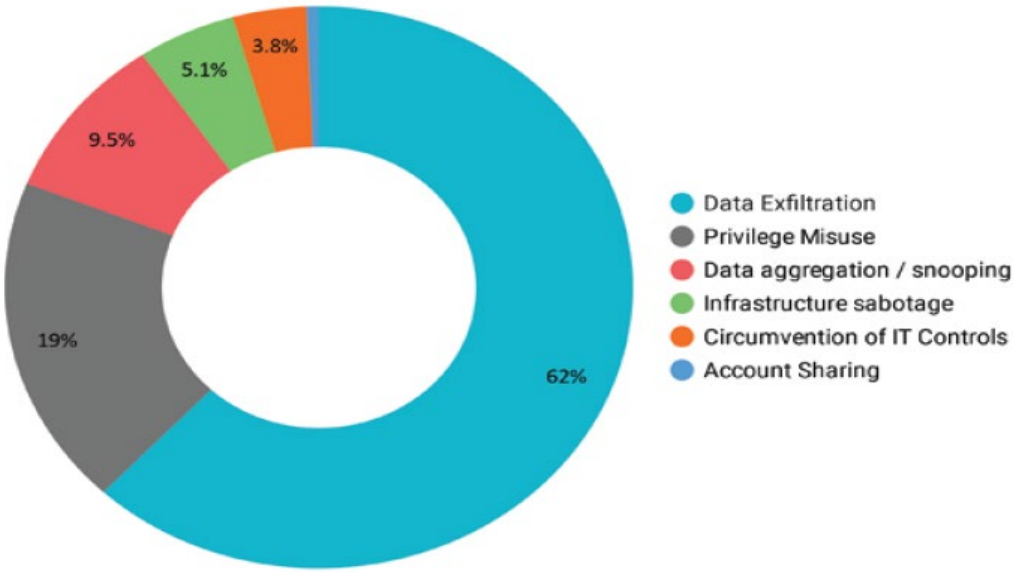
---

[217] Comments of Intel Corporation, to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (Intel Corporation, November 4, 2021).
[218] Comments of Microsoft Corporation to Request for Information, 86 Fed. Reg. 52127 (Sept. 20, 2021), (Microsoft Corporation, November 4, 2021).
[219] Dr. Trey Herr, William Loomis, Stewart Scott, June Lee, "Breaking Trust: Shades of Crisis Across An Insecure Software Supply Chain," Atlantic Council, July 26, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/.
[220] NIST Special Publication 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, December 2020. https://doi.org/10.6028/NIST.SP.1800-25.
[221] "Defending Against Software Supply Chain Attacks," Cybersecurity and Infrastructure Security Agency, April 2021, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[222] Ayman Al Issa et al., "Enterprise Cybersecurity: Aligning Third Parties and Supply Chains," May 12, 2021, McKinsey & Company, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/enterprise-cybersecurity-aligning-third-parties-and-supply-chains.

legitimate through digital signatures or other approvals. These vulnerabilities could then be exploited later by malicious actors. Malicious actors do this to gain access to systems, networks, and data, and leverage that access to collect personal or sensitive data or to sabotage the system.

Furthermore, companies often develop software that collects data through escalated user permissions or network privileges. While the company may develop legitimate software or applications, the data may be stored in an untrustworthy country, or in a network that is not secure. This permits malicious parties to access sensitive data, including personally identifiable information, financial information, as well as written communications. A study indicates that local area network (LAN) access is the top vector for insider threats/misuse (71percent), followed by physical (28 percent) and remote access (21 percent).[223] In addition, a study conducted in 2020 regarding insider threat incidents found that data exfiltration was the most common insider threat, accounting for 62 percent of recorded incidents, in an assessment of 300 total incidents (see Figure 17).[224]

Figure 17: Categories of Threat Detected



According to Carnegie Mellon's Software Engineering Institute, insider threats within the software development life cycle can occur in requirements and system design, implementation, deployment, and maintenance:[225]

[223] "Combating the Insider Threat," Department of Homeland Security, May 2, 2014, https://www.cisa.gov/uscert/security-publications/Combating-Insider-Threat.
[224] Shareth Ben, Amruta Bhat, "2020 Securonix Insider Threat Report," May 2020, https://pages.securonix.com/rs/179-DJP-142/images/Insider-Threat-Report-May-2020-Securonix.pdf.
[225] Randy Trzeciak and Dan Costa, "Insider Threats in the Software Development Lifecycle," CERT Insider Threat Center, Software Engineering Institute, Carnegie Mellon University, November 5, 2014, https://resources.sei.cmu.edu/asset_files/Presentation/2014_017_101_423710.pdf.

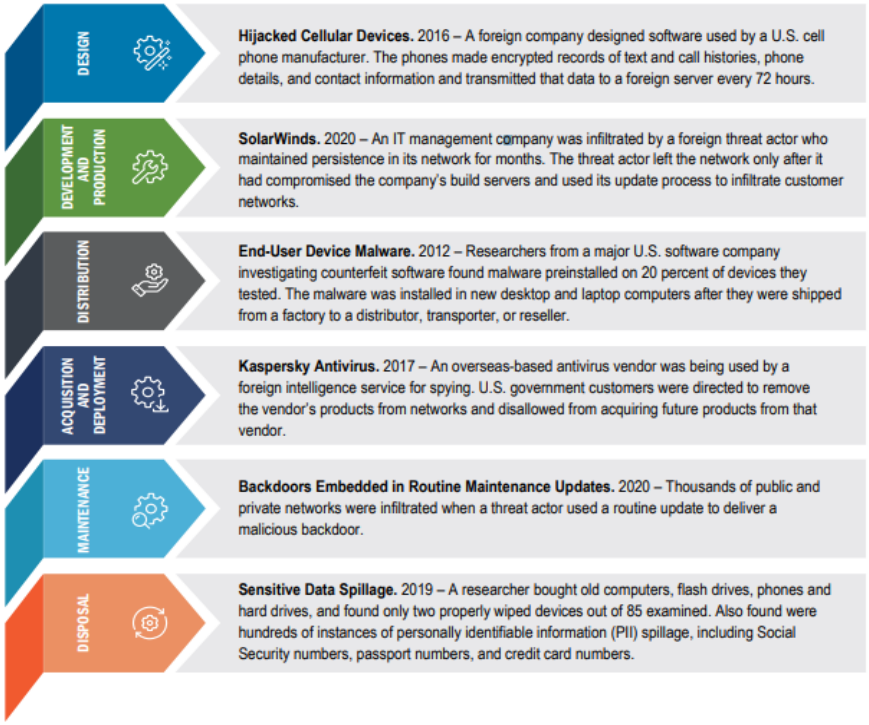


Figure 18: Software Supply Chain Attacks[226]

As discussed in Section 5, adversaries generally conduct software supply chain compromises by hijacking updates or compromising code signing or open-source code. Hijacking updates involves infiltrating a network to insert malware in an outgoing update, or using the update to provide control over the software's normal functionality.[227] With undermining code signing, threat actors impersonate a trusted software vendor, using software updates to insert malicious code and facilitate further intrusions against the user.[228] In open-source code compromises, threat actors insert malicious code into publicly available code libraries, which developers then add (often unwittingly) to their own third-party code.[229]

Initiatives are underway to address software security supply chain risks. For example, pursuant to Section 4 of E.O. 14028, *Improving the Nation's Cybersecurity*, NIST is responsible for identifying existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security.[230] This guidance includes, but is not limited to: identifying standards, procedures, or criteria for secure software development environments;

---

[226] "Defending Against Software Supply Chain Attacks," Cybersecurity & Infrastructure Security Agency and National Institute of Standards and Technology," April 2021, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

[227] CISA, Alert TA17-181A, "Petya Ransomware," Last revised February 15, 2018, https://us-cert.cisa.gov/ncas/alerts/TA17-181A.

[228] "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," U.S. Department of Justice, September 16, 2020, https://www.justice.gov/opa/pr/seven-internationalcyber-defendants-including-apt41-actors-charged-connection-computer.

[229] Dr. Trey Herr, William Loomis, Stewart Scott, June Lee, "Breaking Trust: Shades of Crisis Across An Insecure Software Supply Chain."

[230] U.S. President, Executive Order, "Improving the Nation's Cybersecurity, Executive Order 14028 of May 17, 2021."

employing automated tools, or comparable processes, to maintain trusted source code supply chains; and developing minimum standards for developer verification of software. In addition to NIST's efforts, DOC's National Telecommunications and Information Administration (NTIA) was directed to develop and establish minimum elements for a Software Bill of Materials (SBOM). An SBOM provides information about the provenance of the software and allows for better visibility into the quality and security of the source code.

7.7 Extended Supply Chains

Extended supply chains for both the hardware and software spaces consisting of third-party suppliers, vendors, and service providers can expose sensitive data to malicious actors, and may have insufficient vulnerability management frameworks and techniques, and weaker software assurance and security controls.

Hardware device manufacturers rely on a complex chain of component suppliers, which may present organizational risks for software security, particularly for firmware as discussed in detail in Section 5. Device vulnerabilities stemming from the supply chain make firmware an attractive target. Vulnerabilities buried in device components are almost invisible to most users, and enterprises may be unaware of or incapable of identifying these vulnerabilities. In such specialized industries, only a few manufacturers may produce the vast majority of these parts. A notable example of this is the Ripple20 vulnerabilities, a set of hackable bugs in the software library of an Internet protocol suite (Transmission Control Protocol/Internet Protocol stack, or TCP/IP stack) manufactured by Treck Inc. As Treck Inc. is one of the major stack producers, these vulnerabilities are believed to exist in billions of devices, to include products made by companies like Intel, HP, Caterpillar, and Rockwell Automation, and currently reside in power grid data centers, medical devices manufacturing systems, and retail point-of-sale systems.[231]

While there is ever-increasing awareness of supply chain vulnerabilities, it can be difficult for organizations to ensure that all third-party vendors and products are taking the necessary efforts to secure data. There are opportunities for more thorough vetting of third parties, through the use of vendor SCRM templates, like those developed by CISA's ICT Supply Chain Risk Management Task Force. Other efforts include the adoption of secure software development, testing and verification practices and associated tools, and ensuring that requirements and expectations for secure and trustworthy software flow to upstream supply chain entities. Third-party vendors and suppliers may not employ appropriate cybersecurity hygiene or follow industry standards that help to secure sensitive data and components. Some third-party vendors may themselves be bad actors and can be associated with foreign adversaries. To that end, third-party vendors may develop parts or components in countries that have laws or standards that do not grant access to their supply chains.

[231] "Ripple20," JSOF, https://www.jsof-tech.com/disclosures/ripple20/; Dos Santos, Daniel, "Identifying and Protecting Devices Vulnerable to Ripple20," Forescout Blog (August 17, 2020), https://www.forescout.com/blog/identifying-and-protecting-devices-vulnerable-to-ripple20/; and Brash, Ron, "7 Steps to Protect Against Ripple20 Vulnerabilities in OT/ICS," Verve Industrial (June 23, 2020), https://verveindustrial.com/resources/blog/7-steps-to-protect-against-ripple20-vulnerabilities-in-ot-ics/.

8. External Risks to the ICT Industrial Base Supply Chain

The ICT sector is also vulnerable to external risks attributable to geopolitical tensions, economic dependencies, labor, and climate concerns. Drawing on current global dynamics and the existing architecture of the global ICT supply chain, the risks covered below are deemed highly likely and are judged to have a significant impact on the continuity, integrity and predictability of the ICT supply chain which would directly affect both the security and competitiveness of the United States. This section evaluates risks in the following four issue areas: cyber espionage and IP theft, economic investment, forced labor, and climate.

The ICT industry is particularly vulnerable to supply chain shocks. According to a study by the McKinsey Global Institute, which analyzed 23 industry value chains to determine their exposure to specific types of shocks, as outlined in Figure 18 below, the communications equipment value chain has the highest exposure to the collection of shocks that were analyzed. "As a heavily traded, geographically concentrated value chain, it may be caught up in trade disputes—and most of its footprint is in the Asia-Pacific region, which is vulnerable to earthquakes, tsunamis, and typhoons." The centrality of intellectual property and digital assets also heightens vulnerability to cyberattacks.[232]

Figure 18: Value Chains' Exposure to Shocks

Less exposed — More exposed

	Value chain	Overall shock exposure	Rank of exposure (1 = most exposed) Pan-demic[1]	Large-scale cyber-attack[2]	Geo-physical event[3]	Heat stress[4]	Flood-ing[5]	Trade dispute[6]
Global innovations	Chemical	11	16	4	6	19	16	8
	Pharmaceutical	19	23	2	17	23	19	4
	Aerospace	8	2	1	18	20	21	5
	Automotive	14	6	9	12	21	18	6
	Transportation equipment	4	5	12	7	13	5	15
	Electrical equipment	16	17	11	9	15	15	10
	Machinery and equipment	18	9	10	20	17	20	7
	Computers and electronics	6	15	5	4	14	14	9
	Communication equipment	1	13	3	2	16	7	2
	Semiconductors and components	9	19	6	1	18	23	1
	Medical devices	23	22	8	22	22	22	3

[232] Susan Lund, et al., "Risk, Resilience, and Rebalancing in Global Value Chains."

8.1 Theft of Intellectual Property and Cyber Intrusions

Malicious cyber incidents are fundamentally corrosive to the development, utilization and innovation of both hardware and software applications throughout the ICT supply chain. State sponsored cyber intrusions from countries opposed to U.S. interests threaten domestic industry and national security. According to a 2020 report by the Atlantic Council, state actors have been prominent in targeting software supply chains with almost 25 percent of compromises originating from state actors.[233] Techniques used included hijacking updates, undermining code signing, and using vulnerabilities in open-source codes to gain access to sensitive information or processes within the ICT supply chain.

State actors increasing rely on cyber intrusions to achieve economic objectives, including industrial espionage and the theft of intellectual property (IP). Since 2000, there have been more than 1,200 cases of IP theft litigation brought by U.S. companies against Chinese companies alone, of which 41 percent involved the use of cyber intrusions with increasing sophistication and regularity.[234] In addition, within the past couple of years, the Federal Bureau of Investigation has had upwards of 1,000 IP theft cases involving individuals associated with China.[235] According to the National Counterintelligence and Security Center, state-sponsored entities with support from China, Russia, and Iran are expected to remain aggressive and capable collectors of sensitive U.S. information and technologies while deploying significant resources to acquire intellectual property and proprietary information. The ICT industry is identified as one of six key industries that are most likely to be targeted by foreign actors given the advanced nature of R&D in this sector.[236]

The risk of cyber incidents resulting in IP theft or supply chain disruption in the ICT industry is exacerbated by the production presence in supplier countries like China that have weaker regulatory enforcement and standards. Industrial scale IP theft ultimately erodes the resilience and competitiveness of the whole U.S. ICT industry, as years' worth of research/progress can be lost to foreign competitors. In one case, when the American Superconductor Corporation had its wind-energy software code stolen by a major customer in China, it lost not only that customer, but also 90 percent of its stock value.[237] The risks in this space are two-fold, as cyber incidents may be used to disrupt the movement or integrity of ICT hardware on its way from a production facility to the consumer, or they may be used to plunder the intellectual property, which is the greatest value-add for American companies operating in this sector.

As ICT supply chains have become more extended, the number of threat vectors that can be exploited to access proprietary information flows along the supply chain has grown exponentially. State actors continue to exploit vulnerabilities in hardware and software inputs along the commercial supply chain in an effort to subsidize the competitiveness and address

---

[233] Dr. Trey Herr et al., "Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain."
[234] "Survey of Chinese Espionage in the United States since 2000," Center for Strategic and International Studies, 2021, https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000.
[235] Megan Gates, "An Unfair Advantage: Confronting Organized Intellectual Property Theft," ASIS International, July 2020, https://www.asisonline.org/security-management-magazine/articles/2020/07/an-unfair-advantage-confronting-organized-intellectual-property-theft/.
[236] "Foreign Economic Espionage in Cyberspace," National Counterintelligence and Security Center, 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.
[237] Michael Riley, and Ashlee Vance, "China Corporate Espionage Boom Knocks Wind out of U.S. Companies," *Bloomberg*, March 15, 2012, https://www.bloomberg.com/news/articles/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.

shortcomings of foreign government and locally domiciled ICT companies. In the context of the commercial supply chain, cybersecurity needs to be thought of as more than just intrusion detection, firewalls, network design and other security activities. Instead, it needs to include the hardware and therefore the supply chain that is used to build network products.[238] This is especially important when considering the number of component-compromised networks that are built into embedded software codes. The ever-changing landscape of inputs underscores the complexity associated with mitigating the risks posed from cyber intrusion(s).

8.2 Economic Risks

The economic risks associated with the current supply chain arrangements stem from the off shoring of significant ICT production, thus limiting capital inflows to the United States and impeding the development of a vibrant ICT manufacturing ecosystem that is crucial to sustain innovation. Furthermore, the outsourcing of production activity exposes potential dependencies of U.S. industry (and the wider U.S. economy) on foreign government subsidies in order to remain competitive in global markets, as was detailed in section 7.3., and reduces domestic manufacturing employment.

One of the primary economic risks posed by the current structure of the global ICT supply chain is that it incentivizes companies to allocate capital outside of the United States, particularly for manufacturing. When the majority of manufacturing capacity for a particular industry is moved to another country, domestic innovation is affected. Several studies, including one by the National Bureau of Economic Research (NBER), have identified a causal relationship between offshoring and innovation, suggesting that firm innovation is hindered as a result of moving manufacturing abroad.[239][240] At the same time, manufacturing has an outsized impact on the U.S. economy, employing around 8 percent of the workforce while contributing an estimated 11 percent of total GDP, or 24 percent if adjusting for direct and indirect value-added (i.e., including purchases from other industries) as portrayed in the figure below. U.S. small business has been acutely affected by this trend, accounting for more than 98 percent of companies[241] and more than 44 percent of employees[242] in the wider manufacturing sector.

---

[238] Taylor Wilkerson, "Cybersecurity in the Supply Chain – LMI," LMI, Accessed November 19, 2021, https://www.lmi.org/sites/default/files/media/LMI_article_USCYSU14.pdf.
[239] Lee Branstetter et al., "Does Offshoring Manufacturing Harm Innovation in the Home Country? Evidence from Taiwan and China" (Department of Economics - Harvard University, October 2017), https://economics.harvard.edu/files/economics/files/glennon-britta_offshoring_innovation_in_taiwan_wp_6oct_2017.pdf.
[240] Lee G. Branstetter et al., "Does Offshoring Production Reduce Innovation: Firm-Level Evidence Taiwan (NBER Working Paper Series)" (National Bureau of Economic Research, August 2021), https://www.nber.org/system/files/working_papers/w29117/w29117.pdf.
[241] Bridget Weston, "How Small Manufacturing Businesses Drive the U.S. Economy," SCORE, May 9, 2019, https://www.score.org/blog/how-small-manufacturing-businesses-drive-us-economy.
[242] "2019 Small Business Profile" (U.S. Small Business Administration Office of Advocacy, April 2019), https://cdn.advocacy.sba.gov/wp-content/uploads/2019/04/23142719/2019-Small-Business-Profiles-US.pdf.

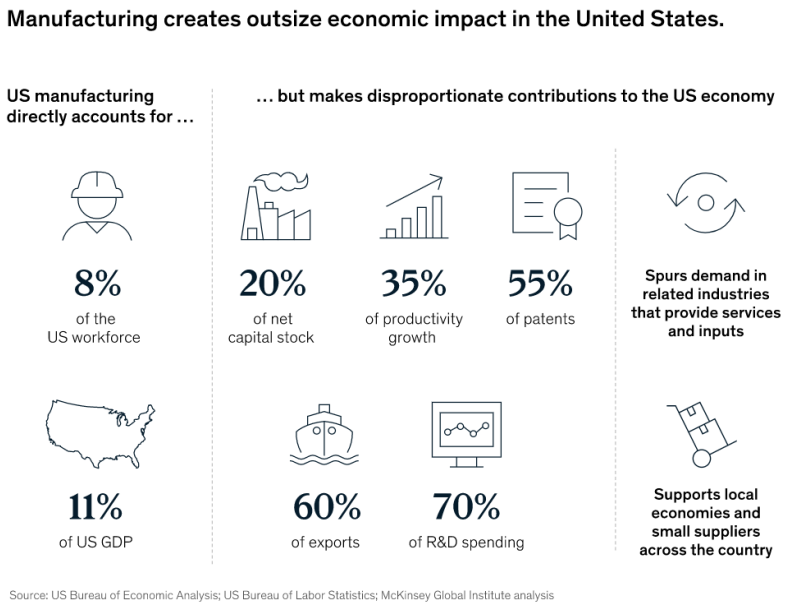


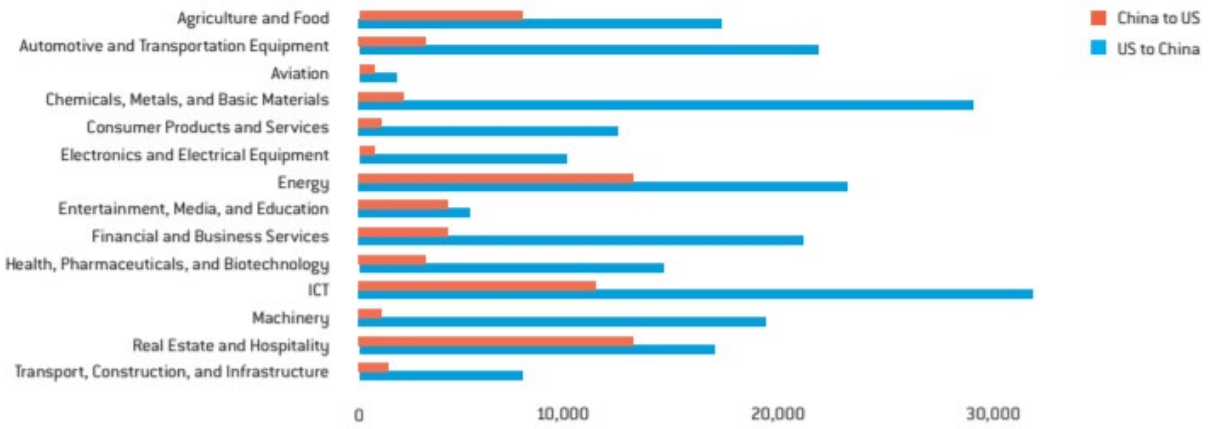
Figure 20: Economic Impact of Manufacturing[243]

Global ICT companies often look to developing economies that offer a skilled workforce and above average growth prospects to pursue foreign direct investment (FDI). Capital flows to developing markets, where it has a more widespread impact than do equivalent capital flows to developed markets in North America and Europe. In 2020, U.S. corporations invested nearly $14 billion into Chinese manufacturing of computers and electronics products. During that same period, Chinese companies invested only $141 million into U.S. manufacturing in the same industry. More broadly, over the course of the past five years, U.S. investment in computer and electronics manufacturing throughout all countries in the Asia-Pacific region has averaged roughly two times that of reciprocal investment from those same countries.[244] A significant portion of American investment in China's ICT industry is allocated towards the manufacturing of hardware products. Studies in recent years have indicated that the ICT manufacturing sector has a higher degree of backward linkage than both the ICT services sector and the non-ICT manufacturing sector.[245] This means that investments that are allocated to the ICT manufacturing sector not only aid the development of the human capital and physical infrastructure, but they serve as catalysts to spur further economic activity throughout the supplier network. Thus, failure to garner investment in the ICT manufacturing sector can have widespread impact throughout the broader economy.

---

[243] James Manyika et al., "Building a More Competitive US Manufacturing Sector," McKinsey & Company, September 23, 2021, https://www.mckinsey.com/featured-insights/americas/building-a-more-competitive-us-manufacturing-sector.
[244] "Two-Way Street: 25 Years of US-China Direct Investment" (National Committee on United States - China Relations, November 11, 2016), https://www.ncuscr.org/sites/default/files/page_attachments/Two-Way-Street-2016_Exec-Summary.pdf.[245] Li, Yongfei, Sang-Gun Lee, and Myungjai Kong. "The Industrial Impact and Competitive Advantage of China's ICT Industry." *Service Business* 13, no. 1 (2018): 101–27. https://doi.org/10.1007/s11628-018-0368-7.
[245] Li, Yongfei, Sang-Gun Lee, and Myungjai Kong. "The Industrial Impact and Competitive Advantage of China's ICT Industry." *Service Business* 13, no. 1 (2018): 101–27. https://doi.org/10.1007/s11628-018-0368-7.

Figure 21: Cumulative Investment by Industry in China and the U.S. 1990-2015 (USD Millions)[246]



Source: Rhodium Group.

8.3 Forced Labor Risks

Labor-related risks are an issue in the ICT supply chain. Forced labor is a particular concern in developing markets, where a majority of ICT manufacturing takes place.

Given the thousands of components that are used as inputs to ICT hardware, the ICT supply chain is more complex than other industries' production networks. This added complexity lends to labor exploitation, due to inconsistent cross-border legal protections, and can obfuscate the presence of illicit activity due to the limited sharing of information on secondary and tertiary suppliers. As such, DHS's Customs and Border Protection (CBP) advises that U.S. importers must exercise reasonable care over their supply chains and understand where and how their products are manufactured or produced, stating "[t]hose companies operating in industries and geographies at higher risk of forced labor, are generally advised…to address forced labor risks through supply chain due diligence, maintaining a comprehensive social compliance system, obtaining U.S. import certifications of origin and, including forced labor prohibition provisions in contract terms."[247] Furthermore, given the regularity with which critical minerals are used in ICT hardware, it is vital to assess labor risks throughout the entirety of the value chain to include mining activities.

At the early stages of the ICT supply chain, minerals like tantalum, tungsten, and silicon (among numerous others) represent a small number of the naturally occurring elements that are required to produce the ICT hardware that enables communication and information processing. More

[246] "Two-Way Street: 25 Years of US-China Direct Investment" (National Committee on United States - China Relations, November 11, 2016), https://www.ncuscr.org/sites/default/files/page_attachments/Two-Way-Street-2016_Exec-Summary.pdf.
[247] Catherine Cimino-Isaacs, Christopher A Casey, and Katarina C O'Regan, "Section 307 and U.S. Imports of Products of Forced Labor: Overview and Issues for Congress," Congressional Research Service, February 1, 2021, https://sgp.fas.org/crs/misc/R46631.pdf.

than 50 of the world's 90 naturally occurring elements are used in more than 8.5 billion computing devices.[248] Top mining locations for these minerals include countries such as the Democratic Republic of Congo, China, and Brazil, all of which have documented cases of forced labor occurring in more than isolated incidents.[249] Section 307 of the Tariff Act of 1930 prohibits U.S. imports of any product that was mined, produced, or manufactured wholly or in part by forced labor. While the complicated and sometimes opaque nature of certain supply chains can make it difficult for U.S. companies to ensure that all entities in a supply chain do not use forced labor, goods that are produced with forced labor may not enter the United States.

Further human rights concerns exist at the assembly and manufacturing stages of ICT hardware product. Major locations for ICT hardware production exist throughout East and Southeast Asia, several of which rank among the top 10 countries in terms of the total number of goods produced from forced labor.[250] A large migrant population paired with underdeveloped working conditions throughout this region underscores the fact that the labor climate is particularly hospitable to recruiters looking to exploit migrant workers. The complex and generally opaque nature of ICT supply chains necessitates further efforts from governments and industry to ensure that labor protections are observed and respected throughout.

Labor risks represent not only a clear violation of international and U.S. law, but also present other risks to the companies that directly or indirectly benefit. The reputational risks associated with companies utilizing forced labor may result in financial consequences as consumers choose to "vote with their feet" in increasing numbers. "In an economy where 70 percent to 80 percent of market value comes from hard-to-assess intangible assets such as brand equity…and goodwill, organizations are especially vulnerable to anything that damages their reputation."[251] While developing markets can reduce the operating costs of ICT companies by a significant margin, weak civil society and an ineffectual forced labor monitoring infrastructure significantly increases the risk of utilizing forced labor in the supply chain. The recent signing of the Uyghur Forced Labor Prevention Act by President Biden underscores the United States' commitment to combating forced labor.

8.4: Climate Risks

The ICT supply chain is both extended and concentrated, with vast geographic distances between each successive portion of the supply chain while at the same time high levels of concentration within each of these 'links' in the chain. This design makes the ICT industry vulnerable to supply chain disruptions caused by climate-related events.

The ICT supply chain's globalized procurement and production processes can contribute to environmental degradation and are due to be examined for ways to manage climate issues with increased responsibility.[252] According to the International Telecommunication Union's (ITU)

---

[248] Andrew Wheeler, "What Raw Materials Are Used to Make Hardware in Computing Devices?" Engineering.com, September 29, 2018, https://www.engineering.com/story/what-raw-materials-are-used-to-make-hardware-in-computing-devices.
[249] "Better Trade Tool," United States Department of Labor, 2021. https://www.dol.gov/agencies/ilab/better-trade-tool.
[250] "2020 List of Goods Produced by Child Labor or Forced Labor," U.S. Department of Labor, September 29, 2020. https://www.dol.gov/sites/dolgov/files/ILAB/child_labor_reports/tda2019/2020_TVPRA_List_Online_Final.pdf.
[251] Robert G. Eccles, Scott C. Newquist, and Roland Schatz, "Reputation and Its Risks," Harvard Business Review, August 1, 2014. https://hbr.org/2007/02/reputation-and-its-risks.
[252] "Guidance on Green ICT Procurement," International Telecommunication Union, August 15, 2012, https://www.itu.int/dms_pub/itu-t/oth/0B/11/T0B110000133301PDFE.pdf.

Smart 2020 report, "the full life cycle carbon footprint of the ICT industry represents around 2 percent of worldwide emissions, and is projected to grow at a 6 percent annual compound growth rate."[253] As such, one of the most significant challenges for the ICT industry is that in enabling environmental efficiency for other industries, it must also reduce its own environmental impacts. This concern is amplified by the fact that considerable portions of the ICT supply chain have been consolidated in lower- and middle-income countries that lack stringent environmental standards for industry. As climate change presents an increasingly discernable threat in the coming years, companies that remain overly reliant on production in countries with inadequate environmental standards will need to prepare for the potential introduction of more stringent global emissions standards.

Throughout the ICT supply chain, there is a high level of geographic concentration among design, production, and manufacturing sites in each node of the supply chain network. There tends to be a higher level of concentration of facilities in the downstream portion of the product supply chain such as production and assembly. According to a study published by the Alliance for Water Stewardship, over 80 percent of the nearly 3,000 manufacturing locations surveyed, which represented all tiers of the ICT supply chain, had a very high risk of flooding, with another 68 percent of sites facing high or very high risk due to poor water quality.[254] The study further identified that, within China, the Taihu, Dong and Zhu river basins are most crucial to the ICT sector given the concentration of facilities in these areas. Other important, concentrated sites are located in the Danube and Rhine River basins in Europe and the Colorado and Great Lakes River basins in North America. While this study sought to pursue water risks for primary analysis, the concentration of ICT supply chain facilities in Chinese, European, and North American river basins and their concentration in large urban environments would suggest that this industry is subject to the localized risks associated with evolving climate patterns.

This risk can be seen in 2011, when Thailand experienced flooding that caused disruptions for hard disk drive (HDD) components. At the time, Thailand produced about 45 percent of the world's HDDs.[255] The flooding caused shortages, delays, and price increases for the individual components as well as for downstream products such as computers. While industry experts predicted this event would lead to increased geographic diversity for HDD manufacturing, the reverse occurred. HDD production further consolidated in Thailand increasing the risk for future disruptions.[256] As noted in Section 4, many other components are experiencing similar geographic consolidation and future climate events could have an oversized impact on the ICT industry. Supply chain facilities ranging from R&D to fabrication and packaging sites can be affected by adverse, localized conditions that are expected to occur more frequently due to climate change.

---

[253] "Toolkit on Environmental Sustainability for the ICT Sector," International Telecommunication Union (ITU), 2012. https://www.itu.int/dms_pub/itu-t/oth/4B/01/T4B010000060001PDFE.pdf.
[254] "Water Risk In The ICT Sector: The Case For Action," Alliance for Water Stewardship, March 22, 2021. https://a4ws.org/download/water-risk-in-the-ict-sector-the-case-for-action/.
[255] Wendy Kaufman, "Thai Floods Disrupt Computer Hard Drive Supply," NPR (NPR, November 25, 2011), https://www.npr.org/2011/11/25/142767696/thai-floods-disrupt-computer-hard-drive-supply.
[256] James Sanders, "Why HDD Factory Closure Means You May Need to Migrate to Solid State," TechRepublic, July 17, 2018, https://www.techrepublic.com/article/why-hdd-factory-closure-means-you-may-need-to-migrate-to-solid-state/.

9. Recommendations to Strengthen ICT Supply Chain Resiliency

Resilient and secure ICT supply chains are critical to U.S. economic and national security, and this report has detailed important structural vulnerabilities and external risks that have been exacerbated by the COVID-19 pandemic. These vulnerabilities, including a lack of domestic production capacity for many product categories, overreliance on single-source and region suppliers, and a shortage of qualified workers, threaten to continue to disrupt the ICT industry and the broader economy if left unaddressed.

Promoting a more secure and resilient ICT supply chain will require significant effort from the U.S. government, including consideration of the recommendations listed below. However, government alone cannot wholly accomplish this goal. There is also important work to be done by the private sector and other non-governmental partners. ICT is a global industry, and ICT supply chain vulnerabilities are not confined to the United States. Addressing these challenges successfully will require close coordination and collaboration with international allies and partners.

To address the vulnerabilities and risks identified in the assessment, and to strengthen supply chain resiliency, the Secretaries of Commerce and Homeland Security recommend implementing the following comprehensive strategy.

Revitalize the U.S. ICT Manufacturing Base

Over the past 30 years, the U.S. ICT industrial base has evolved to be 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. The Secretaries of Commerce and Homeland Security, in consultation with industry stakeholders, are 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:

- Support domestic investment and production of key ICT products, potentially including printed circuit boards (PCBs) and semiconductors, through appropriate federal procurement incentives and funding of programs like Title III of the Defense Production Act and the Creating Helpful Incentives to Produce Semiconductors for America (CHIPS) Act.
- Provide incentives through the National Institute of Standards and Technology's (NIST) Manufacturing Extension Partnership (MEP) to domestic manufacturers for upgrades to ICT manufacturing plants to improve productivity, competitiveness, and resiliency, as well as facilitate entry of new domestic manufacturers into the supply chain. MEP, the

only federal program with a national footprint in small manufacturing, is meeting these needs with existing and growing programs like supplier scouting, training and workforce, supply chain resilience, cyber security, as well as technology and innovation.

- Implement strong Buy America provisions used in projects financed by the Bipartisan Infrastructure Law and coordinate with the Office of Management and Budget to initiate a consultation process to identify ICT products, such as printed circuit boards and fiber optic cables, eligible for such provisions. Any waivers granted from Buy America requirements should be time-limited and consistent with U.S. international trade obligations.
- Coordinate with the Federal Acquisition Regulatory Council to review the U.S. government's direct procurement policies of ICT products, services, and components through the Buy American Act. Additional consideration should be given to enhanced Buy American Act provisions that incentivize the production of ICT products and services with significant U.S. value add, including design contribution, and with tolerances for assembly in allied or partner nations. Any extension of Buy American provisions should be consistent with U.S. international trade obligations.
- Encourage the inclusion of information related to ICT manufacturing supply chains in applicable Comprehensive Economic Development Strategies (CEDS). A CEDS is an Economic Development Administration (EDA)-funded, regional economic development plan run by DOC which is designed to build capacity and guide the economic prosperity and resiliency of an area or region. By recommending that applicable regions consider ICT manufacturing supply chains in the development and implementation of their CEDS, regions that have existing ICT manufacturing assets can enhance focus on efforts to maintain and/or improve their ICT manufacturing supply chain pipelines as a key component of regional economic development.
- Leverage E.O. 13985 and the Minority Business Development Act of 2021 to increase diversity, equity and inclusion of underserved communities to build local capacity of minority owned manufacturing and packaging firms within the ICT global supply chain. Facilitate national programs to accelerate the modernization and digital infrastructure of diverse U.S. businesses impacted by the pandemic and supply chain disruption.

<u>Build Resilience through Secure and Transparent Supply Chains</u>

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:

- Implement or promote Assured Supplier Program for ICT products, including PCBs and semiconductors, for Federal Government and critical sectors. Federal agencies that

procure ICT for sensitive equipment should consider a preference for vendors that participate in a voluntary qualified bidder or manufacturer program to assess their qualifications and assurance of the reliability, integrity, and security of their products by demonstration of conformance to one or more applicable industry standards, such as IPC-1791 "Trusted Electronic Designer, Fabricator, and Assembler Requirements."

- Congress should authorize and appropriate funding to establish the proposed supply chain office at the Department of Commerce, and in consultation with DHS, 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.
- Continue and expand software supply chain security initiatives under E.O.14028, including publishing guidance that identifies practices that enhance software supply chain security, with references to standards, procedures, and criteria; developing recommendations for pilot programs for consumer software and IoT labeling; developing minimum elements for a Software Bill of Materials (SBOM); and prioritizing security initiatives for open-source software, recently developed through White House coordination.
- Continue to support the supply chain transparency and resilience work of CISA's 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.

<u>Collaborate with International Partners to Improve Supply Chain Security and Resiliency</u>

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

Improve international collaboration to advance shared interests:

- Advance international engagement on ICT supply chain resiliency, security, and diversity for critical products. To achieve these international engagement goals, we will seek to coordinate with key partners on topics such as investment in ICT manufacturing capacity, information-sharing on supply chain challenges, workforce and other capacity building opportunities, and promotion of strong sustainability, labor and security standards. As appropriate, this engagement can build on existing semiconductor supply chain dialogues with international partners, such as the U.S.-Mexico High Level Dialogue. Other fora to achieve these efforts could include the U.S.-EU Trade and Technology Council, the Americas Competitiveness Exchange, the North American Leaders Summit, the Quad Critical and Emerging Technology Working Group, and the Indo-Pacific Economic Framework, as well as other bilateral and multilateral discussions.

- Facilitate international trade and strengthen international trade enforcement mechanisms. Encourage partners and allies that have not yet joined the World Trade Organization (WTO)'s Information Technology Agreement (ITA) or agreed to the WTO ITA Expansion to participate in those agreements. In addition, work with partners and allies to implement a comprehensive strategy to counter unfair foreign competition that erodes the resilience of ICT supply chains.
- 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.
- Enhance federal government support for diversifying ICT supply chains, including potential financial support from the Export-Import Bank for eligible companies engaged in friend- and near-shoring manufacturing of critical ICT supply chain components, particularly those that are unlikely to be produced domestically in the near-term.
- Establish international workforce exchange programs and technical assistance with partner nations and industry to educate and train workers in the specific skills needed to strengthen the ICT workforce pipeline and diversify manufacturing outside of China.
- Ensure U.S. and likeminded leadership in standards bodies as well as relevant international organizations, including the International Telecommunication Union (ITU). Specifically, the U.S. Government should encourage likeminded governments to provide their full support to elect Doreen Bogdan-Martin as the next ITU Secretary General.

Invest in Future ICT Technologies

Innovation through research and development (R&D) efforts is the foundation for a thriving ICT industry. While the United States 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:

- To enhance the U.S. ICT ecosystem, increase federal funding for programs such as the National Science Foundation's Computer and Information Science and Engineering research and development and computing graduate fellowship initiatives. These programs allow for nascent technologies to be researched and developed.
- Dedicate funding for a NIST-sponsored Manufacturing USA institute focused on the ICT industry and for projects at existing institutes to advance ICT manufacturing technology, and to provide education and workforce training for high-paying ICT jobs.
- Promote R&D investment by startup and small companies and emerging technology companies by expanding R&D tax credit legislation. Congress should double the annual amount of payroll taxes that can be offset by the research tax credit for qualified small businesses and delay until December 31, 2025, the requirement to amortize R&D expenses over five years, as proposed in the Build Back Better Act, passed by the U.S. House of

Representatives. In addition, Congress should fully fund the semiconductor manufacturing and research provisions authorized by the CHIPS Act. Funding for these provisions is needed to ensure that the semiconductor technology needed for ICT is manufactured in the United States, and that the semiconductor and advanced packaging research needed for next-generation ICT is led by the United States.

- Prioritize R&D to improve the energy efficiency of ICT networks, products, and equipment. Improved energy efficiency is essential to enabling the continued growth of computational capacity and for mitigating the exponential growth in energy demand of the ICT sector.
- Increase federal investments that build the research capacity and curriculum within Minority Serving Institutions to expand the participation of underserved communities into public and private R&D ICT ecosystems.

Strengthen the ICT Workforce Pipeline

The U.S. ICT industry's struggle to find qualified workers threatens its ability to fulfill increased demand for key ICT products, impacting implementation of federal and state broadband programs as well as measures to increase manufacturing in the United States.

Support and expand programs that attract, educate, and train the ICT workforce:

- Continue to prioritize and fund programs such as the EDA's Build Back Better Regional Challenge (BBBRC) and Good Jobs Challenge (GJC) to invest in the U.S. ICT workforce and enhance U.S. global competitiveness in this sector. BBBRC brings together coalitions of industry and community partners to apply for investment assistance to grow new, or scale existing, industry clusters. To date, EDA has awarded 60 finalists approximately $500,000 each to develop proposed projects in advance of applying for an additional $25-$100 million in funding to implement those projects. Almost a quarter of these finalists, representing 12 states, are focused on ICT workforce development. Through GJC, EDA will provide $500 million to support regional or sectoral partnerships that will create and implement industry-led training programs that are designed to enhance worker skills and connect unemployed or underemployed works to existing and emerging job opportunities, including in the ICT sector.
- Expand the prevalence of computer science, science, technology, engineering, and mathematics (STEM) programs in the K-12 curriculum through targeted grant programs from the Departments of Education and Labor.
- Leverage the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity to align education, training, and workforce efforts across academia, industry, and government.
- Build the advanced ICT manufacturing and software workforce via multiple secondary and post-secondary pathways, including through registered apprenticeships, career and technical education programs, boot camps, and community college programs. Grant investments should be aligned with employer-led sectoral partnerships that ensure training is linked to real-world job opportunities.
- Prioritize training infrastructure investments in rural and underserved areas.

- Encourage the expansion of specialized university undergraduate and graduate programs, including areas such as supply chain procurement/planning, advanced manufacturing, tax and trade and operations management.
- Encourage 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.

Ensure Sustainability Remains a Cornerstone of ICT Development

The United States should continue to ensure that the highest environmental standards are met for the development and production of ICT products.

Promote environmental standards through financial incentives and government programs:

- Continue to incentivize the adoption of sustainable ICT products through Federal procurement and other mechanisms. Sustainable ICT products – which include products that have a reduced manufacturing footprint (this may include resource consumption/waste as well as other sustainability topics such as greenhouse gas, energy, resource consumption/waste), and greater product longevity, reduced packaging, reduced water use in manufacturing, etc. – are defined through product sustainability standards. These standards are developed by the private sector and referenced in Federal procurement requirements, such as Subpart 23.7 of the Federal Acquisition Regulation (FAR), which currently requires federal agencies to procure electronics products registered by the Electronic Product Environmental Assessment Tool (EPEAT). EPEAT is an ecolabel that addresses many attributes of sustainability and is based on Voluntary Consensus Standards (VCS) and private sector-developed criteria, and private sector conformity assessment (testing and certification) requirements. Support and expand programs such as the Department of Energy's technical assistance to state and local governments aimed at facilitating the construction or retrofit of sustainable ICT production facilities.
- Ensure adequate funding for Federal participation in the development of ICT sustainability standards in order to help ensure that these standards reflect the priorities of the Federal government, as well as industry, academia, non-governmental organizations (NGOs) and other stakeholders.
- Support companies in making decisions that incorporate the best available predictions on climate risks (e.g., heatwaves, flooding, extreme storms), based on climate data and services from the National Oceanic and Atmospheric Administration.

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.
- Through the DOC's Advisory Committee on Supply Chain Competitiveness and United States Manufacturing Council, identify concrete actions the government and industry can take to strengthen the ICT supply chain and ICT domestic manufacturing.
- Engage with industry together with allies and partners to promote awareness and adoption of risk mitigation techniques, establish best practices for securing the ICT supply chain, and create voluntary mechanisms for improving sustainability of operations. This includes diversification of the supply chain, increased visibility into the supply chain, and the identification of measures that enable ICT stakeholders to meet carbon neutral goals.
- Collaborate with the Made in America Office (MIAO) and Made in America Council to share data that can help promote domestic sourcing and communicate best practices used across agencies facing similar challenges for both procurement and financial assistance projects.

Continued Study of the ICT Industrial Base

To monitor developments and guide long-term policy and planning aimed at strengthening ICT supply chain resilience, the Secretaries of Commerce and Homeland Security recommend the Bureau of Industry and Security (BIS) conduct further industrial base studies on critical ICT products such as printed circuit boards and related microelectronic fields. These studies will inform where investments are most needed to revitalize the domestic ICT manufacturing base.

Guide long-term policy through further studies:

- Employ the BIS authority under Section 705 (d) of the Defense Production Act of 1950, as amended, (50 U.S.C. § 4555) and E.O. 13603 and provide adequate funding to conduct an industrial base assessment of critical ICT products, such as printed circuit boards and related value chain in the microelectronics industrial base to better understand the challenges and opportunities facing the industry. The information collected in this assessment will help to support economic and national security planning.

Appendix A

Scorecard Criteria for ICT 1 Year Research Collation

ICT IB/SCRM Field #	Category	Reasoning/What it Measures	USG/Equity Source/Agency
ICT IB/SCRM 1	Essential Goods, Materials and Services	Taxonomy and prioritization of critical ICT goods and materials to produce IT hardware and communication equipment, baseline identification of ICT sector, commodities and services	NIST, Census, ITC, FCC, DLA, BIS, NRMC, NSF
ICT IB/SCRM 2	Financials/Business Practices	Financial statements, disclosures, PP&E investment, profitability/performance, tax, contract/purchase data, M&A, coproduction, patents/IP licensing, productivity	SEC, Treasury, ITA, ESA
ICT IB/SCRM 3	Supply Chain Capacity	Supply chain conditions and its ability to react and recover from disruption. Sourcing practices, import/export information, pricing, where critical materials are bought/manufactured, qualification/re, re/near/offshoring, outsourcing, decoupling, foreign procurements/ dependencies, illumination	NIST, FCC, DOJ, ITA, DOS, EDA, DOD, FLC, DOE
ICT IB/SCRM 4	Policy/Legal	Regulatory barriers and procedures, environmental, ESG, public/private sector incentives, acquisition regulations, municipal, county, state, regional grant making and proposals, liability	DOJ, EDA, EPA, GSA, Education
ICT IB/SCRM 5	Manufacturing/Logistics	Manufacturing and other capabilities necessary to produce critical materials. Distribution, automation/3D/AM, climate mitigation/geospatial, inventory practices, substitutes, method of shipment, insurance, interstate commerce, domestic versus foreign	NIST, EPA, FLC, Energy, DLA, DOT, NIST, EDA, DOD

		production capacity, utilization rate, surge capacity	
ICT IB/SCRM 6	Information/Cyber Security	Data storage/protection, mitigation, critical infrastructure impacts, industry security standards/practices, product security	FCC, CISA, NRMC, BIS, NTIA, NIST, DOJ, NSF
ICT IB/SCRM 7	Risks Posed/Supply Chain Impacts on the Nation	Defense, intelligence, homeland security, infrastructure, health, human-rights, labor, single points of failure, regional Limited global sourcing, environment events, geopolitical events, anti-competitive practices, future projection of risk	NEC, NSC, DHS, DOC, DOD, FBI, DOL, Energy
ICT IB/SCRM 8	R&D/Innovation	Emerging technologies, RDT&E capacity, spending and resources, SBIR/STTR, ICT goods and materials incubation, patents/IP, IOT, OT	FLC, NSF, EPA, DOC, NIST, EDA
ICT IB/SCRM 9	Initiatives/ Recommendations	Executive, legislative, regulatory, and policy changes to strengthen supply chain resiliency, innovation and production capabilities, allied and partner actions to decrease supply chain vulnerabilities, strengthen int'l trade rules, proposals promoting ICT supplier resiliency, health and competitiveness	March 22 Memo/100-day EO 14017 reporting
ICT IB/SCRM 10	Human Capital/ STEM/Education	Employment/human capital and skills data, ICT-related STEM needs, education, occupational distribution, retraining, manufacturing versus IOT-based opportunities, recruitment, immigration, visa prohibitions, labor turnover rates, vacancies, front line workers, automation	DOL, ETA, EDA, NIST MEP, Education, NSF

Appendix B

NAICS Codes Used to Define Scope of ICT Industry

Source: U.S. Census Bureau

NAICS Full	Category
334111 - Electronic Computer Manufacturing	Manufacturing
334112 - Computer Storage Device Manufacturing	Manufacturing
334118 - Computer Terminal and Other Computer Peripheral Equipment Manufacturing	Manufacturing
334210 - Telephone Apparatus Manufacturing	Manufacturing
334220 - Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing	Manufacturing
334310 - Audio and Video Equipment Manufacturing	Manufacturing
334412 - Bare Printed Circuit Board Manufacturing	Manufacturing
334413 - Semiconductor and Related Device Manufacturing	Manufacturing
334416 - Capacitor, Resistor, Coil, Transformer, and Other Inductor Manufacturing	Manufacturing
334417 - Electronic Connector Manufacturing	Manufacturing
334418 - Printed Circuit Assembly (Electronic Assembly) Manufacturing	Manufacturing
334419 - Other Electronic Component Manufacturing	Manufacturing
335921 - Fiber Optic Cable Manufacturing	Manufacturing
511210 - Software Publishers	Distributors/Publishers
515111 - Radio Networks	Distributors/Publishers
515112 - Radio Stations	Distributors/Publishers
515120 - Television Broadcasting	Distributors/Publishers
517311 - Wired Telecommunications Carriers	Telecommunications
517312 - Wireless Telecommunications Carriers (except Satellite)	Telecommunications
517410 - Satellite Telecommunications	Telecommunications
517911 - Telecommunications Resellers	Telecommunications
517919 - All Other Telecommunications	Telecommunications
518210 - Data Processing, Hosting, and Related Services	Services
519130 - Internet Publishing and Broadcasting and Web Portals	Distributors/Publishers
541511 - Custom Computer Programming Services	Services
541512 - Computer Systems Design Services	Services
541513 - Computer Facilities Management Services	Services

Appendix C

Top 20 Electronic Manufacturing Services /Original Design Manufacturing Companies by Revenue (2020)

Source: Bloomberg Terminal EMS/ODM (Global) Dashboard

EMS/ODM Company	Headquarter Location	Percent of Market Share			
		2020	2019	2018	2017
Hon Hai Precision Industry	Taiwan	40.9	41.1	40.8	39.6
Pegatron Corp	Taiwan	10.7	10.5	10.3	10
Quanta Computer Inc.	Taiwan	8.3	7.9	7.9	8.6
Flextronics International	United States	5.4	5.7	6.1	6.5
Compal Electronics Inc.	Taiwan	8.0	7.5	7.5	7.5
Jabil Circuit Inc.	United States	6.1	6.0	5.1	4.9
Winstron Corp	Taiwan	6.4	6.8	6.9	7.0
Inventec Corp	Taiwan	3.9	3.9	3.9	3.9
Samina Corp	United States	1.6	2.0	1.7	1.8
Lite-on Technology Corp	Taiwan	1.2	1.4	1.6	1.8
Celestica Inc	Canada	1.3	1.4	1.5	1.6
Qisada Corp	Taiwan	1.5	1.3	1.2	1.2
Universal Scientific Industrial	China	1.6	1.3	1.2	1.1
Advanced Semiconductor Engineering	Taiwan	--	0.0	1.0	1.1
Cal-Comp Electronics Thailand	Thailand	0.8	0.8	0.8	0.8
Plexus Corp	United States	0.8	0.8	0.7	0.6
Benchmark Electronic Inc.	United States	0.5	0.5	0.6	0.6

Siix Corp	Japan	0.4	0.5	0.5	0.5
Winstron NeWeb Corp	Taiwan	0.5	0.5	0.4	0.5
Mitac Holdings Corp	Taiwan	0.3	0.3	0.2	0.4