BUILDING A TRUSTED ICT SUPPLY CHAIN

CSC White Paper #4

UNITED STATES OF AMERICA
CYBERSPACE SOLARIUM COMMISSION

CO-CHAIRMEN
Senator Angus King (I-Maine)
Representative Mike Gallagher (R-Wisconsin)

OCTOBER 2020

CONTENTS

EXECUTIVE SUMMARY

In its March 2020 report, the U.S. Cyberspace Solarium Commission called on the U.S. government to take steps to reduce critical dependencies on untrusted information and communications technologies (ICTs). In addition to recommendations to improve intelligence and information sharing around supply chain risks, core to the Commission's recommended approach is the **creation of an ICT industrial base strategy "to ensure more trusted supply chains and the availability of critical information and communications technologies."**[1] This strategy is tailored to ICTs, but similar efforts are needed for operational technologies that control power, water, transportation, and other critical infrastructure sectors, as well as unique production areas like medical devices and weapons systems. While these technologies fall outside of the scope of this white paper, many of their core materials and components, including semiconductors, are integral to critical technologies more broadly. Thus many of the recommendations contained in this paper lay a firm foundation for technologies beyond ICT and will support efforts in those other areas.

Put bluntly: in the context of our supply chains for ICT, the United States has a China problem. Over the past two decades, China has mobilized state-owned and state-influenced companies to grab a dominant position in markets for several emerging technologies, including the market for telecommunications equipment.[2] This is no accident but rather the result of a concerted, strategic effort by the Chinese government to capture these markets through a mix of government-led industrial policy; unfair and deceptive trade practices, including state-led intellectual property theft; the manipulation of international standards and trade bodies; a growing network of influence built on the back of diplomatic and trade negotiations; and significant investments in research and development in ICT. As a result, the critical strategic competition between China and the United States and its friends and partners is taking place in an international system of commerce that—due to Chinese state intervention—is neither free nor fair, hampering the ability of American and partner companies to compete for global market share. Yet today, the United States lacks a consistent mechanism to align private-sector efforts with broad national security goals. And the battle over the fifth-generation (5G) of telecommunications infrastructure is broader than just who wins contracts to build out the networks. With the promise 5G revolutionizing the way the world connects, the country that holds the keys to the networks holds the keys to the next 20 years of innovation and economic growth and prosperity.

Congress and the executive branch have already begun to take action on the issue. In Congress, several bills have been proposed, each of which funds initiatives aimed at ensuring the availability of more trusted telecommunications equipment and electronics.[3] In the executive branch, the approach consists of disparate, largely disconnected actions, including several executive orders,[4] as well as efforts the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), the Department of Defense (DoD), Department of State, and others, which take square aim at managing ICT supply chain risks to both the federal government and the private sector. However, while these activities are likely to yield some positive outcomes, the lack of a coherent and cohesive overarching strategy to secure America's ICT supply chains runs the risk of encouraging inefficient uses of time, resources, and money, and ultimately undermining the very purpose behind these fragmented efforts. In short, in its eagerness to do something to address an obvious challenge, the United States has leaped into action without adequate analysis or a strategic plan.

In this white paper, the Commission proposes a path forward that will bring the various activities of the U.S. government and of partner nations together to form a comprehensive strategy, with the cooperation of industry, to ensure the continued availability and trustworthiness of critical ICT technologies and to counter Chinese economic aggression. This paper begins by unpacking the United States' critical ICT dependencies, providing an overview of the current state of U.S. high-tech

manufacturing, and highlighting the importance of partners in governments and industries around the world. The white paper specifies a strategy to build trusted supply chains for critical ICT by:

1. ***Identifying key technologies and equipment*** through government reviews and public-private partnerships to identify risk.

2. ***Ensuring minimum viable manufacturing capacity*** through strategic investment, where analysis has determined that the private capital market will not suffice, and through the creation of economic clusters.

3. ***Protecting supply chains from compromise*** through better intelligence, information sharing, and product testing.

4. ***Stimulating a domestic market*** through targeted infrastructure investment, as necessary, and ensuring the ability of firms to offer products in the United States similar to those offered in foreign markets.

5. ***Ensuring global competitiveness*** of trusted supply chains, including American and partner companies, in the face of Chinese anti-competitive behavior in global markets.

The white paper specifies five key and eight supporting recommendations to build trusted supply chains for critical ICT technologies:

- **Supply Chain 1:** Congress should direct the executive branch to develop and implement an information and communication technologies industrial base strategy.

- **Supply Chain 2:** Congress should direct the Department of Homeland Security, in coordination with the Department of Commerce, Department of Defense, Department of State, and other departments and agencies, to identify key information and communication technologies and materials through industry consultation and government review.

- **Supply Chain 3:** Congress should direct the Department of Commerce, in consultation with the Department of Homeland Security, the Department of State, and the Department of Defense, to conduct a viability study of localities fit for economic clustering. It should fund the Department of Commerce, in consultation with the Department of Homeland Security, Department of State, and Department of Defense, to solicit competitive bids and applications from candidate states, municipalities, and localities for the designation of no fewer than three and no more than five critical technology manufacturing clusters.

    - **Supply Chain 3.1:** The federal government should commit significant and consistent funding toward research and development in emerging technologies.

    - **Supply Chain 3.2:** The federal government should, in partnership with partner and ally governments, develop programs to incentivize the movement of critical chip and technology manufacturing out of China.

    - **Supply Chain 3.3:** Congress should direct the President to conduct a study on the viability of a public-private national security investment corporation to attract private capital for investment in strategically important areas.

- **Supply Chain 4:** The President should designate a lead agency to integrate and coordinate government ICT supply chain risk management efforts into an ongoing national strategy and to serve as the nexus for public-private partnerships on supply chain risk management.
    - **Supply Chain 4.1:** Congress should direct the President to construct or designate a National Supply Chain Intelligence Center.
    - **Supply Chain 4.2:** Congress should fund three Critical Technology Security Centers, selected and designated by DHS, in collaboration with the Department of Commerce, Department of Energy, Office of the Director of National Intelligence (ODNI), and Department of Defense.
- **Supply Chain 5**: The Federal Communications Commission (FCC) should tie 5G infrastructure investment to open and interoperable standards and work with the Department of Defense and the National Telecommunications and Information Agency to facilitate the release of more mid-band spectrum in order to ensure a strong domestic market for telecommunications equipment.
    - **Supply Chain 5.1:** The U.S. Agency for International Development (USAID) should work with international partners to develop a digital risk impact assessment that highlights the risks associated with the use of untrusted technologies in implementing digitization and telecommunications infrastructure projects.
    - **Supply Chain 5.2:** Congress should ensure that the Export-Import Bank (EXIM), U.S. International Development Finance Corporation (DFC), and United States Trade Development Agency (USTDA) all operate in legal, regulatory, and funding environments conducive to successfully competing with Chinese state-owned and state-backed enterprises, including their ability to support investments from companies headquartered in partner and ally countries.
    - **Supply Chain 5.3:** USAID, DFC, and USTDA should develop and maintain a list of prohibited contractors and clients, including companies subject to the Chinese national security and national intelligence laws, that may not be used to implement USAID-, DFC-, and USTDA-funded projects.

As we stated at the beginning, this strategy is tailored to ICTs, but similar efforts are needed for operational technologies and unique production areas. While those technologies fall outside of the scope of this white paper, many of the core materials and components discussed here are integral to critical technologies more broadly. Many of the recommendations contained in this paper therefore lay a firm foundation for technologies beyond ICT and will support efforts in those other areas.

Senator Angus King (I-Maine)
Co-Chairman
Cyberspace Solarium Commission

Representative Mike Gallagher (R-Wisconsin)
Co-Chairman
Cyberspace Solarium Commission

A. THE UNITED STATES' CRITICAL DEPENDENCIES

The United States lacks key industrial capacities crucial to the production of essential technologies, including fifth-generation (5G) telecommunications equipment. Among other factors, the willingness of countries such as China to subsidize and support their domestic industries has created the uneven playing field that hinders the competitiveness and, ultimately, the viability of U.S. companies in global markets. The resulting lack of industrial capacity has forced critical dependencies on companies that manufacture in adversary countries, such as China, where companies are beholden to Chinese national intelligence, national cybersecurity, and national security laws. While dependency on foreign production and foreign goods is not inherently bad—indeed, the United States relies on manufacturing and companies headquartered in partner countries such as Finland, Sweden, South Korea, and Taiwan—the U.S. government must emphasize the importance of trusted suppliers, and these dependencies pose three concrete risks to the security of the United States.

First, critical dependencies pose a threat to the consistent and reliable availability of raw materials, intermediate goods, and finished products that are crucial to the uninterrupted operation of the U.S. military, industrial base, and society. The continued reliance on foreign actors for raw materials and intermediate goods, or components that form the basic building blocks of technology, presents adversaries with points of leverage. In a time of crisis, these adversaries may seek to block access to these critical resources. Given the high percentage of raw material processing, semiconductor fabrication, and product assembly, testing, and packaging in East Asia, a future crisis or conflict that rendered the Pacific Ocean a high-risk trading route would starve the United States of critical components for everything from our consumer devices to our weapons systems. In addition, this "availability risk" limits U.S. freedom of action in peacetime by constraining our willingness to act against adversaries upon whom we are dependent or against those, like China, that could hold critical shipping lanes at risk.

The second major risk concerns the trustworthiness of equipment or components the United States receives from overseas. While vulnerabilities are a fact of technology in both hardware and software, vulnerabilities intentionally unaddressed or planted by adversaries in components or finished goods undermine the security and trustworthiness of the critical systems that rely on those products. It is important to acknowledge that building trusted supply chains cannot and should not replace continued efforts to secure infrastructure through design and cybersecurity interventions after products are deployed. Furthermore, the increased prominence of software-defined networking adds another layer of complexity to telecommunications and network architecture, enhancing the potential both to address hardware flaws and to introduce new vulnerabilities.[5] The physical location of a good's production and assembly is only one factor that may dictate the trustworthiness of a technology, but the physical access allotted to adversaries because of critical supply chain dependencies on companies and facilities in countries like China—particularly in the assembly, testing, and packaging stages of manufacturing—makes it easier to compromise technologies during their production.

Finally, these critical dependencies threaten to undermine American competitiveness and innovation in an age of global markets and rapid technological transformation, in part through facilitating forced technology transfer and intellectual property theft. Recently, China has placed great strategic emphasis on semiconductor manufacturing supremacy, leading to a sharp increase in production facilities based in China, even though China, which remains several generations behind the state of the art in semiconductor manufacturing, is heavily dependent on foreign semiconductor manufacturing equipment. Given this context—China's history of intellectual property theft and its institutionalized focus on indigenous innovation—Chinese chip manufacturing facilities present an excellent intermediary environment where the design of semiconductors developed by U.S. firms can be stolen and used in Chinese products. These practices enable Chinese companies to be

technologically competitive internationally, while bypassing the research and development costs incurred by semiconductor producers in the United States and elsewhere.[6]

An unfettered, open economy is critical for U.S. prosperity and innovation. However, national security considerations occasionally warrant government oversight or intervention in free markets. The U.S. government's responsibility to intervene in response to genuine national security imperatives is clear. From the country's earliest days, policymakers were determined that the United States must remain "independent [of] foreign nations, for military and other essential supplies."[7] The same necessity exists today.

B. THE STATE OF U.S. HIGH-TECH MANUFACTURING

A core part of promoting national cybersecurity is ensuring that the critical technologies that constitute and connect to cyberspace—as well as the building blocks of that equipment—are free from intentional compromise during their production. Among these critical technologies is the equipment needed to build networks, including 5G telecommunications equipment, as well as the devices that connect to those networks and underpin core aspects of our society, economy, and government. The manufacture and production of these critical technologies rely on a myriad of raw materials and intermediate goods. Put simply, when supply chains are less complex and more local, it is far easier and more efficient for the U.S. government to assist companies in protecting their supply chains from compromise. In assessing supply chain risk, it is therefore important to understand the current and potential capability of local manufacturing. The focus of this paper is ICT. Thus, while the discussions below on materials and semiconductors are broadly relevant, the subsection on ICT equipment is narrowly focused. Similar subsections could be written for operational technology, medical devices, weapons systems, and more, but those subsets of critical technology are beyond the scope of this paper.

1. MATERIALS

Raw materials used in the production of high-tech products, such as silicon, germanium, and other minerals, are found all over the globe. The United States sometimes mines and extracts these materials, though it often relies on other countries for their refinement and also imports them.

Silicon is a critical element used in creating semiconductor chips. Although it is one of the most abundant minerals in the world, it needs to be refined and processed to produce the high-quality materials used in telecommunications devices, a process in which East Asian countries largely specialize.[8] In 2018, China produced 4.8 million metric tons of silicon, far outpacing its next few competitors combined.[9] Nonetheless, the 430 thousand metric tons of silicon produced by the United States in 2018 came close to its total demand of 600 thousand metric tons.[10] While the United States exports some silicon, it imports far more—particularly from Russia, which accounted for 20 percent of total U.S. silicon imports between 2015 and 2018.[11]

Germanium, like silicon, is a semiconductor; but unlike silicon, which has a wide variety of applications, it is principally employed in electronic devices. Germanium is used to power fiber optic systems, infrared optics, satellite solar cells, and more. Thirty percent of germanium is produced from recycled materials, taken from such sources as the windows of older military vehicles or the manufacturing process for optical devices, which recovers much of the germanium that it uses.[12] It can be replaced with silicon metal, though at a cost to performance. The United States lacks the capacity to produce

germanium and has limited capacity to refine it for use in electronics systems, leaving the country with a critical dependence on foreign imports.[13] Between 2015 and 2018, 59 percent of U.S. imports of germanium came from China, which leads the world in the production of this mineral as well.[14]

Finally, the greatest shortfall is in rare earth elements (REEs) such as lanthanum, samarium, and terbium,[15] which improve conductivity and imbue hardware with special properties enabling peak performance; they are not found in abundance within the United States, leaving it with a critical dependence on other nations.[16] In the past, these materials, which are typically found in ores produced by other mining operations, were often discarded. But in the past decade, with the advent of smart technologies, they have become critical for semiconductor conductivity, display, and touch panel functionality; improved radio transmission; and fiber optics. United States defense platforms, from precision-guided missiles to Navy weapons systems, rely on REEs for critical components. Yet, while the United States might possess the ability to mine REEs, the extraction of REEs from ores is an extremely costly process that causes considerable environmental damage. For these reasons, the United States has fallen behind China, which has taken advantage of lower production costs, government subsidies, and fewer environmental restrictions, and has become dependent on them for its REE supply.[17] China is the leading REE supplier by a wide margin, followed by the United States, Estonia, South Korea, Malaysia, and Japan.[18] China in particular has geographic, political (especially around environmental regulations), and economic advantages in producing REEs and will likely not be overtaken by other nations for some time to come.

2. SEMICONDUCTORS

Semiconductors are a critical component for most technologies and a key building block for consumer electronics, communications and networking equipment, and the computers that control most industrial processes. A 2017 National Defense University publication highlighted the importance of semiconductors to national and economic security, recommending that the U.S. government "incentivize continued growth in the U.S. semiconductor industry."[19] Doing so remains imperative today.

The process of producing semiconductors has three phases: design; production; and testing, assembly, and packaging.[20] Two different types of semiconductor business models exist, followed by integrated device manufacturers (IDMs) and foundries, respectively. An IDM completes every step of the process in-house and operates its own fabrication plants.[21] Faced with increasing research and development costs—as well as costs associated with manufacturing—some companies have decided to focus their businesses on specific parts of the production process.[22] They therefore created what is known as the fabless-foundry model, in which firms fall into one of three specializations. Some companies solely design and market semiconductors; these are called "fabless foundries," because they lack fabrication facilities ("fabs") of their own.[23] Others are "pure-play foundries," which do not design semiconductors but manufacture the devices for fabless companies.[24] Finally, firms that specialize in the testing, assembly, and packaging area of production are known as outsourced semiconductor assembly and test firms (OSATs).[25]

Despite the prevailing narrative about Chinese technology domination and Chinese efforts to capture large swaths of global electronic markets, American companies are still global leaders in semiconductors.[26] However, the share of production in the United States has been in decline for the past ten years, and most new semiconductor manufacturing capacity is located outside the United States, as many U.S. companies have chosen to go fabless in order to stay competitive.[27] As of June 2020, "nearly 80 percent of semiconductor foundries and assembly/test operations are concentrated in Asia,"[28] and this number is expected to rise. By way of further example, in July 2020, Intel, which has traditionally produced its own semiconductors, placed a multibillion-dollar order with the Taiwan Semiconductor Manufacturing Company (TSMC) to outsource a portion of wafer fabrication.[29] Despite these trends, as of 2018, only 14 percent of semiconductors used in China were

produced by Chinese companies.[30] However, China's "Made in China 2025" plan seeks to change this reality by ensuring Chinese self-sufficiency in semiconductor fabrication and manufacturing by 2025. Although the Chinese market share for semiconductors remains relatively low and the country is unlikely to meet this goal within the specified timeline, the Chinese government's history of success in capturing markets—such as the telecommunications market, the solar industry, and the smartphone market[31]—and in building industrial capacity is cause for concern.

3. FINISHED ICT EQUIPMENT

Information and communications technology equipment includes networking equipment for both radio access networks (RANs) and local area networks (LANs), such as modems, routers, circuit-switch systems, and base transceiver stations. Most companies that produce this equipment differ from semiconductor IDMs in that they get most or all of the components that make up their products from third parties. The global telecommunications equipment integrator market has consolidated over the past 15 years as bigger incumbent firms have achieved economies of scale. Among the main players left in this market are Cisco, Ericsson, Nokia, Samsung, and companies subject to China's national intelligence law, like Huawei and ZTE.[32] Today, the United States is highly reliant on the services and products of international suppliers in this industry. Cisco, the only remaining major telecommunications equipment manufacturer in the United States, does not provide all the equipment necessary to build a telecommunications network; as a result, most telecommunications providers rely on Nokia and Ericsson as their primary equipment suppliers,[33] though Samsung is making inroads in the United States through a contract with Verizon.[34] Like nearly all telecommunications equipment companies, Cisco, Nokia, Ericsson, and Samsung maintain diverse and regionalized global supply chains but manufacture some of their products in China, though many have moved or have pledged to move the production of their U.S. supply out of China.

Standards are critical both to the development of new telecommunications equipment and to the competitiveness of firms developing and manufacturing those technologies. Despite their importance, the U.S. government's participation in technical specification and standards organizations in the past decade has waned—and where it does continue to engage, it has been less effective. This is true of bodies such as the International Telecommunication Union (ITU), the UN specialized agency focusing on ICT issues, and the 3rd Generation Partnership Project (3GPP), a group of standards organizations developing protocols for 5G. The lack of robust and effective U.S. government participation has allowed adversaries, especially China, to fill the gap, shaping technology standards in ways that undermine interoperability and do not promote a shared, democratic vision for technologies moving forward. In 5G, China has undertaken a massive effort to set and influence standards; it has dedicated significant government resources to coordinate with industry and supported companies in submitting standards that favor its preferred approach, including sending huge delegations to standards meetings and providing financial rewards for standards adopted and leadership positions gained.[35] The ITU is itself headed by a Chinese representative; and where Chinese participation in groups like 3GPP has increased,[36] the U.S. government has abdicated its leadership role in the standards processes, leaving U.S. companies and partner industries to fend for themselves.

The development of standards often equates to the ownership of patents for that technology. While there is debate about whether Chinese companies like Huawei are leading the race for 5G standard-essential patents,[37] they are likely submitting the most patents for this technology. With this devotion to success, backed by huge research and development budgets, China will continue to seek to position itself for long-term leadership in 5G. Huawei and others have effectively co-opted standards bodies to undermine interoperability between different vendors. The resulting difficulties in switching vendors for companies seeking to upgrade from 4G to 5G equipment have solidified Huawei's incumbent position as the dominant producer in the market for telecommunications devices.[38]

The Story of Lucent Technologies

As recently as 2000, the United States was home to the world's largest supplier of telecommunications equipment: Lucent Technologies. Throughout the 1990s and early 2000s, Lucent was a powerful integrator, producing everything from semiconductors and other components to finished network technologies. In 2000, Lucent's revenues surpassed $40 billion, eclipsing its nearest competitors by nearly $10 billion.[39] Built on the back of the storied Bell Laboratories, Lucent Technologies was the global leader in network technologies. However, from 2000 to 2006, poor management and steadily declining revenue ultimately resulted in a merger with the French telecommunications equipment provider Alcatel.[40] A series of questionable business decisions led Alcatel-Lucent to gradually cede its incumbent advantage as a network technology provider, as it failed to keep pace with Nordic and Chinese competitors that were able to innovate faster and bring cheaper and more advanced technology to market sooner.[41]

At its height, Lucent's robust manufacturing capability supplied more than just finished network equipment: it provided the component parts for a myriad of electronics, including semiconductors.[42] With the demise of Lucent Technologies, the United States lost more than just a telecommunications equipment provider—it lost its only true integrator. Today, while U.S. corporations such as Intel, Micron, Texas Instruments, and Globalfoundries retain some semiconductor fabrication capability in the United States, all of these companies also manufacture overseas, and "most new semiconductor manufacturing capability is located outside of the United States."[43]

C. THE IMPORTANCE OF PARTNERS

The United States cannot achieve a more secure supply chain and remain competitive on its own. The U.S. government cannot succeed without the private sector, and the country as a whole cannot succeed without a strong network of allies and partners. It must leverage existing public- and private-sector allies and partners at home and abroad to ensure the security of its critical technology supply chains. While the United States must build its domestic manufacturing capacity, it will continue to be reliant on a trusted zone of suppliers, assemblers, packagers, and testers for high-tech goods. This means it must strengthen ties with partners that share similar goals, such as moving the supply chain for critical components out of untrusted nations or not relying on critical infrastructure technologies that come from untrusted nations. When building partnerships, the United States needs to be cognizant of the following principles: (1) trustworthiness, (2) the influence of China, (3) the impact of geography, and (4) stability.

1. CORE PRINCIPLES FOR STRENGTHENING PARTNERSHIPS

As the advent of 5G network technology has shown, ensuring the trustworthiness not only of technologies but also of the nation-states upon which the United States relies for parts of its ICT supply chain is of utmost importance for cybersecurity. The United States has existing and potential partners with capacity: Japan, South Korea, Taiwan, Sweden, Finland, and the United Kingdom. In addition to these core partners, the United States should look for additional allies or partners that are relatively free from Chinese influence, including Chinese economic policy and Chinese military positioning. When identifying new partnerships, the United States should take a risk-based approach, prioritizing relationships with those nation-states that are physically closer to the United States, thereby lessening the potential for disruption by the closure of overseas trade routes, and those countries with existing facilities within U.S. territory. Geography should be considered, to ensure not only access but also a diversity of manufacturing hubs around the world. A wide range of geographic locations of manufacturing will ensure that if a natural disaster, war, or other crisis damages a manufacturing plant, production can continue elsewhere, thereby minimizing the risk of disruption. Stability is also important for any new partner state that is participating in the high-tech supply chain. For example, while some countries in South America, Southeast Asia, or eastern Europe might

have friendly regulatory and economic environments for production, the long-term benefits of locating manufacturing in these areas might be outweighed by risk of disruption due to ongoing conflicts, irregular economic policy shifts, and lack of government oversight.

The Five Eyes countries, members of the North Atlantic Treaty Organization (NATO), allies and partners in southeast Asia, and trade partners in the Americas are natural allies in facilitating this process. Though geography is one important factor when considering partners, it is not the only factor, and the overall state of U.S. political and trade relationships with countries in these spheres is of paramount importance in any efforts to build trusted supply of critical technologies and encourage continued innovation and competitiveness. A first step for building a strong foundation of partnership is to critically assess the criteria for partnership and the matrix of what partner countries should look like.

2. LEVERAGING PARTNERSHIPS TO IMPROVE SUPPLY-CHAIN SECURITY

To best leverage existing and new partnerships to improve supply-chain security, the United States should first increase collaboration with allies and partners in developing critical technologies. There are examples of the United States' collaborating with allies and partners, in both the civilian and military spaces, to develop critical technologies and working with like-minded partners to establish international norms that promote security and stability in advanced technology. In the civilian arena, the creation of the imaging and particle-detecting instruments for NASA's twin Solar Terrestrial Relations Observatory (STEREO) spacecraft highlights how the United States has collaborated with its allies to make best use of individual comparative advantages to increase efficiency and minimize costs. To enable this mission, scientific institutions in the United States, United Kingdom, France, Germany, Belgium, Netherlands, and Switzerland collaborated in the design and build of the imaging and particle-detecting instruments that would be attached to the spacecraft and enable STEREO to achieve its mission objective.[44] In the military space, the collaborative construction of the Lockheed Martin F-35 aircraft by 10 countries and more than 1,500 global suppliers suggests the capability of the United States to successfully work together with its allies to develop critical technologies.[45] As in these examples, the U.S. government should encourage collaboration with allies and partners for the development of emerging and next-generation technologies to create a network of trusted suppliers globally by fusing the innovation prowess of the United States with that of its allies and partners.

Second, the United States, jointly with partners and allies, should increase its participation and leadership in international standards-setting bodies to ensure the security of standards and protocols. In recent years, China has taken active measures to increase its impact in standards-setting bodies, by acquiring leadership roles and submitting the majority of standards proposals in areas such as 5G. The United States cannot afford to let adversarial countries like China set the agenda. A lack of participation from the United States, as well as partners and allies, comes with the risk that the standards created will be less secure.

Third, the United States must work with allies and partners to withstand increasing economic and military pressure from China. This trend highlights the growing need to ensure that U.S. allies and partners continue working together to maintain high standards of trustworthiness, stability, and freedom from Chinese influence. Although a significant portion of the U.S. supply chain is located outside of China, many critical production zones are still located within the sphere of Chinese influence. Allies in these areas, while not always friendly toward China, have experienced significant negative effects from aggressive Chinese economic policy and military activity. For example, Taiwan is a key supplier and foundry location for semiconductors used in U.S. advanced technologies. Proximity and economic entanglement make Taiwan more likely to bend to Chinese influence than to that of the United States and of U.S. allies, another means of introducing risk into the U.S. supply chain. Similar issues exist with regional allies Japan, South Korea, and the Philippines.

The Importance of Taiwan

Taiwan is an example of the complex economic and security relationships that are intertwined in our ICT supply chain. Today, the United States and China both depend heavily on the production of semiconductors by the Taiwanese chip manufacturer Taiwan Semiconductor Manufacturing Company. Because most new semiconductor manufacturing capacity is located outside the United States, the United States increasingly lacks the semiconductor manufacturing capacity necessary to meet its own demand.[46] The U.S. government and American firms depend on TSMC to provide the silicon chips crucial for the production of critical U.S. civilian and military applications, from personal computers and smartphones to drones and satellites. In the first quarter of 2020, TSMC had a market share of 54.1 percent in the global semiconductor foundry market.[47] In the coming years, this market dominance is expected only to grow, as TSMC plans to play a key role in the supply chain for 5G technology by increasingly focusing on the development of smart semiconductors.[48]

In recent years, China has combined its persistent security and political pressure on Taiwan with financial pressure as it has increased its trade and investment, creating economic dependency all as part of its strategic goal of reunification.[49] In 2018, Taiwan depended on the United States for 11.8 percent of its total trade and on China, its largest trading partner, for 23.9 percent.[50] Similarly, analysts estimate that while around 60 percent of TSMC's revenue came from customers based in North America, over a fifth of its revenue was from companies headquartered in China such as Huawei, suggesting strong trade relations with the mainland.[51] Until recently, Huawei was TSMC's biggest customer after Apple,[52] although TSMC stopped shipping to Huawei in September 2020 and has not taken orders from Huawei since May 2020.[53] TSMC is further entangled with China, as some of its chip production facilities operate within China's borders.[54] Should a choice have to be made between the United States and China in a crisis, proximity and the current economic entanglement between the mainland and Taiwan and its firms make the outcome uncertain. The current influence of China on Taiwan, together with the United States' critical dependence on TMSC for the near future, makes clear the importance of Taiwan to both countries and the need to minimize China's influence on Taiwan. Any United States effort to further integrate its supply chain with Taiwan will need to recognize these deep economic ties to China, and require a joint U.S.-Taiwan effort to determine what steps need to be taken to reduce this influence and protect United States supply chain integrity and security as we continue to partner with Taiwan. Conversely, such an effort may also need to include changes in U.S. security policy to create a more credible, and possibly formal, bilateral partnership than currently exists.[55]

D. STRATEGY FOR SECURING AMERICA'S ICT SUPPLY CHAIN

Economic coupling with East Asia on technology manufacturing has been enormously fruitful, bringing greater manufacturing efficiencies, driving down the cost of technologies, and yielding innovation. Yet this coupling has also resulted in supply chain dependencies that pose concrete risks to U.S. national security, which have the potential to undermine the availability and trustworthiness of critical technologies and hinder U.S. competitiveness in global markets. Understanding these dependencies is crucial to identifying vulnerabilities, determining risks, and, where appropriate, executing mitigation policies.

Numerous departments and agencies of the executive branch have projects and programs under way that strive to address pieces of the challenge. The Department of Homeland Security's ICT Supply Chain Risk Management Task Force, for example, brings stakeholders from the ICT industry together with relevant federal departments and agencies to develop a framework for information sharing, build threat-based evaluation schema for ICTs, identify market segments and evaluation criteria for government procurement, and produce policy recommendations to incentivize the purchase of ICT from trusted sources.[56] In addition, the State Department,[57] the National Counterintelligence Security Center,[58] the Department of Defense, and the National Institute of Standards and Technology[59] provide separate guidance for supply chain risk

management. Similarly, numerous proposals from Congress have authorized programs to steer investment to building a trusted supply base (see the text box below). Yet the United States lacks a clear overarching strategy to guide all of these activities, leading to confusion, causing inefficient allocation of resources, and threatening to undermine progress toward the very goals these efforts profess to achieve.

The United States' primary competitor in this context, China, does have a strategy. Guided by Made in China 2025,[60] China Standards 2035,[61] and the Military-Civil Fusion,[62] China has effectively seized considerable market share in several critical technologies and components through a mix of investments; engagement in international forums, especially those that set standards; and other protectionist policies. To be clear, this is a strategy to dominate these markets through autarky, not a strategy to decouple and limit risk.

In its March 2020 report, recognizing the imperative to compete with growing Chinese economic prowess in these technologies and components and to build more secure supply chains, the Commission recommended that **Congress should direct the U.S. government to develop and implement an information and communications technology industrial base strategy to ensure more trusted supply chains and the availability of critical information and communications technologies**.[63] This strategy must be underpinned by a series of principles that guide all underlying policies, activities, and funding and ensure coordinated effort, with all participants pulling and pushing in the same direction. These efforts

Supply Chain Proposals in Congress

Congress has begun to act on supply chain security. According to the U.S.-China Business Council, nearly 400 pieces of China-related legislation have been introduced in Congress.[64] Of those proposed bills, more than 60 pertain to supply chain security. Parts or all of several of these proposals are likely to pass; of particular note are the Creating Helpful Incentives to Produce Semiconductors for America Act (CHIPS Act),[65] the American Foundries Act,[66] the Utilizing Strategic Allied (USA) Telecommunications Act,[67] the Secure 5G and Beyond Act,[68] and sections of the FY2021 National Defense Authorization Act.

The FY2021 NDAA advances many of these proposals by proposing the creation of several programs and funds to stimulate semiconductor and telecommunications equipment production and alternatives to Chinese suppliers, as well as advancing American participation in international standards bodies. The creation of a wireless technologies security fund, including a multilateral fund in coordination with foreign partners, would increase research and development spending targeted at critical ICTs.[69] In addition, a suite of semiconductor-related clauses creates programs and grants to advance semiconductor research and development, mandates a study to understand the capacity of the U.S. industrial base to produce semiconductors, and codifies prohibitions relating to foreign adversaries.[70] The clauses of the FY2021 NDAA pertaining to PCBs seek to lessen dependence on adversarial countries for these compounds used in critical defense technologies by creating a certification program.[71]

Additional sections in the Senate version call for an assessment of critical technology trends pertaining to artificial intelligence, microchips, and semiconductors and related supply chains.[72] The House calls for reports on rare earth material supply chain security and supply chain cooperation with Taiwan, as well as assistance for small manufacturers in the defense industrial supply chain on matters relating to cybersecurity.[73] While these actions should help secure the United States' ICT supply chains, the lack of a coherent strategy will likely result in programs that are disjointed, inefficient, and unable to work in coordination to meet America's most pressing challenges.

must be supported by robust and meaningful partnerships with American industry, state and local governments, and partner countries. This is not a matter of conscious coupling or decoupling with China. Rather, a strategy to secure the United States in the digital age and beyond must ensure that the United States can create an environment that assures American security against adversary actions and allows American and partner companies to compete with and succeed against state-owned and state-backed enterprises.

Actionable recommendations are highlighted in bold in this section, and a full list of recommendations, explained in greater detail, can be found in Annex I.

1. IDENTIFY KEY TECHNOLOGIES AND MATERIALS

As a first step toward securing supply chains and enabling U.S. competitiveness, the U.S. government must work with industry, partner countries, and state and local governments to identify key equipment and the components and materials required for its assembly. **Congress should direct the Department of Homeland Security, in coordination with the Department of Commerce, Department of Defense, and Department of State, to identify key technologies and materials through industry consultation and government review.** This equipment is likely to include weapons systems and telecommunications equipment, as well as general purpose computing equipment. Some components, like semiconductors, are more complicated to produce and require more technical manufacturing capability. Because of this complexity, these types of components are likely to require standing, specific manufacturing capability, as it may not be feasible to repurpose existing manufacturing. Other components, such as packaging, wires, and other conductors, are simpler to produce, and existing manufacturing can likely be repurposed in a time of crisis to meet U.S. needs. Efforts should leverage and build on existing efforts, including those by the Department of Homeland Security (DHS), to create a common taxonomy of the hardware, software, and services that collectively underpin the connected world.[74]

On critical minerals, efforts should build on existing initiatives, including that of the National Science and Technology Council (NSTC) Critical Minerals Subcommittee (CMS), which has been working to develop "policies, procedures, and plans relating to identification and forecasting of mineral criticality, and risk mitigation in the procurement and downstream processing of minerals identified as or forecasted to become critical."[75] The federal strategy calls for the convergence of state and federal policy, public-private partnerships, science, information sharing, and new approaches. As directed by Executive Order 13817,[76] the Department of the Interior, working together with other executive branch agencies and taking comment through the CMS, developed a critical minerals list. Published in 2018, it identified 35 critical minerals, including germanium and the rare earth elements group.[77]

2. ENSURE MINIMUM VIABLE MANUFACTURING CAPACITY

Following the identification of key technologies and materials, the U.S. government must implement a plan to establish minimum viable capacity to produce the most critical components and finished products to ensure their availability in a time of crisis. Separate from building a strategic reserve of components or equipment, the United States should strive to build the latent manufacturing capacity and expertise required for the continued production of critical components and equipment in a crisis. That several American car manufacturers could switch during the COVID-19 pandemic from producing and assembling car parts to building respirators is a prime example of the importance of reserve manufacturing capacity. The decline in U.S.-based semiconductor manufacturing capability could prove problematic during any event, such as a war or natural disaster, that cuts off the supply chain from abroad. In such a scenario, the United States does not have the capability to ramp up sufficient front-end manufacturing to keep up with the demand. This issue could be partly addressed by locating manufacturing in more areas of the country; however, even this geographic diversity would not fully resolve the problem. Nonetheless, as the National Security Telecommunications Advisory Committee notes in a 2019 report, a "strong

Challenges to Reinvigorating American High-Tech Manufacturing

Three main challenges confront attempts to rebuild U.S. high-tech manufacturing capacity: (1) lack of patient funding capital, (2) high investment barriers to entry, and (3) standards and intellectual property barriers to entry. These challenges arise from the simple fact that the economics of the hardware industry are not as attractive as those of many other technology sectors. One of the major shortcomings of U.S. efforts to date to secure ICT supply chains is their failure to address how the United States got to this point, where ICT equipment manufacturing and production is a critical economic weakness. In order to craft an effective strategy to rebuild high-tech manufacturing and gain greater industrial independence, policymakers must first understand the challenges to reinvigorating the United States' high-tech manufacturing industry. Only then can they comprehend why market forces have pushed U.S. high-tech industrial capacity to atrophy over the past two decades and recognize the issues that they must tackle in developing an industrial base strategy.

The first challenge is that of patient capital.[78] While private capital is flowing into some kinds of technology, firms on the cutting edge of hardware development and manufacture in the United States face a competitive market for financial capital. In 2019, for the second straight year, the venture capital ecosystem invested over $136 billion in U.S. companies.[79] However, a meager 2.8 percent, or $3.8 billion, was invested in hardware, a symptom of a growing long-term trend. Whereas hardware investment has faltered, software and biotech have seen steady increases year over year.[80] When other viable options for short-term profitability, higher profit margins, and overall greater return on investment exist, patient capital from private funders dries up for hardware.[81] Today, the financial capital market for high-tech investment in the United States reflects these conditions. In short, challenge number one for policymakers is to assist a market for patient capital directed to long-term investments in hardware and other critical technologies.

Second, manufacturing, with its high capital and start-up costs, typically favors incumbent firms and presents obstacles to businesses attempting to break into the market. As the high-tech manufacturing center of gravity pivoted to Asia in the 2000s, to stay competitive many American and European firms shifted portions of their manufacturing and production to Chinese factories. Today, although U.S. companies enjoy a large share of the overall market share for semiconductors, the share of global semiconductor manufacturing that takes place in the United States is just 12 percent.[82] While the loss of semiconductor fabrication capability is just cause for concern, the challenges for the electronics supply chain are compounded by the fact that "[f]oreign markets accounted for 83% of semiconductor sales by U.S.-headquartered firms in 2015,"[83] meaning that much of the integration of semiconductors into final products takes place outside of the United States. Myriad factors contribute to this concentration of assembly and production; some are benign, such as cheaper labor, supply chain advantages, and investment in automating manufacturing,[84] while others are more malicious, such as protectionist economic policies, intellectual property theft, and patent violations.[85]

The byzantine amalgam of international and industry standards as well as patent laws poses a third challenge for new entrants to the telecommunications equipment market that U.S. policymakers must consider. When a firm patents a technology that becomes popular or a standard, it establishes licensing agreements to allow other firms to use that technology. Standards-setting bodies attempt to mitigate the monopoly power that can arise from an actor holding standards-essential patents,[86] but technology-licensing agreements can be lucrative and are an important incentive for companies to innovate.[87] However, any new entrants to the telecommunications equipment market encounter established firms already sitting on top of the powerful revenue streams that derive from being a patent holder and a dominant voice in establishing standards. More subtly beneficial than the impact of standards-essential patents is the opportunity enjoyed by incumbent firms to shape the technological landscape to their advantage by their ability to promote standards that will be most compatible with their own technology.[88]

None of these barriers are insurmountable, but the reality is that the United States has lost much of its market share for the manufacture of electronics components and nearly all of its market share for the manufacture and assembly of finished electronics products. Nonetheless, a U.S. strategy to secure its ICT supply chain from all threats must include a plan to identify the key technologies and materials, and then attract more patient investment in hardware manufacturing, devise a method to retrain the atrophied muscles of production, and set the conditions to overcome barriers to entry posed by the constraints of standards and intellectual property.

semiconductor industry [is] critical to ICT resiliency . . . [but] the U.S. leadership position is threatened by several factors," including "the laws of physics . . . [pushing] the boundaries of Moore's Law" (limiting the potential for further innovation); Chinese gains in semiconductor manufacturing, due in part to relaxed environmental regulations; and an aging scientific and high-tech manufacturing workforce in the United States.[89]

In the past—including during its founding era—when America recognized critical shortcomings that could harm national security and were unlikely to be adequately addressed by markets, it took measures to shape those markets and production toward more optimal outcomes.[90] In some cases, as in the early formation of Silicon Valley or SEMATECH, government interventions have been light. In others, as in establishing the Tennessee Valley Authority and the Radio Corporation of America, more heavy-handed approaches have yielded positive returns.[91] Today, although U.S. companies are increasingly moving their manufacturing to other countries in pursuit of cost savings, some high-tech manufacturing capability remains in the United States. The first pillar of a strategy to ensure minimum viable manufacturing capability must center on retaining this capacity. It is unlikely to be fully sufficient, however, and the U.S. government must be prepared to put incentives in place to further grow manufacturing capacity and encourage U.S. and global firms to move production to the United States and other partner countries. In doing so, it must create a regulatory and business environment that promotes cost savings, allowing non-monopolies and non-integrated device manufacturers to benefit from the same economies of scale enjoyed by Chinese integrators and government-backed monopolies.

The U.S. government should strive to encourage the continued viability of domestic high-tech manufacturing by intervening with a light touch to set the conditions in which innovation and industry thrive, incentivizing the creation of economic clusters, or "agglomeration economies," in given geographic areas both in the United States and in partner and ally countries. Agglomeration economies enable firms in related industries to benefit from economies of scale as they cluster together, a move that translates into cost savings and greater efficiency in production.[92] Colocation of firms that produce critical components, such as semiconductors, wiring, and casing, with the firms that produce finished products, such as routers and switches, enables each member of the ecosystem to enjoy lower costs of production and higher marginal returns on its investments. Furthermore, economic clusters are likely to yield higher levels of innovation due to the social and business networks that naturally arise from proximity. For this approach to succeed, several core industries must be present to support the clustered industry. In most cases, these industries include the marketing industry as well as the financial and accounting sectors. In the United States, most major metropolitan areas possess robust marketing, financial, and accounting industries, so this requirement should not be a barrier. In addition, a cluster must have anchor institutions, like an industry leader or a research university, around which to develop.

To realize this strategy of building economic clusters for critical technologies, **Congress should direct the Department of Commerce, in consultation with the Department of Homeland Security, the Department of State, and the Department of Defense, to conduct a viability study of localities fit for economic clustering.** To build these clusters, **Congress should fund the Department of Commerce, in consultation with the Department of Homeland Security, Department of State, and Department of Defense, to solicit competitive bids and applications from candidate states, municipalities, and localities for the designation of no fewer than three and no more than five critical technology manufacturing clusters.** The U.S. government, working with states and localities, must then set the conditions under which colocation is incentivized and clusters thrive. Doing so requires a mix of special economic protections, such as tariffs and foreign trade zones, and incentives, such as tax breaks, government grants, and research and development investment.

Several mechanisms are already proposed or exist that could support such investment. The CHIPS for America, American Foundries, and USA Telecommunications Acts, elements of which are in the House and Senate drafts of the FY2021

National Defense Authorization Act, provide mechanisms to unlock key public investment in wireless technology, advanced manufacturing capability, and semiconductor manufacturing.[93] In addition, the federal government should **commit significant and consistent funding toward research and development in emerging technologies** to prevent future overreliance on untrusted technology, as the Commission recommended in March 2020.[94]

Finally, these efforts should be coupled with leveraging existing capability or incentivizing foreign firms to build additional or backup facilities in the United States. These firms should possess relevant patents, expertise, and infrastructure. **The federal government should, in partnership with partner and ally governments, develop programs to incentivize the movement of critical chip and technology manufacturing out of China**. Japan, for instance, recently created a government subsidy for companies that agree to shift production out of China. To that end, Japan's government set aside roughly $2.2 billion as part of a COVID-19-related economic stimulus package, as it found critical dependencies on China unsustainable.[95] This package is an attempt to move high-added-value product manufacturing back to Japan and to move other production across Southeast Asia.

The U.S. government has two options to incentivize movement out of China. First, Congress could create a dedicated fund for a grants program to provide incentives to companies for projects that move manufacturing out of China and into the United States.[96] Alternatively, Title III of the Defense Production Act (DPA) allows federal entities to provide loan guarantees to private actors "in support of production capabilities or supplies" deemed "necessary to create, maintain, expedite, expand, protect, or restore production and deliveries of services essential to the national defense."[97] Federal agencies may also provide loans directly to private businesses (including nonprofits) to create, expand, protect, or restore "capacity, the development of technological processes, or the production of essential materials," if that loan will address "current or projected shortfalls of industrial resources, critical technology items, or material essential for the national defense."[98] The executive branch could use the DPA's Title III authorities to subsidize the movement of critical chip manufacturing out of China.

While many of the interventions described here require robust commitment by the government, and while the U.S. government possesses considerable financial power, the scale of investment needed to reinvigorate American high-tech manufacturing and facilitate the movement of critical production, manufacturing, assembly, and testing into partner countries likely outstrips both the U.S. government's financial capacity and the U.S. taxpayer's willingness to subsidize such efforts. In short, while the U.S. government must signal a stake in these investments, success in this endeavor will require unlocking private capital. To do so, **Congress should direct the President to conduct a study on the viability of a public-private national security investment corporation to attract private capital to strategically important areas for investment.** The public-private investment partnership should not rely on public funding but rather should serve as a clearinghouse for private investment with opportunities for government guarantees on debt or equity.

3. PROTECT SUPPLY CHAINS FROM COMPROMISE

The United States and its partners may never decouple from adversaries like China and are likely to continue to source critical components and technologies from countries within the reach of its adversaries. The U.S. government should recognize these dual realities and devise a strategy to identify concrete risks to our supply chains and mitigate them through intelligence and information sharing as well as product testing.

Domestic Efforts to Reduce Risk and Minimize Vulnerability

The U.S. government, as well as the private sector, must continue to engage in supply chain risk management efforts to reduce its risk and minimize vulnerability. There are a variety of efforts already under way to improve supply chain risk

management, led both by the government and by the private sector. These projects are focused on collaborating to identify critical knowledge of vulnerabilities, determining where additional research is needed, and developing new strategies to address existing risks. The government-led initiatives involve a wide range of strategies, task forces, advisory committees, and programs to study supply chain risks and approaches to mitigate them. These strategies and programs, which should be assessed and consolidated where possible under a single vision, include DHS's Cybersecurity and Infrastructure Security Agency's Information and Communications Technology (ICT) Supply Chain Risk Management Task Force and 5G strategy,[99] the President's National Security Telecommunications Advisory Committee,[100] DoD's Cybersecurity Maturity Model Certification (CMMC) and 5G strategy,[101] the Department of State's Clean Network program,[102] and the National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management (C-SCRM) program.[103] At the same time, many industry associations, including the Information Technology Industry Council, the Semiconductor Industry Association, and the Telecommunications Industry Association, are also intensely studying the supply chain risks for their specific sectors to minimize them.

The problem here is not the lack of a strategy or priorities, but rather too many different strategies and too many "number one" priorities. **The President should designate a lead agency to integrate and coordinate civilian and government ICT supply chain risk management efforts into an ongoing national strategy and to serve as the nexus for public-private partnerships on supply chain risk management.** In addition to a lead department or agency, a National Cyber Director, as recommended by the Commission,[104] would play a crucial role, serving as the nexus for the issue within the White House and a key intermediary with the private sector.

Better Supply Chain Risk Intelligence and Information Sharing

To better protect the supply chain, the United States government must work with allies and partners to improve its capability to collect and disseminate intelligence on supply chain risks. This information is critical not only to government agencies but also to private-sector stakeholders, who own and operate 85 percent of the nation's critical infrastructure.[105] Without the information required to fully understand the risks, the private sector will not be able to implement comprehensive strategies to address the potential for compromise.

In order to begin addressing this gap, the Supply Chain and Counterintelligence Risk Management Task Force was established within the Office of the Director of National Intelligence (ODNI) as part of the FY2020 National Defense Authorization Act.[106] The goal of this task force is to improve the U.S. intelligence community's ability to provide supply chain intelligence, specifically for U.S. government acquisition. As it works with private-sector entities to identify both their needs and their mechanisms to improve information sharing on supply chain risk, the supply chain task force should leverage the ongoing work and findings of the DHS-led ICT Supply Chain Risk Management Task Force.[107] Finally, the task force should work toward understanding and defining additional ways that the U.S. government can make greater use of publicly available and proprietary sources in informing supply chain and foreign investment risk assessments.

In addition to the work of the Supply Chain and Counterintelligence Risk Management Task Force, **Congress should direct the President to construct or designate a National Supply Chain Intelligence Center.** The Center, which could take the form of either a new or existing structure, should be designed to integrate supply chain intelligence efforts from across the federal government with those of other public and private partners and should serve as the central and shared knowledge resource for threats to supply chain activities or supply chain integrity. As part of the process of creating the Center, Congress should direct the President to conduct a review of existing intelligence authorities for major departments and agencies and assess whether any departments and agencies currently lacking Title 50 intelligence authorities should be granted them.

Device and Technology Security Testing

Testing the security of devices and technologies is critical to determining the vulnerabilities of products and the strategies to mitigate those vulnerabilities. To gain insight into the security and testing practices of suppliers, the U.S. government must engage with companies that develop the technologies underpinning our networks and critical infrastructure. Some of the national laboratories currently have programs that do just this by testing and red-teaming products and networks, such as Sandia National Lab's Information Design Assurance Red Team (IDART) and Idaho National Lab's Wireless Test Bed.[108] These kinds of government-sponsored security testing programs provide valuable information about vulnerabilities and risks associated with specific technologies that can help reduce overall vulnerability. As more advanced technologies continue to be brought online, it is critical to promote and expand similar efforts to secure both new and existing systems and to evaluate the security practices of suppliers—but the government must go one step further. It must establish centralized research entities to test the security of products, help identify vulnerabilities and develop mitigation measures, and support efforts to certify the security of critical technologies.

To this end, the Commission has already recommended that **Congress fund three Critical Technology Security Centers, selected and designated by DHS, in collaboration with the Department of Commerce, Department of Energy, ODNI, and DoD**.[109] These centers would comprise a Center for Network Technology Security to test the security of hardware and software, a Center for Connected Industrial Control Systems (ICS) Security to test the security of ICS and other connected industrial equipment, and a Center for Open-Source Software Security to test for vulnerabilities in open-source software repositories, which serve as the foundation for most of today's software.

Bans of and Tariffs on Critical or Pervasive Technology

In order to ensure that trade policy is aligned with critical national security goals, the U.S. government should critically assess the use of tariffs. In recent years, the United States has sought to implement tariffs on select products in an attempt to incentivize companies to move their supply chains to the United States. In particular, the Trump administration has explored placing tariffs on high-tech imports in a strategic effort to reduce critical supply chain dependencies on foreign nations.[110] There are costs and benefits to heavy reliance on these tools, especially if they are being employed without a clear and cohesive strategic purpose. Indeed, tariffs have failed to entice businesses to move supply chains stateside and have led other countries to impose costly retaliatory tariffs further harming U.S. industry, leading to an estimated reduction of real GDP by 0.5 percent in 2020.[111]

In addition to tariffs, the United States has tried bans on particular brands and products both for commercial and civilian use and for government use, targeting untrusted telecommunications companies on the grounds of their threat to cybersecurity. Thus in 2019 Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, imposed a broad set of restrictions on the purchase and use of telecommunications equipment from a company owned by a "foreign adversary."[112] Though the ultimate goal of bans is to restructure the international market to favor trusted companies, the actual result is still too early to assess, as some U.S. allies are moving away from suppliers seen as untrusted while others are continuing to use their services. In addition, for 5G mobile networking equipment, bans made sense as a way to significantly reduce foreign cyber espionage prospects and eliminate U.S. dependence on foundational technologies fraught with vulnerabilities. Yet the United States has failed to provide cost-effective alternatives to Chinese giants like Huawei even as it tries to persuade its international allies and partners with whom it shares intelligence to follow the same path.

A core strategic principle for the United States in this space should be to incentivize the use of trusted partners and suppliers at every stage of the U.S. ICT supply chain in order to enhance the cybersecurity of end products and the networks on

which they rely. None of this is to say that either existing punitive mechanism is completely useless: both have the potential for long-term impact if they are part of a broader and cohesive strategy to secure the U.S. ICT supply chain. But if policymakers are going to continue using these tools in the future, it is necessary to assess the impacts of their use and perhaps adjust policy tools accordingly. Pairing more punitive tools like tariffs and bans with incentives and widening the scope of trusted international partners might provide a more viable path forward.

4. STIMULATE A DOMESTIC MARKET

The U.S. government can take steps to bolster demand at home for critical technologies, including network technologies. Domestic infrastructure investment and greater public investment in the area can provide a significant boost to productivity in the long run by improving the public capital stock.[113] To do so, **the Federal Communications Commission (FCC) should tie 5G infrastructure investment to open and interoperable standards and work with the Department of Defense and the National Telecommunications and Information Agency to facilitate the release of more mid-band spectrum in order to ensure a strong domestic market for telecommunications equipment.** Advanced industrial economies like the United States must focus on repairing and replacing aging infrastructure to help enhance the country's overall productivity levels. The FCC should require that all infrastructure purchased through projects funded by the Universal Service Fund and related programs must conform to open and interoperable systems standards and guidance, including proposals of the Open Radio Access Network (ORAN) Alliance, the Open Networking Foundation (ONF), 3GPP, and the Telecom Infra Project (TIP). As the name suggests, the ORAN approach to building out new networks relies on an open plan that will not lock in buyers to a single proprietary vendor. This approach diversifies the supply chain, allowing integration of different vendors for 5G hardware and software solutions. Ultimately, it creates opportunities for innovation as well as allowing smaller vendors, which would otherwise be locked out because of their inability to produce a fully integrated 5G technology solution, to participate in the marketplace. The ORAN Alliance principles create the kind of level playing field that feasibly could unseat Huawei from its current dominant position in the market.

Further, crucial to ensuring competitiveness for American and partner companies is ensuring that companies seeking to deploy in the United States do not have to build different equipment to different standards. Currently, the rest of the world has chosen mid-band radio spectrum as the primary range for 5G. The FCC must continue to make more mid-band spectrum available so that manufacturers of crucial radio equipment can produce the same version for U.S. as for international consumption.

5. ENSURE GLOBAL COMPETITIVENESS

In 2019, the Chinese telecommunications giants Huawei and ZTE saw their market share for telecommunications equipment increase to 28 percent (Huawei) and 10 percent (ZTE). By contrast, the only major American company in the market, Cisco, saw its share decrease to 7 percent.[114] Ericsson and Nokia—Swedish and Finnish companies, respectively—offer viable alternatives in partner countries but still hold only a 30 percent market share combined. Further highlighting the rise of China's telecom companies, trends over the past five years point toward companies that are subject to the Chinese national intelligence law, like Huawei and ZTE, increasing their shares, likely at the expense of Western firms.[115]

Huawei's and ZTE's success in capturing broader swaths of global market share in telecommunications equipment has been attributable in large part to their ability to offer similar equipment at a lower cost than many of their competitors,[116] their willingness to undermine or ignore interoperability standards,[117] and their capacity to offer their clients integrated services—such as cell phones, smart city technology, and business services, in addition to their traditional carrier services—in a way that few companies around the globe can match.[118] These factors, combined with the high level of support both companies

Open Radio Access Networks

Today's telecommunications networks are a mix of hardwired and wireless components. Radio access networks (RANs) are core parts of these networks, enabling telecommunications signals to travel from base stations, where hardwire cables end, out into the world, where they connect cellphones and other mobile devices. Major RAN equipment providers include Ericsson and Nokia, as well as Huawei and ZTE. As is true of the production of other telecommunications equipment, Huawei is a dominant player internationally and has even supplied RAN equipment for rural networks in the United States. Radio access networks increasingly rely on software to help direct and manage network traffic; while many RAN equipment vendors have created radio equipment that is readily interoperable with equipment from other vendors, Huawei's equipment often lacks that interoperability, making it difficult if not impossible to integrate devices from other vendors into networks running off of Huawei equipment. This challenge has been particularly salient as telecommunications providers seeking to upgrade from Huawei 4G equipment to another vendor for their 5G networks have been forced either to rip out their Huawei 4G equipment and replace it with another vendor's or to build out their 5G networks using Huawei.

Partly in response to this reality, some in the telecommunications equipment vendor market have promulgated the concept of open radio access network, or ORAN, specifications. These encourage vendors to build to open hardware specifications and use open-source code that makes possible interoperability between different vendors. Ultimately this approach would enable smaller vendors to introduce their own services to the networks or customize offerings, as well as enabling telecommunications network providers to use different vendors in their networks.

Working with allies and partners, the U.S. government must set forth a shared, democratic vision for technology moving forward. Doing so will require reengaging with standards bodies. For this reason, the United States must provide greater support for this open, interoperable framework and for the standards that accompany it. Coordinated engagement is necessary from the Department of State, as well as the broader U.S. government along with the governments of our partners and allies, to highlight the benefits of the ORAN framework and to actively participate in standards bodies that support it, including the 3GPP and other industry standards organizations.

receive from the Chinese government in brokering favorable trade deals, have enabled them to consolidate their gains and continue to grow their market share. In short, given that Chinese competitors are offering cheap alternatives, it is unclear that market demand would exist to meet the supply even if the United States were able to reinvigorate its high-tech manufacturing base for components and microelectronics.

To create a viable, secure high-tech manufacturing ecosystem, the U.S. government must collaborate with its partners and allies to ensure the global competitiveness of U.S. and partner firms in the face of anticompetitive interventions in global markets by the Chinese government. The U.S. government should utilize all available tools at its disposal to support and promote national champions and champions from partner nations in international markets. To that end, **the U.S. Agency for International Development (USAID) should work with international partners to develop a digital risk impact assessment that highlights the risks associated with the use of untrusted technologies in implementing digitization and telecommunications infrastructure projects.**

Another set of tools at the federal government's disposal lies with Export-Import Bank (EXIM), the U.S. International Development Finance Corporation (DFC), and the United States Trade Development Agency (USTDA), each of which

plays an important role in supporting American businesses in foreign markets. The EXIM can assist American businesses export their goods to customers by providing financial assistance, in the form of loans, loan guarantees, and insurance. As an independent federal agency, the EXIM fills the gap in private export financing to help bolster U.S. industries.[119] Working together with commercial lenders, EXIM aids U.S. exporters in selling goods around the world by providing government-backed loans as well as offering guarantees and insurance that the commercial market is unable to provide.[120] DFC, formed in December 2019, consolidated the Overseas Private Investment Corporation and USAID's Development Credit Authority. DFC provides equity financing, debt financing, political risk insurance, and technical development assistance.[121] Finally, USTDA "helps companies create U.S. jobs through the export of U.S. goods and services for priority development projects in emerging economies."[122] Going forward, **Congress should ensure that EXIM, DFC, and USTDA all operate in legal, regulatory, and funding environments conducive to successfully competing with Chinese state-owned and state-backed enterprises, including their ability to support investments from companies headquartered in partner and ally countries.** Furthermore, **USAID, DFC, and USTDA should develop and maintain a list of prohibited contractors and clients, including companies subject to the Chinese national security and national intelligence laws, that may not be used to implement USAID-, DFC-, and USTDA-funded projects.**

Finally, the United States must support its partners and allies in moving away from untrusted network components and suppliers to relying instead on vendors with more transparent, traceable, and trusted supply chains. Doing so will increase not only their security but also the security of the United States itself. For example, the U.S. military and U.S. intelligence community rely on foreign networks in these partner nation-states as part of the network infrastructure for supporting overseas bases, sharing intelligence, and conducting military operations. Similarly, diplomatic facilities and U.S. companies stationed abroad rely on foreign networks for general operations. While security measures are often taken to ensure the secure transmission of sensitive data throughout overseas networks, the underlying hardware through which that data travels must remain secure. The U.S. government must do more both to provide partners and allies with better information and intelligence on supply chain threats and to work in building collaborative programs and relationships to help manage those threats and build viable alternatives to risky vendors.

E. CONCLUSION

The Commission's March 2020 report contained "Recommendation 4.6: Congress should direct the U.S. government to develop and implement an information and communications technology industrial base strategy to ensure more trusted supply chains and the availability of critical information and communications technologies."[123] This white paper updates the original recommendation by providing a robust path forward, underscoring the imperative of partnership and outlining four key strategic principles upon which to build a U.S. strategy to compete with Chinese high-tech economic aggression and build more secure and trusted supply chains for ICT equipment. While this paper focuses on ICT, many of its recommendations are relevant to tackling challenges in the supply chains for other critical technologies, including operational technologies, medical devices, weapons systems, and more. The United States will need parallel strategies that build on the recommendations of the Commission to secure the supply chains of these vital technologies.

In procuring ICT, as well as other critical technologies, the United States participates in a global marketplace. Merely limiting the access of untrusted firms and their technologies to our cyber ecosystem not only will be inadequate to contain their risks; but, in the absence of suitable alternatives, could stifle our economic growth and deprive core aspects of the U.S. economy of access to potentially transformative technologies. Nowhere is this truer than in technologies like 5G, which

are pursued by strategic competitors that, like China, bolster their companies' market share and subsidize their growth as a matter of national policy—effectively dominating a global market without having to respond to market forces.

The imperative is clear. Chinese government interventions in its own domestic industry, in global trade, and in standard-setting bodies has created an uneven playing field on which companies in the United States and partner countries struggle to compete. The ability of Chinese manufacturers to undercut competitors has led to a growing web of Chinese technologies in critical systems—from telecommunications networks to power grids to ports—in the United States and elsewhere. The challenge facing the United States is therefore multifaceted: it involves in equal parts economics and security. Faced with the need to combat these problems, U.S. policymakers have taken a piecemeal approach. Executive orders to secure supply chains have been written. Voluntary agreements with allies and partners have been struck, but it is too early to assess their results. Congressional bills that tackle symptoms or isolated challenges are moving forward. Most of these efforts are undoubtedly necessary and part of a broad strategic effort that the United States and its allies and partners must undertake. Now is the time for strategic cohesion. Without an ICT industrial base strategy, America risks falling behind competitively and leaving its citizens at serious risk.

ANNEX I: RECOMMENDATIONS

Supply Chain 1: Congress should direct the executive branch to develop and implement an information and communication technologies industrial base strategy.

The United States participates in a global marketplace. Merely limiting the access of untrusted firms and their technologies to our cyber ecosystem not only will be inadequate to contain their risks but, in the absence of suitable alternatives, could stifle our economic growth and deprive core aspects of the U.S. economy of access to potentially transformative technologies. Nowhere is this truer than in technologies like 5G, which are pursued by strategic competitors that, like China, bolster their companies' market share and subsidize their growth as a matter of national policy—effectively dominating a global market without having to respond to market forces.

Congress should direct the U.S. government to assess the United States' information and communications technology (ICT) supply chain and to develop and implement an ICT industrial base strategy in order to reduce dependency and ensure greater security and availability of these critical technologies. This strategy should emphasize the importance of global partnership and focus on (1) identifying critical materials and equipment, (2) working to ensure a minimum viable manufacturing capacity to produce these goods should global supply chains be disrupted, (3) protecting supply chains from compromise, (4) stimulating a domestic market for telecommunications equipment, and (5) ensuring the global competitiveness of trusted firms in the face of Chinese state-backed competition.

Identify Key Technologies and Equipment: To identify critical materials and equipment, Congress should direct and fund the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Secretary of Commerce, the National Security Advisor, and the National Economic Advisor, to conduct a review of technologies, components, and materials critical to the continual function of the economy, government, and military; clearly identify domestic and allied ICT industrial capacity; and identify barriers to a market-based solution. Under existing Title VII authorities of the Defense Production Act, the President should convene industry representatives and approve of "voluntary agreements and plans of action" to identify critical materials and equipment.[124]

Ensure Minimum Viable Manufacturing Capacity: To ensure minimum viable manufacturing capacity, Congress should task the executive branch with identifying candidates for critical manufacturing clusters. In addition, Congress should ensure consistent funding of cutting-edge manufacturing and research and development by passing the Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America, American Foundries, and Utilizing Strategic Allied (USA) Telecommunications Acts. Moveover, to ensure continuity of effort, Congress should appropriate consistent funding and task the executive branch, including the National Science Foundation, the Defense Advanced Research Projects Agency, and the Intelligence Advanced Research Projects Agency, to develop and implement the Office of Science and Technology Policy's 2021 research and development priorities.[125] Finally, through the Department of Homeland Security (DHS), the executive branch should identify five suitable candidates for establishing critical technology clusters and work with relevant state and local government and private stakeholders to facilitate their launch through Foreign Trade Zone designations, tax incentives, and government investment in research and development.

Protect Supply Chains from Compromise: The 2020 National Defense Authorization Act laid the groundwork for strengthening the U.S. intelligence community's capacity to provide better supply chain intelligence: it established a Supply Chain and Counterintelligence Risk Management Task Force within the Office of the Director of National Intelligence (ODNI) to

improve supply chain intelligence for U.S. government acquisition.[126] The supply chain task force should explore additional avenues to expand this support to critical infrastructure, including:

- Leveraging the ongoing work and findings of the DHS-led ICT Supply Chain Risk Management Task Force[127] to work with the private sector in order to identify both its needs and its mechanisms to improve information sharing on supply chain risk.
- Determining appropriate funding, resourcing, and authorities for U.S. intelligence community efforts to serve as the central and shared knowledge resource for threats to supply chain activities or supply chain integrity and to aggregate all-source information relating to supply chains, including whether and how to construct a National Supply Chain Intelligence Center, and how to share strategic supply chain warning and counterintelligence risk assessments with public and private partners.
- Understanding and defining additional measures the U.S. government can adopt to make greater use of publicly available and proprietary sources in informing assessments of risk to supply chains and foreign investments.

Stimulate a Domestic Market: The U.S. government can take steps to bolster demand at home for critical technologies, including network technologies. Domestic infrastructure investment and greater public investment in the area can provide a significant boost to productivity in the long run by improving the public capital stock. To do so, the Federal Communications Commission (FCC) should tie 5G infrastructure investment to open and interoperable standards and work with the Department of Defense and the National Telecommunications and Information Agency to facilitate the release of more mid-band spectrum in order to ensure a strong domestic market for telecommunications equipment.

Ensure Global Competitiveness: To ensure the global competitiveness of U.S. and partner companies, the U.S. government should leverage the U.S. Agency for International Development (USAID), the Export-Import Bank of the United States (EXIM), the U.S. International Development Finance Corporation (DFC), and bi- and multilateral trade negotiations to ensure favorable conditions in emerging markets where U.S. government aid and institutional investment are present. In addition, programming at the EXIM should continue to provide loans, loan guarantees, and insurance to investment projects in critical infrastructure leveraging critical network technologies from U.S. companies and should review authorities to provide similar protections for projects leveraging non-U.S. network technology provided by firms in partner countries, such as Nokia, Ericsson, and Samsung.

Supply Chain 2: Congress should direct the Department of Homeland Security, in coordination with the Department of Commerce, Department of Defense, and Department of State, to identify key information and communication technologies and materials through industry consultation and government review.

As a first step toward securing supply chains and enabling U.S. competitiveness, the U.S. government must work with industry, partner countries, and state and local governments to identify key equipment and the components and materials that make its assembly possible. This equipment is likely to include not just weapons systems and telecommunications equipment, but also general purpose computing equipment. Some components, like semiconductors and printed circuit boards, are more complicated to produce and require more technical manufacturing capability. Because of this complexity, such components are likely to require standing, specific manufacturing capability, as it may not be feasible to repurpose existing manufacturing. Other components, such as packaging, wires, and other conductors, are simpler to produce and existing manufacturing can likely be repurposed in a time of crisis to meet needs. The U.S. government must identify critical materials and equipment and work to ensure a minimum viable capacity to produce those goods should global supply chains be disrupted.

Further, to promote non-military initiatives that address shortfalls in technology capacity generally—not simply within the defense industrial base—Congress has explicitly broadened the scope of the Defense Production Act (DPA) by expanding the definition of a central term: national defense. This was an important step, because the exercise of DPA authorities generally requires a nexus with national defense. Initially the DPA defined "national defense" as "programs for military and energy production or construction, military assistance to any foreign nation, stockpiling, space, and any directly related activity."[128] In 2003, recognizing a need for non-military programs that could help prepare for and respond to threats against critical infrastructure, Congress decided to include "critical infrastructure protection and restoration" in the statutory definition of "national defense."[129] These statutes and the "direct threat to the national defense or its preparedness programs" posed by ICT supply chain insecurity enable the President to leverage the DPA's Title VII authorities to convene industry representatives and approve of "voluntary agreements and plans of action," including the creation of advisory committees.[130] The statute creates a corresponding defense against antitrust or contract suits.[131] The President should employ these authorities to convene relevant industry stakeholders to build a better understanding of key technologies and materials used by entities critical to national defense, the government, and the economy. The President can further mandate the disclosure of information "if necessary or appropriate"—such as information about supply chain dependencies.[132]

In addition to the convenings of industry led by the White House, the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Secretary of Commerce, the National Security Advisor, and the National Economic Advisor, should conduct a 365-day review to identify key potential points of failure in critical supply chains. The review should consist of three phases. First, the review committee should work with partners in industry to undertake a 180-day review to identify technologies, components, and materials critical to the continual function of the economy, government, and military. As a second phase, the review committee should identify where the United States is reliant on China for part or all of the supply chain for the identified technologies, components, and materials. Finally, the review should identify alternatives to Chinese facilities where dependence on China is present.

Supply Chain 3: Congress should direct the Department of Commerce, in consultation with the Department of Homeland Security, the Department of State, and the Department of Defense, to conduct a viability study of localities fit for economic clustering. It should fund the Department of Commerce, in consultation with the Department of Homeland Security, Department of State, and Department of Defense, to solicit competitive bids and applications from candidate states, municipalities, and localities for the designation of no fewer than three and no more than five critical technology manufacturing clusters.

The U.S. government must implement a plan to ensure minimum viable capacity to produce the most critical components and finished products required in a time of crisis. The U.S. government should strive to encourage the continued viability of domestic high-tech manufacturing by intervening with a light touch to set the conditions in which innovation and industry thrive, through the creation of economic clusters, or "agglomeration economies," in given geographic areas. The viability study recommended above should include localities that are partially or fully in partner countries. Likewise, the critical technology clusters should contain designated Foreign Trade Zones,[133] and and they should be granted special eligibility for special research and development grant opportunities as well as further DPA-enabled investment.

Supply Chain 3.1: Congress should appropriate an increase in research and development funding for critical technologies.

In addition to implementing the Commission's recommendations for increased research and development funding from the March 2020 report,[134] Congress should create a supply chain innovation fund to be administered by the

National Telecommunications and Information Administration to provide grants to develop technologies that will advance the competitiveness of the 5G marketplace, advance equipment that conforms to open and operable software-based network solutions guidance—including from the Open Radio Access Network (ORAN) Alliance, the Open Networking Foundation (ONF), the 3rd Generation Partnership Project (3GPP), and the Telecom Infra Project (TIP)—and improve integration of multi-vendor network environments. The Endless Frontier Act, which would establish a new Directorate of Technology within the National Science Foundation and redesignate NSF as the National Science and Technology Foundation, is another crucial step for research and development in critical technologies.[135] In addition to supporting domestic projects, a portion of the fund should be allocated to multilateral projects to support multilateral research and development initiatives with partners and allies.[136]

Supply Chain 3.2: The federal government should, in partnership with partner and ally governments, develop programs to incentivize the movement of critical chip and technology manufacturing out of China.

The U.S. government has two options to incentivize movement out of China. First, Congress could create a dedicated fund for a grants program to provide incentives to companies for projects that move manufacturing out of China and into the United States.[137] Alternatively, Title III of the Defense Production Act allows federal entities to provide loan guarantees to private actors "in support of production capabilities or supplies" deemed "necessary to create, maintain, expedite, expand, protect, or restore production and deliveries of services essential to the national defense."[138] Federal agencies may also provide loans directly to private businesses (including nonprofits) to create, expand, protect, or restore "capacity, the development of technological processes, or the production of essential materials," if that loan will address "current or projected shortfalls of industrial resources, critical technology items, or material essential for national defense."[139] The executive branch should explore whether DPA's Title III authorities allow the government to subsidize the movement of critical manufacturing out of China.

Supply Chain 3.3: Congress should direct the President to conduct a study on the viability of a public-private national security investment corporation to attract private capital for investment in strategically important areas.

While the U.S. government possesses considerable financial power, the scale of investment needed to reinvigorate American high-tech manufacturing and facilitate the movement of critical production, manufacturing, assembly, and testing into partner countries likely outstrips both the U.S. government's financial capacity and the U.S. taxpayer's willingness to subsidize such efforts. In short, although the U.S. government must signal a stake in these investments, this endeavor will succeed only if private capital is unlocked. Congress should therefore direct the President, in consultation with the Secretary of Defense, Secretary of Homeland Security, Secretary of State, Secretary of Commerce, Secretary of the Treasury, Director of National Intelligence, Chairman and President of the Export-Import Bank, the Chief Executive Officer of the United States Development Finance Corporation, the Director of the United States Trade and Development Agency, and the Administrator of the United States Agency for International Development, to provide a report to Congress that assesses the need for and viability of a public-private investment corporation to serve as a clearinghouse for public and private investment in critical technologies.

The report should assess the need for a public-private partnership to stimulate greater investment in critical technologies; it should identify gaps in the private capital market for long-term investments in critical technologies, identify gaps in the federal government's ability to fund long-term investments in critical technologies, and

estimate the overall level of investment required over the next 10 years to fill those gaps. In addition, the report should identify strategic priorities for investment, including semiconductors, microchips, printed circuit boards, rare earth element mining, rare earth element refining, information and communications technology equipment, defense and weapons systems, and other technologies deemed by the President to be critical to the national security, public safety, and economic vitality of the United States. The report should clearly delineate the potential mission of the corporation to serve as a clearinghouse to identify investment opportunities and facilitate private investment in projects that directly or indirectly support national security or national economic security objectives or have the potential to save the federal government money or lead to the disruption of predatory monopolistic practices of adversaries, including China. It should further assess the tools available to the corporation, including government guarantees of debt, government guarantees of return on investment, prioritized government contracting, and government investment. The study should identify the range of projects eligible for investment by the corporation as well as the eligibility requirements for those projects. The study should also examine how the corporation should be structured, including whether it should take the form of a for-profit or a not-for-profit entity, as well as the structure and role of the board of directors and the appropriate level of government oversight and involvement. Finally, the study should assess the corporation's estimated cost to taxpayers over 10 years.

Supply Chain 4: The President should designate a lead agency to integrate and coordinate civilian and government ICT supply chain risk management efforts into an ongoing national strategy and to serve as the nexus for public-private partnerships on supply chain risk management.

The U.S. government, as well as the private sector, must continue to engage in supply chain risk management efforts to reduce its risk and minimize vulnerability. There are a variety of efforts already under way to improve supply chain risk management, led both by the government led and by the private sector. These projects are focused on collaborating to identify critical knowledge of vulnerabilities, determining where additional research is needed, and developing new strategies to address existing risks. The government-led initiatives involve a wide range of task forces, advisory committees, and programs to study supply chain risks and strategies to mitigate them. These programs, which should be assessed and consolidated where possible under a single vision and strategy, include DHS's Cybersecurity and Infrastructure Security Agency's Information and Communications Technology (ICT) Supply Chain Risk Management Task Force,[140] the President's National Security Telecommunications Advisory Committee,[141] DoD's Cybersecurity Maturity Model Certification,[142] and the National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management (C-SCRM) program.[143] At the same time, many industry associations, including the Information Technology Industry Council, the Semiconductor Industry Association, and the Telecommunications Industry Association, are also intensely studying the supply chain risks for their specific sectors to minimize risks. The executive branch should designate a department or agency to serve as the lead agency to integrate and coordinate these efforts into an ongoing national strategy.

Supply Chain 4.1: Congress should direct the President to construct or designate a National Supply Chain Intelligence Center.

To better protect the supply chain, the United States government must improve its capability to collect and disseminate intelligence on supply chain risks. This information is critical not only to government agencies but also to private-sector stakeholders, who own and operate 85 percent of the nation's critical infrastructure.[144] Without the information required to fully understand the risks, the private sector will not be able to implement comprehensive strategies to address the potential for compromise. To better position the U.S. government to take in, fuse, and disseminate relevant information to key stakeholders, the executive branch should construct a National

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

Supply Chain 4.2: Congress should fund three Critical Technology Security Centers, selected and designated by DHS, in collaboration with the Department of Commerce, Department of Energy, ODNI, and Department of Defense.

While various public and private entities currently provide security evaluations and testing, the U.S. government lacks trusted, centralized entities to perform these functions.[145] Congress should direct and appropriate fund DHS, in partnership with the Department of Commerce, Department of Energy, ODNI, and DoD, to competitively select, designate, and fund up to three Critical Technology Security Centers in order to centralize efforts directed toward evaluating and testing the security of devices and technologies that underpin our networks and critical infrastructure.[146] These Centers would provide the U.S. government with the capacity to test the security of critical technologies and, when appropriate, assist in identifying vulnerabilities, developing mitigation techniques with relevant original equipment manufacturers, and supporting new and ongoing efforts to certify technologies as secure. The Centers could also play an important role as project managers and, in some cases, would provide funding for the broader research community already working toward similar ends. To the greatest extent possible, these Centers should be designated from existing efforts and institutions, such as ongoing industrial control system work at the Idaho National Lab, rather than created as new entities.

The Centers should be focused on technologies critical to the security of the national cyber ecosystem and of critical infrastructure. This initial list of Centers could be expanded in the future to focus on other critical technologies, including Internet of Things (IoT) devices:

- *A Center for Network Technology Security* to test the security of hardware and software that underpins our cyber ecosystem, including routers, radio equipment, modems, switches, and other core network technology.
- *A Center for Connected Industrial Control Systems Security* to test the security of connected programmable logic controllers, supervisory control and data acquisition servers and systems, and other connected industrial equipment.
- *A Center for Open-Source Software Security* to systematically identify critical open-source libraries and test and fix vulnerabilities in open-source software repositories, which provide the basis for most software in use today.[147]

Supply Chain 5: The Federal Communications Commission (FCC) should tie 5G infrastructure investment to open and interoperable standards and work with the Department of Defense and the National Telecommunications and Information Agency to facilitate the release of more mid-band spectrum in order to ensure a strong domestic market for telecommunications equipment.

The U.S. government can take steps to bolster demand at home for critical technologies, including network technologies. Domestic infrastructure investment and greater public investment in the area can provide a significant boost to productivity in the long run by improving the public capital stock.[148] Advanced industrial economies like the United States must focus on repairing and replacing aging infrastructure to help enhance the country's overall levels of productivity.

Infrastructure Investment: The executive branch should develop and implement a National 5G Deployment Plan to achieve trusted 5G nationwide by 2025. As part of the plan, the FCC should require that all infrastructure purchased through projects funded by the Universal Service Fund and related programs must conform to open and interoperable standards, including proposals of the ORAN Alliance, the ONF, 3GPP, and TIP.

Spectrum Availability: Crucial to ensuring competitiveness for American and partner companies is ensuring that companies do not have to build different equipment to different standards in order to deploy in the United States. Currently, the rest of the world has chosen mid-band radio spectrum as the primary range for 5G. The FCC must make more mid-band spectrum available so that manufacturers of crucial radio equipment can produce the same version for U.S. as for international consumption.

Supply Chain 5.1: The U.S. Agency for International Development (USAID) should work with international partners to develop a digital risk impact assessment that highlights the risks associated with the use of untrusted technologies in implementing digitization and telecommunications infrastructure projects.

Impact assessments are tools that enable a development project manager to easily understand the effect their project will have on an issue in the project's location. Human rights impact assessments and environmental impact assessments are commonplace for development projects across the board. Today, the development community lacks similar frameworks or assessment tools to help development workers understand and manage digital risks, including the risks of data theft, surveillance, and compromise present in the deployment of technology from companies like Huawei and ZTE that are subject to Chinese intelligence and cybersecurity laws. To fill this gap and help steer the development projects of USAID and others toward more trusted technologies, USAID should develop a Digital Risk Impact Assessment tool.

Supply Chain 5.2: Congress should ensure that the Export-Import Bank (EXIM), DFC, and USTDA all operate in legal, regulatory, and funding environments conducive to successfully competing with Chinese state-owned and state-backed enterprises, including their ability to support investments from companies headquartered in partner and ally countries.

Significantly, numerous countries, including China, employ their export credit agencies to further their geopolitical aspirations. China, the most aggressive in this regard, is a catalyst for the increasing assertiveness of other countries' official export finance activities. In particular, China uses its two official export credit agencies (ECAs), along with a number of other state entities such as state-owned banks and state-owned enterprises, to expand influence and gain competitive advantages—including in high-technology sectors critical to long-term prosperity and security. This strategy necessitates a robust and integrated U.S. government response, in which the EXIM, DFC, and USTDA are crucial elements of statecraft.

In December 2019, Congress established the EXIM's Program on China and Transformational Exports.[149] In doing so, Congress made clear EXIM's role in directly neutralizing export subsidies for competing goods and services financed by China, advancing the comparative leadership of the United States with respect to China, and supporting U.S. innovation, employment, and technological standards in 10 key areas, including 5G. This program should continue to be supported and funded at a level commensurate with its importance.

Congress should direct EXIM, DFC, and the USTDA to assess the authorities available to each to support investments in infrastructure provided by companies in partner and ally nations. For example, the DFC's authority to conduct projects in higher income countries currently is ambiguous. The assessment of authorities should highlight such ambiguities and explore the feasibility of national security waivers to allow these organizations to work outside of their authorized countries and regions.

Supply Chain 5.3: USAID, the U.S. International Development Finance Corporation (DFC), and the United States Trade Development Agency (USTDA) should develop and maintain a list of prohibited contractors and clients, including companies subject to the Chinese national security and national intelligence laws, that may not be used to implement USAID-, DFC-, and USTDA-funded projects.

Some USAID, DFC, and USTDA contracts already exclude certain suppliers on the basis of criteria like trustworthiness. To facilitate the consistent application of these bans, USAID, DFC, and USTDA should develop and maintain a list of prohibited contractors and untrusted vendors who may not be used to implement USAID, DFC, and USTDA-funded projects. Designation should be based on security and risk, as well as on anticompetitive behavior.

ANNEX II: U.S. INDUSTRIAL POLICY CASE STUDIES

While the phrase "industrial policy" is associated by many with communism, the United States has engaged in industrial policy throughout its history in a number of ways ranging from state-owned enterprises to more subtle interventions that align market forces for greater efficiency and competitiveness. In an era when foreign governments overtly support their own domestic industry, free and fair trade in markets for certain goods no longer exists. The Chinese government's interventions on behalf of its technology national champions has created an uneven playing field for companies wishing to compete in critical technology markets, including for 5G telecommunications equipment. Here, the Commission provides detailed background on the ways in which the United States has conducted industrial policy in the past.

STATE-OWNED ENTERPRISE: TENNESSEE VALLEY AUTHORITY

The Tennessee Valley Authority (TVA), a government-owned and -operated agency that provides electricity for business, customers, and local power companies, serving 10 million people in parts of seven southeastern states, was created during the Great Depression to provide flood control and hydroelectric power.[150] Today, the TVA receives no taxpayer dollars; it is a self-funded company that generates its revenue from the sale of electricity. Alongside the generation and maintenance of its electrical system, TVA provides many other services to its constituents. It helps manage land for the Tennessee River system, including the creation and implementation of plans for flood control. It also works with local power companies and state and local governments to aid in the economic development of the area and to help stimulate job growth.

President Franklin D. Roosevelt took office in the midst of the Great Depression. In his inaugural presidential address to the nation, he promised bold action and jobs for people.[151] The series of programs enacted by President Roosevelt to reinvigorate the economy and create jobs became known as the New Deal. Like many places, the Tennessee Valley was hard hit by the Depression, but it was uniquely positioned to support a New Deal project because more almost two decades earlier, in 1916, President Wilson had authorized the building of a hydroelectric dam in Muscle Shoals, Alabama, on the southern bank of the Tennessee River.[152] This dam was intended to provide power to a nearby munition plant during World War I; however, the war ended before the hydroelectric dam was completed. Senator George Norris later introduced the Muscle Shoals bill to fund and complete the dam, but President Herbert Hoover vetoed it, stating that the federal government, as a matter of course, should not own or operate a power and manufacturing business.[153] But as the Depression deepened in the country, so too did the belief that private utility companies were price gouging. Growing public sentiment in support of a government-run utilities company drove the passage of the 1933 TVA Act.[154]

PROTECTIONISM: THE RADIO CORPORATION OF AMERICA AND SEMATECH

In the middle ground between outright state ownership and lighter touch interventions like the facilitation of economic clusters is robust protection of and investment in a given industry to support its continued or renewed global competitiveness. While free trade enthusiasts disparage the notion of protected industry, in global markets that do not resemble free trade—like that for telecommunications equipment—some government protection and investment may be necessary to create a level playing field. Two cases from recent history illustrate how the U.S. government may take advantage of tools at its disposal to bolster and protect selected industries: the Radio Corporation of America and SEMATECH.

Radio Corporation of America

In the late 1800s and early 1900s, the Marconi Wireless Telegraph Corporation of America (American Marconi)—a subsidiary of a British company—was the predominant supplier of radio equipment, in large part because it had a patent advantage. When the United States entered World War I in 1917, the U.S. government took control of most radio stations.

Recognizing the strategic importance of radio equipment and wary of the threat of foreign control of American telecommunications and radio systems, the U.S. government, led by the Navy Department, sought to ensure that an American company retained control of U.S. infrastructure for international communication .

At the time, General Electric (GE), an American corporation, was the primary producer of the Alexanderson alternator, one of the first devices capable of producing the continuous radio waves needed to transmit signals across long distances, like oceans. Immediately following World War I, and seeking a monopoly on radio communications in the United States, American Marconi opened negotiations with GE for exclusive rights to use the Alexanderson alternator in the United States. The U.S. government opposed any such agreement; but rather than enacting an outright ban or blocking the sale of alternators in some other way, agents of the U.S. government appealed to GE's patriotism and emphasized the perils of allowing a British firm to gain a monopoly over American communications infrastructure.[155]

In mid-1919, following a series of meetings with representatives from the Navy Department, GE relented. However, in canceling its contract with American Marconi, GE was left in an "awkward position":[156] after investing a considerable sum in the development of a product that was now ready for market—the Alexanderson alternator—it was left with no viable customer. Under pressure from the federal government, British Marconi, American Marconi's parent corporation, agreed to sell American Marconi to GE, enabling GE to establish a radio monopoly. The name of this new GE subsidiary was the Radio Corporation of America (RCA).

The RCA case is a good example of how the U.S. government has taken advantage of close relationships between companies to produce desired outcomes. American Marconi required equipment from GE to stay competitive, and the U.S. government, appealing to GE's patriotism, was able to leverage that relationship to back American Marconi into a corner. Facing the threat of being frozen out of the American market, British Marconi was forced to make the only viable decision: cut its losses and sell its American stake to an American business. In this way, the U.S. government ensured the recapture and control of a critical industry.

SEMATECH

Following World War II, the United States entered the dawn of the information age, when new industries emerged and existing sectors were transformed by broad infusions of new technology.[157] The most significant technology introduced during this period, with the most lasting impact on the global economy and society, may have been the semiconductor. This transformative technology was invented in the United States in 1947 by three Bell Labs researchers, William Shockley, John Bardeen, and Walter Brattain; for this work, they shared the Nobel Prize in Physics in 1956.[158] Today, semiconductors are the critical component of all modern electronics that "enable advances in medical devices and health care, communications, computing, defense, transportation, clean energy, and technologies of the future such as artificial intelligence, quantum computing, and advanced wireless networks."[159] Therefore, protecting semiconductor technology is essential not only to advancing the United States' competitiveness in the global market but also to preserving its national security interests.

While the federal government's initial support and funding played a key role in the creation and development of the U.S. semiconductor industry, by the 1980s increasing competition from Japan and the U.S. DoD's growing concern about increasing dependence on foreign-sourced components for advanced weapons forced the United States to take action.[160] Congress created and appropriated funding for an industry-led consortium called SEMATECH,[161] a name derived from "semiconductor manufacturing technology," in the National Defense Authorization Act (NDAA) of Fiscal Years 1988 and 1989; to encourage the U.S. semiconductor industry to conduct research and development (R&D) focused on advanced semiconductor manufacturing techniques in order to secure the United States' future commercial and defense needs.[162]

Headquartered in Austin, SEMATECH launched in 1987; the initial members of the R&D consortium were 14 U.S.-based semiconductor manufacturing firms and the U.S. DoD.[163]

One of the primary tools used by the federal government was direct, multiyear funding. From 1988 until 1993, the DoD, via its Defense Advanced Research Projects Agency (DARPA), provided $100 million annually to SEMATECH, and the private companies that are consortium members matched the federal funding.[164] By 1993, according to the General Accounting Office (GAO), SEMATECH achieved many of its original objectives, including technical manufacturing goals and establishment of an industry forum to share data and to cooperate on future R&D.[165] In 1998, DARPA and SEMATECH formally suspended most of the terms and conditions of their 1988 memorandum of understanding, leaving only limited information sharing and an observer-level relationship.[166] Less tangibly the federal government could encourage the private-sector members of the consortium by appealing to their sense of patriotic duty to protect the national and economic security of the United States.

CLUSTERING: SILICON VALLEY

The origin and successes of Silicon Valley[167] cannot be attributed to a single event or factor. Since the early 1950s, many government and private-sector entities intentionally designed and executed planned programs and investments; but the serendipitous convergence of multiple disparate, yet interrelated, forces involving many incremental actions created one of the most fertile entrepreneurial environments in the world, which has produced historically unparalleled advances in science and technology. The high-tech cluster in Silicon Valley is a product of a symbiotic partnership between the U.S. government, academia, and the private sector that unfolded over multiple generations whose experiences created an extraordinary depth of understanding of innovation, investments, and entrepreneurship.

The U.S. government also played a key in the birth and development of Silicon Valley: national security needs generated demand and the initial customer base, it funded programs that later matured to a private venture capital model, it transferred technology from government to private control, and its policies supported the new firms.

Market Demand Generated by National Security Interests: For nearly a half century, the United States' direct involvement in global conflicts and geopolitical tension—specifically, World War II and the Cold War—required a security posture with a more powerful and technologically advanced military than that of its adversaries. Starting in 1958 with Fairchild Semiconductor's transistors, which were key components of the B-70's onboard computer and the Minuteman ballistic missile,[168] demand for Silicon Valley's technology has remained strong, and for decades the U.S. government was its primary customer. As the space race escalated in the 1960s, NASA became the largest consumer of Intel's integrated circuits.[169] In 1962, the federal government—NASA and the U.S. Air Force—bought 100 percent of integrated circuits produced in the world.[170]

The Pacific Theater of World War II and numerous military installations on the West Coast required the Pentagon to inject federal money into the area, which was received mainly by universities and by the private industries developing aerospace and electronics technologies for military applications. The U.S. government's demand for defense technology during wartime and into the Cold War also created a market for defense contractors such as the Lockheed Corporation, which was the biggest employer in Silicon Valley from the 1950s to the 1980s. By bringing thousands of engineers to Silicon Valley, Stanford University and Lockheed laid the groundwork for the area's most essential element: a tech talent cluster.[171]

Funding Model—Federal to VCs: Between the 1940s until the late 1970s, the U.S. government created "ideal economic conditions for technology innovation and commercialization to thrive in Silicon Valley."[172] The Small Business Investment

Act (SBIA) of 1958 enabled the Small Business Administration (SBA) to create a 2:1 fund-matching program in order to encourage venture capital investment: for every dollar invested by a private entity, the SBA would grant two.[173] As the Cold War and the space race with Soviet Union intensified in the 1960s, the U.S. federal government spent more on R&D every year than the rest of the world combined.[174] While federal funding continued, the government's decisions in 1978 to cut the capital gains tax and to allow pension funds to invest in venture funds launched the venture capital (VC) industry.[175] In recent decades, financial institutions such as the Silicon Valley Bank have played a critical role in making the VC model successful. The U.S. Export-Import Bank's (EXIM) Working Capital Loan Guarantee program matched technology and life science companies interested in exporting their products with financial institutions that could provide the necessary VC.[176] The spirit of entrepreneurship in the region shaped how VC investments were viewed, for there the scientific approach decoupled failure in experimentation from fear or stigma.[177]

Gifts of Technology: Technology does not mature and adapt in a vacuum. It requires careful nurturing from the earliest glimmerings of an idea that sprouts innovation. Government money, priorities, and support alone cannot force innovation to occur; however, by encouraging dual-use applications of innovative technology, the government's myriad investments, ranging from basic research to advanced R&D programs, and its subsequent selfless transfers of new technology can most broadly benefit the general population. Without government's creation of or investments in the internet, the global positioning system, touch screens, voice activation, and so forth, as well as its already noted demand for integrated circuits, Silicon Valley as we know it would not exist. Every key component in the iPhone, as well as in all Apple products dating back to the Apple I computer, was developed by the U.S. government.[178] As one technology writer has observed, "Aside from the internet itself, which is the basis of every single 21st century high-tech company (including the 60+ 'unicorns,' Silicon Valley start-ups valued at more than $1 billion), the whole succession of technologies that power our devices has emerged from publicly-funded science."[179] The federal government made possible the development of the core technologies that are the foundation of Silicon Valley today.

Favorable Policies: Wide-ranging decisions by the federal government regarding immigration, education, taxation, and industrial policies helped shape favorable conditions for Silicon Valley. While political struggles over federal immigration policy have led to uncertainties regarding visas for tech workers in recent decades, the federal government's actions in the early days of Silicon Valley fostered the growth and development of its entrepreneurial ecosystem.[180] By ending the racist quotas inscribed in the Immigration Act of 1924, the Immigration and Naturalization Act of 1965 allowed ambitious newcomers from around the world into Silicon Valley—and among them were many future entrepreneurs.[181] To advance education, federal government policies and programs have focused primarily on funding key R&D. In higher education, the National Science Foundation (NSF) provides basic research grants to students and faculty in colleges and universities. Indeed, an NSF grant that initially funded Sergey Brin's research helped create Google.[182] Also, as mentioned above, the 1978 change to tax policy boosted the investment capital available to startups. As a final example, the federal government's critical industrial policy decisions protected the U.S. semiconductor firms from intense competition from their Japanese counterparts in the 1980s.

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
5G	fifth-generation
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CMS	Critical Minerals Subcommittee
C-SCRM	Cyber Supply Chain Risk Management
DARPA	Defense Advanced Research Projects Agency
DFC	U.S. International Development Finance Corporation
DHS	Department of Homeland Security
DoD	Department of Defense
DPA	Defense Production Act
EXIM	Export-Import Bank of the United States
FCC	Federal Communications Commission
FY	fiscal year
GAO	General Accounting Office / Government Accountability Office
GE	General Electric
ICS	industrial control system
ICT	information and communications technology
IDM	integrated device manufacturer
ITU	International Telecommunication Union
LAN	local area network
NASA	National Aeronautics and Space Administration
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
PCBs	Printed Circuit Boards
ODNI	Office of the Director of National Intelligence
ONF	Open Networking Foundation

O-RAN	Open Radio Access Network
OSAT	outsourced semiconductor assembly and test firm
R&D	research and development
RAN	radio access network
RCA	Radio Corporation of America
REE	rare earth elements
SBA	Small Business Administration
SEP	standards-essential patent
STEREO	Solar Terrestrial Relations Observatory
TIP	Telecom Infra Project
TSMC	Taiwan Semiconductor Manufacturing Company
TVA	Tennessee Valley Authority
USAID	U.S. Agency for International Development
USTDA	United States Trade Development Agency
VC	venture capital

ENDNOTES

1 U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission* (March 2020), 99, https://www.solarium.gov/report.

2 Semiconductor Industry Association, "Presentation Slides for CSC" (slides, July 24, 2020).

3 See, for example, Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act, H.R. 7178, 116th Cong., 2nd sess. (June 11, 2020), https://www.congress.gov/bill/116th-congress/house-bill/7178?r=5&s=1; American Foundries Act of 2020, S.4130, 116th Cong., 2nd sess. (July 1, 2020), https://www.congress.gov/bill/116th-congress/senate-bill/4130; Utilizing Strategic Allied Telecommunications Act of 2020, H.R. 6624, 116th Cong., 2nd sess. (April 24, 2020), https://www.congress.gov/bill/116th-congress/house-bill/6624; National Defense Authorization Act (NDAA) for Fiscal Year 2021, S. 4049, Title X, Subtitle H—Wireless Supply Chain Innovation and Multilateral Security, and Subtitle I—Semiconductor Manufacturing Incentives, 116th Cong., 2nd sess. (July 23, 2020), https://www.congress.gov/bill/116th-congress/senate-bill/4049/text.

4 See, for example, Exec. Order No. 13873, 3 C.F.R. 22689 (2019), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain; and Exec. Order No. 13932, 3 C.F.R. 22689 (2020), https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system.

5 National Security Telecommunications Advisory Committee (NSTAC), "NSTAC Report to the President on Software-Defined Networking" (Cybersecurity and Infrastructure Security Agency, August 12, 2020), https://www.cisa.gov/sites/default/files/publications/NSTAC%20SDN%20Report%20(8-12-20).pdf.

6 See, for example, Cheng Ting-Fang, "China Hires over 100 TSMC Engineers in Push for Chip Leadership," *Nikkei Asian Review*, August 12, 2020, https://asia.nikkei.com/Business/China-tech/China-hires-over-100-TSMC-engineers-in-push-for-chip-leadership.

7 Alexander Hamilton, "Report on the Subject of Manufactures" (December 5, 1791), https://founders.archives.gov/documents/Hamilton/01-10-02-0001-0007.

8 U.S. Geological Survey, "Silicon," in *Mineral Commodity Summaries* (January 2020), 149, https://pubs.usgs.gov/periodicals/mcs2020/mcs2020-silicon.pdf.

9 U.S. Geological Survey, "Silicon," 149.

10 U.S. Geological Survey, "Silicon," 149.

11 U.S. Geological Survey, "Silicon," 148.

12 U.S. Geological Survey, "Germanium," in *Mineral Commodities Summary* (January 2020), 68, https://pubs.usgs.gov/periodicals/mcs2020/mcs2020-germanium.pdf.

13 U.S. Geological Survey, "Germanium," 68–69.

14 U.S. Geological Survey, "Germanium," 68.

15 Keith Kirkpatrick, "Electronics Need Rare Earths," *Communications of the ACM* 62, no. 3 (March 2019): 17–18, https://cacm.acm.org/magazines/2019/3/234917-electronics-need-rare-earths/fulltext#:~:text=Some%20of%20the%20rare%2Dearth,%2C%20and%20dysprosium%20(66).

16 Hannah Kirk, "The Geo-Technological Triangle between the US, China, and Taiwan," *The Diplomat*, February 8, 2020, https://thediplomat.com/2020/02/the-geo-technological-triangle-between-the-us-china-and-taiwan/.

17 Wayne M. Morrison, "Trade Dispute with China and Rare Earth Elements" (Congressional Research Service, June 28, 2019), https://crsreports.congress.gov/product/pdf/IF/IF11259; Marc Humphries, "Rare Earth Elements: The Global Supply Chain" (Congressional Research Service, December 16, 2013), https://fas.org/sgp/crs/natsec/R41347.pdf.

18 U.S. Geological Survey, "Rare Earths," in *Mineral Commodity Summaries* (January 2020), 132, https://pubs.usgs.gov/periodicals/mcs2020/mcs2020-rare-earths.pdf.

19 Khalid Alothman et al., "Spring 2017 Industry Study: Industry Report, *Electronics*" (Dwight D. Eisenhower School for National Security and Resource Strategy, National Defense University, 2017), 12, https://es.ndu.edu/Portals/75/Documents/industry-study/reports/2017/es-is-report-electronics-2017.pdf.

20 "U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy" (Congressional Research Service, June 27, 2016), 6, https://www.everycrsreport.com/files/20160627_R44544_77fdee097eaaac05bcf7bd6041d5bdf44b24c7b9.pdf; Falan Yinug, "Semiconductor Industry Primer: The Stages of Production and Business Models," *Semiconductor Industry Association* (blog), February 25, 2015, https://www.semiconductors.org/semiconductor-industry-primer-the-stages-of-production-and-business-models/; John VerWey, "The Health and Competitiveness of the U.S. Semiconductor Manufacturing Equipment Industry," Office of Industries Working Paper ID-058 (U.S. International Trade Commission, July 2019), https://www.usitc.gov/publications/332/working_papers/id_058_the_health_and_competitiveness_of_the_sme_industry_final_070219checked.pdf.

21 "Fabless Companies vs. IDMs in the Semiconductor Industry," *Samsung* (blog), October 23, 2012, https://www.samsung.com/semiconductor/minisite/exynos/newsroom/blog/fabless-companies-vs-idms-in-the-semiconductor-industry/; "Redefining Compute through Process and Packaging: A New Paradigm for Moore's Law," Intel, accessed October 2, 2020, https://www.intel.com/content/www/us/en/silicon-innovations/6-pillars/process.html?wapkw=%22Integrated%20Device%20Manufacturer%22. Both South Korea's Samsung and the United States' Intel are examples of IDMs, though both increasingly rely on third parties, such as the Taiwan Semiconductor Manufacturing Company (TSMC) for fabrication of some semiconductors.

22 Intel, "Redefining Compute through Process and Packaging."

23 "U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy" (Congressional Research Service, June 27, 2016), https://www.everycrsreport.com/files/20160627_R44544_77fdee097eaaac05bcf7bd6041d5bdf44b24c7b9.pdf;"What Are 'Fabless' Chip Makers?" Investopedia, November 29, 2019, https://www.investopedia.com/ask/answers/050615/what-are-fabless-chip-makers-and-why-are-they-important-semiconductor-market.asp. Examples of fabless companies include the U.S. firms Intel Advanced Micro Devices (AMD), Nvidia, Qualcomm, and Broadcom Inc.

24 Peter Clarke, "'Fab Four' Emerges from Pure-Play Foundry Ranks," *EETimes*, August 10, 2004, https://www.eetimes.com/fab-four-emerges-from-pure-play-foundry-ranks/. The Taiwan Semiconductor Manufacturing Company (TSMC), the United States' Globalfoundries, and Taiwan's United Microelectronics Corporation (UMC) are all pure-play foundries.

25 *Beyond Borders: The Global Semiconductor Value Chain* (Semiconductor Industry Association and Nathan Associates Inc., May 2016), 7, https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Beyond-Borders-Report-FINAL-May-6-1.pdf.

26 Semiconductor Industry Association, "Presentation Slides for CSC" (slides, July 24, 2020). In 2019, the U.S. ranked number one in the global semiconductor market, capturing 47 percent of the revenue. The next closest competitor is South Korea, with 19 percent of the market.

27 Congressional Research Service, "U.S. Semiconductor Manufacturing," 11. On July Semiconductor Industry Association, conversation with Commission staff members, July 24, 2020.

28 "2020 State of the U.S. Semiconductor Industry" (Semiconductor Industry Association, July 2020), 8, https://www.semiconductors.org/wp-content/uploads/2020/07/2020-SIA-State-of-the-Industry-Report-FINAL-1.pdf.

29 Arne Verheyde, "Intel Places Multi-Billion-Dollar Wafer Order at TSMC, Murthy Gone," *Seeking Alpha*, August 5, 2020, https://seekingalpha.com/article/4364603-intel-places-multi-billion-dollar-wafer-order-tsmc-murthy-gone.

30 Semiconductor Industry Association, "Presentation Slides for CSC" (slides, July 24, 2020).

31 Semiconductor Industry Association, "Presentation Slides for CSC" (slides, July 24, 2020).

32 Thomas Donahue, "The Worst Possible Day: U.S. Telecommunications and Huawei," *PRISM* 8, no. 3 (January 2020): 14–35, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3.pdf.

33 Stu Woo and Dustin Volz, "U.S. Considers Requiring 5G Equipment for Domestic Use Be Made Outside China," *Wall Street Journal*, June 23, 2019, https://www.wsj.com/articles/u-s-considers-requiring-5g-equipment-for-domestic-use-be-made-outside-china-11561313072;

Stefan Pongratz, "The Telecom Equipment Market 2019," *Dell'Oro Group* (blog), March 2, 2020, https://www.delloro.com/the-telecom-equipment-market-2019/. In 2019, Ericsson and Nokia held the second and third highest shares in the worldwide telecommunications suppliers market, capturing 16 percent and 14 percent of the market respectively. They are followed by China's ZTE with 10 percent of the market and the United States' Cisco with 7 percent. Comparatively, China's Huawei earned the number one spot with 28 percent of the market. Samsung has very little market share in the telecommunications equipment market, but is a major player in the integrated equipment manufacturing market.

34 Elizabeth Koh, "Samsung, Verizon Sign $6.65 Billion 5G Contract," *Wall Street Journal*, September 7, 2020, https://www.wsj.com/articles/samsung-verizon-sign-6-65-billion-5g-contract-11599469883.

35 William Morrissey and John Givens, "The Measure of a Country: America's Wonkiest Competition with China," *War on the Rocks*, August 21, 2020, https://warontherocks.com/2020/08/the-measure-of-a-country-americas-wonkiest-competition-with-china/.

36 Guang Yang, "Who Are the Leading Players in 5G Standardization? An Assessment for 3GPP 5G Activities," *Strategy Analytics*, March 16, 2020, available at https://www.strategyanalytics.com/access-services/service-providers/networks-and-service-platforms/reports/report-detail/who-are-the-leading-players-in-5g-standardization-an-assessment-for-3gpp-5g-activities.

37 Dan Strumpf, "Where China Dominates in 5G Technology," *Wall Street Journal*, February 26, 2019, https://www.wsj.com/articles/where-china-dominates-in-5g-technology-11551236701; Robert Clark, "Who Rules 5G Patents? It Depends How You Ask," *Light Reading*, January 14, 2020, https://www.lightreading.com/asia-pacific/who-rules-5g-patents-it-depends-how-you-ask/d/d-id/756790; "Who Is Leading 5G Development?" *twoBirds Pattern*, accessed August 12, 2020, https://www.twobirds.com/~/media/pdfs/who-is-leading-5g-development.pdf.

38 Pongratz, "The Telecom Equipment Market 2019."

39 William Lazonick and Edward March, "The Rise and Demise of Lucent Technologies" (March 2010), figure 1, p. 2, http://www.theairnet.org/files/research/lazonick/Lazonick%20and%20March%20Lucent%20COMPLETE%2020110324.pdf.

40 Carol J. Loomis, "The Whistleblower and the CEO," *CNN*, July 7, 2003, https://money.cnn.com/magazines/fortune/fortune_archive/2003/07/07/345538/index.htm.

41 Lazonick and March, "The Rise and Demise of Lucent Technologies," 55.

42 Donahue, "The Worst Possible Day," 19.

43 Congressional Research Service, "U.S. Semiconductor Manufacturing," 11.

44 "STEREO (Solar-Terrestrial Relations Observatory)," ESA Earth Online, accessed August 21, 2020, https://earth.esa.int/web/eoportal/satellite-missions/s/stereo.

45 "F-35 Global Partnership," Lockheed Martin, accessed September 28, 2020, https://www.lockheedmartin.com/en-us/products/f-35/f-35-global-partnership.html.

46 Congressional Research Service, "U.S. Semiconductor Manufacturing," 11; Semiconductor Industry Association, conversation with Commission staff, July 24, 2020.

47 "Foundry Revenue Estimated to Grow by 30% YoY in 1Q20, while COVID-19 Pandemic May Hinder Future Market Demand, Says TrendForce," Trendforce, March 19, 2020, https://www.trendforce.com/presscenter/news/20200319-10246.html.

48 Matthew Strong, "Taiwan to Play Key Role in Global 5G Supply Chain: Economics Minister," *Taiwan News*, September 18, 2019, https://www.taiwannews.com.tw/en/news/3779473.

49 "A Policy of 'One Country, Two Systems' on Taiwan," Ministry of Foreign Affairs of the People's Republic of China (2014), https://www.fmprc.gov.cn/mfa_eng/ziliao_665539/3602_665543/3604_665547/t18027.shtml.

50 "Taiwan – Market Overview," Export.gov, International Trade Administration, November 8, 2019, https://www.export.gov/apex/article2?id=Taiwan-Market-Overview#:~:text=Mainland%20China%20is%20Taiwan's%20largest,Hong%20Kong%20(7.1%20percent).

51 Josh Horowitz and Yimou Lee, "Taiwan's TSMC keeps eye on China with $12 billion U.S. plant," *Reuters*, May 15, 2020, https://www.reuters.com/article/us-usa-semiconductors-tsmc-china-analysi/taiwans-tsmc-keeps-eye-on-china-with-12-billion-u-s-plant-idUSKBN22R1Z7.

52 Qu Hui and Isabelle Li, "Other Customers Could Fill Gap Left By Huawei, TSMC Chief Says," Caixin, June 10, 2020, https://www.caixinglobal.com/2020-06-10/other-customers-could-fill-gap-left-by-huawei-tsmc-chief-says-101565626.html.

53 Cheng Ting-fang and Lauly Li, "TSMC Plans to Halt Chip Supplies to Huawei in 2 Months," *Nikkei Asia*, July 16, 2020, https://asia.nikkei.com/Spotlight/Huawei-crackdown/TSMC-plans-to-halt-chip-supplies-to-Huawei-in-2-months.

54 Chen Cheng-hui, "TSMC New Nanjing Fab to Ship Earlier Than Expected," *Taipei Times*, December 11, 2017, http://www.taipeitimes.com/News/biz/archives/2017/12/11/2003683759.

55 Taiwan Relations Act, 22 U.S.C. § 3301(1979). https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter48&edition=prelim. Close relations between the United States and Taiwan are challenged by the "One China" Policy, according to which the United States does not legally recognize the legitimacy of Taiwan or maintain formal diplomatic relations with it. Economic, military, and diplomatic relations must occur within the bounds of the Taiwan Relations Act.

56 "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force," Cybersecurity and Infrastructure Security Agency, last modified June 15, 2020, https://www.cisa.gov/ict-scrm-task-force.

57 "The 5G Future Incredible Promise, Significant Risk," U.S. Department of State, accessed August 20, 2020, https://policy.state.gov/5g/.

58 "Supply Chain Risk Management," National Counterintelligence and Security Center, accessed August 20, 2020, https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats.

59 "NIST Offers Strategies to Help Businesses Secure Their Cyber Supply Chains," National Institute of Standards and Technology, February 4, 2020, updated May 18, 2020, https://www.nist.gov/news-events/news/2020/02/nist-offers-strategies-help-businesses-secure-their-cyber-supply-chains.

60 Karen M. Sutter, "'Made in China 2025' Industrial Policies: Issues for Congress," CRS Report No. IF10964 (Congressional Research Service, updated August 11, 2020), https://fas.org/sgp/crs/row/IF10964.pdf.

61 Morrissey and Givens, "The Measure of a Country."

62 "The Chinese Communist Party's Military-Civil Fusion Policy," U.S. Department of State, accessed August 19, 2020, https://www.state.gov/military-civil-fusion/.

63 U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission* (March 2020), 88–92, https://www.solarium.gov/report.

64 "Congressional Legislative Tracker," The U.S.-China Business Council, accessed October 7, 2020, https://www.uschina.org/congressional-legislative-tracker.

65 Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Act, H.R. 7178, 116th Cong., 2nd sess. (June 11, 2020), https://www.congress.gov/bill/116th-congress/house-bill/7178?r=5&s=1.

66 American Foundries Act of 2020, S. 4130, 116th Congress, 2nd sess. (July 1, 2020), https://www.congress.gov/bill/116th-congress/senate-bill/4130.

67 USA Telecommunications Act of 2020, H.R. 6624, 116th Cong., 2nd sess. (April 24, 2020), https://www.congress.gov/bill/116th-congress/house-bill/6624.

68 Secure 5G and Beyond Act of 2020, S. 893, 116th Cong., 1st sess. (March 27, 2020), https://www.congress.gov/bill/116th-congress/senate-bill/893/text.

69 NDAA for FY2021, S. 4049, Title X, Subtitle H.

70 NDAA for FY2021, S. 4049, Subtitle I.

71 William M. (Mac) Thornberry National Defense Authorization Act of Fiscal Year 2021, H.R. 6395, § 826, 116th Cong., 2nd sess. (August 5, 2020), https://www.congress.gov/bill/116th-congress/house-bill/6395; NDAA for FY2021, S. 4049, § 808.

72 NDAA for FY2021, S. 4049, § 9504. 1

73 NDAA for FY2021, H.R. 6395, §§ 830D, 1259, and 1633.

74 "Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services," Cybersecurity and Infrastructure Security Agency (April 2020), https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf.

75 Subcommittee on Critical and Strategic Mineral Supply Chains Committee on Environment, Natural Resources, and Sustainability, "Assessment of Critical Minerals: Updated Application of Screening Methodology" (National Science and Technology Council, February 2018), ii, https://www.whitehouse.gov/wp-content/uploads/2018/02/Assessment-of-Critical-Minerals-Update-2018.pdf.

76 Exec. Order No. 13817, 82 F.R. 60835 (2017), https://www.federalregister.gov/documents/2017/12/26/2017-27899/a-federal-strategy-to-ensure-secure-and-reliable-supplies-of-critical-minerals.

77 U.S. Department of the Interior, "Final List of Critical Minerals 2018," 83 Fed. Reg. 23295 (2018), https://www.federalregister.gov/documents/2018/05/18/2018-10667/final-list-of-critical-minerals-2018.

78 Stephen B. Kaplan, "The Rise of Patient Capital: The Political Economy of Chinese Global Finance," Institute for International Economic Policy Working Paper Series, IIEP-WP-2018-2 (George Washington University, 2018), https://www2.gwu.edu/~iiep/assets/docs/papers/2018WP/KaplanIIEP2018-2.pdf.

79 "US Venture Capital Investment Surpasses $130 Billion in 2019 for Second Consecutive Year," NVCA (blog), January 14, 2020, https://nvca.org/pressreleases/us-venture-capital-investment-surpasses-130-billion-in-2019-for-second-consecutive-year.

80 "The Q1 2020 PitchBook-NVCA Venture Monitor," NVCA (March 31, 2020), 3, https://nvca.org/recommends/q1-2020-pitchbook-nvca-venture-monitor-xls/. As overall venture capital has steadily increased over the past 14 years, from $29.4 billion in 2006 to $140 billion in 2018 and $136 billion in 2019, investment in information technology hardware has atrophied from $5.5 billion and $6.6 billion in 2006 and 2007, respectively, to $3.2 and $3.8 billion in 2018 and 2019, respectively.

81 Software, cybersecurity, biotech, and other sectors offer quick wins with higher returns on investment for private investors because of their relatively low startup costs and capital expenditures. By contrast, hardware firms seeking investors take a longer time to see profits, often have smaller profit margins than software firms, and face a high degree of low-cost competition from China and others.

82 Semiconductor Industry Association, "Presentation Slides for CSC" (slides, July 24, 2020). Today, the semiconductors manufactured in the United States are mostly used for logic. Memory semiconductors are mostly manufactured in East Asia. While logic chips remain important, memory semiconductors are critical for the function of new and emerging technologies. U.S. companies invest in research and development for semiconductor technologies in general, but the U.S. government overall does not invest in the manufacturing technology research and development required to make those high-end semiconductors. This lack of investment makes it difficult for any domestic production capacity to exist.

83 Congressional Research Service, "U.S. Semiconductor Manufacturing," 11. Semiconductor Industry Association, conversation with Commission staff members, July 24, 2020.

84 See, for example, Anna-Katrina Shedletsky, "Made in China? Three Trends Driving Electronics Manufacturing in 2019," *Forbes*, January 24, 2019, https://www.forbes.com/sites/annashedletsky/2019/01/24/made-in-china-three-trends-driving-electronics-manufacturing-in-2019/#452df4072903; Charles Duhigg and Keith Bradsher, "How the U.S. Lost Out on iPhone Work," *New York Times*, January 21, 2012, https://www.nytimes.com/2012/01/22/business/apple-america-and-a-squeezed-middle-class.html; "Electronics: Where to Invest?," Association of Southeast Asian Nations, accessed August 20, 2020, http://investasean.asean.org/index.php/page/view/electronics.

85 White House Office of Trade and Manufacturing Policy, "How China's Economic Aggression Threatens the Technologies and the Intellectual Property of the United States and the World" (June 2018), https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

86 "Standards and Patents," World Intellectual Property Organization, accessed July 16, 2020, https://www.wipo.int/patent-law/en/developments/standards.html.

87 Strumpf, "Where China Dominates in 5G Technology"; "Who Is Leading 5G Development?" *twoBirds Pattern*. ctoFor example, the U.S. company Qualcomm earns more than a fifth of its total revenue—some $5.2 billion—from technology licensing agreements. Huawei does not disclose its revenue from these sources; but according to one methodology, Qualcomm holds 787 standards-essential patents (SEPs) to 5G technology, Huawei holds 1,529, and ZTE holds another 1,208. According to other methodologies, Huawei and ZTE hold the fifth

and seventh most 5G SEPs, at 10.9 percent and 8.6 percent respectively, while Qualcomm is in third place with 12.6 percent. What is indisputable, however, is that Huawei sits in first place for the most patents submitted.

88 For example, companies with outsize influence in the standards process can shape standards to the technologies that they intend to produce in the future. Today, many of the international standards around telecommunications equipment, particularly 5G equipment, are being driven by Chinese firms. Huawei alone has submitted 11,423 proposals for 5G standards—more than any other firm, and double the number submitted by its largest American competitor. See Strumpf, "Where China Dominates in 5G Technology."

89 National Security Telecommunications Advisory Committee, "NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem" (Cybersecurity and Infrastructure Security Agency, September 3, 2019), B-1, https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_0.pdf.

90 Gareth Sitaraman, "Industrial Revolutionaries," *The American Prospect*, September 10, 2020, https://prospect.org/economy/industrial-revolutionaries-franklin-hamilton-madison-jackson/.

91 For more detail on these case studies, see Annex II of this report.

92 Natasha Cohen et al., "Cybersecurity as an Engine for Growth" New America (September 2017), https://d1y8sb8igg2f8e.cloudfront.net/documents/FINAL_Clusters.pdf.

93 See NDAA for FY2021, S. 4049, Subtitle I; NDAA for FY2021, H.R. 6395, Subtitle F; NDAA for FY2021, S. 4049, § 808.

94 U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission*, 90–92.

95 "Japan to Pay Firms to Leave China, Relocate Production Elsewhere as Part of Coronavirus Stimulus," *South China Morning Post*, April 9, 2020, https://www.scmp.com/news/asia/east-asia/article/3079126/japan-pay-firms-leave-china-relocate-production-elsewhere-part.

96 See, for example, NDAA for FY2021, S. 4049, Subtitle I.

97 50 U.S.C. § 4531.

98 50 U.S.C. § 4532.

99 CISA, "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force"; "CISA 5G Strategy: Ensuring the Security and Resilience of 5G Infrastructure in Our Nation," Cybersecurity and Infrastructure Security Agency (August 24, 2020), https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf.

100 "About NSTAC," Cybersecurity and Infrastructure Security Agency, last updated March 6, 2019, https://www.cisa.gov/about-nstac. The NSTAC is a collaboration between the government and private sector to provide the President with advice and expertise regarding enhancing cybersecurity, maintaining the global communications infrastructure, and addressing critical infrastructure interdependencies and dependencies, among others.

101 "Cybersecurity Maturity Model Certification," Office of the Under Secretary of Defense for Acquisition and Sustainment, Department of Defense, accessed August 21, 2020, https://www.acq.osd.mil/cmmc/; "Department of Defense (DoD) 5G Strategy," U.S. Department of Defense (May 2, 2020), 2020), https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf.

102 "The Clean Network," U.S. Department of State, accessed August 24, 2020, https://www.state.gov/the-clean-network/.

103 "Cyber Supply Chain Risk Management," National Institute of Standards and Technology, May 24, 2016, updated June 22, 2020, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.

104 U.S. Cyberspace Solarium Commission, Report of the United States of America Cyberspace Solarium Commission, 37–38 (Recommendation 1.3).

105 "Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics," GAO-07-39 (U.S. Government Accountability Office, October 2006), 1, https://www.gao.gov/assets/260/252603.pdf.

106 National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 6306, 133 Stat. 1198 (2019), https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf.

107 CISA, "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force."

108 "Enabling Successful Wireless Solution Development: Wireless Test Bed," Idaho National Laboratory, accessed August 21, 2020, https://inl.gov/wnuf/; "Information Design Assurance Red Team," Sandia National Laboratories, 2020, https://idart.sandia.gov/.

109 U.S. Cyberspace Solarium Commission, Report of the United States of America Cyberspace Solarium Commission, 75 (Recommendation 4.1.1).

110 Aaron Flaaen and Justin Pierce, "Disentangling the Effects of the 2018–2019 Tariffs on a Globally Connected U.S. Manufacturing Sector," Finance and Economics Discussion Series 2019-086 (Board of Governors of the Federal Reserve System, 2019), https://doi.org/10.17016/FEDS.2019.086.

111 Congressional Budget Office, *The Budget and Economic Outlook: 2020 to 2030* (Washington, DC: CBO, 2020), 33, https://www.cbo.gov/system/files/2020-01/56020-CBO-Outlook.pdf.

112 Exec. Order No. 13873, 3 C.F.R. 22689 (2019), https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/FR-2019-05-17.pdf.

113 Josh Bivens, "The Potential Macroeconomic Benefits from Increasing Infrastructure Investment," Economic Policy Institute, July 18, 2017, https://www.epi.org/publication/the-potential-macroeconomic-benefits-from-increasing-infrastructure-investment/.

114 Pongratz, "The Telecom Equipment Market 2019."

115 Pongratz, "The Telecom Equipment Market 2019."

116 *5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation*, 116th Cong. 1st sess. (2019) (testimony of Peter Harrell, Adjunct Senior Fellow, Energy, Economics, and Security Program, Center for a New American Security), https://www.judiciary.senate.gov/imo/media/doc/Harrell%20Testimony.pdf.

117 David Shepardson, "AT&T CEO Says China's Huawei Hinders Carriers from Shifting Suppliers for 5G," *Reuters*, March 20, 2019, https://www.reuters.com/article/us-att-ceo-huawei-tech/att-ceo-says-chinas-huawei-hinders-carriers-from-shifting-suppliers-for-5g-idUSKCN1R12TX.

118 Xiaoxu Sean Lin, "The Threat of One-Stop Smart City Solutions by Huawei and ZTE," *Epoch Times*, February 28, 2019, updated March 4, 2019, https://www.theepochtimes.com/the-threat-of-one-stop-smart-city-solutions-by-huawei-and-zte_2810513.html.

119 "EXIM: What We Do," Export-Import Bank of the United States, accessed August 21, 2020, https://www.exim.gov/what-we-do.

120 Robert Wolf and Kevin Varney, "Why We Need the Export-Import Bank," *CNBC*, August 5, 2014, https://www.cnbc.com/2014/08/05/why-we-need-the-export-import-bankcommentary.html.

121 "Overview," U.S. International Development Finance Corporation, accessed September 28, 2020, https://www.dfc.gov/who-we-are/overview.

122 "About Us," U.S. Trade and Development Agency, accessed September 28, 2020, https://ustda.gov/about/.

123 U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission*, 88.

124 50 U.S.C. § 4558(c).

125 Russell T. Vought and Kelvin K. Droegemeier, "Fiscal Year 2021 Administration Research and Development Budget Priorities," Memorandum for the Heads of Executive Departments and Agencies (Executive Office of the President, August 30, 2019), https://www.whitehouse.gov/wp-content/uploads/2019/08/FY-21-RD-Budget-Priorities.pdf.

126 National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 6306, 133 Stat. 1198 (2019), https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf.

127 "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force," Cybersecurity and Infrastructure Security Agency, last modified June 15, 2020, https://www.cisa.gov/ict-scrm-task-force.

128 50 U.S.C. § 2152.

129 50 U.S.C. § 4552(14).

130 50 U.S.C. § 4558(c.)

131 50 U.S.C. § 4558(j).

132 50 U.S.C. § 4555(a)

133 Tariffs are a tool commonly used to protect domestic industry, but additional protection is offered by Foreign Trade Zones, which are secure areas under the supervision of U.S. Customs and Border Protection (CBP). These zones allow companies to import components to assemble final goods free of normal import duties. See "About Foreign-Trade Zones and Contact Info," U.S. Customs and Border Protection, last modified March 2, 2020, https://www.cbp.gov/border-security/ports-entry/cargo-security/cargo-control/foreign-trade-zones/about.

134 U.S. Cyberspace Solarium Commission, Report of the United States of America Cyberspace Solarium Commission, 90–92 (Recommendation 4.6.2).

135 Endless Frontier Act, S. 3832, 116th Cong., 2nd sess. (May 21, 2020), https://www.congress.gov/bill/116th-congress/senate-bill/3832/text.

136 See, for example, National Defense Authorization Act for Fiscal Year 2021, S. 4049, Title X, Subtitle H—Wireless Supply Chain Innovation and Multilateral Security, 116th Cong., 2nd sess. (July 23, 2020), https://www.congress.gov/bill/116th-congress/senate-bill/4049/text.

137 See, for example, NDAA for FY2021, S. 4049, Title X, Subtitle I—Semiconductor Manufacturing Incentives.

138 50 U.S.C. § 4531.

139 50 U.S.C. § 4532.

140 CISA, "Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force."

141 "About NSTAC." Cybersecurity and Infrastructure Security Agency, last modified March 6, 2019, https://www.cisa.gov/about-nstac. The NSTAC is a collaboration between the government and private sector to provide the President with advice and expertise on enhancing cybersecurity, maintaining the global communications infrastructure, and addressing critical infrastructure interdependencies and dependencies, among other matters.

142 "Cybersecurity Maturity Model Certification," Office of the Under Secretary of Defense for Acquisition and Sustainment, accessed August 21, 2020, https://www.acq.osd.mil/cmmc/.

143 "Cyber Supply Chain Risk Management," National Institute of Standards and Technology, May 24, 2016, updated June 22, 2020, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.

144 "*C*ritical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics," GAO-07-39 (Government Accountability Office, October 2006), 1, https://www.gao.gov/assets/260/252603.pdf.

145 This recommendation is taken directly from the Commission's March 2020 report: see U.S. Cyberspace Solarium Commission, *Report of the United States of America Cyberspace Solarium Commission*, 75 (Recommendation 4.1.1.).

146 President's National Infrastructure Advisory Council, "Transforming the U.S. Cyber Threat Partnership" (December 12, 2019), 11, https://www.cisa.gov/sites/default/files/publications/NIAC-Working-Group-Report-DRAFT-508.pdf. The President's National Infrastructure Advisory Council made a similar recommendation to test the security of critical technologies.

147 Open-source software forms the basis for most software written and deployed today: one survey found that 96 percent of applications contain open-source components (Zeljka Zorz, "The Percentage of Open Source Code in Proprietary Apps Is Rising," Help Net Security, May 22, 2018, https://www.helpnetsecurity.com/2018/05/22/open-source-code-security-risk/). When vulnerabilities are found in open-source code, many of the projects that rely on that code have neither mechanisms for fixing those vulnerabilities nor mechanisms for notifying users of the code about the patch.

148 Josh Bivens, "The Potential Macroeconomic Benefits from Increasing Infrastructure Investment," Economic Policy Institute, July 18, 2017, https://www.epi.org/publication/the-potential-macroeconomic-benefits-from-increasing-infrastructure-investment/.

149 Further Consolidated Appropriations Act, 2020, Pub. L. 116-94, 133 Stat. 3021 (2019).

150 "About TVA," Tennessee Valley Authority, accessed August 21, 2020, https://www.tva.com/about-tva.

151 "First Inaugural Address of Franklin D. Roosevelt," March 4, 1933, Yale Law School, Lillian Goldman Law Library: The Avalon Project, https://avalon.law.yale.edu/20th_century/froos1.asp.

152 "TVA," History.com, August 3, 2017, updated June 10, 2019, https://www.history.com/topics/great-depression/history-of-the-tva.

153 Herbert Hoover, "Veto of the Muscle Shoals Resolution," March 3, 1931, http://college.cengage.com/history/ayers_primary_sources/vetoesmuscle_shoalsbill_1931.htm.

154 Tennessee Valley Authority Act of 1933, 16 U.S.C. § 831 (1933), https://tva-azr-eastus-cdn-ep-tvawcm-prd.azureedge.net/cdn-tvawcma/docs/default-source/default-document-library/site-content/about-tva/tva_act.pdf?sfvrsn=99c2b8c4_0.

155 For these details, see Captain L. S. Howeth, USN (Ret.), "The Navy and the Radio Corporation of America," chap. 30 of History of Communications-Electronics in the United States Navy (Washington, DC: Government Printing Office, 1963), 353–70, https://earlyradiohistory.us/1963hw30.htm.

156 Howeth, "The Navy and the Radio Corporation of America."

157 "U.S. Semiconductor Manufacturing: Industry Trends, Global Competition, Federal Policy" (Congressional Research Service, June 27, 2016), 6, https://www.everycrsreport.com/files/20160627_R44544_77fdee097eaaac05bcf7bd6041d5bdf44b24c7b9.pdf.

158 "The Nobel Prize in Physics 1956," Nobel Prize Organisation, accessed August 25, 2020, https://www.nobelprize.org/prizes/physics/1956/summary/.

159 "Building America's Innovation Economy," Semiconductor Industry Association (March 2020), https://www.semiconductors.org/wp-content/uploads/2020/03/2020_SIA_Industry-Facts_5-14-2020.pdf.

160 Katie Hafner, "Does Industrial Policy Work? Lessons from Sematech," *New York Times*, November 7, 1993, https://www.nytimes.com/1993/11/07/business/does-industrial-policy-work-lessons-from-sematech.html.

161 "SEMATECH," Defense Advanced Research Projects Agency, accessed August 21, 2020, https://www.darpa.mil/about-us/timeline/sematech.

162 U.S. Department of Defense and SEMATECH, "Memorandum of Understanding: SEMATECH" (May 12, 1988, amended February 10, 1998), https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/10-F-0709_Memorandum_of_Understanding_SEMATECH.pdf.

163 Douglas A. Irwin and Peter J. Klenow, "Sematech: Purpose and Performance," *Proceedings of the National Academy of Sciences* 93, no. 23 (November 1996): 12739–42, https://doi.org/10.1073/pnas.93.23.12739.

164 Congressional Budget Office, *Reducing the Deficit: Spending and Revenue Options,:A Report to the Senate and House Committees on the Budget as Required by Public Law 93-433* (Washington, DC: U.S. Government Printing Office, 1993), 84–85, https://www.cbo.gov/sites/default/files/103rd-congress-1993-1994/reports/93doc08.pdf; Keith Bradsher, "Business Technology; U.S. to Aid Industry in Computer Battle with the Japanese," *New York Times*, April 27, 1994, https://www.nytimes.com/1994/04/27/us/business-technology-us-to-aid-industry-in-computer-battle-with-the-japanese.html.

165 Congressional Budget Office, *Reducing the Deficit*, 84.

166 DoD and SEMATECH, "Memorandum of Understanding: SEMATECH."

167 Zoë Bernard, "Here's the Story behind How Silicon Valley Got Its Name," *Business Insider*, December 9, 2017, https://www.businessinsider.com/how-silicon-valley-got-its-name-2017-12.

168 "1958: Silicon Mesa Transistors Enter Commercial Production," Computer History Museum, 2020, https://www.computerhistory.org/siliconengine/silicon-mesa-transistors-enter-commercial-production/.

169 Charles Fishman, *One Giant Leap: The Impossible Mission That Flew Us to the Moon* (New York: Simon & Schuster, 2019), 11.

170 Fishman, *One Giant Leap*, 303.

171 Robert D. Atkinson, and Jackie Whisman, with Margaret O'Mara, "The Real History of Silicon Valley and the Lesson It Holds for Innovation Policy Today," June 8, 2020, in *Innovation Files: Exploring the Intersection of Technology, Innovation, and Public Policy,* produced by Information Technology & Innovation Foundation, podcast, MP3 audio, 32:42, https://itif.org/publications/2020/06/08/podcast-real-history-silicon-valley-and-lessons-it-holds-innovation-policy.

172 Vitaly M. Golomb, "The Government Once Built Silicon Valley," *Techcrunch*, July 4, 2014, https://techcrunch.com/2014/07/04/the-government-once-built-silicon-valley/.

173 Golomb, "The Government Once Built Silicon Valley."

174 Golomb, "The Government Once Built Silicon Valley."

175 Golomb, "The Government Once Built Silicon Valley."

176 "Silicon Valley Bank Breaks Export-Import Bank Record; Helps Clients Expand and Export Globally," Silicon Valley Bank, news release, April 12, 2004, https://www.svb.com/news/company-news/silicon-valley-bank-breaks-export-import-bank-record-helps-clients-expand-and-export-globally.

177 Golomb, "The Government Once Built Silicon Valley."

178 Mariana Mazzucato, *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*, rev. ed. (New York: Public Affairs, 2015), 93–119; Atkinson and Whisman, with O'Mara, "The Real History of Silicon Valley."

179 Nigel Cameron, "The Government Agency That Made Silicon Valley," *UnHerd*, June 18, 2018, https://unherd.com/2018/06/government-agency-made-silicon-valley/#en-14687-5.

180 Heidi Hackford, "The Valley and the 'Swamp': Big Government in the History of Silicon Valley," *Computer History Museum* (blog), October 10, 2019, https://computerhistory.org/blog/the-valley-and-the-swamp-big-government-in-the-history-of-silicon-valley/.

181 Hackford, "The Valley and the 'Swamp.'"

182 Atkinson and Whisman, with O'Mara, "The Real History of Silicon Valley."

COMMISSIONERS

CO-CHAIRMEN

Angus S. King Jr., U.S. Senator for Maine

Michael "Mike" J. Gallagher, U.S. Representative for Wisconsin's 8th District

COMMISSIONERS

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Thomas A. "Tom" Fanning, Chairman, President, and Chief Executive Officer of Southern Company

John C. "Chris" Inglis, U.S. Naval Academy Looker Chair for Cyber Studies

James R. "Jim" Langevin, U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Benjamin E. "Ben" Sasse, U.S. Senator for Nebraska

Suzanne E. Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

STAFF

SENIOR STAFF

Mark Montgomery, Executive Director

Deborah Grays, Chief of Staff

Erica Borghard, Senior Director and Task Force One Lead

John Costello, Senior Director and Task Force Two Lead

Val Cofield, Senior Director and Task Force Three Lead

Cory Simpson, Senior Director and Directorate Four Lead

Benjamin Jensen, Senior Research Director and Lead Writer

WHITE PAPER LEAD WRITER

Robert Morgus, Senior Director for Research and Analysis

FULL TIME STAFF

Laura Bate, Senior Director for Cyber Engagement

Tatyana Bolton, Policy Director

Gregory Buck, Deputy Chief of Staff

Madison Creery, Cyber Strategy and Policy Analyst

Matthew Ferren, Cyber Strategy and Policy Analyst

Chris Forshey, Facility Security Officer

Karrie Jefferson, Director for Cyber Engagement

Ainsley Katz, Cyber Strategy and Policy Analyst

Alison King, Strategic Communications and Congressional Advisor

Sang Lee, Director for Cyber Engagement

Diane Pinto, Cyber Strategy and Policy Analyst

Brandon Valeriano, Senior Advisor

LEGAL ADVISORS

Stefan Wolfe, General Counsel

Corey Bradley, Deputy General Counsel

Cody Cheek, Legal Advisor

David Simon, Chief Counsel for Cybersecurity and National Security

PRODUCTION SUPPORT

Alice Falk, Editor

Laurel Prucha Moran, Graphic Designer


U.S. CYBERSPACE SOLARIUM COMMISSION
E PLURIBUS UNUM