



HOMELAND SECURITY ADVISORY COUNCIL

Final Report: Economic Security Subcommittee

NOVEMBER 2020



**Homeland
Security**

This publication is presented to the Honorable Chad F. Wolf, Acting Secretary of the Department of Homeland Security (DHS) on behalf of the Homeland Security Advisory Council (HSAC), Subcommittee on Economic Security. The Economic Security Subcommittee is led by Frank Cilluffo (Chair), and Stewart Baker and Robert Rose (Co Vice Chairs).

<SIGNATURE OBTAINED FOR PDF COPY>

signature

Chair, Frank Cilluffo

Director of Auburn University's

McCrary Institute for

Cyber and Critical Infrastructure Security

Co Vice Chair, Stewart Baker

Steptoe & Johnson

Co Vice Chair, Robert Rose

Founder and President

Robert N. Rose Consulting LLC

This page is intentionally left blank.

TABLE OF CONTENTS

TABLE OF CONTENTS	4
EXECUTIVE SUMMARY AND RECOMMENDATIONS	5
INTRODUCTION	9
The Threat to American Economic Security is Growing	9
China	9
Chinese Communist Party Strategy.....	10
Economic Espionage and Theft of U.S. Technology.....	11
“Supply Chain Independence for Me, But Not for Thee”-China’s Quest for Self-.....	12
U.S. Dependence and Supply Chain Vulnerability.....	13
Russia	14
Responding to Our New Vulnerability	15
Defense Department.....	15
Treasury Department.....	19
Commerce Department.....	19
State Department.....	20
Intelligence Community.....	21
Export-Import Bank of the United State.....	22
Cyberspace Solarium Commission.....	23
The Role of the Department of Homeland Security	26
Recommendation 1.....	27
CISA.....	27
The Office of Management.....	28
Recommendation 2.....	28
The Office of Strategy, Policy and Plans.....	28
Recommendation 3.....	29
Recommendation 4.....	30
Recommendation 5.....	30
Recommendation 6.....	31
Recommendation 6a.....	31
Recommendation 6b.....	32
Recommendation 6c.....	32
Recommendation 6d.....	33
Recommendation 6e.....	33
Recommendation 7.....	33
Federal Emergency Management Agency.....	34
Recommendation 8.....	34
Recommendation 8a.....	34
Recommendation 8b.....	35
Recommendation 8c.....	35
The Trade Enforcement and Immigration Agencies — CBP, ICE/HSI, and USCIS.....	35
Recommendation 9.....	36
Recommendation 10.....	36
Recommendation 11.....	36
The Transportation Security Administration (TSA).....	36
Recommendation 12.....	38
Recommendation 13.....	39
Additional Homeland Security Stakeholders.....	39
Recommendation 14.....	39
Acknowledgments.....	40
Appendix 1: Tasking Letter.....	41
Appendix 2: Subcommittee Membership.....	43
Appendix 3: List of Witnesses.....	44

Executive Summary and Recommendations

As COVID-19 began to ravage the United States, Americans got a disturbing insight into the price we might ultimately pay for inexpensive imports from China. An op-ed in that country's official Xinhua site talked openly about the leverage the pandemic would give them over the United States. China made most of the face masks used in this country, the article noted, so "if China prohibits the export of masks to the United States, the United States will fall into a mask shortage."¹ The United States also imports most of its pharmaceuticals, so if China banned exports "the United States would sink into the hell of a novel coronavirus epidemic."² Later, China actually did impose export restrictions on masks and ventilator components, preventing U.S. companies like 3M and General Electric from getting deliveries even from their own subsidiaries; and many suspected that China's government was indeed using its control of the medical supply chain to extract concessions from the United States.³

This may have been the moment when Americans realized that the comfortable assumptions underlying a generation of policy were fundamentally wrong. Economic interdependence was not easing either China's confrontational diplomacy or its authoritarianism.⁴ Encouraging American companies to cut costs by outsourcing their supply chain to China might have a cost greater even than lost jobs and community investment. Just when we need those components the most, an adversarial Chinese government might decide to cut off deliveries.

Discovering that cold fact with thousands of lives at risk has galvanized bipartisan concern about the nation's economic security. For national security, we have long maintained a defense industrial base so that our economy can produce the goods we need to keep our military in the field. Yet few had asked, until now, whether the United States has a similar ability to ensure economic security — to keep the civilian side of our economy functioning in a time of crisis.

No more. Having seen the risk, leaders in the Administration and on both sides of the aisle in Congress are focused on how to avoid dependence on hostile nations for critical parts of our civilian supply chain.

How can the Department of Homeland Security (DHS) contribute to the goal of greater economic security? That is the question this Subcommittee has been asked to address. It is, we conclude, the kind of job for which the Department was built. The Department's mission is to prepare the nation for disasters of every sort — whether terrorist attacks, hurricanes, or pandemics. It understands better than most what the country needs in a crisis. And it knows that planning for bad news is the best way to keep the news from getting worse. If we want to make sure our critical civilian infrastructure keeps working in time of need, the Department's culture and tools will be an essential part of the solution.

Accordingly, this report makes a series of recommendations for how the Department should galvanize itself to address the current economic security threat. We begin by acknowledging the valuable contribution of the bipartisan Cyberspace Solarium Commission and its White Paper on supply chain security risks, which aims many of its recommendations at DHS. In addition to

those steps, the Subcommittee recommends the following actions, all of which are discussed in detail in the body of the report:

Recommendation 1: The department should institutionalize the Economic Security Council. Congress should provide a legislative mandate for the establishment and maintenance of the council to identify concentrated risks, to set priorities and to coordinate enterprise-wide action on economic security matters.

Recommendation 2: DHS must lead by example in procurement practices that foster cybersecurity, including supply chain security. The Secretary should ensure effective coordination through the Economic Security Council or some other mechanism among the many offices that can contribute to security in acquisitions, including the Office of Management, the Office of Acquisition, the acquiring component, CISA, the Chief Information Officer, and the Office of Science and Technology.

Recommendation 3: A Deputy Assistant Secretary for Economic Security should be institutionalized within the Office of Strategy, Policy, and Plans.

Recommendation 4: The intelligence community and DHS should create a joint supply chain intelligence center with private sector entities as participants and customers. This center should provide practical guidance about suppliers that may pose a particular risk. The center should also influence intelligence collection priorities and provide feedback to improve the quality of supply chain intelligence.

Recommendation 5: The Secretary should define roles and missions and coordination responsibilities between CISA and the Office of Strategy, Policy and Plans, for the task of mapping civilian supply chain and economic security risks.

Recommendation 6: At the start, the DHS economic security effort should be incremental, focused on high-impact, focused reviews of priority topics/sectors.

- DHS should formalize its role in supplying data and risk management analysis to the Commerce Department pursuant to E.O. 13873.
- DHS should conduct a joint DoD-DHS analysis of the industries identified by China as its priorities for ensuring China's economic security (and reducing the economic security of the United States). The study should ask two questions about every industry on China's shopping list: which U.S. producers are put at risk by China's mercantilist policies and what can the U.S. do to ensure their survival?
- DHS should conduct industry-wide supply chain assessments of particular companies or industries based on referrals from CFIUS, from Team Telecom, and from the E.O. 13873 interagency process.
- DHS's economic security unit should also accept referrals from the Federal Acquisition Security Council. It should be possible for the Council to seek a broader

study of a particular industry or company than the Council itself is designed to perform. DHS's economic security unit should be prepared to accept such referrals.

- The DHS economic security unit should accept nominations for economic security reviews from DHS components concerned about their critical components.

Recommendation 7: DHS's economic security unit should be a focal point for Hart-Scott-Rodino reviews where the merger could reduce competition or security in sales of equipment that is vital to DHS missions, such as icebreakers and cargo and traveler scanning equipment.

Recommendation 8: FEMA, in coordination with DHS and the interagency, should put forward a framework for an executive order or legislation that revives and makes best use of existing authorities under the Defense Production Act and related executive and statutory authorities.

- FEMA should rebuild its internal structures and programs to ensure that it has the resources necessary to respond to sudden national shortages during a national emergency.
- FEMA and DHS should strengthen their engagement with the Title III program under the Defense Production Act, and develop an institutional capability to sponsor and follow through on the use of Title III funds to meet homeland economic security goals.

Recommendation 9: The Secretary should direct CBP and ICE/HSI to make enforcement of economic security measures a measurable enforcement priority — and an intelligence collection target.

Recommendation 10: The Secretary should direct USCIS and ICE to increase coordination on student visas, granting USCIS appropriate access to SEVIS data and working together on site visits and investigations in technology-heavy visa programs such as CPT and OPT. The Secretary should direct CBP, ICE, and USCIS to standardize and make available to each other data on foreign nationals coming to the U.S. for research and study; the State Department should join in this initiative.

Recommendation 11: USCIS and the relevant HSAC subcommittee should review the EB-5 program for the risk that Chinese applicants may be operating as agents of the Chinese government.

Recommendation 12: DHS should engage its interagency partners to:

- Spur creation of a technology oversight and regulating task force to ensure that rapidly evolving Chinese technology does not evade necessary regulation;
- Expand UAS regulatory resources (with support from Congress);
- Encourage and actively support innovation in the development and production of UAS in the United States by U.S. companies, particularly for those UAS intended for U.S. government use;
- Regulate the export of data (such as imagery) collected by UAS manufacturers;

- Consider requiring validation of the security of software, firmware, hardware and other UAS elements; and
- Ensure effective detection and tracking of UAS and identification of UAS registrants

Recommendation 13: TSA and the Deputy Assistant Secretary for Economic Security should jointly review the threat posed by Nuctech and other passenger and cargo screening equipment from China, with particular emphasis on Nuctech's access to data and algorithms used by security agencies. DHS should decide whether the use of insecure equipment is consistent with TSA's foreign airport security assessment standards.

Recommendation 14: In coordination with the federal interagency process, the Department should identify relevant global standard-setting activities likely to have an impact on DHS and determine whether Chinese government efforts to influence the standards require monitoring or action.

INTRODUCTION

DHS has a unique contribution to make to the security of U.S. trade lanes, supply chains, investments abroad, cyberinfrastructure, and immigration systems. At the same time, many other parts of the federal government are equally essential to the effort. In the face of a highly coordinated and well-financed strategic competitor — namely China — we cannot resort to bureaucratically siloed efforts. If we do, we can expect China (and others) to find new and destructive ways to exploit our dependence.

With those considerations in mind, this report will focus first on the challenge posed by adversary nations hoping to use economic interdependence against the United States. It will then provide an overview of the work already being done in other U.S. government agencies on economic security issues and how DHS can assist them. Finally, the report will take a closer look at what components of the Department are doing on the issue. Because this is a report to the Secretary of Homeland Security, we have aimed our recommendations principally at the activities and organization of that Department.

The Threat to American Economic Security is Growing

China

China's conduct during the global pandemic is only the most recent evidence that China does not intend to smoothly integrate into the multilateral globalized trade and tariff arrangements that the United States helped to build and maintain over the past five decades.⁵ Those arrangements have lowered tariffs and trade barriers, creating a presumption that international trade will be shaped by each nation's comparative economic advantages rather than its mercantilist power. While China has grown rich under this open, rules-based economic order, it has not accepted the underlying premises of that order. Instead, China's success has deepened its commitment to an authoritarian and mercantilist economic system.

China's new prosperity has also made more obvious its lack of respect for the system that made possible its rise. It now has far more weight in the international trading system, so when it throws that weight around, everyone notices. It is no longer possible to assume, as a generation of policymakers did, that trade with China would mean cheaper goods in the U.S. in the short term and more democracy and commitment to the trading system in Beijing over the long haul.

Instead, it is clear that for at least the near future, China will remain a deeply authoritarian state in which economic activity is subordinated to the political goals of the Chinese Communist Party. Those goals include military, economic, and technological power sufficient to dominate Asia and force the United States to accept the legitimacy of China's political system and its primacy in large parts of the world.⁶

The emerging strategic competition between the United States and China is more than military. While China's growing military power is undoubtedly a concern, the new long-term “threats” are decidedly economic, and the new “weapons” are trade deals, innovation, technology and intellectual property, global standards (data, e-commerce, customs), infrastructure, and critical supply chain dependencies (weaknesses exacerbated and laid bare by COVID-19).⁷ The U.S.-China strategic competition is increasingly driven by who controls the underlying systems, technologies, and rules by which we advance our economic interests.

We now know how China will pursue that competition. It has already rejected the political reform that most Americans hoped would come with greater prosperity. It has rejected freedom of speech and press, human rights, transparent governance, and religious freedoms, and its commitment to economic reform is limited by its ruler’s determination to maintain political and ideological control of even its largest companies.⁸ That determination means that China will take two roads at once. It will participate and pursue its interests inside the existing multilateral system while at the same time undercutting that system with actions and institutions that run counter to the assumptions of multilateral trade.

The United States finds itself at a critical moment. It must reconsider in light of the Chinese challenge all the assumptions on which America’s global trade patterns rest. As Beijing works to gain power and influence in both developing economies as well as the historically open economic and political systems of the U.S. and its allies, protecting the homeland requires that the U.S. understand and prepare for the ways in which trade with China exposes us to economic pressure.

Chinese Communist Party Strategy

For nearly three decades, the Chinese Communist Party (CCP) has been developing and expanding a new form of authoritarian mercantilist government. This governance model has resulted in China emerging as a strategic competitor to the United States. The relationship is unique in U.S. history because China is a large trading partner that also threatens the United States economically, technologically, and militarily. China has a population four times that of the United States.⁹ Most economic studies project China’s GDP to exceed that of the U.S. by 2030, though some caution that a reduced birth rate means that China may “grow old before it grows rich.”¹⁰ Even so, its unprecedented economic growth seems certain to allow China to increase its economic coercion and expand its military.

Over the past two decades, developing commercial technologies have caused a shift in the nature of global power. Technology is transforming entire economies and creating a gusher of wealth for some companies and some countries. The People’s Republic of China sees this as an opportunity to gain advantage over its western rivals. China's grand strategy has been to use its vast domestic market to attract foreign technical expertise and technology and then gradually turn the market over to national champions able to push out the foreign firms, with as much help from Beijing as those champions may need.¹¹ The goal is to build an advanced Chinese technology industry independent of the rest of the world. In the end, protected from challenge in China, its companies will be free to challenge western competitors in their home markets.

For the CCP, economic competition is part of a struggle to advance China against what it sees as a U.S.-led effort to contain China and suppress its rise. The CCP's system of strategic competition and authoritarian control has long depended on aggressive use of digital technology. The CCP employs the same sorts of data, sensors, and artificial intelligence as U.S. high-tech companies, and it has turned that technology into an effective method of social control.¹² Originally designed to keep its own population in check, the party has discovered that it can also use its technology and economic influence to constrain political expression and action around the world. In recent years, the CCP has expanded its efforts to control or influence foreign companies, governments, media, and populations. Wherever it perceives a dependence on the Chinese economy, it has wielded that dependence as a weapon. Just since the COVID-19 crisis, China's leaders have threatened western governments, arrested and expelled journalists, and stopped U.S. and other companies from operating in China because of statements or actions that did not fully support the CCP regime.¹³ In addition to the use of economic leverage, China's effort to control countries and companies outside its borders has included payments to corrupt government officials, extensive cyber attacks, and media influence campaigns.

At the core of China's global strategy is the goal of altering the current international rules-based order. Changing the current international order is essential for China to fulfill its stated objective of "reascending to its rightful place at the top of the world" by 2049, when it intends to be the dominant power in Asia and an economic, technological, and military global superpower.¹⁴

The principal obstacle to this goal is the United States. To achieve "national rejuvenation," therefore, China has carried out economic aggression, cyberespionage, covert influence campaigns, and intellectual property theft against U.S. interests. The National Security Strategy and the National Defense Strategy of the United States both warn of the risks posed by China's economic rise and by the CCP's stated objectives of altering the world order.¹⁵

Economic Espionage and Theft of U.S. Technology

To obtain the cutting-edge technology China needs to meet its ambitious goals, China has been prepared to use whatever leverage it has.

In many cases, this leverage comes from China's ability to steal secrets from commercial firms that cannot defend themselves against nation-state espionage. China's economic espionage and illegal acquisition of technology in the United States have been primarily directed at aerospace, information, and energy technologies as well as biopharma and new materials development.¹⁶ These activities are actively encouraged by the CCP at the central government and provincial levels. At least 75 percent of the prosecutions involving Chinese economic espionage are tied to the key technologies identified in China's industrial planning document *Made in China 2025*.¹⁷ A conservative estimate is that the U.S. has in total lost over \$1 trillion to China's collection efforts. This does not include the impact on the U.S. economy, such as loss of jobs and market share, and losses from counterfeit and pirated tangible goods, and software piracy.

In other cases, China's leverage comes from the eagerness of western firms to participate in China's massive domestic market. The government actively pressures western firms hoping to sell in China to turn over key strategic technologies in order to do business there.¹⁸ China has

adopted a set of policies designed to reinforce the pressure. In many cases, technology transfers are effectively required by China's foreign direct investment regime, which closes off important sectors of the economy to foreign firms unless they enter into joint ventures with Chinese entities. In addition, China's 2017 Cybersecurity Law requires that foreign firms' technology and services pass national security reviews; that they store all data in China; that western data center providers form joint ventures with the Chinese companies who will eventually become their competitors; that they use Chinese government-approved encryption and virtual private networks whose effectiveness against Chinese government spying is questionable; and that data transfers to the home office require Chinese government approval.¹⁹

“Supply Chain Independence for Me, But Not for Thee” — China's Quest for Self-Reliance

For at least fifteen years, the goal of all this theft and pressure has been clear: China is determined to achieve autonomy in digital technology products.

In 2006, China officially announced its plans for indigenous innovation. In 2008, the CCP Organization Department implemented the Thousand Talents Program. This program is only one of more than 300 such programs designed to enlist the talents of foreign-educated scientists and researchers to serve China's national development needs. To date, these programs have enlisted more than 60,000 foreign experts.²⁰ However, these programs were not designed to be permanent. They were only designed to advance China's scientific, technical, and financial expertise to the point of self-sufficiency. Many of the Thousand Talents Program contracts require western academics to establish shadow laboratories in Chinese universities and train Ph.D. students.²¹ The recent expulsion from the United States of Chinese researchers and students suspected of exploiting critical research and academic networks suggests that our historically open engagement and spirit of cross-border educational inclusion is increasingly being weaponized against U.S. economic security interests.

Beijing has also begun a relentless drive to self-reliance in semiconductors. In 2016, President Xi Jinping said, “the fact that core technology is controlled by others is our greatest hidden danger.”²² Vice Premier Ma Kai made similar remarks at the 2018 National People's Congress: “We cannot be reliant on foreign chips.”²³ China's investment in semiconductors is \$118 billion over five years, including \$60 billion from provincial and municipal governments.²⁴

All countries want to foster technologically sophisticated industries, assuming that such industries produce good jobs in a field that is likely to grow. But China's aspiration to replace all western technologies with indigenous capabilities is not just about better jobs for its citizens. It assumes that dependence on western technology will ultimately lead to domination by western countries. That may or may not be true, but it does open a window on how China would use western dependence on its technology. China is likely to act the way it thinks the West will act — by exploiting our technological dependence to achieve dominance.

Indeed, China may already be exploiting our growing digital dependence. Long before America comes to rely on sophisticated Chinese chips, the U.S. will be dependent on imports of less sophisticated components. But even a relatively low-value and unsophisticated digital

component could be used to facilitate espionage or to fail in a crisis, leaving command and control of military operations at risk.

Among the fastest growing technology sectors is the use of embedded technology to communicate, sense, and interact with the external environment. The adaptation and evolution of what many call the “Internet of Things” (IoT) will also become the greatest cyber vulnerability for U.S. critical infrastructure over the next decade. It is estimated there will be 30 billion devices on the IoT by 2030, and many will be small, cheap, and made outside the United States, principally in China. The Department of Defense recently estimated that from 2010 to 2019, the number of Chinese suppliers in the Department’s supplier base had increased by 420 percent.²⁵

To describe IoT devices is to understand the risks they pose. They often have radio frequency, optical, and acoustic sensors, and geolocation information that could yield lucrative intelligence. In addition, the ability to identify, track, and control devices will provide foreign governments and criminal organizations unprecedented opportunities to sabotage the U.S. economy from the macro level to individual households.

IoT devices are already used in all sectors of our critical infrastructure ranging from city-wide traffic control systems to individual medical devices. Over the next decade IoT devices will be pervasive throughout the U.S. economy and infrastructure. These devices will be part of the industrial control systems on which the electric grid, water systems, refineries, pipelines, and most manufacturing plants depend. The ability to disrupt the functioning of these devices in time of crisis is a potent weapon in an adversary’s hands.²⁶ Unlike the Defense Department, however, U.S. critical infrastructure industries rarely have knowledge of the third- and fourth-tier subcontractors on whose products they depend.

U.S. Dependence and Supply Chain Vulnerability

Until recently, the United States has ignored these threats. We have assumed that the basic trading rules in place for more than half a century will continue. We have allowed our industries to aggressively outsource their production chain to the cheapest locations, with the expectation that the costs and savings from that outsourcing are matters for the individual firms’ bottom lines. The global supply chain has made U.S. industries globally competitive, but it has also become America’s greatest vulnerability.²⁷ While U.S. industries have benefited from inexpensive parts and labor, the United States — particularly our critical infrastructure and defense sectors — are now vulnerable to cyberattacks, insider threats, part modifications, and sabotage. And the cost of that vulnerability, in many cases, will fall not on the firms that offshored their suppliers, but on the Americans who depend on them for goods and services in time of crisis.

The evidence is overwhelming that China has successfully exploited supply chain vulnerabilities to the detriment of U.S. economic security. Hundreds of economic espionage, cyber, and illegal export cases over the last ten years reveal how China has exploited the U.S. supply chain. According to the 2018 Office of the Director of National Intelligence (ODNI) National Counterintelligence and Security Center report, *Foreign Economic Espionage in Cyberspace*:

China has expansive efforts in place to acquire U.S. technology to include sensitive trade secrets and proprietary information. It continues to use cyber espionage to support its strategic development goals — science and technology advancement, military modernization, and economic policy objectives. China's cyberspace operations are part of a complex, multipronged technology development strategy that uses licit and illicit methods to achieve its goals. Chinese companies and individuals often acquire U.S. technology for commercial and scientific purposes. At the same time, the Chinese government seeks to enhance its collection of U.S. technology by enlisting the support of a broad range of actors spread throughout its government and industrial base.²⁸

China combines cyber exploitation of supply chain operations, human recruitment, and the knowledge of some scholars in U.S. universities, as part of a strategic technology acquisition effort. Most tier two and below supply chain companies cannot afford the cyber defense or insider threat programs necessary to combat China's systematic collection and exploitation effort.

The CCP leadership has also sought to exploit supply chains in more direct ways. We have already described the Chinese state media suggestion that it could let the United States “drown in a sea of COVID.”²⁹ China has also threatened on several occasions to stop the export of rare earth minerals, which would dramatically impact U.S. production of electronics.³⁰

To put the matter starkly, the United States cannot afford to rely entirely on China for products, or even for precursors and components, that America will need in a crisis — because it is precisely when the crisis comes that China will be most tempted to use its leverage for diplomatic, commercial, or even military advantage.

Russia

China is not alone in seeking to exploit the globalization of American supply chains. While it lacks the sheer economic might of China, the Russian Federation yields to no country in its fondness for imaginative, even reckless, cyberoperations, many of which can only be carried out with access to some part of the information technology supply chain.

Russia is a strategic competitor of the U.S. and in some areas, such as energy and arm sales, an economic competitor.³¹ Russian President Vladimir Putin makes no secret of his ambition to force the U.S. to treat Russia as an equal in the military, intelligence, and diplomatic spheres. An important part of his strategy is to develop Russia's cyber capabilities and to integrate cyber with traditional military power to conduct hybrid warfare. Information warfare looks to him like a cheap way to create unrest, uncertainty, and paralysis in the homelands of Russia's strategic rivals.³² The U.S. has been a target of Russian cyber operations for many years, most notably the DNC hack during the 2016 U.S. presidential campaign. By most accounts, Russia is again trying to manipulate social media to influence the outcome of the 2020 elections.

Given the skill of its hackers, Russia can be expected to exploit (and to create) supply chain dependencies that foster espionage and denials of service. Russia may also work with China to create and exploit supply chain weaknesses. During Putin's 20-year tenure as Russia's leader,

Russia and China have developed closer relations. Russia and China now conduct joint military exercises, have developed close cooperative relations in energy, and have signed agreements on establishing cyber norms of behavior.³³ Considering the statements made by both Putin and Chinese President Xi about the strategic threat posed by the U.S., it is reasonable to assume that their cooperation may include identifying supply chain vulnerabilities. Indeed, with the relatively recent emergence of Chinese efforts to manipulate U.S. social media, one wonders whether the Russians have already shared some of their expertise.³⁴

Responding to Our New Vulnerability

Recognition of the threat to U.S. economic security has been steadily growing in recent years. President Trump's approach to trade with China spurred a notable change of direction in every corner of the executive branch, often with strong bipartisan support.

The Subcommittee began its investigation by examining what other agencies and Congress have already done. DHS is, after all, the youngest cabinet department. While its responsibilities place it at the center of the economic security issue, it can learn a great deal from others, whether in Congress, on federal commissions, or in other agencies, some of which have been addressing the issue far longer. We believe that in many cases, DHS will do best to learn from or support existing economic security initiatives rather than reinventing its own competing structures or missions.

Defense Department

The best example of an agency with a mature economic security capability is the Department of Defense (DoD). DoD needs a reliable civilian supply chain to prevail in a military conflict. From a DoD perspective, economic security is a strong Defense Industrial Base (civilian and defense sectors) to support DoD in military conflicts.³⁵ Protecting this capability requires first identifying globalized trade flows that create vulnerabilities for DoD's mission and then adopting measures to minimize or eliminate those risks. The proliferation of high-tech commercial technology and the globalized shift of manufacturing have had tremendous economic benefits for the United States and other countries around the world, but the risks of offshoring, just-in-time manufacturing, and global supply chain optimization have become increasingly visible in the defense industrial base in the second decade of the 21st century.

While national security priorities and Buy America laws ensure that the vast majority of the development and production of defense systems occurred in the United States, the production of some critical subcomponents and materials have migrated overseas. DoD's annual Industrial Capabilities reports to Congress summarized the Department's guidance, assessments, and mitigation actions, and have identified weaknesses in the industrial base.³⁶ The reports note, for example, that the production of microelectronics and materials such as rare earth elements as well as specialty chemicals and energetics used in explosives are increasingly produced only outside of the United States — in some cases, almost exclusively in China. The production of these components and materials moved overseas due to market forces, because these items are

used overwhelmingly for commercial purposes in electronics such as computers and smartphones. The challenge for DoD, however, is that these are also essential components in critical advanced defense systems such as radars and precision-guided munitions.

As a result, DoD's focus on the industrial base has sharpened in recent years. The Office of Industrial Affairs, which had been demoted in stature in the early 2000s, was elevated and eventually strengthened further in 2013 with the creation of the Office of Manufacturing and Industrial Base Policy (MIBP). In addition to the traditional focus on industrial base assessments, anti-trust reviews of defense-related mergers and acquisitions, and Title I and III of the Defense Production Act (DPA), responsibility for the Committee on Foreign Investment in the United States (CFIUS) was transferred to MIBP. Now the Office of Industrial Policy, headed by a Deputy Assistant Secretary, maintains a direct-report relationship to the Under Secretary of Defense for Acquisition and Sustainment, giving DoD a strong focal point for industrial base analysis and mitigation efforts across the department.

The current Industrial Policy office (IndPol) is structured around three main activities (total budget around \$200 million, at least half for industry support):³⁷

Assessments. This team focuses on critical warfighting capabilities identified mainly by the military services — missiles, electronics, shipbuilding, radars, ground transport, materials, and so on. The assessments team conducts regular reviews and analyses of industrial base sectors, and produces the annual Industrial Capabilities Report to Congress.

This group also leads reviews under Title I of the DPA for DoD. Title I gives the U.S. government authority to require that suppliers of a particular product enter into supply contracts with DoD and give priority to those contracts. In supporting this function, IndPol works with the military services to rate priority orders under the DPA, giving the highest level ratings for the most critical national security programs (Columbia class submarines, Ground-Based Strategic Deterrent, etc.). In the conduct of these functions, IndPol's Title I team works closely with the Department of Commerce, which manages the Defense Priorities and Allocation System (DPAS) program for Title I actions across the U.S. Government.³⁸ In recent years, this group also played the lead DoD role in Section 232 and Section 301 investigations concerning steel and aluminum.

National security reviews. A critical IndPol function is the review of corporate transactions to assess their impact on national security. Specifically, IndPol leads the DoD reviews of defense-related mergers and acquisitions (M&A) and of foreign direct investment under their respective regulatory regimes. M&A reviews are focused on maintaining competition and are governed by the Hart Scott Rodino (HSR) Antitrust Improvements Act of 1976.³⁹ In general, government policy relies on market forces to determine the shape of the government contracting market, but the U.S. government will intervene if a merger might leave DoD depending on a monopoly supplier in a particular market.

IndPol also leads CFIUS reviews for DoD as part of the interagency committee led by the Treasury Department. These reviews have grown more challenging in recent years. Transactions originating from Chinese firms were less than 4 percent of transactions reviewed during 2007-2009, for example, but had become the largest number of cases filed by 2016-2018 (26.5 percent). Moreover, the nature of the Chinese transactions drew increased scrutiny because the

vast majority of these proposed acquisitions (84 percent) were focused on the manufacturing, finance, information, and services sectors.⁴⁰ That scrutiny in turn led to passage of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), discussed below.

Industry support programs. IndPol manages a number of programs focused on strengthening the defense industrial base through public-private partnerships that can build U.S. domestic industrial capabilities and capacities in particular sectors (e.g. materials, microelectronics) where the commercial market alone is not sufficient to support DoD requirements. DPA Title III is the principal authority used to fund such projects, and it has been used actively for decades. Funding has varied, but averaged \$40-70 million per year until the COVID-19 pandemic.

Title III has traditionally focused on projects to build or modernize capacity, such as the ability to do complex forgings for naval propulsion shafts and to produce beryllium domestically. In a cautionary tale about industrial policy and shifting political winds, however, Title III was also used to support biofuels development for DoD at a time when U.S. dependence on foreign oil was coming to an end. For a time, one of the biggest programs under Title III, involving hundreds of millions of dollars, was the Navy's biofuels program. In a drive to build a "Great Green Fleet," the Navy at one point paid \$424 a gallon for fuel based on oil from algae.⁴¹ The thin connection to national security made the funding controversial, which led to significant restrictions on future Title III efforts.

While Title III is a Presidential authority, all projects prior to 2020 were initiated and led by DoD with one exception – an effort by DHS's Office of Science and Technology to initiate a Title III project on "secure shipping containers." After numerous delays, this project was awarded \$20 million in late 2018. It is being executed by DoD with DHS sponsorship from S&T. The period of performance for the project runs through 2022.

The Coronavirus Aid, Relief, and Economic Security (CARES) Act added \$1 billion to the DPA Fund and removed funding restrictions on individual Title III projects.⁴² The tremendous infusion into the DPA Fund was its largest ever, and some of these funds have already been used as the current administration greatly accelerated Title III projects. Whereas, for example, it took 18 months to get rare earth Title III projects to the point of award, two COVID-19 pandemic-focused Title III projects, each over \$120 million, were started in less than a month utilizing those DPA funds.⁴³

There are three additional IndPol programs that support industry:

- The Industrial Base Analysis and Sustainment (IBAS) program was created in 2013 and has a similar mandate to Title III. It has generally been funded at \$10-30 million over the past several years, but received funding greater than \$50 million in FY2019. IBAS was recently used for a competition to reshore heavy rare earth processing in the United States.
- The Trusted Capital Marketplace (TCM) program was established to foster venture capital investment and deal flow in the interest of creating opportunities for U.S.-based startups and other non-traditional sources of defense technology. The goal is to help them

partner with DoD, as opposed to taking funds from adversarial sources such as Chinese-backed venture funds.

- Small Business programs support the industrial base by focusing on policies and programs to strengthen small companies and new entrants into the defense marketplace. One example of a capability area where many or all of these industrial base capabilities is brought to bear is semiconductors. DoD has recognized that the Trusted Foundry program, designed to ensure secure production of semiconductors, has been unable to keep U.S. semiconductor manufacturing at the cutting edge.⁴⁴ DoD is working with these and related programs to reshore microelectronics capability in the most expeditious way possible.

IndPol is a potential model for DHS's approach to economic security. While DHS may never have DoD's scale, many IndPol functions are appropriate for a DHS-led economic security strategy. (IndPol staffing is currently around 100 FTEs, approximately 30 government civilians and 70 contractors). IndPol tools are readily applicable for DHS use, however:

- Assessments. Economic security assessments of areas of DHS concern — civilian supply chain, information technology, and the like — may provide immediate value to DHS components and have an outsized impact outside the Department. (See recommendation 5d).
- Regulatory reviews. DHS is already one of the more aggressive and effective participants in CFIUS reviews of foreign investment. This capability should be combined with other economic security missions. DHS has not played a similar role in the conduct of HSR merger reviews that might impact large DHS procurements. We conclude that it should. (See recommendation 8).
- Industrial support programs. Title III of the DPA is a Presidential authority that can be delegated to any department that makes procurements for national security needs. Until the coronavirus crisis, the DoD has been the only department to use appropriated funding for Title III programs. DHS has sought support from Title III in the past but its projects were not funded. Having a focal point for DPA Title III within DHS would create a natural opportunity to identify, vet, and muster support for capacity-building efforts. This is how the Department of Health and Human Services is handling its DPA Title III efforts as part of the COVID-19 response.

A review of DoD's economic security capabilities would not be complete without a mention of the U.S. Air Force Office of Commercial and Economic Analysis (OCEA). OCEA is also a potential model for DHS, particularly for how economic security assessments could be done. OCEA performs strategic commercial assessments to measure actual U.S. commercial strength in DoD-relevant industries. OCEA's experience has taught it several relevant lessons: (1) Authorities are good to have; but analytic capability is essential. (2) OCEA is influential only because its assessments are useful; it has no strong authorities or institutional "mandate," and it does not think it needs them as long as its work product is useful to policymakers. (3) Most implementation authority at DoD begins with DoD procurements; DHS should where possible use its procurements to support economic security. (4) Even DoD, with its large purchasing

power, rarely finds that its own purchases are sufficient to incentivize necessary security measures; it needs to enlist large U.S. critical infrastructure companies in the private sector to reach a scale that can drive the market. With its ties to the private sector, DHS can play a supportive role in this effort.

Treasury Department

The Treasury Department administers and chairs CFIUS. CFIUS was created in the 1970s to address the special risks created by foreign investment in certain American industries. Foreign investment in the U.S. is usually welcome but it can sometimes pose a real threat to economic security. Companies based in adversary countries, whether they are nominally private or state-owned enterprises, may buy U.S.-based technology companies and move that technology out of the U.S. permanently. Indeed, as the Defense Department has learned, these transactions do not have to be outright purchases. They can include many joint ventures and equity investments as well.

Many such transactions were beyond the reach of CFIUS until the adoption of FIRRMA. FIRRMA strengthened CFIUS's authorities to reach joint ventures, police transfers of critical technology, and mitigate risks through national security agreements.

That said, CFIUS by itself still cannot address all threats to U.S. economic security. For one thing, it covers investments in U.S. companies. It does not deal with foreign companies that build their businesses in the U.S. from scratch, either through investment here or through imports. Second, CFIUS exists to shine an intense spotlight on a single transaction by a single foreign buyer at a single point in time, and its only recourse is to prohibit or limit that particular acquisition. In many cases, a broader view of the industry and global competition is necessary to appreciate the risk and to fashion a remedy more effective than just saying "no" to the deal at hand. We believe that conducting such a broader review is one valuable role that DHS's economic security unit should undertake in the future. See recommendation 6b.

Commerce Department

The Department of Commerce is explicitly tasked with fostering economic growth through fair trade and innovation. Among the Department's strategic goals is strengthening U.S. national and economic security. Recently, the Commerce Department has taken steps to assess and categorize goods and supply chains that are critical to the U.S., identifying 700 products needed in an emergency. The Department then sought to assess U.S. domestic capacity to produce these products but discovered key gaps in the data regarding, for example, domestic cost of production and demand, and possible alternative suppliers. In addition, the U.S. government as a whole lacks the expertise to assess the relative strength or weakness of an industry; and often lacks access to existing trade datasets that may hold critical information about key industries, including which are being offshored. Given its cross-cutting border authorities, DHS may be a logical place to monitor existing economic security datasets and to house any which are developed in future.

Growing or reshoring essential industries is at the heart of any long-term plan for economic security. Ways to incentivize that effort include U.S. government procurement mechanisms, trade remedies protecting U.S. suppliers, and international cooperation to foster suppliers independent of Chinese influence. DHS can play a key role in the growth and protection of domestic industry through the Department's tariff and import enforcement authorities, particularly those exercised by Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). Indeed, Commerce Department officials told the Subcommittee that DHS's ability to use customs, sanctions, trade remedy, and export control enforcement authorities in a policy-sensitive fashion would be a valuable tool in economic security. We have incorporated this suggestion into recommendation 9. In addition, these witnesses suggested that DHS's Cybersecurity and Infrastructure Security Agency (CISA) can play an important role in assessing cybersecurity vulnerabilities related to the communications and information technology (IT) supply chain, pursuant to Executive Order 13873. These observations are reflected in recommendation 6a.

The Bureau of Industry and Security within the Commerce Department is responsible under the DPA for prioritization of government contracts for industrial products in an emergency. Commerce has delegated to DHS (and other departments) the authority to prioritize contracts needed for national defense. At DHS, FEMA generally exercises this authority. In emergency situations, Commerce often relies on FEMA for contract prioritization — experience that could be replicated for other industries in non-emergency situations. This authority is an important part of the economic security structure created by the DPA, and FEMA's execution of it should be closely coordinated with other parts of DHS through the Department's Economic Security Council. See recommendation 1.

State Department

The State Department in the Trump administration has focused closely on economic security, with attention to U.S. economic resilience and vulnerability, particularly in relation to China. The Department has pursued a number of international initiatives in economic security:

- The Clean Network program, an economic security initiative which seeks to protect critical U.S. telecommunications and technology infrastructure from adversaries such as China. The program includes five lines of effort: Clean Carrier (protecting telecommunications networks from PRC carriers), Clean Store (eliminating untrusted surveillance applications from U.S.-based mobile app stores), Clean Apps (preventing covert surveillance smartphone applications from being preinstalled or available for installation), Clean Cloud (protected cloud-based storage), and Clean Cable (protecting undersea cables). The Clean Networks initiative is perhaps the highest-profile example of State Department efforts to counter China's 5G challenge and that country's digital authoritarian ambitions.
- The Blue Dot Network, a joint endeavor with Australia's Department of Foreign Affairs and Japan's Bank for International Cooperation, which provides public-private financing for infrastructure projects that meet rigorous standards for transparency and private sector-led development.⁴⁵ This effort seeks to counterbalance state-led economic investment, particularly in developing countries targeted by China's Belt and Road

Initiative — which subsidizes and develops infrastructure, thereby indebting emerging economies to China and creating commercial dependence on China in those economies' private sector.⁴⁶ (The use of these funds to dominate international ports and shipping is properly of particular concern to DHS's components like the Coast Guard and Customs and Border Protection.) Blue Dot investment thus helps to safeguard supply chains and global networks, in turn supporting U.S. economic security.⁴⁷

- The Prague Proposals were developed at a 2019 security conference in that city; they seek to foster both security and resilience in the context of transnational supply chains for information and communications technology (ICT) equipment. Foreign influence is of particular concern here, which is why the Prague principles emphasize transparency in relation to suppliers' ownership and corporate governance structures (among other things).⁴⁸
- The Deal Team Initiative, launched by the State Department in February 2020, aims to better coordinate the resources of the U.S. economic interagency community in order to help U.S. companies win business overseas and promote the economic foreign policy of the United States.

As a complement and foundation for its initiatives, State Department witnesses before the Subcommittee welcomed a DHS role in more strategic analysis of economic vital interests and risks, akin to the assessments done routinely by the Department of Defense. While the Subcommittee is not persuaded that DHS has the current capability and resources to perform all of the tasks currently performed by the Defense Department, we have recommended several more focused reviews that could serve the State Department's purposes. See recommendations 6a-6d. By the same token, the State Department needs to do more to include DHS in its international initiatives beyond economic security issues. DHS has the third largest workforce outside the United States (after State and DoD), and it has a host of international engagements and points of tension that should be recognized by the State Department.

Intelligence Community

Identifying deliberate or negligent flaws in the components on which our critical infrastructure depends is at least in part a matter of good intelligence. But it is intelligence of a particular kind — a thorough mix of open source, proprietary, and classified information. It requires gathering information about U.S. as well as foreign suppliers, and the audience for any analysis is more likely to be a private company than the government, because it is the private owner of critical infrastructure who must cure the threat.

The Intelligence Community has growing interest in and concern about supply chain risks, but it has faced institutional difficulties in creating effective intelligence programs to address the issue.⁴⁹ From the standpoint of the Intelligence Community, there are both real and perceived legal constraints on its authority to collect information about, to analyze, and to report on the U.S. companies that participate in a given supply chain. Effective supply chain analysis cannot be done without understanding suppliers' competitiveness, financial viability, vulnerability to compromise, and dependence on Chinese government favor. These are not traditional topics for intelligence collection and reporting.

By comparison, DHS does and must look both outward — at foreign threats, and inward — at the U.S. persons it protects. That is required by its homeland-oriented mission. Moreover, DHS is already a center for sharing supply chain information. Pursuant to a recent Office of Management and Budget (OMB) regulation implementing the Federal Acquisition Supply Chain Security Act, DHS is the executive agency for sharing information on supply chain risks for the federal government. In this capacity, DHS will support an interagency task force to collect and distribute information from government and private sources. The information will be used to order mitigation of supply chain risks, including removal of risky products from the federal IT infrastructure.

In the broader Intelligence Community, supply chain security for the private sector is not given priority. The reasons for this are many. The Intelligence Community has concerns about whether classified information can be protected if conveyed to private industry. It is uneasy that providing information to one company or a few companies will be seen as improper favoritism. At the same time, the Intelligence Community also faces knowledge gaps; a lack of familiarity with the alternative sources of supply and mitigation strategies may mean that it too often delivers “nuggets” of derogatory information about a particular supplier without the context that would enable companies to mitigate the risk. In short, the Intelligence Community is not used to interacting with the private sector as a customer. Yet, often the party most involved in supply chain decisions is an individual private company or a few companies.

Notwithstanding these institutional difficulties, the Intelligence Community sees both the need for and value of a Supply Chain Intelligence Center to pull together and make actionable intelligence on supply chain security. It is not often that intelligence agencies agree that a sister agency is the best place to house an intelligence function, but we were told by multiple witnesses that they saw DHS as the logical place for such a center, given its closer relationship with the private sector and its better legal tools for working with private companies, along with its mission in critical infrastructure and risk management. The Subcommittee agrees.

The Subcommittee also believes that the center should provide feedback on the intelligence it receives, and it should play a large role in setting intelligence collection priorities. This is necessary to remedy the current dearth of actionable supply chain intelligence. The quality of intelligence collection could be greatly improved if the intelligence collection agencies were challenged by a demanding and sophisticated consumer; that is a role that DHS can and should play.

For this reason, the Subcommittee has recommended that a supply chain intelligence center be established under the leadership of the Department, and that the center, through DHS, be given a strong voice in setting intelligence collection priorities for supply chain risks. See recommendation 4.

Export-Import Bank of the United States

The Export-Import Bank of the United States (EXIM) offers credit and assumes risk when the private sector is unable or unwilling to do so. Newly reauthorized for seven years, EXIM is

positioned to support U.S. economic security by facilitating U.S. exports, thereby supporting the creation and retention of domestic production. EXIM is especially helpful for small businesses, which may lack the necessary assets and diversified financial structure to compete with foreign companies subsidized by their home governments.

EXIM's Program on China seeks to meet Chinese subsidies with U.S. assistance, reserving at least 20% of total financing authority to match the rates and conditions of loans, guarantees, and insurance offered to Chinese companies by China's government. Focused on ten key areas which broadly align with the Made in China 2025 Initiative, this EXIM Program prevents Chinese manufacturers from undercutting U.S. companies and also incentivizes reshoring.⁵⁰ This targeted support allows U.S. companies to develop products and technologies crucial to U.S. economic security that have a longer arc to profitability.

In 2019, EXIM stood ready to offer \$27 billion (USD) in export financing assistance, while China poured \$76 billion (USD) into export support for Chinese companies.⁵¹ EXIM witnesses before the Subcommittee noted that many U.S. manufacturers, particularly small businesses, were unaware of EXIM resources. The witnesses indicated further that DHS advice on strategic deployment of lending would be welcomed, given the Department's substantial overseas footprint and the fact that DHS may identify needs (e.g. TSA for scanning gear, CISA for information and communications technology) before other parts of the U.S. government.

Cyberspace Solarium Commission

The most recent and important recognition of the need for new economic security measures comes from the bipartisan Cyberspace Solarium Commission. The Commission was formed to address risks in the cyber domain, one of the fastest growing areas of national and economic security vulnerability for the United States. Most concerning for nation-states, some cyberattacks could disrupt the most critical of our infrastructures and essential services, such as the power grid.⁵² Such an attack could be launched by itself or combined with some other crisis, like a kinetic attack or natural disaster. Short of nuclear war, it may be the gravest threat to the security of the American homeland.

Our adversaries understand the potential impact of cyberattacks on the United States. Chinese military thinkers have incorporated cyberattacks on our critical infrastructure into their plans for war and near-war. A key to successful attacks is the exploitation of supply chain vulnerabilities in our information, communications, and industrial control systems. Because China produces so many of the components that go into those systems, it has an outsized ability to cause system failures. In some cases, simply refusing to supply critical components could cause havoc, but even more disruption is possible if the components are shipped and installed with a feature that causes them to stop working at the remote command of the People's Liberation Army.

There is no more significant economic security vulnerability for the United States, which is why so many of the Cyberspace Solarium Commission's recommendations deal with what might be called supply chain risks. The Subcommittee has studied the Commission's report with care and supports its recommendations for supply chain security. We recommend that Congress and the administration adopt them, and that DHS build upon them.⁵³ In particular, the Subcommittee

endorses the following Solarium Commission recommendations, which are most relevant to economic and supply chain security and which in our judgment require new steps from DHS:

- *Cyberspace Solarium Recommendation 3.1: Increase Cybersecurity and Infrastructure Security Agency (CISA) authority to coordinate the sector-specific regulatory agencies.* Critical infrastructure resilience and national risk management depend upon partnerships between the Federal government and the private sector. These relationships are managed by sector-specific agencies; but these agencies' approaches have been inconsistent and sometimes hobbled by a lack of authority or expertise. Congress should increase the cybersecurity supervisory and coordinating authorities of the Department's Cybersecurity and Infrastructure Security Agency and recognize the Agency's lead role in managing civilian national risk.
- *Cyberspace Solarium Recommendation 3.1.2: Create and resource a joint CISA-FEMA fund for resilience initiatives.* Market forces do not provide sufficient private sector incentives to mitigate cyber risk and improve national resilience. While the Homeland Security Grant Program and resourcing for national preparedness under the Federal Management Agency (FEMA) are well-established, no equivalent funding stream exists for cybersecurity preparedness. A grant system specifically targeted at cyber preparedness and attack prevention would significantly enhance the security and resilience of critical infrastructure. A joint program between CISA and FEMA would leverage domain expertise (CISA) and administrative experience (FEMA), increasing the likelihood of success.
- *Cyberspace Solarium Recommendation 3.3.1: Designate DHS as lead agency for identifying cybersecurity services essential to national security.* No single Federal agency is currently tasked with this mission. To prioritize and designate responsibility for continuity of cyber operations, the President or Congress should task DHS to do the planning necessary for successful civilian defense and recovery from cyberattack. This would include identifying: cybersecurity-related services essential to national security, the private sector's incident response capacity, and the critical infrastructure that must be protected or swiftly repaired in the event of an attack.
- *Cyberspace Solarium Recommendation 4.1.1: Set up and staff Critical Technology Security Centers to test critical infrastructure devices.* The U.S. government currently lacks trusted entities to perform cybersecurity evaluations and testing, resulting in uneven threat assessments of critical infrastructure. By funding three Critical Technology Security Centers, Congress would help remedy this gap. The Centers would serve as a national focal point for existing and new research into cybersecurity, and would help provide a more holistic picture of U.S. cyber-preparedness. Administered by DHS, these Centers should include personnel from the Department of Energy, Department of Commerce, Office of the Director of National Intelligence, and the Department of Defense.
- *Cyberspace Solarium Recommendation 5.1: Codify the concept of systemically important critical infrastructure and provide support while imposing obligations on the owners of that infrastructure.* This Commission recommendation expands on Executive Order 13636, which called for special attention to the cybersecurity of such critical infrastructure. DHS, with its risk management capabilities, should continue to play a large role in the process of

identifying systemically important infrastructure and setting cybersecurity expectations for that infrastructure. The Subcommittee believes that the Cyberspace Solarium’s recommendation, which imposes obligations on all systemically important infrastructure, implicitly corrects a serious omission from the executive order. E.O. 13636 exempts from its obligations some of the infrastructure at the heart of our economy — commercial and consumer IT. To the extent this exception ever made sense, its justification fell apart in the 2020 pandemic, when the main thing that kept our economy from collapse was the use of commercial and consumer IT. We could not have easily withstood a successful cyberattack on the internet and videoconferencing tools that enabled many to keep working. Therefore, Congress and the President should extend the definition of critical infrastructure to cover information technology, and should task DHS with the identification and administration of systemically important IT infrastructure.

- *Cyberspace Solarium Recommendation 5.1.2: Coordinate with DHS to collect private sector input on intelligence priorities relating to cybersecurity.* There is no formal process to solicit private sector input into U.S. national intelligence priorities and collection efforts. Because of its unique ability to coordinate on cybersecurity with the private sector, DHS is in the best position to assist in dissemination and analysis of intelligence affecting the private sector. The Subcommittee therefore endorses the Cyberspace Solarium Commission’s recommendation that this effort be led by DHS. Congress should provide the authorities and resources DHS will need to play this role.

More recently, the Commission has issued a White Paper focused entirely on supply chain issues in information and communications technology.⁵⁴ The White Paper offers several valuable recommendations, three of which bear directly on DHS’s role in economic security. The Subcommittee endorses these recommendations in particular.

- *Cyberspace Solarium Supply Chain Recommendation 1: Congress should direct the executive branch to develop and implement an information and communication technologies industrial base strategy.* While Congressionally mandated “strategies” without executive branch support are too often paper exercises, the administration should support this effort to approach economic security strategically. DHS, particularly CISA and the Policy office, have much to contribute to the effort and should support it with enthusiasm, leveraging existing work from CISA to create a taxonomy of especially critical hardware, software, and services within the ICT ecosystem.
- *Cyberspace Solarium Supply Chain Recommendation 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.* The Subcommittee fully supports legislation directing such a review and ensuring that DHS has the resources necessary to carry it out.
- *Cyberspace Solarium Supply Chain Recommendation 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.* The Subcommittee strongly supports this

recommendation, particularly Recommendation 4.1, calling for creation of a supply chain intelligence center. The Subcommittee concludes that this center should be led by and benefit from DHS and its authorities and relationships. See Subcommittee Recommendation 4 below.

The Role of the Department of Homeland Security

We now turn to the Department of Homeland Security itself. Like the rest of government, it has taken several steps to protect economic security. And also like the rest of government, the steps it has taken are just the beginning of what is needed. In this section, we will describe briefly what DHS components are now doing to improve the nation's economic security and make recommendations for additional steps that Congress, the President, and principally the Department itself can take in that direction.

The listing of recommendations for particular components is not meant to suggest that other components lack important responsibilities for economic security. The Coast Guard, to take one example, has a major role in ensuring the security of American ports; in so doing it needs to be alert to new potential threats to port functioning arising from concentrated foreign ownership of port facilities or neighboring properties. Similarly, the Under Secretary for Management (with help from Congress) should ensure that DHS procurement policies match the advice the Department is providing to others, including enforcement of cybersecurity requirements for contractors and an examination of those contractors' supply chain below the first tier of subcontractor.

One further point: Perhaps one or two of our recommendations can be accomplished with minimal additional resources. But by far the majority will require budget support from the Secretary, the President, and the Congress. Like most of the operational departments, DHS makes policy principally by deciding how it will spend appropriated funds. Economic security will never be a DHS (or a national) priority until it becomes a budgetary priority.

Background for Recommendation 1

DHS has no choice but to play a large role in economic security issues. It is charged with preparing for all manner of crises and unpleasant surprises, from major hurricanes to terrorist attacks.⁵⁵ What these events have in common is the need to prioritize and restore essential services that may have been disrupted, at least locally. Put another way, DHS is challenged every year, and sometimes every day, to understand what parts of our infrastructure are essential to the functioning of the country.

This means that the Department is well-positioned to grasp the implications of supply chain vulnerabilities for the functioning of American society and the American economy. While the Department of Defense has done significant work to protect the defense industrial base, there is no analogous framework for assessing risks outside the defense base.

DHS should take responsibility for this mission, acting as a complement to the Defense Department's IndPol (discussed above) and addressing critical gaps in the supply chains that determine the resilience and security of critical functions and infrastructure. To do this job, DHS needs to engage in a disciplined analysis of events likely to strain the nation's resilience and preparedness. Some are obvious — terror attacks and natural disasters — and have been the subject of DHS preparation for decades. That experience should be brought to bear on other events, from pandemics to a prolonged electric grid failure, with a goal of identifying concentrated systemic dependencies that could interfere with quick recovery. To bring together the components that have relevant economic security expertise, the department recently established an Economic Security Council. It coordinates internal DHS activities relating to continuity of the civilian economy, particularly focused on supply chain issues. The Subcommittee supports this innovation; intradepartmental coordination is essential for the economic security mission.

Recommendation 1: The department should institutionalize the Economic Security Council. Congress should provide a legislative mandate for the establishment and maintenance of the council to identify concentrated risks, to set priorities and to coordinate enterprise-wide action on economic security matters.

CISA

Background for Recommendation 2

CISA is one of the key components of DHS that could advance economic security. CISA already plays two large roles in identifying and remediating supply chain vulnerabilities.⁵⁶

- **Federal Cybersecurity.** Along with the National Security Agency (NSA), CISA is the nation's resource on cybersecurity. While NSA focuses on the digital vulnerabilities of the Defense Department and its suppliers, CISA's Cybersecurity Division has responsibility for improving the cybersecurity of all civilian agencies and the rest of the private sector. It also has large, shared responsibility under the Federal Acquisition Supply Chain Security Act of 2018 and in support of the Federal Acquisition Security Council (FASC), for addressing threats to the federal government's communications and information technology procurements. Within the FASC, CISA has been formally designated as the Information Sharing Agency.
- **Critical Infrastructure.** CISA is charged with addressing the resilience of all civilian infrastructure. CISA leads an ICT Supply Chain Risk Management Task Force with industry partners. CISA also offers a range of voluntary tools, assessments, training, and information sharing mechanisms to enable partners to be more vigilant against the rapidly evolving threat landscape of cyber, physical, supply chain, and other digitally enabled threats

In addition, CISA's National Risk Management Center (NRMC) identifies and takes the lead in addressing a wide range of public-private risks that go beyond cybersecurity, many tied to supply chain vulnerabilities. The Risk Management Center must identify those parts of the nation's

infrastructure that should be prioritized in any crisis. This is the intellectual foundation on which economic security measures should be built; NRMC has identified a list of 55 National Critical Functions, from supplying water to conducting elections, that are essential for achieving what the Cyberspace Solarium Commission aptly describes as “Continuity of the Economy.”

CISA and its Risk Management Center have already provided “Continuity of the Economy” assistance to policymakers. NRMC played a role in responding to the COVID-19 emergency by identifying operators so critical to infrastructure resilience that their workers should be exempted from state travel restrictions. NRMC also maintained a risk snapshot of commodity shortages in the COVID-19 crisis. Finally, the center supported the Commerce Department’s study of U.S. dependence on unreliable suppliers, identifying the most critical sectors facing such dependence.

The Office of Management

As CISA’s responsibility for advising others about cybersecurity has grown more prominent, it has become critical that DHS lead by example in its own cybersecurity and supply chain practices. This requires considerable coordination among multiple offices. The Acquisition Office, the Chief Information Officer, CISA, and the component engaged in a procurement — all have a legitimate interest in the security and supply chain provisions of the contract. Even the Science and Technology Office, which currently tests products to make sure they meet the Department’s needs, should be involved at the outset to make sure that its security testing corresponds to standards set from the start. This is a knotty coordination problem, and unless the Secretary insists on coordination, conflicts will arise after it is too late to resolve them easily.

Ideally, many of these concerns can be addressed by early use of tools like DevSecOps and model-based systems engineering. But proper coordination, like proper security design, can get lost in a rush to implementation. The Secretary needs to make clear that he or she expects components to bring new IT projects forward for coordination before the schedule is jammed, and that the other offices with a stake in security need to match the component’s urgency when the project is brought forward. While in the end the responsibility for enforcing coordination lies with the Secretary, the mechanism for carrying it out can and should be the Economic Security Council, where all the cybersecurity stakeholders will be represented.

Recommendation 2: DHS must lead by example in procurement practices that foster cybersecurity, including supply chain security. The Secretary should ensure effective coordination through the Economic Security Council or some other mechanism among the many offices that can contribute to security in acquisitions, including the Office of Management, the Office of Acquisition, the acquiring component, CISA, the Chief Information Officer, and the Office of Science and Technology.

The Office of Strategy, Policy and Plans

The DHS Policy Office has taken the lead in developing requirements for supply chain mapping and should be commended for its willingness to devote resources to the issue. Like CISA, it has a sustained history of engagement with economic security issues. Its CFIUS and Team Telecom

unit has long been among the federal government’s more determined advocates for protecting the nation’s civilian information and communications infrastructure from risky foreign influence.

The Policy Office has now combined its nascent economic security capabilities with its established CFIUS and Team Telecom staff under a Deputy Assistant Secretary for Economic Security. We support this organizational structure, which reinforces the significance of the issue and allows the transactional expertise of the CFIUS and Team Telecom staff to be deployed on a wider scale. There is a clear need for a political-level policy official to conduct day-to-day policy coordination and representation of the Policy Office, both at the interagency level and in working with CISA.

Recommendation 3: A Deputy Assistant Secretary for Economic Security should be institutionalized within the Office of Strategy, Policy, and Plans.

Background for Recommendation 4

As the Cyberspace Solarium Commission has recognized, collecting and sharing intelligence on supply chain threats has proven to be a challenge; it calls for a National Supply Chain Intelligence Center.⁵⁷ DHS has a vital interest in the best possible intelligence on supply chain risks, both those affecting federal civilian networks and those that touch critical private infrastructure. As already discussed, DHS is in the best position to bring together intelligence from other agencies and to create a protected channel of communication to and from private industry about supply chain risks. The Center can draw on and coordinate with other DHS efforts to address supply chain risk, including the Supply Chain and Counterintelligence Risk Management Task Force, called for in Section 6306 of the 2020 National Defense Authorization Act (NDAA), the Information Sharing Agency activity recognized by the FASC, and the Communications Supply Chain Risk Information Partnership (C-SCRIP) created in accordance with Section 8(a) of the Secure and Trusted Communications Networks Act of 2019 (Public Law No. 116-124). In addition, the Department can and should become a voice for the private sector in dealing with the intelligence community, both in prioritizing supply chain risks and in pressing for more intelligence that private sector entities can actually use.

A Supply Chain Intelligence Center should do more than pass on intelligence about particularly risky suppliers. Working with the National Risk Management Center, it should identify both the infrastructure whose failure would cause the greatest harm – and indicators that will tell us when a hostile power seeks the ability to attack that infrastructure.

One way to share supply chain intelligence may be fusion centers. The purpose of the fusion centers is to “enhance critical infrastructure protection” with “a broad and secure exchange of sensitive but unclassified ... information between federal agencies, owners and operators, and state and local governments.”⁵⁸ Today, some centers, such as the Pennsylvania Criminal Intelligence Center, are actively working with the private sector, while others have very limited engagement. The Pennsylvania Criminal Intelligence Center provides regular briefings and alerts on threats and vulnerabilities to hundreds of private sector and critical infrastructure partners. It was able to quickly pivot to information sharing on coronavirus developments in 2020 and could no doubt expand to supply chain risks just as quickly.

Recommendation 4: The intelligence community and DHS should create a joint supply chain intelligence center with private sector entities as participants and customers. This center should provide practical guidance about suppliers that may pose a particular risk. The center should also influence intelligence collection priorities and provide feedback to improve the quality of supply chain intelligence.

Background for Recommendation 5

While combining the economic security unit with the CFIUS and Team Telecom unit makes sense, more capacity is needed. Currently, the Policy Office focuses on economic security in the context of single transactions, usually with a 45-day deadline. Such decisionmaking can produce focused and prompt resolutions, but it does not deal well with broader supply chain issues, such as competitors who expand organically rather than through acquisition, or who have received state assistance in the form of subsidies or cyberespionage support. CFIUS cases are enormously valuable in identifying a supply chain problem but they rarely provide a complete solution to the problem they uncover. To go beyond individual cases to more strategic assessments and solutions will require more resources, and perhaps substantially more resources.

CISA also has a role in supply chain analysis, and it currently has more resources dedicated to the issue than any other part of DHS. That said, in order for the Department to manage its enterprise-wide activities and functionally coordinate within the interagency, the Office of Strategy, Policy and Plans has an important function to play. The roles of CISA and the Office of Strategy, Policy and Plans could be harmonized and integrated. The Deputy Assistant Secretary for Economic Security could perform this function, serving as a bridge between Policy and CISA. For efficient coordination, however, the roles and responsibilities of CISA and the Office of Strategy, Policy and Plans need to be better defined. Ultimately, this is a question for the Secretary and perhaps Congress.

Recommendation 5: The Secretary should define roles and missions and coordination responsibilities between CISA and the Office of Strategy, Policy and Plans, for the task of mapping civilian supply chain and economic security risks.

No matter how responsibilities are divided, the task is essential. In the long run, the nation needs the capability to identify all supply chain threats to its economic security, to prioritize them, and to construct a strategy for remediating the threats. This is what the Defense Department's IndPol does for our industrial base, and the events of recent years have demonstrated that we can no longer leave our economic security to chance and the market. DHS is a necessary participant in any such effort.

Background for Recommendation 6

That said, comprehensively mapping supply chains that might impact national economic security is a daunting task. Further, a comprehensive but superficial analysis of many key supply chains will not be nearly as useful as an in-depth understanding of a few high-priority industries that

includes risk-informed assessments and recommendations for mitigation. DHS would make more progress more quickly in this mission by focusing its efforts on a handful of tasks, using those efforts to establish the right methodologies and capabilities and to build interdepartmental and interagency cooperation.

Put another way, DHS should not try immediately to do for the entire civilian economy what the Defense Department's IndPol does for the defense industrial base. Defense has much more experience and more resources focused on a much narrower set of industries and supply chains. DHS needs to pick its shots, emulating in some respects the Air Force Office of Commercial and Economic Analysis, which performs case studies rather than boil-the-ocean analyses and which has earned a strong reputation by doing those studies well, rather than by seeking broad authorities and the bureaucratic competition that can engender.

Recommendation 6: At the start, the DHS economic security effort should be incremental, focused on high-impact, focused reviews of priority topics/sectors.

With that limitation in mind, we offer a set of suggestions for ways in which DHS's economic security unit can focus its efforts on topics that will be most useful and that can ultimately form the foundation of a comprehensive economic security plan for the civilian economy.

Background for Recommendation 6a

First, the Commerce Department welcomed the assistance of DHS in its past assessments of critical industry vulnerabilities, and the Commerce Department has just been assigned sweeping but ill-defined authority to exclude from the nation's information and communications networks any foreign-owned technology that poses undue risks of sabotage or subversion.⁵⁹ To carry out this responsibility, the Commerce Department will need the kind of analytic capabilities DHS seeks to build.

Recommendation 6a: DHS should formalize its role in supplying data and risk management analysis to the Commerce Department pursuant to E.O. 13873.

Background for Recommendation 6b

A second and urgently needed project concerns the "Made in China 2025" policy described earlier. This is the policy that has driven over 75% of China's mercantilist practices, including intellectual property theft, cyberespionage, and predatory trade actions. By and large, the purpose of Made in China 2025 and similar mandates is to improve China's economic and national security at the expense of the United States in the same fields.⁶⁰

So, as a first-order metric for defending U.S. economic security, why not start with China's plan of attack? The Department could conduct an analysis of how successful the Made in China 2025 plan and the broader Chinese industrial planning strategy have been or are likely to be in hollowing out U.S. sources of supply. Where needed, the Department could follow up with policy responses to ensure the continued viability of the industries China wants to take away.

Recommendation 6b: DHS should conduct a joint DoD-DHS analysis of the industries identified by China as its priorities for ensuring China’s economic security (and reducing the economic security of the United States). The study should ask two questions about every industry on China’s shopping list: which U.S. producers are put at risk by China’s mercantilist policies and what can the U.S. do to ensure their survival?

Background for Recommendation 6c

A third way for DHS to expand its economic security capabilities is to build on a foundation laid by CFIUS and Team Telecom. It often occurs that a CFIUS or Team Telecom matter exposes a vulnerability not previously understood. But these authorities only allow the government to permit or veto a particular transaction. Often, though, the transaction simply brings to light a much broader supply chain problem; a wider study of the industry and of remedial actions is frequently needed.

As an example, the government was first forced to consider the risks posed to U.S. critical infrastructure by Chinese telecommunications equipment makers in 2007, when CFIUS was asked to rule on a transaction that would have given Huawei a large role in the U.S. company, 3Com.⁶¹ After the deal caused concern at the highest levels of government, it was rejected.⁶² Unfortunately, once they had voted against the transaction, the Cabinet officials who mistrusted Huawei had no easy way to ask for a broader review of the company and the risks it might pose. So, when an economic stimulus bill was written in a hurry in 2009, it included \$7.2 billion in broadband grants and loans — without anyone asking whether the funds might be spent installing Chinese telecommunications gear in U.S. networks. In fact, many rural and smaller carriers were offered Chinese equipment at low prices. These carriers installed so much Chinese equipment that, ten years later, the Federal Communications Commission had to go back to Congress and ask it to appropriate \$1.8 billion to get those same carriers to rip the Chinese gear out of their networks.⁶³ One reason for this debacle was the loss of institutional memory following the rejection of the 3Com transaction. While CFIUS continued to be suspicious of any Huawei (and ZTE) acquisitions, the remaining elements of U.S. policymaking were never engaged in addressing the threat that such acquisitions posed to U.S. economic security. The DHS economic security unit should be made available to build on what is learned in CFIUS reviews and to recommend broader responses to threats identified during those reviews. The same is true for referrals from members of Team Telecom and from the Commerce Department after actions under E.O. 13873.

Recommendation 6c: DHS should conduct industry-wide supply chain assessments of particular companies or industries based on referrals from CFIUS, from Team Telecom, and from the E.O. 13873 interagency process.

Background for Recommendation 6d

Fourth, the Federal Acquisition Security Council (FASC) is just beginning its work of searching out suppliers who should not be part of federal procurements. But a supplier who is deemed too risky for federal purchase is probably also too risky for critical civilian infrastructure. However

the FASC does not have authority over private procurement decisions. Where the FASC is concerned about the security of a product but lacks a complete set of tools for addressing the private-sector side of the problem, DHS should be willing to accept referrals from the FASC to assess the supplier and to recommend appropriate steps to counteract any economic security risks posed by the supplier.

Recommendation 6d: DHS's economic security unit should also accept referrals from the Federal Acquisition Security Council. It should be possible for the Council to seek a broader study of a particular industry or company than the Council itself is designed to perform. DHS's economic security unit should be prepared to accept such referrals.

Background for Recommendation 6e

Fifth, the Coast Guard, CBP, and the Transportation Security Administration all purchase big-ticket hardware from suppliers whose products they must trust; they have an interest in the long-term viability and security of their suppliers — and in having a choice of secure bidders in future. These DHS components could refer one or more of these suppliers or endangered capabilities to the economic security unit for a deeper dive into the conditions of competition in specific sectors and the risk that insecure suppliers may supplant those on whom DHS relies. The Economic Security Council can help the Secretary in prioritizing these concerns, and the economic security unit can conduct the analysis and develop the options for ensuring security of supply.

Recommendation 6e: The DHS economic security unit should accept nominations for economic security reviews from DHS components concerned about their critical components.

Background for Recommendation 7

DoD's economic security unit, IndPol, weighs in routinely with the Justice Department and Federal Trade Commission (FTC) on mergers and acquisitions that affect the defense industrial base, particularly where a combination would reduce competition for defense procurement. While DHS has fewer large procurements, it has some (icebreakers, scanning equipment) and it has an interest in a competitive communications and information technology market. DHS should therefore establish a central ability to respond effectively when the FTC or Justice seeks comment on filings under the Hart-Scott-Rodino merger procedures.

Recommendation 7: DHS's economic security unit should be a focal point for Hart-Scott-Rodino reviews where the merger could reduce competition or security in sales of equipment that is vital to DHS missions, such as icebreakers and cargo and traveler scanning equipment.

Federal Emergency Management Agency

Though best known for its disaster response role, the Federal Emergency Management Agency (FEMA) has a number of authorities and programs that can help strengthen economic security.

Background for Recommendation 8

As the nation mobilized for the Korean War, officials realized that the federal government lacked the domestic authorities needed to successfully confront our Cold War adversaries. The Defense Production Act of 1950, together with other mobilization and civil defense authorities, gave rise to the nation's ability to prepare itself for war.⁶⁴ The agency responsible for executing these authorities is FEMA.⁶⁵

President Reagan embraced FEMA's Cold War mission and empowered it with additional authorities during the 1980s. However, since the 1950s this had become a patchwork of statutes and executive orders that were successively layered on top of each other, rather than a comprehensive set of actionable plans. And since the end of the Cold War, the FEMA programs supporting the DPA and related authorities have atrophied.

Faced with shortages of medical and personal protective equipment during the 2020 pandemic, the Trump Administration utilized the DPA to speed acquisition. While FEMA was able to successfully implement the DPA, the experience demonstrated the need to be better prepared for future supply disruptions. While several DPA Titles have been actively employed before and during the COVID-19 pandemic, there is a clear need to reframe the DPA at the national level to make the best use of its authorities to address future national emergencies.

The DPA also includes measures that can stop the decline of an industry or exclude a dangerous supplier. Title III of the DPA funds a variety of programs to preserve or jumpstart U.S. industries that are critical to the U.S. supply chain, and has been used successfully by the U.S. Department of Defense in the past.

While Title III has been delegated to DOD for execution, the COVID-19 response has clearly shown its potential to support industrial base and economic security needs across the spectrum, through numerous projects in support of HHS requirements in the areas of personal protective equipment and public health. DHS has one active-in-Title III project underway, but it should strengthen this connection and its use of Title III by partnering with DoD to build an institutional capacity to identify homeland industrial base weaknesses and develop Title III projects to mitigate these areas.

Recommendation 8a: FEMA, in coordination with DHS and the interagency, should put forward a framework for an executive order or legislation that revives and makes best use of existing authorities under the Defense Production Act and related executive and statutory authorities.

Recommendation 8b: FEMA should rebuild its internal structures and programs to ensure that it has the resources necessary to respond to sudden national shortages during a national emergency.

Recommendation 8c: FEMA and DHS should strengthen their engagement with the Title III program under the Defense Production Act, and develop an institutional capability to sponsor and follow through on the use of Title III funds to meet homeland economic security goals.

The Trade Enforcement and Immigration Agencies — CBP, ICE/HSI, and USCIS

Background for Recommendations 9, 10 and 11

The trade and immigration components of the Department have important roles to play in economic security arising both from their enforcement responsibilities and from the situational awareness that enforcement can provide. Many of the policy tools that support economic security depend on CBP and ICE/Homeland Security Investigations (HSI) for enforcement. This obviously includes antidumping and countervailing duty tariffs, where circumvention through transshipment and other origin fraud is a serious problem. It also includes trading with sanctioned parties. ICE/HSI Global Trade enforcement should make these activities a measurable enforcement budget priority.

The intelligence arms of these agencies could also be used on a priority basis to look for evasions of economic security measures. CBP's National Targeting Center (NTC) and the ICE Global Trade unit could both be tasked to prioritize enforcement of economic security measures. The NTC collects and fuses data across both outbound and inbound shipments and individuals. NTC data, tools, and analysis are an important contribution to the broader economic security analyses and intelligence gathering efforts envisioned in the DHS economic security unit. CBP should assess whether its targeting applications need to be retooled to address emerging economic security threats; and the proposed economic security unit should leverage NTC data and analysis wherever possible.

Enforcement prioritization at ICE/HSI is in the end a matter of enforcement hours spent on particular categories of violation. It would make sense, for example, for the Executive Associate Director for HSI at ICE to set targets for enforcement hours in this category of investigation in coordination with the Economic Security Council.

We are aware that another Homeland Security Advisory Committee subcommittee will be looking closely at visa reforms, many of which will require legislation to implement. That said, we urge that subcommittee, and U.S. Citizenship and Immigration Services (USCIS), to closely scrutinize the EB-5 Investor Visa Program, which attracts foreign capital and investors, offering residency in exchange for targeted investments in the U.S. economy and associated job creation.

EB-5 has long attracted Chinese nationals, and applications from China represent the majority of those received by USCIS.⁶⁶ Concerns have been raised regarding Chinese state-sponsored nationals seeking U.S. residency through this program as a means of extending surveillance and intelligence gathering. Potential risks and vulnerabilities should be identified, addressed and monitored closely. As other avenues of immigration have closed, EB-5 is likely to be exploited more systematically by the Chinese government.

Finally, the standards and scrutiny for visas granted to students and technology workers from countries of concern are obviously relevant to possible economic espionage and the future competitiveness of U.S. companies. USCIS and ICE already have authority to improve information sharing with each other, specifically by increasing USCIS access to Student & Exchange Visitor Information System (SEVIS) data and increased coordination between USCIS's Fraud Detection and National Security Directorate and ICE's Student and Exchange Visitor Program. They should work more closely on investigations and site visits for technology-heavy visa programs such as CPT (Curricular Practical Training), OPT (Optional Practical Training), and Science, Technology, Engineering, and Mathematics OPT. Further, to make it easier to screen high-risk populations, the State Department, CBP, ICE, and USCIS should be capturing standardized data (such as employment history, current/prior R&D affiliations, participation in foreign government-sponsored talent recruitment programs, etc.) on those who seek visas to study or conduct research in the United States; that data should be automatically available to all three agencies through their respective IT systems.

Recommendation 9: The Secretary should direct CBP and ICE/HSI to make enforcement of economic security measures a measurable enforcement priority — and an intelligence collection target.

Recommendation 10: The Secretary should direct USCIS and ICE to increase coordination on student visas, granting USCIS appropriate access to SEVIS data and working together on site visits and investigations in technology-heavy visa programs such as CPT and OPT. The Secretary should direct CBP, ICE, and USCIS to standardize and make available to each other data on foreign nationals coming to the U.S. for research and study; the State Department should join in this initiative.

Recommendation 11: USCIS and the relevant HSAC subcommittee should review the EB-5 program for the risk that Chinese applicants may be operating as agents of the Chinese government.

The Transportation Security Administration (TSA)

TSA's responsibility for aviation security has put it on the front line of multiple economic security issues. The most pressing concerns are drones and the machines that TSA uses to inspect cargo and passengers for dangerous items.

Drones. Unmanned aerial systems (UAS) range from toys capable of staying airborne for a few minutes to highly sophisticated military-grade systems capable of autonomous, long-range, zero-radio frequency emissions flight. UAS are rapidly becoming more sophisticated, with complex

features like altitude and GPS or waypoint navigation. These devices are technically complex enough to use artificial intelligence programs like machine vision and networked sensing to operate with a high degree of coordination and with limited operational oversight. While “swarming” is still some years down the road, in 2020 drones are already fully capable of coordinated flight.⁶⁷ Further, many UAS have customizable settings that alter their level of detectability.

UAS raises a host of new policy issues, and TSA will need both more resources and new partners. The primary focus of American legislation on UAS has been to authorize certain agencies to detect, monitor, track, and disrupt UAS. TSA needs to be part of this effort, but in the long run, state and local law enforcement will require counter-UAS capabilities. Up to now, less attention has been paid to securing the supply chains, proprietary technology, or device integrity of UAS. This is growing more urgent as agencies like CBP and FEMA begin to use UAS routinely. As UAS come to play a more significant role in the American economy and in resiliency planning, the fact that the majority of UAS manufacturing occurs overseas represents a vulnerability to state-based adversaries, particularly China.

In recognition of this vulnerability, Presidential Determination No. 2019-13 called for the reshoring of UAS. Without domestic production capability for small UAS, as the American economy becomes reliant on drones to function, state adversaries like China will have an inappropriate ability to negatively influence American economic security. However, little functional action has been taken and the small-UAS market remains dominated by Chinese manufacturer DJI, whose UAS have been found to be one-tenth of the cost of an equivalent American manufactured product.⁶⁸ This financial disparity means that American manufacturers may not be able to meet demand for small UAS in a conflict, particularly one involving the PRC. This represents a significant national security challenge. It is unlikely that American companies will be able to compete directly with Chinese UAS manufacturers without USG support.

Background for Recommendation 12

If, as expected, American airspace is fully integrated with UAS by 2030, state adversaries like China will have a greater incentive to build electronic backdoors into UAS manufactured in their areas of influence. These backdoors could be used for a range of problematic activities, from the passive collection of information on American operations and operators to direct interference with crisis response. UAS manufactured by market leader DJI have been found to be insecure, with no way to stop device information sharing with the manufacturer.⁶⁹ In 2020, the Department of the Interior grounded all non-emergency UAS use over such national security concerns.⁷⁰

Even less overt interference, like slowing the supply of UAS and UAS materials during a crisis could have tremendous effects on a UAS-integrated economy. For example, in 2020, UAS are used commercially to deliver packages, measure the height and density of crops, monitor infrastructure, inspect power lines and utilities, and explore for oil, gas, and precious minerals.⁷¹ As companies and industries become reliant on UAS to carry out essential tasks, the UAS threat shifts from irresponsible individual users (pilots) to a hostile nation-state. As things stand now, domestic manufacturers are unable to provide an alternative to Chinese supplies in a cost-effective manner.

We do not write on a blank slate here. The HSAC Subcommittee on Emerging Technologies issued a Final Report on Unmanned Aerial and Ground-Based Systems on February 24, 2020.⁷² This report relies upon and fully endorses the recommendations in that report.

Recommendation 12: DHS should engage its interagency partners to:

- Spur creation of a technology oversight and regulating task force to ensure that rapidly evolving Chinese technology does not evade necessary regulation;
- Expand UAS regulatory resources (with support from Congress);
- Encourage and actively support innovation in the development and production of UAS in the United States by U.S. companies, particularly for those UAS intended for U.S. government use;
- Regulate the export of data (such as imagery) collected by UAS manufacturers;
- Consider requiring validation of the security of software, firmware, hardware and other UAS elements; and
- Ensure effective detection and tracking of UAS and identification of UAS registrants

Cargo and Passenger Screening Equipment. Nuctech, a Chinese state-owned enterprise founded in 1997 by the son of former Chinese Prime Minister Hu Jin Tao, is a leading supplier of screening technologies in more than 160 countries.⁷³ Founded at Tsinghua University, the company's roots lie in the nuclear industry. Their systems are used to screen personnel, passengers, cargo, vehicles, parcel/post, explosives, liquids, and in other environments, both within and outside the United States.

Background for Recommendation 13

Nuctech has faced public scrutiny of a number of its actions, including investigations into corrupt practices related to procurements of airport screening technologies in Namibia and Taiwan in 2009.⁷⁴ The European Union issued an anti-dumping order against Nuctech around the same time, after it flooded the market with Nuctech screening systems priced well below the market. China retaliated by slapping tariffs on European-produced screening equipment. However, Nuctech's market share has continued to grow.⁷⁵ In the last few weeks, the company has come under public scrutiny by the Canadian Commission on Trade for a recent award to provide screening technologies in 170 Canadian embassies, consulates and high commissions worldwide.⁷⁶

Concerns have been expressed to the Subcommittee about the security of screening algorithms and data collected or used by Nuctech. Another significant concern is the requirement that maintenance on Nuctech equipment be completed by Chinese technicians. This creates a vulnerability where the technician could either recover screening data or alter the equipment's performance without visibility by the operator. If the data and algorithms are not secure from theft or tampering, the use of such equipment in foreign airports should be a negative factor in TSA's assessment of those airports' security.⁷⁷

Nuctech is no stranger to controversy in the United States. In 2016, Nuctech applied to be listed on TSA's approved air cargo screening technology list, enlisting the help of Washington

lobbyists Cassidy and Associates to help its efforts.⁷⁸ The company's application was ultimately denied by TSA (the results of the review are not public). Nonetheless, this is a good example of a company that fell outside of both formal interagency channels of review (e.g. CFIUS) and more recent executive orders (e.g. those covering the IT supply chain).

Recommendation 13: TSA and the Deputy Assistant Secretary for Economic Security should jointly review the threat posed by Nuctech and other passenger and cargo screening equipment from China, with particular emphasis on Nuctech's access to data and algorithms used by security agencies. DHS should decide whether the use of insecure equipment is consistent with TSA's foreign airport security assessment standards.

Additional Homeland Security Stakeholders

A fundamental cornerstone of the homeland security enterprise is that it is truly a national enterprise and not just the activities of one agency or even the federal government. Private citizens, the private sector, nongovernmental organizations, tribal, local and state governments all have a role to play. Indeed, it is critically important not to over-federalize response and mitigation. Resilience and response are weakened when states and local communities become more dependent on the federal government.

This doctrinal approach to homeland security activities should be reflected in department and interagency activities regarding economic security. In many cases, government should be informing and enabling private sector, civil society, local government and community response — not supplanting it.

Background for Recommendation 14:

The United States government has traditionally relied heavily on the private sector to suggest, comment on, and in some cases adopt standards for emerging technology. But it has a strong interest in the fairness, security, and reliability of the standards adopted by industry, and this interest is exemplified by the breadth of activities by the Commerce Department's National Institute of Standards and Technology. In recent years, China has launched a major government and industry effort to influence a range of global standards, including those affecting 5G technology, data security, e-commerce, security screening equipment, and other critical areas. Of a piece with China's push to change the rules of global engagement and global governance, the standards initiative seeks to produce standards outcomes more favorable to — and even controlled by — Beijing. The engagement of the Chinese government in this effort means that the United States can no longer rely entirely on the American private sector to ensure fair, secure, and reliable outcomes in international standards processes. Like other parts of the federal government, DHS should identify Chinese government influence on standards important to the Department and bring its concerns to the relevant interagency coordination bodies.

Recommendation 14: In coordination with the federal interagency process, the Department should identify relevant global standard-setting activities likely to have an impact on DHS and determine whether Chinese government efforts to influence the standards require monitoring or action.

ACKNOWLEDGEMENTS

Many people contributed to this report and deserve special thanks. In addition to the witnesses who shared so much of their time and expertise, the Subcommittee is indebted to Evan Hughes, of the Homeland Security Advisory Council staff, who worked overtime to keep the witnesses and the report on track; to Sharon Cardash of Auburn University and Katherine Petrich, of the Center for Policy Research for their rigorous review of multiple drafts; to Karl Staudinger, graphic designer in the office of the DHS Chief Information Officer, who made the report more reader-friendly; and to Michael Miron, Acting Executive Director of the HSAC, Garret Conover, Director of the HSAC, and to Colleen Hughes, HSAC Analyst, for their consistent care and support.

Appendix 1: Tasking Letter

Secretary


U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

February 21, 2020

MEMORANDUM FOR: Judge William Webster
Chair
Homeland Security Advisory Council

FROM: Chad F. Wolf 
Acting Secretary, Department of Homeland Security

SUBJECT: **Four New Homeland Security Advisory Council (HSAC)
Taskings**

Pursuant to the February 24, 2020 meeting of the Homeland Security Advisory Council, I am requesting that you establish four new HSAC subcommittees to undertake reviews of critical homeland security issues. The new subcommittees will be: (1) Economic Security; (2) Information and Communications Technology Risk Reduction; (3) Building Youth-Focused Engagements; and (4) Biometrics. An explanation and proposed scope for each subcommittee is listed below in items A through D.

Recommendations are due to the full Council no later than 180 days from the date of each subcommittee's formation. I would like an update and provisional findings from each subcommittee or panel at our next public meeting, which we will hold in early May 2020.

Thank you for your work on these important matters, your service on the HSAC, and your dedication to securing our homeland.

www.dhs.gov

Subject: Four New Homeland Security Advisory Council (HSAC) Taskings
Page 2

A. Economic Security Subcommittee

Given the pace of rapidly emerging technologies, the multifaceted threat presented by nation-state competitors and non-state actors, as well as the multiple lines of effort underway to combat those threats, economic security has become a high-risk concern to a number of government stakeholders. The Department may be missing important opportunities and authorities implied by its mandate (e.g., to safeguard the American people, our homeland, and our values with honor and integrity) or may not be optimally aligning and synchronizing our interagency efforts as they relate to economic security and emerging technology. The Economic Security Subcommittee will examine the Department's authorities to ensure it has effectively aligned its efforts to support its mission; and to provide recommendations regarding how we can better protect our nation's economic security. The Subcommittee's mandate will include, but is not necessarily restricted to, the following:

1. Identify and analyze DHS entities at the Headquarters and Component levels that currently or could have capabilities to ensure the nation's economic security.
2. Provide recommendations for how DHS can best use its resources and authorities to actively ensure our economic security, as well as enhance the nation's preparedness for and resilience to such dangers.
3. Provide recommendations to ensure that the Department is optimally positioned, resourced, and organized to safeguard this important component of the American market system and way of life.
4. What programs, services, and outreach should DHS prioritize that would provide the greatest benefit to its stakeholders in reducing economic security risks?
5. Identify how DHS could improve/establish an interagency effort in order to secure the nation's economic security.

Appendix 2: Subcommittee Membership



Frank Cilluffo (Chair)

Director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security



**Stewart Baker
(Co Vice Chair)**
Steptoe & Johnson



**Robert Rose
(Co Vice Chair)**
Founder and President
Robert N. Rose
Consulting LLC



James Carafano
Vice President of The
Heritage Foundation's
Davis Institute for
National Security and
Foreign Policy



Robert Dannenberg
Retired Intelligence
Official and Former
Chief Security Officer at
Goldman Sachs



Elaine K. Dezenski
Founder and Managing
Partner
LumiRisk, LLC



Nick Eftimiades
Assistant Teaching
Professor
School of Public Affairs
Penn State Harrisburg



Daniel J. Kaniewski
Managing Director
Marsh & McLennan
Companies



John G. McGinn
Executive Director
Center for Government
Contracting, School of
Business
George Mason
University

Appendix 3: List of Witnesses

1. Matthew C. Allen, Acting Deputy Executive Associate Director, Homeland Security Investigations
2. Stephen R. Astle, Deputy Director for Strategic Initiatives, Office of Commercial & Economic Analysis, U.S. Air Force
3. Rachel Canty, Deputy Assistant Director, Homeland Security Investigations
4. Michael D'Ambrosio, Assistant Director, Office of Investigations, U.S. Secret Service
5. Robert Dannenberg, Retired Intelligence Official and Former Chief Security Officer at Goldman Sachs
6. Joseph Edlow, Deputy Director for Policy, U.S. Citizenship and Immigration Services
7. Nick Eftimiades, Assistant Teaching Professor, School of Public Affairs, Penn State Harrisburg
8. William R. Evanina, Director, National Counterintelligence and Security Center
9. Stephen Feinberg, Chief Executive Officer of Cerberus Capital Management
10. Ashley Feng, Research Associate, Energy, Economics, and Security Program, Center for a New American Security
11. Stacey Fitzmaurice, Executive Assistant Administrator, Operations Support, Transportation Security Administration
12. Scott Friedman, Acting Deputy Assistant Secretary for Economic Security, Office of Strategy, Policy & Plans, U.S. Department of Homeland Security
13. Adam Frost, Director, Office of Commercial & Economic Analysis, U.S. Air Force
14. Scott Glabe, Under Secretary (Senior Official Performing the Duties), Strategy, Policy, & Plans, U.S. Department of Homeland Security
15. Claire Grady, Former Acting Deputy Secretary, U.S. Department of Homeland Security
16. Christine Harbin, Principal Deputy to the SVP, External Engagement, Export-Import Bank of the United States
17. Robert Kolasky, Assistant Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency
18. Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency
19. Dr. Zara F. Larsen, Senior Advisor, Economic Growth, Energy and the Environment, U.S. Department of State
20. Quinton Lucie, Legal Advisor, Office of the Chief Counsel, Federal Emergency Management Agency
21. Patrick McElwain, Deputy Assistant Director, Counter Proliferation Unit, Director of the Federal Export Enforcement Coordination Center, Homeland Security Investigations
22. John G. McGinn, Executive Director, Center for Government Contracting, School of Business, George Mason University
23. Heather McMahan, Senior Director, President's Intelligence Advisory Board
24. Timothy N. Moughon, Director, Economic Security Mission Center, Intelligence and Analysis, U.S. Department of Homeland Security

25. Brian J. Murphy, Former Acting Under Secretary, Intelligence and Analysis, U.S. Department of Homeland Security
26. Dan Negrea, Special Representative for Commercial and Business Affairs, Bureau of Economic and Business Affairs, U.S. Department of State
27. Kirstjen Nielsen, Former Secretary, U.S. Department of Homeland Security
28. Nazak Nikakhtar, Assistant Secretary, Industry & Analysis, U.S. Department of Commerce, International Trade Administration
29. Reza Nikfarjam, Origination Officer, Head of Business Development, Technology Sector, Export-Import Bank of the United States
30. Thomas Overacker, Executive Director, Field Operations, Customs and Border Protection
31. Todd Owen, Executive Assistant Commissioner, Customs and Border Protection
32. Christopher Porter, National Intelligence Officer for Cyber, Office of the Director of National Intelligence
33. Tony Porter, Director of Strategic Initiatives, Office of Commercial & Economic Analysis, U.S. Air Force
34. Dr. Samantha Ravich, Chairman, Center on Cyber and Technology Innovation, Foundation for Defense of Democracies
35. Katherine Reid, Director, Defense Production Act Program, Office of Policy and Program Analysis, Federal Emergency Management Agency
36. Matthew Travis, Deputy Director, Cybersecurity and Infrastructure Security Agency
37. David Trulio, Counselor to the Chairman & Senior Vice President for the Program on China and Transformational Exports, Export-Import Bank of the United States
38. Henry Willis, Director of the Strategy, Policy, and Operations Program; Acting Director of the Personnel and Resources Program; Homeland Security Operational Analysis Center, RAND Corporation
39. Juan Zarate, Chairman & Co-Founder, Financial Integrity Network

ENDNOTES

¹ Shengkan Huang, *理直气壮, 世界应该感谢中国-新华网* [Confidently, the world should thank China], XINHUA (2020), http://www.xinhuanet.com/2020-03/04/c_1125660473.htm (last visited Oct 6, 2020).

² *Id.* as quoted in <https://www.reuters.com/article/us-health-coronavirus-usa-china-idUSKBN21C3KS>

³ Lisette Voytko, *China's Export Restrictions Reportedly Delaying Medical Supply Shipments To U.S.*, FORBES, 2020, <https://www.forbes.com/sites/lisettevoytko/2020/04/16/chinas-export-restrictions-reportedly-delaying-medical-supply-shipments-to-us/> (last visited Oct 6, 2020).

⁴ MICHAEL T. MCCAUL, *China Task Force Report* 1–149 (2020), <https://gop-foreignaffairs.house.gov/wp-content/uploads/2020/09/CHINA-TASK-FORCE-REPORT-FINAL-9.30.20.pdf> (last visited Oct 6, 2020).

⁵ ADAM SCHIFF, *The China Deep Dive: A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China* 1–30 (2020), https://intelligence.house.gov/uploadedfiles/hpsci_china_deep_dive_redacted_summary_9.29.20.pdf (last visited Oct 6, 2020).

⁶ Graham Allison, *What Xi Jinping Wants*, THE ATLANTIC, 2017, <https://www.theatlantic.com/international/archive/2017/05/what-china-wants/528561/> (last visited Oct 6, 2020).

⁷ Anthony Vinci, *How to Stop China From Imposing Its Values*, THE ATLANTIC, 2020, <https://www.theatlantic.com/ideas/archive/2020/08/like-nato-but-for-economics/614332/> (last visited Oct 6, 2020); Aaron Klein, *Economic warfare: Four takeaways from being in China when the trade war started*, BROOKINGS (2018), <https://www.brookings.edu/blog/up-front/2018/07/31/economic-warfare-four-takeaways-from-being-in-china-when-the-trade-war-started/> (last visited Oct 6, 2020).

⁸ MCCAUL, *supra* note 4.

⁹ Brenda P. Wenning, *China vs. U.S.A.*, THE PATRIOT LEDGER, December 23, 2019, <https://www.patriotledger.com/news/20191223/china-vs-usa> (last visited Oct 6, 2020).

¹⁰ THE WORLD IN 2050, <https://www.pwc.com/gx/en/issues/economy/the-world-in-2050.html> (last visited Oct 6, 2020); Sumio Saruyama & Kengo Tahara, *US and China to fight for top GDP in 2060 while Japan dips to 5th*, NIKKEI ASIA, August 1, 2019, <https://asia.nikkei.com/Economy/US-and-China-to-fight-for-top-GDP-in-2060-while-Japan-dips-to-5th> (last visited Oct 6, 2020).

¹¹ SCHIFF, *supra* note 5.

¹² ANGUS KING & MIKE GALLAGHER, *Cyberspace Solarium Commission Report* 1–184 (2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFk10MxIXJGT4yv/view?usp=embed_facebook (last visited Sep 9, 2020).

¹³ Karl von Holt, *China Manages the Virus With Surveillance, Organisation and Repression*, THE WIRE, July 31, 2020, <https://thewire.in/world/china-manages-the-virus-with-surveillance-organisation-and-repression> (last visited Oct 6, 2020); OLIVIA ENOS, *Holding the Chinese Communist Party Accountable for Its Response to the COVID-19 Outbreak* (2020), <https://www.heritage.org/asia/report/holding-the-chinese-communist-party-accountable-its-response-the-covid-19-outbreak> (last visited Oct 6, 2020).

¹⁴ Rush Doshi, *Xi Jinping just made it clear where China's foreign policy is headed*, WASHINGTON POST, October 25, 2017, <https://www.washingtonpost.com/news/monkey-cage/wp/2017/10/25/xi-jinping-just-made-it-clear-where-chinas-foreign-policy-is-headed/> (last visited Oct 6, 2020).

¹⁵ The National Defense Strategy states: "China is leveraging military modernization, influence operations, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to their advantage. As China continues its economic and military ascendance, asserting power through an all-of-nation long-term strategy, it will continue to pursue a military modernization program that seeks Indo-Pacific regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future." JIM MATTIS, *Summary of the 2018 National Defense Strategy of the United States of America* 14 (2018), <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

¹⁶ Ellen Nakashima & Devlin Barrett, *U.S. accuses China of sponsoring criminal hackers targeting coronavirus vaccine research*, WASHINGTON POST, July 21, 2020, https://www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html (last visited Oct 6, 2020).

¹⁷ *Id.*

¹⁸ This has been going on for decades. See United States International Trade Commission, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, Investigation No. 332-519 USITC Publication 4226 May 2011; *Report of the Commission on the Theft of American Intellectual Property* (2013), at https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf; *Update to the IP Commission Report* (2017) at https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf. Each work noted the ways in which the Chinese government and companies misappropriate foreign technology. Estimates of these losses are in the hundreds of billions of dollars annually. In May 2019, the European Union Chamber of Commerce in China reported results from its annual survey of European businesses operating in the country. The survey noted that 20% of members reported being compelled to transfer technology for market access. This figure was up from 10% in 2017. Researchers have suggested that these percentages are understated because Chinese officials often exert pressure to transfer technology orally to avoid creating a written record. Also, the Chinese government can be expected to retaliate against companies that raise the issue. See: *Doing Business in China in 2019 Harder for European Firms*, BLOOMBERG NEWS, May 19, 2019, <https://www.bloomberg.com/news/articles/2019-05-20/doing-business-in-china-in-2019-harder-for-european-companies> (last visited Oct 6, 2020).

¹⁹ OVERVIEW OF CHINA'S CYBERSECURITY LAW, 16 (2017), <https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf>.

²⁰ James Jin Kang, *The Thousand Talents Plan is part of China's long quest to become the global scientific leader*, THE CONVERSATION, August 31, 2020, <http://theconversation.com/the-thousand-talents-plan-is-part-of-chinas-long-quest-to-become-the-global-scientific-leader-145100> (last visited Oct 6, 2020).

²¹ Ellen Barry & Gina Kolata, *China's Lavish Funds Lured U.S. Scientists. What Did It Get in Return?*, THE NEW YORK TIMES, February 7, 2020,

<https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html> (last visited Oct 6, 2020).

²² JAMES LEWIS, *China's Pursuit of Semiconductor Independence* (2019), <https://www.csis.org/analysis/chinas-pursuit-semiconductor-independence> (last visited Oct 6, 2020).

²³ *Id.*

²⁴ *Id.*

²⁵ Marjorie Censer, *Govini: Despite DOD efforts to “reshore,” Chinese suppliers have dramatically increased*, INSIDE DEFENSE, August 20, 2020, <https://insidedefense.com/insider/govini-despite-dod-efforts-reshore-chinese-suppliers-have-dramatically-increased> (last visited Oct 6, 2020).

²⁶ KING AND GALLAGHER, *supra* note 12.

²⁷ RUSH DOSHI, *The United States, China, and the contest for the Fourth Industrial Revolution* (2020), <https://www.brookings.edu/testimonies/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/> (last visited Oct 6, 2020).

²⁸ FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE, 1–20 (2018), <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf> (last visited Oct 6, 2020).

²⁹ Huang, *supra* note 1.

³⁰ Keith Johnson & Robbie Gramer, *U.S. Struggles to End Reliance on Rare-Earth Minerals From China*, POLITICO, 2020, <https://foreignpolicy.com/2020/05/25/china-trump-trade-supply-chain-rare-earth-minerals-mining-pandemic-tensions/> (last visited Oct 6, 2020).

³¹ MATTIS, *supra* note 15.

³² PILLARS OF RUSSIA'S DISINFORMATION AND PROPAGANDA ECOSYSTEM, 1–77 (2020), https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

³³ Neil MacFarquhar, *Xi Jinping's Visit to Russia Accents Ties in Face of Tensions with U.S.* (Published 2019), THE NEW YORK TIMES, June 5, 2019, <https://www.nytimes.com/2019/06/05/world/europe/xi-jinping-china-russia.html> (last visited Oct 6, 2020).

³⁴ Sarah Cook, *Welcome to the New Era of Chinese Government Disinformation*, THE DIPLOMAT, May 11, 2020, <https://thediplomat.com/2020/05/welcome-to-the-new-era-of-chinese-government-disinformation/> (last visited Oct 6, 2020).

³⁵ Defense Industrial Base Sector, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), <https://www.cisa.gov/defense-industrial-base-sector> (last visited Oct 6, 2020).

³⁶ Reports for FY 2013 through FY 2019 are available at U.S. Department of Defense, Industrial Policy, “Congressional Interests and Reports,” <https://www.businessdefense.gov/resources/> (accessed July 10, 2020).

³⁷ Industrial Policy, UNITED STATES DEPARTMENT OF DEFENSE, <https://www.businessdefense.gov/> (last visited Oct 6, 2020).

³⁸ Defense Priorities & Allocations System Program (DPAS), UNITED STATES DEPARTMENT OF COMMERCE, <https://www.bis.doc.gov/index.php/other-areas/strategic-industries-and-economic-security-sies/defense-priorities-a-allocations-system-program-dpas> (last visited Oct 6, 2020).

³⁹ 15 U.S.C. § 18a.

⁴⁰ Reports from December 2008 through calendar year 2018 are available at U.S. Department of the Treasury, “CFIUS Reports and Tables,” <https://home.treasury.gov/policy->

issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-reports-and-tables (accessed July 10, 2020).

⁴¹ David Alexander, “*Great Green Fleet*” using biofuels deployed by U.S. Navy, REUTERS, January 21, 2016, <https://www.reuters.com/article/us-usa-defense-greenfleet-idUSKCN0UY2U4> (last visited Oct 6, 2020).

⁴² H.R. 748, Coronavirus Aid, Relief, and Economic Security (CARES) Act, Public Law 116-136, 116th Cong., March 27, 2020, <https://www.congress.gov/bill/116th-congress/house-bill/748/text?loclr=bloglaw%23toc-H0D9C019E301D4A9584058F8DA59D1CC8> (accessed July 11, 2020).

⁴³ DOD Awards \$126 Million Contract to 3M, Increasing Production of N95 Masks, [https://www.defense.gov/Newsroom/Releases/Release/Article/2178152/dod-awards-126-million-contract-to-3m-increasing-production-of-n95-](https://www.defense.gov/Newsroom/Releases/Release/Article/2178152/dod-awards-126-million-contract-to-3m-increasing-production-of-n95-masks/#:~:text=‘The%20Department%20of%20Defense%2C%20in,month%2C%20starting%20in%20October%202020;DOD%20Awards%20$138%20Million%20Contract%20Enabling%20Prefilled%20Syringes%20for%20Future%20COVID-19%20Vaccine,)

masks/#:~:text=“The%20Department%20of%20Defense%2C%20in,month%2C%20starting%20in%20October%202020; DOD Awards \$138 Million Contract Enabling Prefilled Syringes for Future COVID-19 Vaccine, [https://www.defense.gov/Newsroom/Releases/Release/Article/2184808/dod-awards-138-million-contract-enabling-prefilled-syringes-for-future-covid-19/source/GovDelivery/supra note 42.](https://www.defense.gov/Newsroom/Releases/Release/Article/2184808/dod-awards-138-million-contract-enabling-prefilled-syringes-for-future-covid-19/source/GovDelivery/supra%20note%2042.)

⁴⁴ Mark LaPedus, *A Crisis In DoD’s Trusted Foundry Program?*, SEMICONDUCTOR ENGINEERING (2018), <https://semiengineering.com/a-crisis-in-dods-trusted-foundry-program/> (last visited Oct 6, 2020).

⁴⁵ Blue Dot Network: Frequently Asked Questions, UNITED STATES DEPARTMENT OF STATE , <https://www.state.gov/blue-dot-network-frequently-asked-questions/> (last visited Oct 6, 2020).

⁴⁶ China's Belt and Road Initiative (BRI) exemplifies Beijing's aggressive expansion of its global footprint to secure natural resources, trade lanes, economic and political influence, and military access. BRI offers developing economies (and their leadership) fast and cheap money with few visible strings of conditionality attached — all in exchange for Beijing-sponsored goods, services, labor, and technology. However, projects have often fallen short of providing the high-quality infrastructure that so many countries need; and lack of conditionality has contributed to an explosion of corruption. High profile examples include Kenya (the overpriced Kenya Standard Gauge Railway), Malaysia (1MDB and Chinese political influence), and Sri Lanka (the problematic Port of Hambantota). BRI has laid bare both the potential of Chinese investment and, increasingly, the political and economic risks and challenges to recipient countries that have fueled the rapid growth of Beijing's influence in developing economies. The scope of BRI as a geopolitical enterprise extends well beyond typical brick and mortar infrastructure projects. Its promotion of the BRI "digital silk road," where Beijing offers 5G capabilities that bring connectivity to millions (in theory, a laudable goal), also enables and facilitates large-scale surveillance, manipulation, and control of information. See: PETER CAI, *Understanding China’s Belt and Road Initiative* (2017), <https://www.lowyinstitute.org/publications/understanding-belt-and-road-initiative> (last visited Oct 6, 2020); Andrew Chatzky & James McBride, *China’s Massive Belt and Road Initiative*, COUNCIL ON FOREIGN RELATIONS (2020), <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative> (last visited Oct 6, 2020); China’s Belt and Road Initiative in the Global Trade, Investment and Finance Landscape, 61–101 (2018), https://doi.org/10.1787/bus_fin_out-2018-6-en.

⁴⁷ Leigh Hartman, *What is the Blue Dot Network for infrastructure financing?*, SHAREAMERICA (2020), <https://share.america.gov/what-is-blue-dot-network-for-infrastructure-financing/> (last visited Oct 6, 2020).

⁴⁸ Prague 5G Security Conference announced series of recommendations: The Prague Proposals, GOVERNMENT OF THE CZECH REPUBLIC (2019), <https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/> (last visited Oct 6, 2020); Joint Statement on United States - Czech Republic Joint Declaration on 5G Security, UNITED STATES DEPARTMENT OF STATE (2020), <https://www.state.gov/joint-statement-on-united-states-czech-republic-joint-declaration-on-5g-security/> (last visited Oct 6, 2020).

⁴⁹ RICHARD J DANZIG, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* 64 (2014), https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf?mtime=20161010215746.

⁵⁰ These industries include: artificial intelligence, biotechnology, biomedical sciences, wireless communications equipment (5G technology), quantum computing, renewable energies, semiconductor manufacturing, emerging financial technologies, water treatment and sanitation, and high performance computing. Program on China and Transformational Exports, EXPORT-IMPORT BANK OF THE UNITED STATES, <https://www.exim.gov/who-we-serve/external-engagement/program-on-china-and-transformational-exports> (last visited Oct 6, 2020).

⁵¹ *Id.*

⁵² KING AND GALLAGHER, *supra* note 12.

⁵³ *Id.*

⁵⁴ Cyberspace Solarium Commission, Building a Trusted ICT Supply Chain, CSC White Paper # 4 (October 2020).

⁵⁵ Mission, DEPARTMENT OF HOMELAND SECURITY (2012), <https://www.dhs.gov/mission> (last visited Oct 6, 2020).

⁵⁶ About CISA, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), <https://www.cisa.gov/about-cisa> (last visited Oct 6, 2020).

⁵⁷ Cyberspace Solarium Commission, *supra* note 54 at 13.

⁵⁸ GUIDE TO CRITICAL INFRASTRUCTURE AND KEY RESOURCES PROTECTION AT THE STATE, REGIONAL, LOCAL, TRIBAL, AND TERRITORIAL LEVEL, 1–100 (2008), <https://www.hsdl.org/?view&did=233432> (last visited Oct 8, 2020).

⁵⁹ Exec. Order No. 13873, 84 FR 22689 (2019).

⁶⁰ JAMES MCBRIDE & ANDREW CHATZKY, *Is 'Made in China 2025' a Threat to Global Trade?*, <https://www.cfr.org/background/made-china-2025-threat-global-trade> (last visited Oct 8, 2020); MADE IN CHINA 2025, 1–9 (2018), <https://isdpeu.org/content/uploads/2018/06/Made-in-China-Backgrounder.pdf> (last visited Oct 8, 2020).

⁶¹ Reuters Staff, *3Com plans to file Bain, Huawei deal with CFIUS*, REUTERS, October 4, 2007, <https://www.reuters.com/article/3com-bain-cfius-idUSWEN149720071004> (last visited Oct 8, 2020).

⁶² Grant Gross, *Security issues scuttle Bain/Huawei bid for 3Com*, NETWORK WORLD (2008), <https://www.networkworld.com/article/2283966/security-issues-scuttle-bain-huawei-bid-for-3com.html> (last visited Oct 8, 2020).

⁶³ Natalie Gagliardi, *US telecoms would spend \$1.8 billion to replace ZTE, Huawei network equipment*, BETWEEN THE LINES (2020), <https://www.zdnet.com/article/us-telecoms-would-spend-1-8-billion-to-replace-zte-huawei-network-equipment/> (last visited Oct 8, 2020).

⁶⁴ Defense Production Act, Pub. L. No. 81-774, 123 Stat. 2006 (1950).

⁶⁵ Quinton Lucie. “How FEMA Could Lose America’s Next Great War.” *Homeland Security Affairs* 15, Article 1 (May 2019). <https://www.hsaj.org/articles/15017>

⁶⁶ Chinese Investors Among Majority Of EB-5 Visa Recipients, ALL THINGS CONSIDERED (2017), <https://www.npr.org/2017/05/22/529550240/chinese-investors-among-majority-of-eb-5-visa-recipients> (last visited Oct 8, 2020).

⁶⁷ Mind of the swarm - Amazing new technology allows drones to flock together as they fly, RAYTHEON MISSILES & DEFENSE (2020), <https://www.raytheonmissilesanddefense.com/news/feature/mind-swarm> (last visited Oct 8, 2020).

⁶⁸ MARK L BATHRICK & BRAD KOECKERITZ, *DJI Unmanned Aircraft System (UAS) Mission Functionality and Data Management Assurance Assessment* 53 (2019), https://www.doi.gov/sites/doi.gov/files/uploads/oas_flight_test_and_technical_evaluation_report_-_dji_uas_data_managment_assurance_evaluation_-_7-2-19_v2.0.pdf.

⁶⁹ *Id.*

⁷⁰ Secretary Bernhardt Signs Order Grounding Interior’s Drone Fleet for Non-Emergency Operations, UNITED STATES DEPARTMENT OF THE INTERIOR (2020), <https://www.doi.gov/pressreleases/secretary-bernhardt-signs-order-grounding-interiors-drone-fleet-non-emergency> (last visited Oct 6, 2020).

⁷¹ Mahashreveta Choudhary, *What are popular uses of drones?*, GEOSPATIAL WORLD (2019), <https://www.geospatialworld.net/article/what-are-popular-uses-of-drones/> (last visited Oct 6, 2020).

⁷² THAD ALLEN, CATHY LANIER & ROBERT ROSE, *Final Report of the Emerging Technologies Subcommittee Unmanned Aircraft Systems* 23 (2020), https://www.dhs.gov/sites/default/files/publications/final_report_hsic_emerging_technologies_subcommittee_uas_508_compliance.pdf.

⁷³ Company, NUCTECH, <http://www.nuctech.com/en/SitePages/SeNormalPage.aspx?nk=ABOUT&k=ACABGD> (last visited Oct 6, 2020).

⁷⁴ Investigation into NucTech corruption expands, the company formerly headed by Hu Haifeng, ASIANEWS, July 22, 2009, <http://www.asianews.it/news-en/Investigation-into-NucTech-corruption-expands,-the-company-formerly-headed-by-Hu-Haifeng-15849.html> (last visited Oct 6, 2020).

⁷⁵ Lauren Cerulus et al., *Chinese tech companies could face trouble in Europe*, POLITICO, 2020, <https://www.politico.eu/article/meet-china-inc-s-firms-that-could-face-trouble-in-europe-2/> (last visited Oct 6, 2020).

⁷⁶ Sam Cooper & Andrew Russell, *Canadian minister promises review after security contracts awarded to Chinese-state tech company*, GLOBAL NEWS, September 10, 2020, <https://globalnews.ca/news/7189962/canadian-border-security-contracts-china/> (last visited Oct 6, 2020).

⁷⁷ See: 49 U.S.C. § 114; 49 C.F.R. ch. XII, subch. C.

⁷⁸ Morgan Chalfant, *Nuctech, Accused of Corruption, Lobbies U.S. Government*, THE WASHINGTON FREE BEACON (2016), <https://freebeacon.com/national-security/chinese-security-company-accused-corruption-lobbies-u-s-government/> (last visited Oct 6, 2020).