NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Ms. Renée James
NSTAC Chair
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

April 2, 2019

The Honorable Donald J. Trump
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear Mr. President:

In August 2018, you tasked the National Security Telecommunications Advisory Committee (NSTAC) to study technology capabilities that are critical to national security and emergency preparedness (NS/EP) functions in the evolving information and communications technology (ICT) ecosystem. The NSTAC would then develop recommendations for Government measures and policy actions to manage near-term risks, support innovation, and enhance vendor diversity for NS/EP-critical capabilities.

The United States is dependent on technologies manufactured in foreign countries to maintain and advance its national strategic interests. While some of these countries are allies of the United States, others have political, economic, and security agendas that run counter to U.S. interests. Compounding the risk, some nations have adopted explicit strategies to dominate various aspects of advanced technologies, including their development, production, and deployment as part of their broader economic strategy (e.g. China's *Made in China 2025* plan). It is imperative that the United States maintain and, in some cases, regain its leadership in key ICT systems as well as ensure the integrity, resiliency, and security of the ICT supply chain.

In this letter, the NSTAC has identified three representative technologies that are highly critical to the United States' NS/EP mission as well as the challenges presented by U.S. dependency on certain technologies.

Further, the NSTAC has several preliminary recommendations as a result of the first phase of the study. Foremost is that the United States needs a holistic national innovation strategy for ICT, which it relies on for its NS/EP mission. The purpose of this strategy would be to enhance coordination between Government and industry, including manufacturers located in allied nations, to ensure that the United States and its allies continue to lead in the development,

production, and deployment of critical NS/EP technologies. By enacting such a strategy, the United States would avoid creating dependencies on untrusted foreign manufacturers to meet its NS/EP critical technology needs. The strategy's objective would not be to exert U.S. Government control over the decisions of private businesses. Rather, the strategy would leverage the U.S. Government's unique authorities and competencies to enable industry partners to play a global leadership role. These authorities and competencies would include the ability to raise visibility of the risks created by reliance upon an untrusted supply chain, set national strategic priorities and allocate Federal resources, convene stakeholders, and incent collaborative action, in part through outcome-based research and development strategies. This national innovation strategy must include a plan for ICT advancement, resiliency, and security that addresses the need for global standards in supply chain resiliency and security. Such standards will help the critical sectors avoid, plan for, and mitigate the risks of ICT dependencies.

During the second phase of this study, the NSTAC plans to examine how certain NS/EP ICT dependencies, market limitations, and supply chain risks began, using the development and deployment of fifth generation (5G) technologies as a case study. The NSTAC will use these findings to formulate recommendations for policies and actions to include in the recommended national innovation NS/EP ICT strategy. This strategy will ensure that the United States is more resilient, has access to trusted technology to support its NS/EP mission, and leads in the development and use of ICT technology critical to NS/EP missions in the future.

The Challenge

Since 2017, cyber attacks targeting the ICT global supply chain have been rising, as have reports of widespread compromise of certain modularized software components used by Internet of Things devices.[1,2] The convergence of ICT and operational technology (OT) is occurring rapidly within the critical infrastructure sectors that underpin modern society. The United States relies on ICT infrastructure for the functioning of Government, as well as critical services such as banking, utilities, healthcare, and transportation. The pervasiveness of internet protocol-based networks provides a complex attack surface that malicious actors and U.S. adversaries know they can exploit. Whether the motivation is to quietly subvert critical systems in order to erode U.S. wealth and power over time, to disrupt or destroy these systems on a widespread basis at a time of their choosing, or both, the risk cannot be overstated. The U.S. Government may lack full awareness of how much control its potential adversaries have attained over key ICT systems until they choose to demonstrate those capabilities, potentially during a crisis or conflict.

The United States' dependence on foreign-controlled or owned technologies is not a new issue for the national security community, but it no longer affects only a few isolated mission systems. NS/EP systems depend on a vast array of ICT and componentry, and the United States has lost some control over certain phases of the life cycle for these products. There are many examples of U.S. national security functions depending on the same critical infrastructure as the private

1 Kelly Jackson Higgins, "Supply Chain Cyberattacks Surged 200% in 2017," Dark Reading, March 22, 2018, accessed December 31, 2018, https://www.darkreading.com/attacks-breaches/supply-chain-cyberattacks-surged-200--in-2017/d/d-id/1331337.

2 John Chen, et. al,, *China's Internet of Things* (Washington: U.S.-China Economic and Security Review Commission, October 25, 2018), U.S.-China Economic and Security Review Commission website, https://www.uscc.gov/Research/chinas-internet-things.

sector, including commercial off-the-shelf products that comprise the U.S. military's information technology networks and support missions, such as domestic defense, space operations, and border security. The U.S. Government and critical infrastructure providers increasingly depend on technologies, such as sensor-based monitoring systems, global positioning and guidance systems, robotics and autonomous vehicles, high performance computing, and mobile devices and platforms. In turn, these technologies depend on secure and reliable ICT, which, if compromised, could disrupt the performance of the U.S. Government's missions and the delivery of services by critical infrastructure providers. All of these technologies comprise the interconnected and interdependent networked environment that Government decision makers, intelligence and information sharing networks, military command and control systems, and first responders rely on for NS/EP operations.

Several factors have led the United States to lose influence over the design, development, and production of technologies used in NS/EP critical systems. The Nation's failure to support domestic innovation has roots in three decades of underinvestment in people, education, and research. Further, the Nation has historically failed to adequately address intellectual property (IP) theft and has allowed perpetrators of this IP theft to invest in key technologies in the United States. Finally, although there have been prior efforts to address the issue of ICT supply chain risk and resiliency within the Federal Government, the United States has never undertaken a comprehensive, whole-of-nation effort to address ICT resiliency and supply chain security. The lack of a coordinated response by the United States to this problem stands in stark contrast to the long-considered, well-planned, and steadily executed strategies of other world powers.

The Need

The U.S. Government's approach to this problem must be grounded by the realities the Nation faces with respect to national and global economics, as well as societal and market shifts. Accordingly, the NSTAC identified several principles to guide the NSTAC's work on this issue during the next phase of the tasking.

- First, NS/EP functions require secure and resilient internet connectivity. The *NSTAC Report to the President on a Cybersecurity Moonshot* (2018) recommended that the U.S. Government declare a national strategic intent and empower whole-of-nation resources to pursue a more fundamentally safe internet environment for critical services. ICT resiliency and supply chain security are fundamental components of this pursuit.[3] A vital pillar of the Moonshot initiative includes actions targeted to maintain U.S. ICT innovation and leadership in existing technologies and investment for leadership in technologies that will be key to NS/EP in the future.

- Second, in evaluating critical NS/EP technologies, it is necessary to consider the delivery of services by the critical infrastructure sectors during all operating states (e.g. normal

3 NSTAC, *NSTAC Report to the President on a Cybersecurity Moonshot* (Washington: NSTAC, October 31, 2018), 2018 NSTAC Publications, https://www.dhs.gov/sites/default/files/publications/DRAFT_NSTAC_ReportToThePresidentOnACybersecurityMoonshot_508c.pdf.

operations, under duress/attack, during recovery).[4] Traditional definitions of national security have centered on U.S. military command and control, and Federal, State, and local disaster response.[5] However, traditional elements of national security depend on a broad array of private sector actors, including the owners, operators, and providers of certain critical infrastructure (e.g., ICT systems and energy). Future national innovation and ICT resiliency strategies must also involve a whole-of-nation response that features close coordination between the U.S. Government and the critical infrastructure sectors, which the NSTAC explored in its *NSTAC Report to the President on Information and Communications Technology Mobilization* (2014). In particular, any ICT resiliency strategy must help critical infrastructure owners and operators to understand the business value in stronger ICT resiliency and supply chain risk management.

- Third, a deeper understanding of the complexity of the Nation's supply chain security and resilience factors is necessary to inform the development of the NSTAC's recommended national NS/EP ICT innovation strategy. These include internal and external threats, including human error; the layers of manufacturing dependencies owing to an extensive, multi-tiered global supply chain; the challenge of addressing the vast pool of products being integrated into U.S. systems; and device security at the component level and trusted mechanisms for post-production maintenance and operations. Procurement-based strategies can be part of the solution, but ICT supply chain security and resiliency must begin with the holistic and continuous examination of risk at each phase of the product lifecycle.

- Finally, U.S. allies must be included in the NS/EP ICT innovation strategy to ensure that coordinated strategies are in place to foster investment and support markets to counter domination by potentially adversarial nations. Such a coalition can also help to ensure that allied nations are better represented in international standards development and enforcement to counterbalance the overrepresentation by certain nations in these processes.

The NS/EP ICT innovation strategy should address intelligence gaps concerning the vulnerabilities that U.S. adversaries may attempt to exploit as well as the steps necessary to address the vulnerabilities themselves. The U.S. Government must draw a connection between supply chain security and existing methods for evaluating and improving the overall cybersecurity posture of enterprises. It must also encourage or direct the creation of better methodologies to evaluate risk and trust in products. The strategy must include the technology workforce as a core component and examine the need to incentivize the creation of national innovators and national protectors, such as cybersecurity experts. Above all, the NS/EP ICT innovation strategy must be guided by the lifecycles of critical ICT systems, from conception through operation to retirement, and address the risks inherent in each phase.

4 The Department of Homeland Security Critical Infrastructure Sectors, Department of Homeland Security, accessed December 31, 2018, https://www.dhs.gov/cisa/critical-infrastructure-sectors.

5 Robert O. Work, *DOD Directive 8000.01: Management of the Department of Defense Information Enterprise (DoD IE)* (Washington, DC: Department of Defense, 2017), Executive Services Directorate: Washington Headquarters Service, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/800001p.pdf.

Solutions Must Consider All Phases of the Technology Lifecycle

Until now, discussions about ICT resiliency have largely focused on supply chain security and eliminating the possibility of compromise during the manufacturing phase. Policies to limit procurement of certain products (i.e., blacklisting), require procurement of approved products (i.e., whitelisting), or mandate that manufacturers deliver vulnerability-free products are difficult to implement and nearly impossible to enforce. Most users lack a robust, automated way of validating either manufacturer declarations or enterprise procurement policies. Hardware tampering is only one avenue of compromise. U.S. adversaries seek to infiltrate U.S. ICT infrastructure through multiple vectors including clandestine and public techniques and methodologies. Examples include:

- Exploiting unintentional software vulnerabilities in both business systems and OT;
- Using subsidies to encourage the dominance of state-sponsored national champions, causing U.S. producers to exit key global markets and drive U.S. dependence on foreign products;
- Inundating U.S. markets with significantly less expensive foreign government-sponsored national champion products to give those products an advantage over U.S. made alternatives;
- Using legitimate investment opportunities, such as venture, private equity, sovereign wealth funds, and acquisitions, and enrollment in key U.S. universities to gain access to IP of the most promising emerging technologies; and
- Using tactics, such as forced technology transfer or unsupervised source code review provisions, for market access.

This threat's complexity requires that the United States find solutions for the full lifecycle of products in the ICT ecosystem. Future efforts must examine and address risk created in each phase of the product lifecycle, including:

- Conception (innovation, invention, and design);
- Build (assembly and manufacture); and
- Deploy and operate (procurement, use, and disposal).

The United States cannot focus only on the "Build" phase. The NSTAC heard a resounding message from multiple subject matter experts (SME) that, while it is difficult for U.S. adversaries to tamper with products, it is also extremely difficult to prove unequivocally that a hostile actor has *not* tampered with a product. ICT products are commonly developed in places subject to direct or indirect control by potentially adversarial governments. While security protocols can and must be put in place, U.S. companies have limited control over the methods of production and even less control over the people who have access to the manufacturing process in these remote locations.

Similarly, methodologies that only address the "Deploy and Operate" phase, such as bans and blacklists, are only part of the solution. It is important to think comprehensively about all of the ways potential U.S. adversaries may be able to dominate and control NS/EP critical technologies across the device lifecycle. Other techniques, such as whitelists of approved products, can be burdensome and unrealistic in light of the rapid technology changes and the complexity of modern networks. For this tasking, the NSTAC paid particular attention to the often overlooked "Conception" phase, including the problem of decreasing ownership and control by U.S. companies of innovation processes.

Highlighted Technologies

The forthcoming *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem* will highlight the importance of three technologies to future U.S. NS/EP ICT resiliency and security: (1) 5G cellular wireless networks; (2) quantum computing; and (3) artificial intelligence (AI) and machine learning (ML). While this does not represent an exhaustive list of the critical NS/EP technologies, the NSTAC chose to highlight these technologies after hearing from multiple SMEs about the importance of these technologies to national security. The NSTAC identified the three technologies discussed below in the *NSTAC Report to the President on Emerging Technologies Strategic Visio*n (2017) and the *NSTAC Report to the President on a Cybersecurity Moonshot*. The recommendations in this letter are based on U.S. Government and industry experience with these technologies; however, the lessons the NSTAC draws from them and the national innovation strategy will be applicable to a wide range of current and future NS/EP-critical ICT technologies. Such technologies could include global positioning systems, autonomous systems, or high performance computing.

5G: 5G brings significant advancements over previous generations of wireless cellular technology, including greater bandwidth, lower latency, and the ability to support greater numbers of sensors and smart devices. The next age of digital transformation depends on the success of the United States' national and global 5G build out.[6] Multiple studies have indicated that 5G networks will enable applications to drive significant technological advances and add $1.2 trillion and three million jobs to the U.S. economy. Nations that act fast to develop and deploy 5G technology will be best able to capitalize on its many economy-fueling applications. While U.S. carriers are actively deploying 5G, the United States is concerned with falling behind China. There are also concerns about the growing presence of Chinese telecom equipment manufacturers, particularly in networks outside of the United States, and the long-term implications for 5G and the broader communications and internet technology supply chain. This concern is particularly acute in the Radio Access Network (RAN) portion of the network where there are a limited number of RAN equipment suppliers. If Chinese manufacturers continue to gain market share, there will be growing concern about the long-term viability of the existing supply chain for 5G and successor technologies.

Quantum Computing: Quantum computing is the world's next generation of supercomputers. These computers will allow people to solve some of the world's most challenging problems in a fraction of the time it would take a current computer. It will enable researchers to model complex

6 There are only four main purveyors of 5G Radio Access Network (RAN) technology globally, none of which are considered United States-based, and the largest of which is Chinese-based.

chemical processes, simulate and develop new catalysts and materials, enhance medical research, accelerate advances in AI/ML, and even answer fundamental questions about the universe. It will facilitate the breaking of the traditional methods of encryption, which are used across the globe to secure all internet commerce, as well as potentially help to create new methods of encryption. Quantum computing will likely increase society's dependence on connectivity and the Nation's reliance on trusted connectivity to support NS/EP operations. The United States enacted the *National Quantum Initiative Act* (Public Law 115-368) in December 2018, which signaled both Congressional and White House concern over the threat that the United States may fall behind in quantum computing. The law provides a useful model for the appropriate role of the U.S. Government in fostering open innovation across the public, private, and academic sectors. The law, among other things, establishes a 10-year plan to accelerate the development of quantum information science with White House-led strategic oversight, and funds U.S. Government efforts to lead collaborative research and development efforts aligned to quantum information science and its technology applications.[7]

AI/ML: Experts define AI/ML as "Machines that respond to stimulation consistent with traditional responses from humans, given the human capacity for contemplation, judgment, and intention."[8] AI/ML has the potential to contribute in significant ways to many fields, including cybersecurity, medicine, robotics, autonomous systems, and space exploration. AI/ML is already helping to solve important problems, such as preventing social media manipulation and protecting computer networks from hackers. Of particular concern is the impact of weapons systems, used offensively and defensively, that are outfitted with AI/ML. In April 2018, the Under Secretary of Defense for Research and Engineering, Dr. Michael D. Griffin, said "In an advanced society, AI and cyber and some of these other newer realms offer possibilities to our adversaries to [target others successfully], and we must see to it that we cannot be surprised."[9] AI/ML will be a driver in sensor analysis and quick response decision making in future NS/EP operations, making it imperative for the United States to lead its development. On February 11, 2019, President Trump issued Executive Order (EO) 13859, *Maintaining American Leadership in Artificial Intelligence*. The issuance of this EO is an important step towards ensuring that AI development is elevated as a major national priority and addressing the challenge of keeping pace with China and other countries.

During the second phase of this study, the NSTAC will evaluate 5G technology development as a case study in critical technology. As a representative foundational and critical NS/EP technology, the NSTAC chose 5G due to its unique combination of software and hardware, the applicability of supply chain security, and its stage of deployment. 5G, quantum computing, and AI/ML technologies share common challenges, and future NSTAC studies could undertake a more focused review of these technologies.

---

7 National Quantum Initiative Act, P.L. 115-368 (2018), https://www.congress.gov/bill/115th-congress/house-bill/6227/text?q=%7B%22search%22%3A%5B%22NATIONAL+QUANTUM+INITIATIVE+ACT%22%5D%7D&r=3.

8 Darrell M. West, "What is Artificial Intelligence," Brookings Institution, accessed December 31, 2018, https://www.brookings.edu/research/what-is-artificial-intelligence.

9 Matt Stroud, "The Pentagon is Getting Serious About A.I. Weapons," The Verge, April 12, 2018, accessed December 31, 2018, https://www.theverge.com/2018/4/12/17229150/pentagon-project-maven-ai-google-war-military.

Preview of Report

In the second phase of this tasking, the NSTAC will produce a report that will:

- Consider the particular U.S. dependencies, market limitations, and supply chain risks associated with the deployment of 5G and determine what options exist for addressing these challenges across all NS/EP ICT;

- Recommend the creation of a national NS/EP ICT innovation strategy and describe its objectives and foundational components; and

- Make recommendations for policies or actions that could be included in the national innovation strategy for NS/EP technologies. Such policies and actions may include:

    - Providing more support for innovation and development (in the short- and long-term) of NS/EP ICT, and ensuring the United States and key international partners remain at the forefront of innovation.

    - Identifying market drivers and incentives that may guide needed investments (e.g., creating the right conditions for strong domestic investment, more funding for research and development, liability considerations).

    - Highlighting mitigating technologies, including technologies like distributed ledger, which is a transactional database that can be shared amongst parties who do not inherently trust one another. In the realm of ICT and supply chain security, distributed ledgers could potentially facilitate design and functionality verification and provide a means to thwart hardware and software tampering. On critical infrastructure networks, distributed ledgers could be used, among other things, to verify access rights and transaction history with the potential to contribute substantially to future NS/EP capabilities.

    - Recommending mechanisms with which the U.S. Government might incentivize adoption of best practices aimed at both U.S. Government and private sector entities, including new or better ways of measuring their progress toward improving ICT resiliency and supply chain security. One area where the U.S. Government may play a productive role is assisting critical sectors in tailoring effective supply chain risk management frameworks to their specific needs and incentivizing those organizations that make appropriate supply chain risk decisions based on established best practices.

Conclusion

The complexity of technological, economic, and geopolitical factors relating to the global ICT supply chain, combined with the objectives and behaviors of some nations with political, economic, and security agendas that may run counter to U.S. interests, has resulted in increased vulnerability of ICT that is critical to NS/EP functions. The U.S. Government does not control the companies that produce or deploy the components and systems that comprise the Nation's

ICT infrastructure. It cannot encourage or require companies to purchase ICT technology from manufacturers in the United States or U.S. allies if there are no such products available. Similarly, the U.S. Government cannot encourage or require companies to purchase secure ICT if there is no way to evaluate the security of those products. It is vital that the U.S. Government develop a holistic national innovation strategy and, within it, a plan for ICT advancement, resiliency, and security. To be most effective, the U.S. Government must closely coordinate with the critical sectors and partner with allies and like-minded nations.

On behalf of the NSTAC, I thank you for the opportunity to provide the NSTAC's industry insights and recommendations on immediate steps that your Administration can take to improve the security and resiliency of NS/EP ICT.

Sincerely,

Renée James
NSTAC Chair