PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Mr. John Donovan
NSTAC Chair
6306 Norway Road
Dallas, TX 75230

February 10, 2021

The Honorable Joseph R. Biden
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear Mr. President:

For almost 40 years, the President's National Security Telecommunications Advisory Committee (NSTAC) has brought together chief executives and senior leadership from telecommunications, information technology, and aerospace companies to provide recommendations to advance the Government's national security and emergency preparedness (NS/EP) functions through robust information and communications technology (ICT). Although our focus has evolved with technology and threats, we have consistently focused on strengthening global communications infrastructure, enhancing cybersecurity, and addressing critical infrastructure risk.

The NSTAC's mission has never been more important. With the Nation increasingly dependent on ICT for economic continuity and security in the midst of the coronavirus (COVID-19) pandemic, America is challenged by adversaries who have tainted critical supply chains, stolen intellectual property, attempted to influence elections, and worked to capture global ICT markets. Faced with these challenges, there has never been a greater need for a strong, well-informed public-private partnership and coordinated action. The NSTAC historically has met with the President of the United States to share candid views about the challenges we face and the actions we must take to ensure American security and competitiveness. In this vein, we hope to meet with you at our May meeting (either virtually or in-person, as appropriate) and to accelerate the process by which we can serve your Administration.

This letter and its Attachment are meant to provide an overview of the NSTAC's recent work, including recommendations that are ready for implementation, ideas on future NSTAC study topics, and engagements we could pursue to advance the United States' NS/EP priorities. In recent years, the NSTAC has published numerous studies and offered recommendations that fall into two categories: (1) cybersecurity and network resilience; and (2) emerging technology.

In the area of cybersecurity and network resilience, the NSTAC has issued several reports with timely and actionable recommendations. In November 2017, the NSTAC completed the *NSTAC Report to the President on Internet and Communications Resilience* (ICR Report).[1] This report was developed in the wake of continued automated and distributed attacks, such as large-scale denial-of-service attacks, facilitated through botnets threatening the security and resiliency of the internet ecosystem and the Nation's critical infrastructure. In November 2018, the NSTAC issued the *NSTAC Report to the President on a Cybersecurity Moonshot* (Cybersecurity

Moonshot Report),[2] which asserted that the Nation was at an inflection point and called for a fundamentally new strategic approach and action plan to tackle the Nation's systemic cybersecurity challenges. More recently, in August 2020, the NSTAC issued the *NSTAC Report to the President on Software-Defined Networking,*[3] addressing software-defined networking's implications for the communications industry, including security and supply chain impacts. These recent studies are described in more detail in the Attachment.

The 2021 *National Defense Authorization Act*[4] advanced two recommendations from recent NSTAC studies by enacting these concepts:

1. **National Cybersecurity Challenges**, whereby the Secretary of Commerce, in conjunction with the Secretary of Homeland Security, Secretary of Defense, and others establishes national cybersecurity challenges to accelerate innovation and bring national prestige to the achievement of strategically transformative cybersecurity objectives.
2. **National Cyber Director Office within the Executive Office of the President**, who is responsible for cybersecurity and strategy across the Federal Government, including coordination to increase ICT security, promoting national supply chain risk management, and enhancing awareness and adoption of emerging technology changing the cybersecurity posture of the United States.

In the area of emerging technology, the NSTAC has also conducted extensive studies. We believe whole-of-Nation action is necessary to maintain American ICT leadership and competitiveness, which directly impact the United States' NS/EP communications resilience. Policies are most effective when the Government aligns with the private sector to execute a shared holistic and long-term strategic vision grounded in American values and inclusive of allied nations.

The NSTAC studied these critical issues in multiple reports. In July 2017, the NSTAC issued the *NSTAC Report to the President on Emerging Technologies Strategic Vision* (ETSV Report),[5] which addressed how the Government should prepare for unprecedented growth and transformation in the technology ecosystem. In September 2019, the NSTAC issued the *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem* (ICT Ecosystem Report),[6] which analyzed the reliance of Government agencies and critical infrastructure on untrusted products and services, and the implications for U.S. national security.

These prior NSTAC reports contain untapped recommendations that can support the Administration's NS/EP missions. Specifically:

- **The Nation needs a Cybersecurity Moonshot.** The 2018 Cybersecurity Moonshot Report called for an aspirational statement that would catalyze national leadership, political will, and a sustained whole-of-Nation effort to boldly assure digital trust, safety, and resilience for all Americans. It also provided actionable steps the U.S. Government can take to champion, organize, direct, resource, and empower whole-of-Nation activities.
- **Revisit and enhance our cybersecurity strategy.** The 2017 ICR Report recognized that the Nation's previous cybersecurity strategy was inadequate and offered several ideas to improve our cybersecurity posture, including accelerating the adoption of cybersecurity guidelines, promoting software and supply chain assurance, improving the current public-private partnership process, and raising costs for cyber threat actors.
- **Develop a whole-of-Nation approach to ensure U.S. leadership in key emerging technologies.** As outlined in the 2019 ICT Ecosystem Report, there still is not a cohesive

cross-agency strategic plan to address the issue of trusted manufacturers. At the same time, the 2017 ETSV Report highlights the Nation's growing critical dependencies on emerging technologies. While the previous Administration issued its *National Strategy to Secure 5G*,[7] and recently an implementation plan[8] to effectuate that strategy, these issues are broader than 5G. There are discrete elements of a strategy in areas such as 5G, quantum computing, and artificial intelligence; however, they are not highly coordinated.

The NSTAC is currently conducting a two-phased NS/EP communications resiliency study. The first phase resulted in the October 2020 *NSTAC Letter to the President on Communications Resiliency*.[9] This letter provided recommendations to the previous Administration on how to promote the Nation's communications resilience in the face of a digital transformation driven by the COVID-19 pandemic. The second phase, which the committee intends to complete in May 2021, envisions the ICT infrastructure of the future—along with its dependencies—and considers what actions would increase resilience and better technology use to save lives in a variety of distinct disaster scenarios.

The NSTAC conducts studies at the direction of the Administration. Areas under consideration for future study include:

- **The Convergence of Operational and Information Technologies** or the impacts of the transformation of industry to use Internet of Things devices and 5G connectivity to monitor, analyze, and manipulate industrial assets and data, which are expected to provide unprecedented opportunities and new security challenges; and
- **An Emerging Technologies Strategic Assessment** of how emerging ICT is impacting the ecosystem, the U.S. position in the global marketplace (including challenges and opportunities), and national policies to align Government and industry efforts to promote U.S. leadership, competitiveness, and resilience.

In addition to its studies, NSTAC members engage with Government counterparts in robust discussion on relevant and timely topics at their regular meetings, which can inform policy initiatives and the committee's future work. At the November 2020 NSTAC Meeting, the NSTAC dedicated a portion of the agenda to discussing semiconductor supply chain issues, from which a number of significant insights emerged. While this topic is not planned for study in the near-term, we believe that this is a critical issue that requires further discussion.

Mr. President, we greatly appreciate the direct engagement the NSTAC had with the Obama Administration while you were Vice President, including with Deputy Attorney General-designate, Ms. Lisa Monaco. The Administration faces many pressing priorities, and the NSTAC stands ready to support your efforts. We greatly appreciate the opportunity to serve and continue our partnership.

Sincerely,

John Donovan
NSTAC Chair

Attachment: *Overview of Recent Reports and Recommendations*

ATTACHMENT: Overview of Recent Reports and Recommendations

For almost 40 years, Administrations have tasked the President's National Security Telecommunications Advisory Committee (NSTAC) to conduct studies by engaging with experts across the Government, private sector, academia, and member companies internally to produce short letters or full reports with unique insights and policy recommendations. NSTAC members change infrequently, retaining a historical perspective as trends change and strategies evolve. The NSTAC meets quarterly, including semiannually in-person, to approve its publications, provide its members expertise directly to the Administration, identify emerging challenges, and explore potential new study topics focused on promoting the United States' national security and emergency preparedness (NS/EP) functions.

In recent years, the NSTAC has conducted several studies and offered recommendations that fall into two categories: (1) emerging technology (how to maintain U.S. leadership in and address the national security implications of a range of emerging technologies); and (2) cybersecurity and network resilience (how to address ever-increasing cyber threats and maintain communications network resilience). Each category is briefly described below.

Emerging Technology

The NSTAC has conducted several reviews of emerging technology and its impact on NS/EP communications in recent years. In July 2017, the NSTAC issued the *NSTAC Report to the President on Emerging Technologies Strategic Vision* (ETSV Report),[10] which focused on providing guidance for how the Government should think about and prepare for unprecedented growth and transformation in the technology ecosystem. This report was followed by the 2019 *NSTAC Report on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology (ICT) Ecosystem* (ICT Ecosystem Report).[11]

The ETSV Report focused on identifying key strategic emerging technologies, evaluating opportunities and risks for NS/EP communications, and determining how Government should invest in and/or deploy various technologies while ensuring the impacts are both well understood and appropriately addressed. The NSTAC identified several key strategic emerging technologies, including: (1) interconnectivity and processing power, including advancements in communications technology (e.g., software-defined networking [SDN], network functions virtualization); (2) analytics, cognition and autonomy, including artificial intelligence; (3) production and simulation (e.g., virtual/augmented reality, three-dimensional/four-dimensional printing, active nanotechnology); and (4) trust and verification technologies.

The ETSV Report also identified several strategic opportunities, such as positioning the U.S. workforce to make greater use of 21st century technology by investing in education and training programs, assessing new governance, legal, and operational challenges resulting from emerging artificial intelligence, autonomous devices/systems, and material science advances, as well as preparing for the impact of quantum computing on national security.

The 2019 ICT Ecosystem Report analyzed the reliance of the Government and critical infrastructure partners on untrusted products and services, which has serious implications for U.S. national security. A national priority concern is the reduction in the availability of trusted manufacturers from certain ICT markets, which has diminished the choices of those who operate national critical infrastructure. Another key concern is the inability of Government and industry to effectively address the national critical reliance on untrusted technologies due to the multi-disciplinary and multi-stakeholder nature of the problem. The NSTAC concluded there is a need

for a comprehensive national strategy to ensure U.S. leadership in key technologies and for a focal point that cuts across national and economic security and innovation to ensure these communities are effectively working in concert.

These reports offered several key recommendations:

- Developing a whole-of-Nation approach to ensure that trusted manufacturers remain in key markets and create the conditions that foster American innovation in critical areas through a holistic national strategy.
- Establishing a dedicated White House position to coordinate the development and implementation of that holistic strategy across federal departments and agencies, the critical infrastructure provider community, and the broader innovation community.
- Instituting integrated planning and preparation for technology change into existing cross Government efforts and reviewing NS/EP public-private partnerships to assess whether relevant stakeholders are identified and represented.
- Developing a coordinated strategy with the private sector to enhance U.S. and allied participation in global technology standards forums.

Cybersecurity and Network Resilience

The aforementioned reports were developed within a backdrop of daunting technical and non-technical cybersecurity challenges in a tense international environment, a high-level of adversarial activity by both nation-state and non-state actors, and deficiencies in the development or deployment of security techniques and capabilities. Consequently, the other critical area that the NSTAC has addressed in recent years is cybersecurity and network resilience.

In November 2017, the NSTAC issued the *NSTAC Report to the President on Internet and Communications Resilience* (ICR Report).[12] This report was developed in the wake of continued automated and distributed attacks, such as large-scale denial-of-service attacks, facilitated through botnets threatening the security and resiliency of the internet ecosystem and the Nation's critical infrastructure. These risk factors are compounded by the ongoing growth of Internet of Things (IoT) devices that could expand the threat surface and serve as attack vectors. The ICR Report outlines several key lessons learned, including that a greater sense of urgency is required to address cybersecurity threats; public-private partnerships remain key to resolving cybersecurity concerns; solutions depend upon every part of the internet ecosystem; education and awareness is lagging; and unclear international norms complicate the challenge. Finally, the NSTAC concluded that a new trust model is necessary.

In the ICR Report, the NSTAC recommended several actions, including accelerating the adoption of security guidelines for critical infrastructure, facilitated by the Department of Homeland Security and sector-specific agencies; developing IoT device security guidelines for the Federal Government;[13] promoting enterprise security controls; and encouraging software assurance best practices.[14] The report also offers several specific actions for Government, such as the need to: (1) support public-private collaboration; (2) promote and adopt security standards and practices; (3) develop a comprehensive U.S. standards engagement strategy; (4) create an effective international cybersecurity strategy focused on raising the cost to attackers (e.g., deterrence strategy); and (5) implement a Cybersecurity Moonshot.

In November 2018, the NSTAC issued the *NSTAC Report to the President on a Cybersecurity Moonshot*.[15] In this report, the NSTAC concluded that the United States is at an inflection point:

simultaneously faced with a progressively worsening cybersecurity threat environment and an ever-increasing dependence on internet technologies fundamental to the Nation's public safety, economic prosperity, and overall way of life. Therefore, the NSTAC recommended that the United States build on past efforts and current strategies to seize the opportunity to strategically reorient from a largely reactive, incremental cybersecurity posture to a proactive approach that boldly assures digital trust, safety, and resilience for all Americans. The report then outlines a process to conduct a Moonshot—including developing governance within the White House and U.S. Government—to focus on a clear national objective and implement six key pillars of technology, human behavior, education, ecosystem roles and responsibilities, privacy, and policy.

In August 2020, the NSTAC issued the *NSTAC Report to the President on Software-Defined Networking* (SDN Report),[16] addressing SDN's implications for the communications industry, including security and supply chain impacts. In the SDN Report, the NSTAC concluded that networks are quickly migrating to SDN; the United States is a global leader in SDN; and there is an opportunity for the Nation to create a more future-proofed supply chain through the support of SDN technology. Finally, in October 2020, the NSTAC issued the *NSTAC Letter to the President on Communications Resiliency*[17] to assess the impacts of the coronavirus (COVID-19) pandemic on network resilience and performance. The NSTAC reported that, while overall networks performed well in response to the unprecedented challenges presented by COVID-19, there are areas for improvement including coordination between the federal, state, local, tribal, and territorial levels of Government.

---

[1] President's National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on Internet and Communications Resilience*, November 16, 2017, https://www.cisa.gov/publication/2017-nstac-publications.
[2] NSTAC, *NSTAC Report to the President on a Cybersecurity Moonshot*, November 14, 2018, https://www.cisa.gov/publication/2018-nstac-publications-0.
[3] NSTAC, *NSTAC Report to the President on Software-Defined Networking*, August 12, 2020, https://www.cisa.gov/publication/2020-nstac-publications.
[4] *National Defense Authorization Act for Fiscal Year 2021*, H.R. 6395, 116th Cong. § 2 (2021), https://www.congress.gov/bill/116th-congress/house-bill/6395/text/enr.
[5] NSTAC, *NSTAC Report to the President on Emerging Technologies Strategic Vision*, July 14, 2017, https://www.cisa.gov/publication/2017-nstac-publications.
[6] NSTAC, *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem*, September 3, 2019, https://www.cisa.gov/publication/2019-nstac-publications.
[7] Executive Office of the President, *National Strategy to Secure 5G of the United States of America*, March 2020, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.
[8] National Telecommunications and Information Administration (NTIA), *National Strategy to Security 5G Implementation Plan*, January 6, 2021, https://www.ntia.gov/5g-implementation-plan.
[9] NSTAC, *NSTAC Letter to the President on Communications Resiliency*, October 6, 2020, https://www.cisa.gov/publication/2020-nstac-publications.
[10] NSTAC, *NSTAC Report to the President on Emerging Technologies Strategic Vision*, July 14, 2017, https://www.cisa.gov/publication/2017-nstac-publications.
[11] NSTAC, *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem*, September 3, 2019, https://www.cisa.gov/publication/2019-nstac-publications.
[12] NSTAC, *NSTAC Report to the President on Internet and Communications Resilience*, November 16, 2017, https://www.cisa.gov/publication/2017-nstac-publications.
[13] *Internet of Things Cybersecurity Improvement Act of 2020*, H.R. 1668, 116th Cong. § 2 (2020), https://www.congress.gov/bill/116th-congress/house-bill/1668/text,
[14] NTIA, "Software Bill of Materials," accessed January 14, 2021, https://www.ntia.gov/SBOM.
[15] NSTAC, *NSTAC Report to the President on a Cybersecurity Moonshot*, November 14, 2018, https://www.cisa.gov/publication/2018-nstac-publications-0.
[16] NSTAC, *NSTAC Report to the President on Software-Defined Networking*, August 12, 2020, https://www.cisa.gov/publication/2020-nstac-publications.
[17] NSTAC, *NSTAC Letter to the President on Communications Resiliency*, October 6, 2020, https://www.cisa.gov/publication/2020-nstac-publications.