President's National Security Telecommunications Advisory Committee (NSTAC)
Member Meeting Open Session Summary
November 12, 2020

Call to Order and Opening Remarks

Ms. Sandy Benevides, Department of Homeland Security (DHS) and NSTAC Designated Federal Officer, called the meeting to order. She informed attendees that the NSTAC is a federal advisory committee, governed by the *Federal Advisory Committee Act*. As such, the meeting was open to the public. She noted that no one had registered to provide comment, but that written comments would be accepted following the procedures outlined in the meeting's Federal Register Notice. Following roll call, Ms. Benevides turned the meeting over to Mr. John Donovan, NSTAC Chair.

Mr. Donovan opened the meeting and welcomed participants. He then thanked the distinguished Government partners in attendance, including Mr. Kenneth Cuccinelli, Senior Official Performing the Duties of the Deputy Secretary, DHS; Mr. Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency (CISA), DHS; Mr. Joshua Steinman, Deputy Assistant to the President and Senior Director for Cybersecurity, National Security Council (NSC); Mr. Brian Scott, Director for Critical Infrastructure Cybersecurity, NSC; and Dr. Eric Burger, Assistant Director, White House Office of Science and Technology Policy (OSTP).

Mr. Donovan provided an overview of the meeting agenda, noting that NSTAC members would: (1) hear remarks from Mr. Steinman and Director Krebs on the Government's ongoing cybersecurity and national security and emergency preparedness (NS/EP) communications efforts; (2) receive a keynote address from Mr. Cuccinelli; (3) receive an update on the Communications Resiliency (CR) Subcommittee's study from Mr. Jeffrey Storey and Mr. Angel Ruiz, NSTAC Members and CR Subcommittee Co-Chairs; and (3) engage in a discussion with Dr. Burger on the challenges and opportunities for U.S. information and communication and technology (ICT) leadership in the next five years.

Mr. Donovan discussed the NSTAC's last meeting: the October 2020 NSTAC Member Conference Call (MCC). During that meeting, the NSTAC: (1) heard remarks from Mr. Steinman and Director Krebs regarding the Government's efforts to strengthen its NS/EP communications posture and secure the ICT ecosystem; and (2) deliberated, voted on, and unanimously approved the 2020 *NSTAC Letter to the President on Communications Resiliency*. Mr. Donovan then invited Director Krebs to provide his opening remarks.

Director Krebs stated that CISA's three main NS/EP communications priorities include: (1) advancing risk management, engagement, and technical assistance for stakeholders during the coronavirus (COVID-19) pandemic response; (2) promoting the security of the 2020 election; and (3) managing supply chain risks associated with cyber threats and the rollout of fifth generation (5G) networks. He explained that cybersecurity is a vast and complex endeavor, and that the convergence of information technology (IT) and operational technology

(OT) creates an expanded attack surface. He noted that DHS and the Department of Commerce (DOC) released the 2020 *Botnet Roadmap Status Update*, which outlines Government and industry actions needed to enhance the resiliency of ICT ecosystems by mitigating distributed denial of service threats and combatting botnets.

Director Krebs discussed how CISA's *5G Strategy for Ensuring the Security and Resilience of 5G Infrastructure* directly supports the goals outlined in the *National Strategy to Secure 5G of the United States of America*, by detailing the agency's approach for advancing the development and deployment of a secure 5G infrastructure. Similarly, the Federal Communications Commission continues its work with other federal agencies, including the Department of Defense (DOD), to support the rollout of resilient 5G networks. Additionally, Director Krebs mentioned how the Administration has established protocols to prevent communications equipment and services that pose a national security risk from entering U.S. networks, as seen through the implementation of the 2019 Executive Order (EO) 13873: *Securing the ICT and Services Supply Chain*.

Director Krebs then swore in Mr. Patrick Gelsinger, VMware, Mr. Jack Huffard, Tenable Holdings, and Mr. Hock Tan, Broadcom, as the newest NSTAC members. He then turned the meeting over to Mr. Scott.

Mr. Scott thanked NSTAC members for their participation. He also highlighted how the committee's two most recent publications—the 2020 *NSTAC Letter to the President on Communications Resiliency* and the 2020 *NSTAC Report to the President on Software-Defined Networking* (SDN)—have helped the Administration to develop actionable NS/EP communications policy.

Mr. Donovan thanked Director Krebs and Mr. Scott for their remarks.

Homeland Security Update and Outlook Keynote Address

Mr. Scott introduced Mr. Cuccinelli to provide the meeting's keynote address.

Mr. Cuccinelli began by discussing threats to the Nation from malicious nation-state and non-state actors. He emphasized the need for Government and the private sector to understand the nature and scope of threats, like the COVID-19 pandemic, to the Nation's ICT infrastructure, NS/EP communications networks, and economic security. Mr. Cuccinelli described how DHS' 2020 *Homeland Threat Assessment* synthesizes threat information from across the Department's intelligence and operational components, including the Federal Emergency Management Agency and CISA, to prioritize the remediation of risks to the Nation's ICT networks.

Mr. Cuccinelli outlined key elements of the overall threat landscape, including cybersecurity concerns; foreign influence activity; terrorism; transnational criminal organizations; illegal immigration; natural disasters; and economic security, each of which often impact or influence one another. He then addressed the Administration's efforts to promote U.S. leadership and innovation in emerging technology areas. Mr. Cuccinelli explained that the resilience of the ICT

ecosystem has significant effects on U.S. economic security. Therefore, DHS actively supports industry's efforts to protect the domestic ICT ecosystem, and appreciates recommendations from groups like the NSTAC to help mitigate ICT-based threats to the U.S. economy.

Mr. Cuccinelli explained that China, Russia, Iran, and North Korea present the most significant threats to the Nation's ICT ecosystem. Specific threats from China include intellectual property theft; production and distribution of counterfeit ICT products; cyber espionage; unfair trade practices; and promotion of Huawei as a top global provider for 5G infrastructure.

Mr. Cuccinelli added that foreign investment in domestic ICT networks is a critical concern for homeland security. To combat this threat, the Administration issued EO 13873 in May 2019 declaring that threats to the ICT supply chain by foreign adversaries are a national emergency. The EO also gives the DOC the authority to prohibit transactions that could pose significant risks to the security or resiliency of the United States' critical infrastructure or digital economy. Likewise, the EO empowers the Administration to provide dedicated assistance to telecommunications companies seeking to remove unsecure infrastructure components from mission-critical networks. Moreover, Mr. Cuccinelli explained that the Cyberspace Solarium Commission Report provides guidance on how to secure the ICT sector by reducing reliance on untrusted foreign firms. In light of all of these initiatives, DHS realizes the importance of promoting public-private partnerships and their role in protecting the U.S. ICT ecosystem.

Mr. Cuccinelli described how malicious actors have used the COVID-19 pandemic to destabilize the United States' economic and NS/EP network security. For example, these actors have exploited spikes in network traffic across the ICT ecosystem to target consumers, the remote workforce, and the healthcare industry. Attack methods continue to evolve as nation-state and non-state actors utilize U.S.-based servers and other infrastructure (e.g., virtual private networks) to mask their locations, and leverage artificial intelligence (AI)/machine learning (ML) to automate the creation and distribution of misinformation.

Mr. Cuccinelli emphasized that supply chain integrity is a vital component of homeland security, as strong and diverse supply chains are integral to U.S. prosperity. He discussed the Department's ICT Supply Chain Risk Management Task Force, which provides advice on how the Government can best assess and manage risks to the Nation's ICT supply chain. He explained that the 5G supply chain is susceptible to a variety of hazards, including malicious software and hardware; counterfeit components; and outdated maintenance procedures from legacy systems. Since 5G has direct implications for NS/EP communications, Mr. Cuccinelli underscored the importance of promoting trusted ICT providers in a growing marketplace.

Mr. Cuccinelli noted the Government's various efforts to ensure that 5G technologies can support increased resiliency for public safety communications. For instance, DHS' Science and Technology (S&T) Directorate works closely with CISA to ensure secure 5G deployments. In addition, S&T's Mobile Security Research and Development (R&D) Program leverages the Secure and Resilient Mobile Network Infrastructure project to work with industry to encourage resiliency for critical mobile communications networks.

Mr. Cuccinelli emphasized that DHS remains committed to securing and safeguarding the Nation's NS/EP communications networks. He then thanked the NSTAC for its ongoing support of these initiatives.

Mr. Donovan thanked Mr. Cuccinelli for his remarks.

NSTAC Communications Resiliency Subcommittee Status Update

Mr. Donovan introduced Mr. Storey and Mr. Ruiz to attendees, and invited them to provide an update on the NSTAC CR Subcommittee.

Mr. Storey explained that in the 2011 *NSTAC Report to the President on Communications Resiliency*, the committee examined the then-current communications resiliency landscape and provided recommendations to the Government on how to enhance the survivability and availability of NS/EP networks. While networks have performed well during the COVID-19 response, the Nation's reliance on a variety of ICT systems suggests the need to reexamine the expected resiliency of U.S. communications moving forward. As a result, Mr. Storey noted that the NSTAC will conduct a broader, more forward-looking examination of the United States' NS/EP infrastructure resiliency during phase II. He added that the NSTAC will leverage its recent work on emerging technologies, such as quantum computing, network functions virtualization, and SDN, to conduct a strategic assessment of NS/EP communications resiliency challenges. Specifically, the NSTAC will: (1) forecast the general state of the ICT ecosystem in 8 to 10 years; and (2) examine if networks, services, and infrastructure can maintain the necessary level of security and resilience under a variety of scenarios.

Since the October 2020 MCC, the NSTAC has received 12 briefings, which have focused on such topics as quantum computing; AI/ML; 5G and national security impacts; and a review of the power sector's infrastructure, planning, and disaster response efforts.
Mr. Ruiz thanked the NSTAC member companies that have provided briefings to date, and asked others to consider providing insight from their areas of expertise. Currently, the committee is seeking input on the impact of emerging technologies on the changing global environment, as well as NS/EP implications of the United States' digital transformation.
Mr. Ruiz noted that briefings will continue into February 2021, and NSTAC members will receive another update on the study in late January 2021. NSTAC members are expected to deliberate and vote on the 2021 *NSTAC Report to the President on Communications Resiliency* at the May 2021 Member Meeting.

In conclusion, Mr. Storey and Mr. Ruiz thanked briefers, members, and the CISA team for their support of the study.

Mr. Donovan thanked Mr. Ruiz and Mr. Storey for their update.

Discussion on Challenges and Opportunities for U.S. Leadership in ICT in the Next Five Years

Mr. Donovan introduced Dr. Burger to facilitate the discussion on challenges and opportunities for U.S. leadership in ICT in the next five years.

Dr. Burger highlighted that the goal of the discussion was for NSTAC members to provide advice on how the Government and industry can better work together to protect America's NS/EP communications, industrial base, and citizens.

Dr. Burger noted that the Administration has taken several actions to secure the telecommunications supply chain, and advance industrial R&D for communications and cybersecurity. While the United States is a leader in data networking equipment, data center equipment, and hyperscale cloud services, its lack of fully integrated, end-to-end telecommunications network providers leaves it susceptible to threats posed by global providers under the control of authoritarian nation-states. Dr. Burger reiterated Mr. Cuccinelli's point that the United States has seen numerous threats to its network security from sophisticated criminal actors. As a result, the U.S. Government should be mindful of lessons learned, failures, successes, and critical interdependencies as new ICT is produced and deployed in the marketplace.

Dr. Burger asked participants to provide input on domestic innovation and leadership in emerging ICT. Mr. Donovan noted that it is difficult for the NSTAC to discuss data availability and privacy issues as it relates to AI/ML. He underscored the United States, a democracy that values privacy, has to compete with adversaries that can more readily procure user data and build machine models. Dr. Burger instead asked for members' insight on the United States' competitive position in advancing AI/ML techniques. In response, Mr. McLaughlin noted the importance of identifying how inherent human biases in AI can be effectively removed.

Dr. Burger requested insights regarding AI's role in supporting NS/EP communications. Mr. Donovan mentioned that, as society moves towards a more machine-based communications environment, reliable interfaces will become increasingly critical. To this end, the United States should focus on implementing policy that equally secures both device and user connections to networks. Mr. Donovan mentioned that data privacy concerns will continue to affect various forms of communications as entities that have access to more data can improve the accuracy of their AI/ML models. Mr. Scott Charney, NSTAC Vice Chair, also highlighted how root cause analysis can be used to validate machine-based decisions and prevent recurring errors or false positives.

Mr. Donovan asked for Mr. Charney's insight on how emerging technologies can facilitate the issuance and authentication of secure network identity credentials. Mr. Charney stated that he published a paper on establishing trust for each connection to communications networks. Specifically, it is important to know that the device, application, or person that a user is interacting with is verified. Unless there is device authentication, Mr. Charney stated that there

is risk for security events resulting from false data. Therefore, an audit trail around the machine's decision processes is crucial to guaranteeing network security.

Dr. Burger stated that the National Science Foundation and the Defense Advanced Research Projects Agency are researching methods for user/device authentication for next-generation networks. Mr. Charney noted that this research should be publicized more so industry can maintain awareness of Government efforts in this space. Mr. Donovan agreed that the private sector has limited visibility into the Government's R&D programs. Dr. Burger asked members if they were aware that the Executive Office of the President publishes its R&D activity through the Networking and Information Technology R&D Program. Mr. Donovan responded that he was not, but remarked that sharing this information with industry partners would be helpful moving forward.

Dr. Burger asked members to comment on the cybersecurity challenges associated with emerging ICT. Mr. David DeWalt, NSTAC Member, stated that information integrity and deep fakes—synthetic media in which a person in an existing image or video is replaced with someone else's likeness—affect both consumer and corporate data consumption. He highlighted the importance of creating methods (e.g., reputational scoring, browser plug-ins) to verify if content has been altered without permission.

Mr. Huffard noted that more attention should be paid to the IT/OT convergence. He stated that software integrity concerns should be further researched as the world moves toward an increasingly virtual development and IT operations environment. Mr. DeWalt agreed and noted the importance of incorporating security early into the software developmental lifecycle. Dr. Burger noted that the National Institute of Standards and Technology's Cybersecurity Framework encourages the integration of security into baseline system design. Mr. Charney also discussed ongoing efforts to educate developers on how to write secure code for integration into common security platforms. To expedite the adoption of secure coding practices, he recommended that the Government create policies to incentivize R&D, improve the procurement of goods, and encourage the use of the reliable tooling and platforms.

Mr. Donovan remarked that technology companies located on the United States' West Coast are more engaged in developing technology policy and less focused on R&D. More secure and advanced technology could be produced if the Government provided these firms more R&D funding. Dr. Burger mentioned that S&T created the Silicon Valley Innovation Program to help fund innovation around strengthening national security. He asked if this program should be expanded, to which Mr. Huffard replied that it should, as there are many companies across the United States conducting this kind of emerging technology research. Dr. Burger noted that he would share recent OSTP R&D reports and the Administration's R&D strategy to demonstrate how funding is distributed across the enterprise.

Dr. Burger asked what actions should be taken to facilitate U.S. global competitiveness, leadership, and innovation in ICT. Mr. Donovan suggested promoting the United States' market share in key ICT sectors, as current revenue streams will influence future development.

Regarding 5G, Dr. Burger noted that the DOD continues to establish and expand its 5G testbeds in collaboration with industry. He asked if this model could be leveraged moving forward. Mr. Donovan replied that these testbeds do not create immediately sustainable revenue. Mr. DeWalt noted that this partnership could be used to promote successes across several advanced 5G use cases, like smart factories.

Dr. Burger asked participants to assess the challenges for U.S. competitiveness in global ICT. Mr. Charney responded that one area of concern is inconsistency in current industrial policy and direct competition with China. Over time, China has taken several steps to fully integrate its manufacturing and development capabilities. He noted that this allows China to leverage Government support in ways that the United States cannot (e.g., easier access to large datasets of personally identifiable information). Thus, Mr. Charney suggested that the U.S. Government create a comprehensive strategy to encourage U.S. innovation and counteract China's strategic advantages. He added that China requires U.S. companies to have a Chinese partner in order to conduct business in their country. Dr. Burger posited that instituting a similar requirement for Chinese companies operating in the United States might be beneficial. A member stated that leveraging public-private partnerships as models for researching emerging technology topics would be useful.

Dr. Burger inquired as to what technology policy topics merit further NSTAC examination. Mr. Charney said that the NSTAC could assess how U.S. industrial policy could be more uniformly implemented across the ICT ecosystem. Mr. Ruiz stated that the United States should consider how to approach scalable competition with China as the latter becomes more isolated. Ms. Renée James, NSTAC Member, cautioned that the United States should avoid creating market conditions where China, in its isolation, can innovate new technologies faster than the United States.

Hearing no further comments, Dr. Burger thanked participants and concluded the discussion.

Closing Remarks and Adjournment

Mr. Donovan thanked NSTAC members and Government partners for attending and participating in the meeting. He also thanked the CR Subcommittee, Mr. Ruiz, and Mr. Storey for their efforts. Likewise, Mr. Scott thanked NSTAC members for their support, and stated that the NSTAC was one of the most important Presidential advisory committees in operation today. Director Krebs thanked NSTAC members for their insights, and remarked that the committee's work enhances the security and resiliency of the Nation's NS/EP posture.

Mr. Donovan announced that the next NSTAC meeting will be an MCC held on February 10, 2021. More details regarding that engagement are forthcoming.

Mr. Donovan asked for a motion to close the meeting. Upon receiving a second, he thanked participants and officially adjourned the November 2020 NSTAC Member Meeting.

APPENDIX
November 12, 2020, NSTAC Member Meeting Open Session Participants List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corp.
Mr. Scott Charney	Microsoft Corp.
Mr. Matthew Desch	Iridium Communications, Inc.
Mr. David DeWalt	NightDragon Security, LLC
Mr. Raymond Dolan	Cohere Technologies, Inc.
Mr. John Donovan	Formerly of AT&T Communications, LLC
Dr. Joseph Fergus	Communication Technologies, Inc.
Mr. Patrick Gelsinger	VMware, Inc.
Ms. Lisa Hook	Neustar, Inc.
Mr. Jack Huffard	Tenable Holdings, Inc.
Ms. Renée James	Ampere Computing, LLC
Mr. Mark McLaughlin	Palo Alto Networks, Inc.
Mr. Angel Ruiz	MediaKind, Inc.
Ms. Kay Sears	Lockheed Martin Corp.
Mr. Jeffrey Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
NSTAC Points of Contact	
Mr. Jason Boswell	Ericsson, Inc.
Mr. Christopher Boyer	AT&T, Inc.
Mr. Jamie Brown	Tenable, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. Michael Daly	Raytheon Technologies Corp.
Ms. Cheryl Davis	Oracle Corp.
Mr. Thomas Gann	McAfee, LLC
Mr. Jonathan Gannon	AT&T, Inc.
Ms. Katherine Gronberg	Forescout Technologies, Inc.
Ms. Ilana Johnson	Neustar, Inc.
Mr. Michael Kennedy	VMware, Inc.
Mr. Kent Landfield	McAfee, LLC
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Thomas Patterson	Unisys Corp.
Mr. Kevin Riley	Ribbon Communications, Inc.
Mr. Brett Scarborough	Raytheon Technologies Corp.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Robert Spiger	Microsoft Corp.
Ms. Patricia Stolnacker Koch	VMware, Inc.
Mr. Milan Vlajnic	Communication Technologies, Inc.

Other Attendees

Government Participants

Mr. Dwayne Baker	Department of Homeland Security
Mr. Mark Bardwell	Department of Homeland Security
Ms. Sandy Benevides	Department of Homeland Security
Dr. Eric Burger	Office of Science and Technology Policy
Ms. DeShelle Cleghorn	Department of Homeland Security
Mr. Kenneth Cuccinelli	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. Robert Greene	Department of Homeland Security
Mr. Christopher Krebs	Department of Homeland Security
Mr. Patrick Looney	Office of Science and Technology Policy
Ms. Stephanie McCabe	Department of Homeland Security
Ms. Valerie Mongello	Department of Homeland Security
Ms. Renee Murphy	Department of Homeland Security
Mr. Brian Scott	National Security Council
Mr. Joshua Steinman	National Security Council
Ms. Brittney Trotter	Department of Homeland Security
Ms. Bridgette Walsh	Department of Homeland Security
Mr. Bradford Willke	Department of Homeland Security

Contractor Support

Ms. Sheila Becherer	Booz Allen Hamilton, Inc.
Ms. Emily Berg	Booz Allen Hamilton, Inc.
Mr. Evan Caplan	Booz Allen Hamilton, Inc.
Ms. Stephanie Curry	Booz Allen Hamilton, Inc.
Mr. Matthew Mindnich	Insight Technology Solutions, LLC
Ms. Laura Penn	Insight Technology Solutions, LLC
Mr. Barry Skidmore	Insight Technology Solutions, LLC

Public and Media Participants

Ms. Sharla Artz	Utilities Technology Council
Ms. Mariam Baksh	Nextgov
Ms. Christina Berger	Booz Allen Hamilton, Inc.
Mr. Eric Geller	Politico
Mr. Philip Grant	Booz Allen Hamilton, Inc.
Mr. Christopher Jaikaran	Congressional Research Service
Ms. Laura Karnas	Booz Allen Hamilton, Inc.
Mr. Sean Lyngaas	Cyberscoop
Ms. Paula Trimble	Lewis-Burke Associates, LLC

Certification

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Mr. John Donovan
NSTAC Chair