President's National Security Telecommunications Advisory Committee (NSTAC) Member Conference Call (MCC) Open Session Summary
May 13, 2020

Call to Order and Opening Remarks

Ms. Helen Jackson, 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. Ms. Jackson then turned the meeting over to Mr. John Donovan, NSTAC Chair.

Mr. Donovan opened the meeting by welcoming participants and introducing Mr. Patrick Gelsinger, NSTAC Member, and Mr. Jack Huffard, NSTAC Member, as the most recent appointees to the NSTAC. He also thanked distinguished Government partners, Mr. Joshua Steinman, National Security Council (NSC), and Mr. Christopher Krebs, DHS, for their participation. Mr. Donovan then provided an overview of the open session agenda, noting that Software-Defined Networking (SDN) Subcommittee Co-Chair, Mr. Raymond Dolan, NSTAC Member, would provide an update on the subcommittee's activities and that the committee would discuss future NSTAC study topics with the Government. Mr. Donovan then reviewed the outcomes from the last MCC held on February 20, 2020. Specifically, he noted that the NSTAC heard about how the Government is leveraging NSTAC's counsel to craft fifth generation (5G) and cyber workforce policy, received an update on the SDN Subcommittee's activities, and discussed potential study topics. Mr. Donovan then asked Mr. Steinman to provide his opening remarks.

Mr. Steinman began his remarks with a note that the Administration is focused on the coronavirus (COVID-19) pandemic, ensuring a secure upcoming election cycle, and promoting information and communications technology (ICT) supply chain security. Regarding the pandemic response, he commended the telecommunications industry's ability to maintain connectivity, which has been vital to enabling the American economy to respond to the crisis. Mr. Steinman added that the Administration continues to assess the Nation's response to improve upon shortfalls and innovate for the future.

Mr. Steinman said that the Administration is working with Congress on a multifaceted approach to address the security of international supply chains and of the U.S. and global information networks, noting that these issues present national security and economic security imperatives. He added that the Administration is implementing the *National Strategy to Secure 5G of the United States of America.* He underscored that the United States is leading the world in the development, deployment, and management of secure and reliable 5G infrastructure and stated that the President is committed to protecting the Nation's communications networks from untrusted vendors. Mr. Steinman added that the recommendations in the 2019 *NSTAC Report to the President on Advancing Resiliency and*

Fostering Innovation in the ICT Ecosystem informed the Administration when crafting the strategy. Other efforts include Executive Order 13913: *Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector*, which will review foreign ownership and activity in the U.S. telecommunications sector, and the signing of the *Secure and Trusted Communications Networks Act of 2019*, which will provide funding for U.S. telecommunication companies to remove and replace components in their networks provided by unsecure vendors.

In his role as leading the Cybersecurity and Infrastructure Security Agency (CISA), Director Krebs stated that the agency is focusing on three core lines of effort during the COVID-19 pandemic: (1) understanding the new risk landscape; (2) protecting the COVID-19 response; and (3) securing the digital transformation. Some of the agency's activities to protect responders include: releasing and updating its *Essential Critical Infrastructure Workers Guidance* to define who qualifies as a "critical" worker; working with the Centers for Disease Control and Prevention to create guidance for critical infrastructure workers exposed to COVID-19; and issuing a guide for maintaining critical infrastructure operations centers and control rooms in a pandemic environment. To help secure the digital transformation as more of the economy is conducted by telework, CISA has worked with other agencies and international partners to release warnings about hackers attacking institutions working to fight the COVID-19 pandemic. CISA has also set up a resource hub focused on digital transformation security requirements. Director Krebs also shared that CISA remains focused on election security and maintaining a pulse on supply chain security amidst shifts due to reliance on just-in-time delivery, concentrated dependency, lack of diversification, and stockpiling.

NSTAC SDN Subcommittee Status Update and Discussion

Mr. Raymond Dolan, NSTAC Member and SDN Subcommittee Co-Chair, provided an update on the subcommittee's activities. He recalled that the Executive Office of the President tasked the NSTAC to: (1) assess the importance of SDN; (2) define associated challenges and opportunities; (3) determine how SDN is used currently by the public and private sectors; and (4) identify any risks and proposed mitigations.

Mr. Dolan noted that since the last NSTAC member meeting in February 2020, the subcommittee has been briefed by a robust set of subject matter experts (SME) from Government, academia, and industry on SDN's many facets. He stated that these experts represent a diverse group of technology developers, cloud and data providers, telecom infrastructure providers, and industry analysts. He noted that during their briefings, presenters spoke to a variety of technical, operational, and policy considerations surrounding SDN and other virtualization technologies. Mr. Dolan highlighted that the subcommittee continues to use SME input throughout the study process to define the different components of the SDN supply chain, deployment successes, user challenges, and emerging trends that merit Presidential review.

Mr. Dolan shared that the subcommittee has crafted a foundational overview of SDN technology, implementation strategies, and use cases that focus on both the benefits and risks

for SDN deployments. The subcommittee is currently developing key themes and recommended actions while continuing to refine the draft report. Mr. Dolan then highlighted upcoming key milestones the subcommittee will undergo before finalizing the report:

- In the coming weeks, NSTAC members will receive a draft report for review and comment;
- On June 18, 2020, NSTAC members are invited to participate in a subcommittee meeting to discuss proposed recommendations to the President;
- By June 22, 2020, NSTAC members will receive a revised report, inclusive of input received during the June 18, 2020, subcommittee meeting; and
- On August 12, 2020, NSTAC members plan to deliberate and vote on the draft SDN report during the August 2020 MCC. If the report is approved, it will be transmitted to the President.

Mr. Dolan then asked the other SDN Subcommittee Co-Chairs; Mr. Scott Charney, NSTAC Vice Chair, and Mr. Donovan; if they had any additional comments. Mr. Donovan said the ongoing challenges with the COVID-19 pandemic has made the report more relevant than ever. He emphasized the importance for the Government to understand this technology in order to utilize it at its full capacity. Mr. Donovan asked NSTAC members to review the SDN report. He thanked the subcommittee working group co-leads, subcommittee members, and the CISA team for their hard work.

Future NSTAC Study Topics Discussion

Director Krebs provided a brief overview of two potential NSTAC study topics:
(1) communications resiliency; and (2) trusted identity management (IdM). He recalled that the communications resiliency topic was first broached during the November 2019 NSTAC meeting. Director Krebs said this topic would allow the NSTAC to reexamine the information in the 2011 *NSTAC Report to the President on Communications Resiliency* and is a timely and urgent topic due to the COVID-19 pandemic. He mentioned that this study would likely require an 18-month examination period, but that the NSTAC could offer initial insights in a shorter-turn period as they have done in the past with preliminary scoping reports. Regarding the trusted IdM topic, he noted that the Government could benefit from the NSTAC's insights on how it could: (1) establish an improved personal identity management system featuring robust trust mechanisms; and
(2) move past utilizing Social Security Numbers as commonplace unique identifiers.

Mr. Steinman recommended the NSTAC publish an interim product on communications resiliency with a focus on COVID-19 response to inform the legislative cycles in late summer and early fall. Mr. Donovan noted that communications resiliency is the most logical next study due to its feasibility to run parallel to the SDN study. Mr. Mark McLaughlin, NSTAC Member, mentioned that the NSTAC can review the 2011 Communications Resiliency Report as a starting point for scoping this study, looking to determine whether: (1) the recommendations have not changed but implementation has; or (2) the recommendations themselves have changed.

Mr. Angel Ruiz, NSTAC Member, stated that the communications resiliency issue is twofold. There is immediate concern on the amount of stress placed on networks due to the pandemic and more strain would be put on these networks due to regional and national emergencies (e.g., hurricanes, fires). He said it is important to understand how networks will perform with the added stress. Mr. Donovan mentioned that resiliency in prior decades was focused on natural disasters and physical recovery and that it is vital to note the shift from physical strains to virtual ones.

Mr. Jeffrey Storey, NSTAC Member, stated that there has been a 30 to 40 percent increase in network traffic due to COVID-19 over the last few months and that industry and government need to continue to augment where needed. He noted that trends such as: the expansion of the perimeters; moving closer to the edge; and the evolution of cloud computing to edge computing, will continue to emphasize the need for coordination and will help to ensure that networks become more software-defined. Mr. Storey mentioned that it is important to focus on hybrid networking. Specifically, there is a series of networks that need to work together comprehensively to support a COVID-19-type transition, the digital transformation of the industries as a whole, and/or natural disasters. Mr. Patrick Gelsinger, NSTAC Member, shared it would be timely to examine the reason why networks have been able to respond well to the large increase in telework and the new implications of a vastly distributed attack surface.

Ms. Renée James, NSTAC Member, stated that she agreed with the comments on communications resiliency but noted that the trusted IdM topic is critical to national identity. She mentioned that the NSTAC could examine trusted IdM in terms of COVID-19, focusing on reopening the workforce and the resiliency of the economy. She forecasted that doing so would help with contact tracing, vaccination distribution, and other relevant activities. Ms. James asked the Government to consider this topic in terms of emergency preparedness and reiterated that it is an important topic to study in the future. Mr. Huffard added that it would be valuable to research a solution in which to bring employees back to offices safely and with low risk. He noted that resiliency is expanding to operational technology (OT) and critical infrastructure, and that the connectedness of OT and critical infrastructure is something the NSTAC should evaluate.

After hearing NSTAC member comments, Mr. Steinman tasked the Committee with an interim study on communications resiliency that will focus on the COVID-19 response. This tasking was delivered with an understanding that the NSC may commission a subsequent longer study to the NSTAC at a later time. Mr. Donovan noted that the trusted IdM topic has been a subject of interest for several years and asked Mr. Steinman and Director Krebs to continue to keep it on the NSTAC's radar. Mr. Donovan thanked Mr. Steinman and the NSC and accepted the tasking on behalf of the NSTAC.

Closing Remarks and Adjournment

Mr. Donovan thanked the members and Government partners for attending and the input they provided, paying a special thanks to Mr. Steinman for the new study topic. He also thanked his SDN Subcommittee Co-Chairs and the subcommittee staff for their hard work on the draft

SDN report. Mr. Steinman thanked the NSTAC and stated that he believes it is one of the most important advisory committees currently serving the President. Mr. Krebs also thanked the committee and stated that the NSTAC team will work on revising the committee's study cadence to ensure that the committee is able to address both short-term, operational study topics and longer-term, strategic study topics.

Mr. Donovan announced that the next NSTAC meeting will be held via conference call on August 12, 2020.

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

APPENDIX
NSTAC Member Conference Call Open Session Participants List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corp.
Mr. William Brown	L3Harris Technologies, Inc.
Mr. Scott Charney	Microsoft Corp.
Mr. Matthew Desch	Iridium Communications, Inc.
Mr. David DeWalt	NightDragon Security
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 Network Security, Inc.
Ms. Renée James	Ampere Computing, LLC
Dr. Thomas Kennedy	Raytheon Technologies Corp.
Mr. Mark McLaughlin	Palo Alto Networks, Inc.
Mr. Angel Ruiz	MediaKind, Inc.
Mr. Gary Smith	Ciena Corp.
Mr. Jeffrey Storey	CenturyLink, Inc.
Mr. Hock Tan	Broadcom, Inc.
Mr. Brian Truskowski	IBM Corp.
Mr. Christopher Young	TPG Capital, Inc.
NSTAC Points of Contact	
Mr. Christopher Anderson	CenturyLink, Inc.
Mr. Jason Boswell	Ericsson, Inc.
Mr. Christopher Boyer	AT&T, Inc.
Mr. Jamie Brown	Tenable Network Security, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	CenturyLink, 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. Kathryn Ignaszewski	IBM Corp.
Ms. Ilana Johnson	Neustar, Inc.
Mr. Michael Kennedy	VMware, Inc.
Mr. Kent Landfield	McAfee, LLC
Mr. Sean Morgan	Palo Alto Networks, Inc.

Mr. Joshua New	IBM Corp.
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.
Mr. Kent Varney	Lockheed Martin Corp.
Mr. Milan Vlajnic	Communication Technologies, Inc.

Other Attendees

Ms. Sharla Artz	Utilities Technology Council
Ms. Linda Johnson	CenturyLink, Inc.
Ms. Melissa Woodruff	L3Harris Technologies, Inc.

Government Participants

Mr. Dwayne Baker	Department of Homeland Security
Ms. Sandy Benevides	Department of Homeland Security
Ms. DeShelle Cleghorn	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. Paul Gray	Department of Homeland Security
Ms. Helen Jackson	Department of Homeland Security
Mr. Christopher Krebs	Department of Homeland Security
Ms. Kayla Lord	Department of Homeland Security
Ms. Valerie Mongello	Department of Homeland Security
Ms. Ginger Norris	Department of Homeland Security
Mr. Brian Scott	National Security Council
Mr. Joshua Steinman	National Security Council
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.
Ms. Christina Berger	Booz Allen Hamilton, Inc.
Mr. Evan Caplan	Booz Allen Hamilton, Inc.
Ms. Stephanie Curry	Booz Allen Hamilton, Inc.
Ms. Anne Johnson	Insight Technology Solutions, Inc.
Mr. Matthew Mindnich	Insight Technology Solutions, Inc.
Ms. Laura Penn	Insight Technology Solutions, Inc.
Mr. Barry Skidmore	Insight Technology Solutions, Inc.
Ms. Beth Slaninka	Nexight Group, LLC
Ms. Casey Vincent	Insight Technology Solutions, Inc.

Public and Media Participants

Mr. Calvin Biesecker	Defense Daily

Mr. Jason Boose	Government of Canada
Mr. Drew Fitzgerald	The Wall Street Journal
Mr. Christopher Jaikaran	Congressional Research Service
Mr. Mark Rockwell	Federal Computer Week
Mr. Timothy Starks	Politico

Certification

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

Mr. John Donovan
NSTAC Chair