President's National Security Telecommunications Advisory Committee (NSTAC)
Member Conference Call (MCC)
February 20, 2020

Purpose of Meeting

The purpose of the February 20, 2020, NSTAC MCC was to discuss: (1) the status of the NSTAC Software-Defined Networking (SDN) Subcommittee; and (2) potential study topics.

Call to Order

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 one member of the public—Mr. Mark Hadley, Department of Energy—had registered to provide comment. Similarly, written comments would be accepted following the procedures outlined in the meeting's Federal Register Notice. Following roll call, Ms. Jackson turned the meeting over to Mr. John Donovan, NSTAC Chair.

Welcome and Opening Remarks

Mr. Donovan opened the meeting, welcomed participants, and summarized the MCC agenda. He then reviewed the outcomes from the last member meeting held in Washington, D.C., on November 14, 2019. Specifically, he noted that the NSTAC agreed to further investigate potential study topics related to communications resiliency and trusted identity management.

Mr. Donovan welcomed Mr. Hock Tan, Broadcom, and Mr. Brian Truskowski, IBM, as the NSTAC's newest members. He also thanked Mr. Joshua Steinman, National Security Council, and Mr. Bradford Willke, DHS, for their participation. Mr. Donovan then asked Mr. Steinman to provide his opening remarks.

Mr. Steinman stated that the NSTAC's recommendations help the Administration to better understand how its policy decisions impact industry. He noted how the Administration continues to prioritize efforts to:

- Establish national and international fifth generation (5G) network security standards and develop a network of trusted 5G suppliers;
- Secure Positioning, Navigation, and Timing (PNT) services as outlined in Executive Order (EO) 13905: *Strengthening National Resilience Through Responsible Use of PNT Services*; and
- Develop the U.S. cyber workforce, as demonstrated by EO 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*; EO 13870: *America's Cybersecurity Workforce*; the 2018 *National Cyber Strategy*; and the President's Cup Cybersecurity Competition.

Mr. Donovan thanked Mr. Steinman for his comments and invited Mr. Willke to provide his remarks.

In response to increased cyber threats from Iran, Mr. Willke stated that the Cybersecurity and Infrastructure Security Agency (CISA) is currently working with both industry and Government partners to address these risks. As part of this effort, CISA recently released the *CISA Insights: Increased Geopolitical Tensions and Threats* report to discuss what industries may be targeted and the types attacks to expect during this time. Likewise, CISA also released the *CISA Insights: Ransomware Outbreak* document to outline the steps partners can take to increase their resiliency against ransomware attacks. Discussing stakeholder engagement efforts, Mr. Willke noted that CISA was hosting a panel with the Aspen Institute at RSA 2020 to discuss Cybersecurity Grand Challenges, as recommended in the 2018 *NSTAC Report to the President on a Cybersecurity Moonshot*. Finally, he highlighted the *Cybersecurity Vulnerability Identification and Notification Act of 2020*, which is currently under review by the House of Representatives. If enacted, this bill would give CISA the power to subpoena internet service providers on reported cyberattacks, allowing the agency to more quickly address vulnerabilities as they are identified.

Mr. Donovan thanked Mr. Steinman and Mr. Willke for their remarks.

NSTAC SDN Subcommittee Status Update and Discussion

Mr. Raymond Dolan, NSTAC Member, summarized the SDN Subcommittee's progress to date, which has included receiving briefings from a variety of subject matter experts and developing the subcommittee's draft report outline. He then discussed upcoming milestones:

- **April 2020:** NSTAC members will receive a first draft of the report to review;
- **May 2020 NSTAC Meeting:** NSTAC members will discuss proposed recommendations and provide feedback in real-time;
- **June 2020:** NSTAC members will receive an updated report draft for comment; and
- **August 2020 NSTAC MCC:** NSTAC members will deliberate and vote on the final report. If approved, it will be transmitted to the White House.

Mr. Donovan added that this study offers the NSTAC the opportunity to help define Government's response to and deployment of SDN. He also encouraged members to participate in developing the report's recommendations. Mr. Donovan thanked Mr. Dolan for his update.

Public Comment

Mr. Hadley provided an update on Pacific Northwest National Laboratory's (PNNL) operational technology (OT) SDN deployments. He noted that OT-SDN uses the same components as standard SDN but implements machine-to-machine communications to automate network management and security. OT-SDN can identify all network devices to streamline interactions and protect the critical infrastructure. When an unexpected network communication is detected, OT-SDN isolates the command until it can be authorized.

Mr. Hadley said that PNNL's tests have shown that OT-SDN security system renders standard attacks against industrial control systems (ICS) ineffective. As a result, he recommended that the NSTAC consider how OT-SDN protocol is being deployed across a wide range of ICS as it develops its report to the President.

Mr. Donovan thanked Mr. Hadley for his comments.

Potential Study Topics Discussion

Mr. Scott Charney, NSTAC Vice Chair, presented two potential study topics for consideration. The first potential study topic, *Digitally-Secure Social Security Numbers (SSN)*, would address how the Government can create digitally-secure SSNs so that both federal and private transactions, such as those related to national security and emergency preparedness (NS/EP) communications, are more secure. The study could also determine the extent to which digitally-secure SSNs can protect—or even enhance—individual privacy.

Transitioning to the *Fortifying Communications Resiliency in an Evolving Information and Communications Technology Landscape* topic, Mr. Charney explained that this study would focus on how the Government can best ensure public safety communications resiliency during a disaster. As such, this study would reexamine the findings presented in the 2011 *NSTAC Report to the President on Communications Resiliency* to identify ways to promote operable, robust communications between first responders and the public. As part of this effort, Mr. Charney recommended conducting a 90-day examination of a specific issue area, like alerts, warnings, and notifications. In turn, this process would result in a letter or short paper to allow the NSTAC to deliver more timely, actionable recommendations to the President. Mr. Willke suggested that a public health use case, such as disseminating alerts on the spread of the coronavirus, would be valuable for this examination.

Mr. Donovan thanked Mr. Charney for his review. He also encouraged NSTAC members to provide their insights on how to better scope these topics moving forward.

Closing Remarks and Adjournment

Mr. Steinman thanked the NSTAC for supporting the Administration's efforts to address NS/EP risks facing the Nation. Mr. Willke also thanked the committee and noted that the Aspen Institute is developing a Cybersecurity Grand Challenge on trusted identity akin to the *Digitally-Secure SSN* potential study topic.

Mr. Donovan announced that the next NSTAC meeting will be held in Washington, D.C., on May 13, 2020.

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

APPENDIX
NSTAC Member Conference Call Participants List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corporation
Mr. Scott Charney	Microsoft Corporation
Mr. Matthew Desch	Iridium Communications, Inc.
Mr. Raymond Dolan	Cohere Technologies, Inc.
Mr. John Donovan	Formerly of AT&T Communications
Dr. Joseph Fergus	Communication Technologies, Inc.
Ms. Lisa Hook	Neustar, Inc.
Dr. Thomas Kennedy	Raytheon Company
Mr. Mark McLaughlin	Palo Alto Networks, Inc.
Mr. Angel Ruiz	MediaKind, Inc.
Ms. Kay Sears	Lockheed Martin Corporation
Mr. Hock Tan	Broadcom, Inc.
Mr. Brian Truskowski	IBM Corporation
NSTAC Points of Contact	
Mr. Jason Boswell	Ericsson, Inc.
Mr. Christopher Boyer	AT&T, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	CenturyLink, Inc.
Mr. Michael Daly	Raytheon Company
Ms. Cheryl Davis	Oracle Corporation
Mr. John Emling	Broadcom, Inc.
Mr. Thomas Gann	McAfee, LLC
Mr. Jonathan Gannon	AT&T, Inc.
Ms. Katherine Gronberg	Forescout Technologies, Inc.
Ms. Kathryn Ignaszewski	IBM Corporation
Ms. Ilana Johnson	Neustar, Inc.
Mr. Kent Landfield	McAfee, LLC
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Thomas Patterson	Unisys Corporation
Mr. Kevin Riley	Ribbon Communications, Inc.
Mr. David Rothenstein	Ciena Corporation
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Robert Spiger	Microsoft Corporation
Mr. Milan Vlajnic	Communication Technologies, Inc.
Other Attendees	
Ms. Melissa Woodruff	L3Harris Technologies, Inc.

Government Participants

Mr. Dwayne Baker	Department of Homeland Security
Ms. DeShelle Cleghorn	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. Mark Hadley	Department of Energy
Ms. Helen Jackson	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
Mr. Bradford Willke	Department of Homeland Security

Contractor Support

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

Public and Media Participants

Ms. Mariam Baksh	Inside Cybersecurity
Mr. Calvin Biesecker	Defense Daily
Mr. Jerry Ladd	CIWRX, Inc.
Mr. Paul McGinnis	California Governor's Office of Emergency Services
Mr. Tim Starks	Politico
Ms. Patricia Utterback	California Governor's Office of Emergency Services
Mr. Douglas Webb	Evergy, Inc.
Ms. Deborah Williams	Technical and Management Resources, Inc.

Certification

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

Mr. John Donovan
NSTAC Chair