President's National Security Telecommunications Advisory Committee (NSTAC)
Member Conference Call (MCC) Summary
August 12, 2020

Call to Order and Opening Remarks

Ms. Sandy Benevides, Department of Homeland Security (DHS) and NSTAC Designated Federal Officer (DFO), 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. Benevides thanked Ms. Helen Jackson, DHS, for her service as the NSTAC's DFO. She noted the NSTAC appreciates her work and looks forward to collaborating with her in her new role at the Cybersecurity and Infrastructure Security Agency (CISA). Ms. Benevides then turned the meeting over to Mr. John Donovan, NSTAC Chair.

Mr. Donovan opened the meeting by welcoming participants. He welcomed distinguished Government partners, Mr. Joshua Steinman, Deputy Assistant to the President and Senior Director for Cybersecurity, National Security Council; Ms. Robin Colwell, Special Assistant to the President for Economic Policy, Executive Office of the President (EOP); Mr. Bradford Willke, CISA Acting Assistant Director for Stakeholder Engagement, DHS; and Mr. Brandon Wales, CISA Executive Director, DHS. He then acknowledged Mr. Christopher Boyer, Vice President of Global Security and Technology Policy, AT&T, and Chair, Open Radio Access Network (RAN) Policy Coalition; and Ms. Diane Rinaldo, Senior Vice President, Beacon Strategies, and Executive Director, Open RAN Policy Coalition.

Mr. Donovan discussed the meeting agenda, noting that NSTAC members would: (1) receive remarks from Government partners regarding the Administration's and CISA's ongoing cybersecurity and national security and emergency preparedness (NS/EP) efforts; (2) receive an update from the NSTAC Communications Resiliency (CR) Subcommittee; (3) deliberate and vote on the draft *NSTAC Report to the President on Software-Defined Networking* (SDN); and (4) hold a discussion on recent Government and industry trends and innovations in fifth generation (5G) networks.

Mr. Donovan provided a brief overview of the NSTAC's last meeting, the May 2020 NSTAC MCC. He highlighted that Mr. Steinman provided remarks on the Government's efforts to address the coronavirus (COVID-19) pandemic and promote information and communications technology (ICT) supply chain security. Mr. Donovan informed participants that Mr. Christopher Krebs, CISA Director, DHS, provided remarks on the agency's three primary lines of effort to address the COVID-19 pandemic. Mr. Donovan recalled that the participants discussed potential study topics. At the end of this discussion, Mr. Steinman officially tasked the NSTAC with an immediate-term CR study that would focus on the coronavirus (COVID-19) response. Mr. Donovan then asked Mr. Steinman to provide his opening remarks.

Mr. Steinman thanked the SDN Subcommittee co-chairs, Mr. Donovan; Mr. Scott Charney, NSTAC Vice Chair; and Mr. Raymond Dolan, NSTAC Member, for their leadership of the subcommittee. He noted that the Administration's priorities have remained the same since the May MCC, which focus on: (1) responding to the COVID-19 pandemic; (2) ensuring a secure upcoming election cycle; (3) promoting ICT supply chain security; and (4) implementing the *National Strategy to Secure 5G of the United States of America*. Mr. Steinman said that the Administration is working with Congress on a multifaceted approach for addressing the security of international supply chains and U.S. and global ICT networks, as these are issues that remain imperative to national and economic security. Mr. Donovan thanked Mr. Steinman for his update, and turned the meeting over to Mr. Wales.

Mr. Wales thanked Mr. Donovan and stated that CISA is prioritizing election security as the Nation nears the November 2020 Presidential election. Mr. Wales also expressed his appreciation for the NSTAC's ongoing discussions around 5G. To this end, he cited CISA's support of various Government efforts in this space, namely the Administration's *National Strategy to Secure 5G of the United States of* America, CISA's own 5G strategy, and the Department of State's 5G Clean Path and Clean Networks Program, all of which call for a whole-of-Government approach to implementing secure 5G networks in the United States and abroad. He also thanked the committee for calling out the need for a trusted ICT supply chain in the *NSTAC Report to the President on Software-Defined Networking*. He noted how this report, along with the committee's continued attention to 5G, will help inform the Administration's efforts to address the potential risks posed by Chinese companies and lack of domestic foundry capabilities. Finally, Mr. Wales highlighted how the NSTAC's recommendations drive the Government's and current Administration's NS/EP and cybersecurity efforts, and thanked the committee for their engagement across CISA's priority areas.

Mr. Donovan thanked Mr. Wales for his remarks.

Status Update: NSTAC Communications Resiliency Subcommittee

Mr. Donovan introduced Mr. Jeffrey Storey, NSTAC Member and CR Subcommittee Co-Chair, to attendees and asked him to provide an update on the subcommittee's activities.

Mr. Storey explained that the CR will conduct its study in two phases. At the conclusion of phase I of its study, the subcommittee will develop a letter to provide on short-term recommendations to the President to address the successes and challenges that the COVID-19 pandemic has presented to the U.S. ICT ecosystem. Since the last NSTAC member meeting in May 2020, the subcommittee received a total of 19 briefings from subject matter experts (SME) over four weeks. These SMEs represented a variety of groups that either comprise or directly rely on the ICT sector, which included: (1) communications service providers and vendors; (2) cloud and application platform providers; (3) lifeline sectors; (4) user communities (e.g., healthcare, education); and (5) organizations and companies responsible for cybersecurity.

Mr. Storey then thanked the NSTAC companies who provided briefings. Within the next few weeks, he explained that the subcommittee will: (1) construct an outline of the phase I letter; (2) conduct additional research where necessary; and (3) summarize key findings and long-term ICT issues identified during the COVID-19 response. Discussing upcoming phase I milestones, Mr. Storey explained that:

- On August 18, 2020, and September 3, 2020, NSTAC members will be invited to participate in the subcommittee meetings to discuss their feedback on the letter.
- On October 6, 2020, NSTAC members plan to deliberate and vote on the draft letter. If approved, the letter will be transmitted to the President.

Mr. Storey thanked the subcommittee working group co-leads, members, and CISA team for their support.

Mr. Donovan thanked Mr. Storey for his comments.

Deliberation and Vote: *NSTAC Report to the President on Software-Defined Networking*

Mr. Donovan then turned the meeting to Mr. Dolan to provide an update on the SDN Subcommittee and the NSTAC report to the President.

Mr. Dolan recalled that the EOP tasked the NSTAC with examining SDN's implications on the Nation's ICT infrastructure. In response, the NSTAC examined best practices for SDN and related technologies; identified the associated challenges and opportunities; and assessed current utilization and corresponding risk mitigations. He stated that the study sought to make specific recommendations to the EOP regarding SDN policy by examining: (1) best practices for deploying SDN across federal networks and critical infrastructure; (2) how SDN can address risks posed to NS/EP communications and the ICT supply chain; and (3) methods to balance security and cost.

Mr. Dolan mentioned that the NSTAC reviewed existing data on SDN and received briefings from SMEs. These SMEs provided information on the emergence of SDN; how SDN is being deployed in 5G networks; and the security impacts of SDN on the ICT supply chain and the Nation's NS/EP functions.

During the study, the NSTAC discovered that SDN and network functions virtualization represent a major advance in network technology, which will have profound impacts for NS/EP communications. He stated that SDN also pose implications for the global ICT supply chain, as individual and organizational networks move away from dedicated hardware-based devices and appliances to less expensive, flexible software systems. In the near-term, SDN will reduce product development cost and time to market, lowering barriers to market entry, spurring investment, and promoting innovation.

Mr. Dolan noted that SDN is integral to the development of 5G mobile infrastructures. As enhanced security is a core capability of SDN, these technologies can facilitate the

incorporation or addition of sophisticated security features in real-time, using artificial intelligence to rapidly detect and actively mitigate malicious activities. Thus, SDN architectures are designed to be more secure, resilient, adaptable, and resistant to the evolving threat environment than corresponding hardware-based deployments. Mr. Dolan emphasized that the transition to SDN promotes U.S. company leadership in silicon, cloud, and software. Mr. Dolan explained that the United States, along with its allies, is the global leader in the development and deployment of SDN. As such, many network operators have already begun the migration to SDN. This migration: (1) builds on and enhances U.S. leadership in virtualization and ICT innovation; and (2) illustrates that SDN technologies have reached a level of maturity that allows for secure implementation at scale. While there are challenges with operationalization and security, SDN deployments by U.S.-based carriers, service providers, and enterprises demonstrate that these issues can be managed in the context of NS/EP communications.

In summary, Mr. Dolan stated that the NSTAC recommends:

- The Administration should encourage and support the continued deployment of SDN technology in U.S. and allied nation ICT environments. Policymakers also should consider how to best promote the use of open architectures with a particular focus on 5G and beyond.
- The Defense Community and the Intelligence Community (IC) should expand efforts to define requirements and use cases for SDN and related technology specific to their unique needs, which can be shared with private sector SDN providers and relevant standards bodies. In collaboration with the private sector, the Defense Community and IC should also determine how the capabilities might be leveraged for adoption in the national security environment.
- The Government should establish policies to help educate U.S. departments, agencies, and critical infrastructure operators on the full range of SDN and related technology capabilities to enhance their mission performance, improve security, and lower costs.
- Working with Congress, the Administration should: (1) establish policies and incentives to encourage U.S.-based investment and innovation in the research and development of SDN and related technology capabilities and standards; (2) encourage best practices for secure implementation; and (3) promote the deployment of these capabilities within the U.S. Government and allied nation ICT environments. Policymakers should also consider updating acquisition strategies and mechanisms around SDN and related technology-based services.

To this end, the NSTAC believes that SDN can help defend and sustain U.S. leadership in 5G wireless technologies and beyond. As a result, Mr. Dolan maintained that U.S. participation in the evolution of a new SDN supply chain ecosystem is of global importance.

Mr. Dolan then invited Mr. Charney and Mr. Donovan to provide additional comments. Mr. Charney noted that the report underscored the need for a complete and trusted SDN supply chain. He stated that, while the ICT ecosystem continues to shift away from hardware-based

networks to software systems, the hardware still needs to be maintained and secured. As a result, trusted suppliers for hardware and software are needed within the ICT supply chain.

Mr. Donovan made a motion to vote on the *NSTAC Report to the President on Software-Defined Networking*, which members unanimously approved.

Mr. Donovan thanked NSTAC members and staff for their support of the study.

Discussion: Trends and Innovations in 5G and Beyond

Mr. Donovan invited Ms. Colwell to facilitate the "Trends and Innovations in 5G and Beyond" discussion.

Ms. Colwell thanked the NSTAC for the invitation to provide remarks. She then congratulated the Open RAN Policy Coalition for its work on the *National Defense Authorization Act* (NDAA). She said that the grant programs included in the NDAA will accelerate innovation in 5G and SDN, but more financial support is needed to ensure successful, secure deployments.

Ms. Colwell stated that the Administration continues to make significant progress in developing the *National Strategy to Secure 5G Implementation Plan*, for which international outreach is an important pillar. She said that, as the United States continues to promote global market share for trusted vendors, it is seeking ways to engage with the United Kingdom and other allied nations on interrelated initiatives.

Ms. Colwell also expressed her appreciation for industry's response to the National Telecommunications and Information Administration's Request for Comments on the *National Strategy to Secure 5G Implementation Plan*. She noted that many of industry's comments closely align with the Administration's plan for 5G deployment. Moreover, on August 10, 2020, the Administration announced that the Federal Communications Commission would auction 100 megahertz of contiguous mid-band spectrum for commercial use in late 2021. She hoped that this additional spectrum would help accelerate 5G deployments nationwide. Ms. Colwell then invited Mr. Boyer to provide remarks.

Mr. Boyer stated that the Open RAN Policy Coalition was formed in early 2020 with the intent of increasing competition in the open RAN (O-RAN) supply chain. He mentioned that the O-RAN seeks to standardize interfaces between various components in the RAN. Opening these interfaces will allow carriers to deploy quality equipment and leverage a variety of vendors, rather than relying on one entity to integrate all parts of the network (e.g., hardware, software, radio). This more open approach it will: (1) enable vendor competition in the supply chain by standardizing interfaces between components; and (2) promote innovation by moving away from a fully-integrated solution. Mr. Boyer stated that O-RAN is a natural extension of what is already occurring in the core networks in that it pushes de-integration to the network edge and facilitates networks' migration to software. He noted the critical importance of securing both hardware and software subcomponents. Mr. Boyer referenced the 2018 Center for Strategic and International Studies' *How Will 5G Shape Innovation and Security: A Primer*

to underscore how the United States' leadership in the subcomponents sector will need to be maintained through policy. Mr. Boyer stated that it is important for networks to scale over time. As seen during the COVID-19 pandemic, SDN has enabled networks' ability to scale up to meet increased demand as more people work from home. He added that, in terms of network architecture, industry is moving towards a combination of proprietary SDN and O-RAN solutions. Mr. Boyer then turned the meeting over to Ms. Rinaldo.

Ms. Rinaldo noted that many policymakers are trying to determine how to best promote the development and deployment of open source technologies. In response, the Open RAN Policy Coalition is researching how to create more competition within the marketplace. The coalition is also investigating how to implement a private sector market-based solution that, by standardizing interfaces, will drive competition, increase innovation, and decrease pricing. She said that both domestic and international policymakers have been receptive to the coalition's work. To this end, the coalition is working with international regulators and private sector partners to find ways to increase innovation. She stressed the importance of engaging allies worldwide in this effort; the coalition's new members from Telefonica, Vodafone, and Reliance Jio Infocomm Limited are helping make this possible. By educating policymakers on the importance of public and private sector collaboration, it will be possible to implement O-RAN technologies at scale, which will be key to driving a next-generation 5G network.

Mr. Donovan asked how the coalition is addressing the interfaces from metal into the system as it relates to O-RAN. Mr. Boyer stated that the coalition has not examined integration to that level of detail, as it has been focusing on obtaining policy to support O-RAN developments. He said that the O-RAN Alliance, which is separate from the coalition, is researching the technical standards aspect. From a policy perspective, the funding mechanisms included as part of the *U.S. Telecommunications Act* could promote further research and development. Ms. Rinaldo mentioned that Government partners—both in the United States and abroad—are becoming more interested in how networks are built and where components are made. To this end, secure manufacturing for supply chain components is critical.

Mr. Hock Tan, NSTAC Member, stated that, from a chipset perspective, 5G software runs on hardware. As industry continues to move towards a more open standards system on the call networks, he highlighted that a primary lesson learned is to aggregate hardware from software and create application-specific standard products.

Mr. Patrick Gelsinger, NSTAC Member, stated that his company recently made two announcements in the open source realm. The first was an announcement with Dish regarding Rakuten, the first fully O-RAN compliant, software-driven 5G radio deployment. VMware's second announcement was regarding the FlexRAN, a joint reference design with Intel that will standardize an O-RAN compliant solution set. Ms. Rinaldo noted that the coalition is excited to see the outcomes of VMware's partnerships, highlighting the importance of institutional companies leading next-generation architecture efforts.

Mr. Donovan asked how the Administration is addressing the tradeoffs between trusted sources versus open source hardware/software. Ms. Colwell noted the tension between trusted sources and more open source innovation. She said that opening architecture to open source development increases security vulnerabilities, which requires a more collaborative approach to threat monitoring. Mr. Donovan added that this transparency helps mitigates risk.

Mr. Christopher Young, NSTAC Member, cautioned that increased open source deployments will require more active security management. He mentioned that he was pleased to see security architectures addressed in the *NSTAC Report to the President on Software-Defined Networking* and noted the importance of managing supply chain integrity in an open source system. Ms. Colwell agreed, and suggested that more users could be leveraged to monitor threats in an open source-like paradigm.

Mr. Donovan thanked Mr. Boyer, Ms. Colwell, and Ms. Rinaldo for their remarks. He also thanked NSTAC members for their comments.

Closing Remarks and Adjournment

Mr. Donovan thanked: (1) NSTAC members and Government partners for their participation; (2) the SDN Subcommittee for its work on developing the *NSTAC Report to the President on Software-Defined Networking*; and (3) Mr. Storey and Mr. Angel Ruiz, NSTAC Member and CR Subcommittee Co-Chair, for their leadership of the CR Subcommittee. Mr. Steinman, Mr. Wales, and Mr. Willke each thanked the NSTAC for their continued support of the Government's NS/EP and cybersecurity policy.

Mr. Donovan announced that the next NSTAC meeting will be held via conference call on October 6, 2020. Additional details for that meeting are forthcoming.

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

APPENDIX
NSTAC Member Conference Call 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
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.
Ms. Kay Sears	Lockheed Martin Corp.
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.
Ms. Amanda Craig-Deckard	Microsoft Corp.
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. Gregory Lavender	VMware, Inc.

Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Joshua New	IBM Corp.
Mr. Thomas Patterson	Unisys Corp.
Mr. Kevin Riley	Ribbon Communications, Inc.
Mr. David Rothenstein	Ciena Corp.
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. Kent Varney	Lockheed Martin Corp.
Mr. Milan Vlajnic	Communication Technologies, Inc.

Other Attendees

Mr. Bruce Byrd	AT&T, Inc.
Ms. Diane Rinaldo	Beacon Strategies, LLC
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. Robin Colwell	Executive Office of the President
Mr. Daniel Dagher	Department of Homeland Security
Mr. Conner Fitzpatrick	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. Robert Greene	Department of Homeland Security
Ms. Kayla Lord	Department of Homeland Security
Ms. Valerie Mongello	Department of Homeland Security
Mr. Brian Peretti	Department of Homeland Security
Mr. Brian Scott	National Security Council
Ms. Traci Silas	Department of Homeland Security
Mr. Joshua Steinman	National Security Council
Mr. Brandon Wales	Department of Homeland Security
Ms. Bridgette Walsh	Department of Homeland Security
Ms. Sydney White	U.S. House of Representatives Committee on 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.
Mr. Philip Grant	Booz Allen Hamilton, Inc.

Ms. Anne Johnson	Insight Technology Solutions, Inc.
Ms. Laura Karnas	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. Sharla Artz	Utilities Technology Council
Mr. Jason Boose	Government of Canada
Ms. Amanda Bruno	Lewis-Burke Associates, LLC
Mr. Samuel Chanoski	Hitachi ABB Power Grids, Ltd.
Ms. Elizabeth Down	Peck Madigan Jones, Inc.
Ms. Sara Friedman	Inside Cybersecurity
Mr. Slate Herman	Wilkinson Barker Knauer, LLP
Mr. Christopher Jaikaran	Congressional Research Service
Mr. Brett Kilbourne	Utilities Technology Council
Ms. Elizabeth Ludan	Zeichner Risk Analytics, LLC
Mr. David Rardin	Utilities Technology Council
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