President's National Security Telecommunications Advisory Committee (NSTAC) Open Session Meeting Summary
November 14, 2019

Call to Order and Opening Remarks

Ms. Helen Jackson, Department of Homeland Security (DHS) and NSTAC Designated Federal Officer, called the November 2019 NSTAC Meeting to order. She reminded attendees that the NSTAC is a federal advisory committee, governed by the *Federal Advisory Committee Act*. As such, the meeting is open to the public. She shared that written comments had been submitted in response to the meeting's Federal Register Notice (FRN), but no requests for verbal comments have been received. She noted that further written comments were being accepted following the procedures outlined in the FRN. Ms. Jackson then introduced Mr. John Donovan, NSTAC Chair.

Mr. Donovan opened the meeting, welcomed participants, and summarized the agenda. He reported that, during the September 3, 2019, NSTAC Member Conference Call, the committee voted unanimously to approve the *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communication Technologies (ICT) Ecosystem*, which has since been transmitted to the President. Mr. Donovan then asked Mr. Grant Schneider, National Security Council (NSC), to provide his opening remarks.

Mr. Schneider welcomed Dr. Thomas Kennedy, NSTAC Member, to the committee as its newest member. He thanked Ms. Renée James, NSTAC Member, for her time as NSTAC Chair, and for Mr. Donovan for assuming this role.

Mr. Schneider reviewed actions the Administration had recently taken to address cybersecurity and ICT supply chain issues. He noted the release of the *National Cyber Strategy* in 2018, for which the Administration had since developed an implementation plan to address its 42 priority action items. Mr. Schneider stated that the President had also signed: (1) Executive Order (EO) 13873, *Securing the ICT and Services Supply Chain*, to specifically address ICT supply chain issues; (2) EO 13870, *America's Cybersecurity Workforce,* which outlines federal goals for cybersecurity education; and (3) the *Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act* (the Act) into law to help secure the federal acquisition supply chain. He noted that the Act created the Federal Acquisition Security Council (FASC) to establish supply chain risk management (SCRM) standards, guidelines, and practices for federal acquisition processes. Mr. Donovan then invited Cybersecurity and Infrastructure Agency (CISA) Director Christopher Krebs, DHS, to provide his remarks.

Director Krebs stated that November 15, 2019, marked the one-year anniversary of CISA's establishment. During this time, CISA founded the National Risk Management Center (NRMC), which continues to work with industry partners to address the most significant risks to the Nation's critical infrastructure. Director Krebs also stated that the ICT SCRM

Task Force's September 2019 *Information and Communications Technology Supply Chain Task Risk Management Task Force Interim Report: Status Update on Activities and Objectives of the Task Force* outlines its current work to develop consensus on strategies to enhance ICT supply chain security. He also noted that CISA had also released the *CISA Strategic Intent* in August 2019, which included China, supply chain, fifth generation (5G) technologies, election security, soft target security, federal security, and industrial control systems as its top five operational priorities.

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

Homeland Security and Counterterrorism Advisor Remarks

Mr. Schneider introduced Rear Admiral (RADM) Peter Brown, Executive Office of the President. RADM Brown thanked the NSTAC for their work in helping the Government to understand the risks the Nation faces across the ICT ecosystem. He stated that ICT continues to evolve at an extremely rapid rate, playing a significant role in every critical infrastructure sector. Thus, modernizing and securing the ICT supply chain is more critical than ever. RADM Brown said that the Government must also continue to support and improve workforce education and training for the ICT professionals who compromise the Nation's intellectual supply chain.

He reiterated that the committee's work on ICT security is a vital part of ensuring the United States' continued national security and economic prosperity.

Panel Discussion: Ensuring Information and Communication Technology Infrastructure and Supply Chain Integrity

Ms. Jackson introduced Mr. Daniel Kroese, DHS, and Mr. Robert Mayer, USTelecom Association, to attendees.

Mr. Kroese stated that there has been a plethora of activity between the public and private sector on ICT SCRM. As a result, CISA established the ICT SCRM Task Force in 2018. Since then, the task force has launched four working groups around information sharing; threat evaluation; qualified bidder lists and qualified manufacturer lists; and policy recommendations to incentivize purchase of ICT from original equipment manufacturers and authorized resellers.[1] Through these working groups, Government and industry experts seek to address a series of critical questions:

- What are the current ICT supply chain threats?
- What is a reasonable set of criteria to assess these threats?
- Who is doing the assessing and how?
- Who owns and shares information?

[1] CISA, "Information and Communications Technology Supply Chain Task Risk Management Task Force Interim Report: Status Update on Activities and Objectives of the Task Force." September 2019, https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

- How is it applied?

From an operational perspective, Mr. Mayer noted that the task force has identified 180 different supply chain threats to date. In its initial report, the task force identified nine additional threat groups: (1) counterfeit parts; (2) cybersecurity; (3) internal security operations and controls; (4) system development lifecycle processes and tools; (5) insider threats; (6) economic risks; (7) inherited risk through an extended supplier chain; (8) legal risks; and (9) external end-to-end supply chain risks (e.g., natural disasters, geo-political issues).[2] The group also recommended that SCRM education initiatives leverage available work to better shape supply chain security.

Mr. Donovan asked if the task force has considered analyzing the risks posed by foreign entities funding or building key components of the United States ICT supply chain. Mr. Kroese mentioned that such an analysis needed to be further scoped. Mr. Mayer also noted the sensitivities of such an investigation. Mr. Donovan stated that there is considerable attention being given to the low latency, high-reliability communications provided by 5G, software-defined networking (SDN), and other technologies. He cautioned users to consider the emergent threats posed by increased virtualization.

Director Krebs stressed that CISA relies heavily on industry insight to fulfill its mission. Mr. Donovan noted that forums like the NSTAC meetings are important to understand the scope of and context for collaboration between the public and private sectors. He also underscored the need for industry to help Government develop the next generation of networks (e.g., cloud) with security in mind. Director Krebs asked how to drive ICT security consciousness in the commercial and consumer spaces. Mr. Kroese replied that there has been substantial progress made around ICT cybersecurity, but it is important to understand how these devices operate and interoperate before proceeding much further. Mr. Kroese also urged participants to consider operational technology's impact on the supply chain going forward.

Mr. Scott Charney, NSTAC Vice Chair, asked how organizations can manage risk in a dynamic ICT environment. Mr. Kroese said that users should use the ICT SCRM Task Force's environment deconstruction to identify key vulnerability areas. Mr. Mayer noted that, in this context, there are several critical elements that can be managed collectively between Government and industry.

Mr. Donovan thanked Mr. Kroese and Mr. Mayer for their insights.

[2] CISA, "Information and Communications Technology Supply Chain Task Risk Management Task Force Interim Report: Status Update on Activities and Objectives of the Task Force." September 2019, https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf

Keynote Speaker

Mr. Donovan turned the floor to Transportation Security Administration Administrator David Pekoske, DHS. Prior to his address, Administrator Pekoske shared news of a school shooting in Santa Clarita, CA. As such, he highlighted DHS' September 2019 *Security Strategic Framework for Countering Terrorism and Targeted Violence*, which calls for a whole-of-society approach to counteract this persistent threat to the homeland.

Administrator Pekoske highlighted Congress' establishment of the Cybersecurity Solarium Commission, a bipartisan, intergovernmental, and multisector body charged with evaluating divergent approaches to defending the United States in cyberspace. He noted that the Department is quite active on the commission, and that NSTAC members will be pleased with the resulting work. He also remarked how other DHS components, in addition to CISA, are working to safeguard the U.S. in the digital domain. For example, the U.S. Immigration and Custom Enforcement's Homeland Security Investigations Cyber Crime Center investigates cybercrimes like child exploitation, internet-facilitated arms proliferation, goods smuggling, and money laundering.

Administrator Pekoske discussed the importance of advisory bodies like the NSTAC. During its 37 years of service, the NSTAC's recommendations have allowed the United States to maintain a reliable, secure, and resilient national communications posture. In sum, the committee continues to provide a great example of how public and private partnerships serve the Nation.

He addressed some of the NSTAC's greatest achievements, including the: (1) establishment of the National Coordinating Center for Communications, which integrated into the National Cybersecurity and Communications Integration Center in 2009; (2) creation of the Network Security Information Exchange; and (3) development of the Telecommunications Service Priority System, all of which support information sharing between Government and its critical infrastructure partners. He mentioned the NSTAC's recent recommendation to establish a series of grand challenges as part of a larger Cybersecurity Moonshot. In response to this recommendation, CISA has partnered with industry and Government cybersecurity subject matter experts to determine possible next steps towards advancing these challenges.

Administrator Pekoske emphasized that China presents the most pressing long-term strategic threat to the Nation. For years, China has been steadily advancing its efforts to undermine the United States' vitality, national security, and international standing using a variety of means to acquire U.S.' intellectual capital. CISA recently unveiled a Chinese cyber hacking scheme where malicious actors working on behalf of the Chinese government had been carrying out a cyberattack campaign against managed service providers (MSP). These attacks not only targeted MSPs, but also their customers worldwide and across sectors (e.g., finance, banking, automotive, telecommunications). In response, CISA hosted a series of high-profile, public-facing webinars to address public concerns about Chinese malicious cyber activity. CISA is also finding ways to better coordinate with Government and industry on this issue through the FASC and the ICT SCRM Task Force.

While implementing 5G networks will result in improved bandwidth, capacity, and reliability of wireless broadband services, it will also bring new risks. As a result, Administrator Pekoske stressed the need for federal, state, and local government; industry; academia; and international partners to work together to promote a strong U.S. cybersecurity posture. Sharing that "cybersecurity is homeland security," he closed by thanking members and calling for continued vigilance.

Status Update on NSTAC Recommendations

Mr. Donovan invited Director Krebs to provide a high-level overview of the Government's implementation of NSTAC recommendations. Director Krebs affirmed that NSTAC recommendations were integral to Federal Government action on cybersecurity and national security and emergency preparedness (NS/EP) communications concerns.

He began by discussing the *NSTAC Report to the President on Internet and Communications Resilience* (ICR report) (November 2017), which directly influenced the development of the Administration's *National Cyber Strategy*. He remarked that the strategy was produced in response to EO 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, in 2017. The ICR report also reflects the importance of public-private partnerships in addressing cybersecurity policy. Director Krebs cited the Council to Secure the Digital Economy as an example of close public-private coordination. He reported that the council recently released a report entitled the *International Botnet and Internet of Things (IoT) Security Guide 2020*, a comprehensive set of strategies to protect the global digital ecosystem from the growing threat posed by botnets, malware, and distributed attacks.

Regarding the *NSTAC Report to the President on Information and Communications Technology Mobilization* (ICT Mobilization report) (November 2014), Director Krebs noted that the report highlights the importance of ICT incident response mechanisms. Since the publication of the report, the Government has made strides to update its incident response planning for cybersecurity events. The ICT Mobilization report's recommendations paved the way for the development of a *National Cyber Incident Response Plan*, which delineates the Government's activities during cyber crises. The ICT Mobilization report also recommended that the DHS convene a Cyber Unified Coordination Group, a representative group of organizations with specific roles and functions during a cyber crisis. This group would consist of ICT companies, also known as ICT enablers, and lead large-scale response efforts during significant cyber incidents.

Director Krebs noted the difference between incident management, or quick or direct containment, and consequence management, which deals with the longer-term impacts of incidents. He noted that the latter is an approach currently used by Government in the aftermath of physical or natural disasters. Director Krebs expressed a desire to implement a national-level consequence management approach for cybersecurity. In line with this goal, he looks forward to working with partners at the federal, state, and local levels to develop a consequence management doctrine, akin to the Federal Emergency Management Agency's *National Response Framework*. CISA is working to develop its equivalent plan within the next 18 months.

Director Krebs then discussed the *NSTAC Report to the President on Secure Government Communications* (August 2013). This report recommended that the Federal Government modernize Government network security and remove threatening technology services from the surrounding cyber ecosystem. Over the subsequent years, the Government published several binding operational directives (BOD) and founded the FASC to improve procurement processes for Government hardware and software assets. He noted that the largest concern going forward is providing counterintelligence and cybersecurity training to officials supporting said procurement process so that the Government does not need to issue more BODs like the one regarding Kaspersky products in 2017.

Director Krebs briefly mentioned the *NSTAC Report to the President on a Cybersecurity Moonshot* (November 2018), stating that its recommendations are not as easily actionable as other reports. However, events like the National Cybersecurity Moonshot Pillar Workshop, co-hosted by Unisys and Raytheon, November 20-21, 2019 in Auburn, AL, are important steps towards the potential implementation of cybersecurity prize challenge efforts.

DHS continues to prioritize Government innovation and use of emerging technologies, which the NSTAC discussed in its latest report, the *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem* (September 2019). Director Krebs stated that there is a significant opportunity for the United States and its allies to take advantage of 5G technologies in the coming years. The NSTAC also studied 5G adoption in its *NSTAC Report to the President on Emerging Technologies Strategic Vision* (July 2017). He noted that this report helped set the White House's research agenda around such cutting-edge technologies as 5G, artificial intelligence, and quantum computing.

Director Krebs noted that CISA is on the forefront of other emerging technologies, like IoT, which the NSTAC studied in its *NSTAC Report to the President on the Internet of Things* (November 2014). CISA works closely with industry to establish baseline security measures for IoT devices. He stated that the Federal Government should look to foreign government partners, including Australia and Great Britain, for best practices for labeling regimes that can help ensure the integrity and trust of IoT products.

According to Director Krebs, the recommendations in the *NSTAC Report to the President on Cloud Computing* (May 2012) directly informed the *Federal Cloud Computing Strategy*, also known as Cloud Smart. As the Government continues its cloud migration, it is imperative that the appropriate controls are in place to manage third-party risk for MSPs. DHS' legacy device-based cybersecurity monitoring capabilities, like EINSTEIN and email filtering, do not translate to the cloud. As a result, Director Krebs stated that the Government must focus on deploying software-based security tools that can function on cloud networks.

Director Krebs discussed the *NSTAC Report to the President on the National Security and Emergency Preparedness Implications of a Nationwide Public Safety Broadband Network* (May 2013), which influenced the First Responder Network Authority's efforts to implement a nationwide public safety network. Further, the NSTAC reinforced the need to fortify the resiliency of communications networks in the NSTAC *Report to the President on Communications Resiliency* (April 2011). Director Krebs stated that the Government continues to strengthen first responder communications systems, noting the importance of improved coordination with citizens during public safety cybersecurity incidents. This kind of engagement is also outlined in the *NSTAC Cybersecurity Collaboration Report* (May 2009), which laid out a path for Government to strengthen its partnerships for incident detection, prevention, mitigation, and response. Director Krebs offered election security as an example of Government efforts to work with industry (e.g., social media vendors) to detect adversaries and prevent the spread of misinformation.

Director Krebs mentioned that the NSTAC's older reports are still highly relevant. He specifically cited the *NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS)* (February 2008). Earlier this year, the GPS constellation clock was reset, which posed significant concerns regarding the impact first responder communications networks. As GPS receivers had previously relied on larger operational systems (e.g., Galileo) and networks run by Russian and Chinese entities, the Government is beginning to understand that the resilience of U.S.-based GPS is critical.

Director Krebs underscored the importance of providing NSTAC members with meaningful feedback on how the Government has derived value from their work. He offered thanks to the committee and said that he looks forward to their upcoming report on SDN.

Status Update: NSTAC Software-Defined Networking Subcommittee

Mr. Raymond Dolan, NSTAC Member, provided the group with a status update on the NSTAC SDN Subcommittee. He informed participants that the study will last approximately six months. During this period, the subcommittee will examine the importance of SDN, identify the related challenges and opportunities, and assess the current utilization of SDN and other virtualization technologies.

The subcommittee held its kickoff meeting in October 2019. Since then, the group has identified three categories for SDN 101 or baseline briefings: (1) industry trends; (2) architecture; and (3) security. Following these initial discussions, the subcommittee will seek insights from telecommunications service providers, telecommunications infrastructure providers, SDN technology developers, end-users, and cloud service providers. Within each key area, the subcommittee will ensure that security, risk mitigation, and the role of Government are continually addressed as part of the study's scope.

To promote transparency, NSTAC members will be invited to two SDN subcommittee meetings—one in January and one in March 2020—to offer their input on the direction of the report. Mr. Dolan added that the subcommittee also intends to provide a status update during the February 2020 Member Conference Call. By April 2020, the subcommittee will submit its final report to NSTAC members to review, in hopes of finalizing the document for vote by the next in-person meeting in May 2020.

Mr. Donovan emphasized the importance of this study, as it is the first to seriously consider the potential impacts of 5G-based, virtualized infrastructure. Director Krebs agreed, and asked the subcommittee to consider the implications of implementing trusted software on top of untrusted hardware, and the obstacles this may pose for the security of mission critical networks.

Mr. Donovan thanked Mr. Dolan for his remarks.

Closing Remarks and Adjournment

Mr. Donovan thanked Director Krebs for his update regarding the Government's implementation of the NSTAC's recommendations, noting that his remarks shed light on how the NSTAC has helped various Administrations address threats in an evolving technology landscape. Mr. Schneider added that the Government would work to provide more regular updates to members.

Mr. Donovan thanked Government partners for their insights, and his colleagues for their service on the NSTAC. Mr. Schneider also thanked the members for their efforts to make the country safer.

Director Krebs expressed his gratitude for being able to serve in a position that allows him to capture the Government's progress in using the NSTAC's recommendations. He thanked Mr. Dolan for his update on the SDN Subcommittee's efforts and the panelists for their work in securing the ICT supply chain. He also thanked Ms. James for her service as the NSTAC Chair, as well as Mr. Donovan and Mr. Charney for their continued leadership on the committee.

He reminded members that the next meeting would take place on February 20, 2020, from 2:00 to 3:00 p.m. Eastern Time via teleconference.

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

APPENDIX:
NSTAC Meeting Open Session Participants List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corporation
Mr. Robert Carrigan	Formerly of Dun & Bradstreet 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, LLC
Dr. Joseph Fergus	Communications Technologies, Inc.
Ms. Lisa Hook*	Neustar, Inc.
Ms. Renée James	Ampere Computing
Dr. Thomas Kennedy	Raytheon Company
Mr. Mark McLaughlin*	Palo Alto Networks, Inc.
Mr. Angel Ruiz	MediaKind
Mr. Jeffery Storey	CenturyLink, Inc.
NSTAC Member Points of Contact	
Mr. Jason Boswell	Ericsson, Inc.
Mr. Christopher Boyer	AT&T, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Mr. Michael Daly	Raytheon Company
Ms. Cheryl Davis	Oracle Corporation
Mr. Thomas Gann	McAfee, LLC
Mr. Jonathan Gannon	AT&T, Inc.
Ms. Katherine Gronberg	ForeScout Technologies, Inc.
Mr. Sean Morgan	Palo Alto Networks, Inc
Mr. Thomas Patterson	Unisys Corporation
Mr. Kevin Riley	Ribbon Communications, Inc.
Mr. Brett Scarborough	Raytheon Company
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Stephen Szeremeta	Avaya, Inc.
Mr. Milan Vlajnic	Communication Technologies, Inc.
Government Attendees	
Mr. Dwayne Baker	Department of Homeland Security
Ms. Sandy Benevides	Department of Homeland Security
Col. Dustin Bishop	Department of Defense
Rear Admiral Peter Brown	Executive Office of the President
Ms. Cheri Caddy	National Security Agency
Ms. DeShelle Cleghorn	Department of Homeland Security
Mr. Scott Friedman	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
Ms. Carolyn King	Department of Homeland Security
Mr. Christopher Krebs	Department of Homeland Security
Mr. Daniel Kroese	Department of Homeland Security
Mr. Brent Logan	Department of Homeland Security
Ms. Kayla Lord	Department of Homeland Security
Ms. Ginger Norris	Department of Homeland Security
Mr. David Pekoske	Department of Homeland Security
Mr. Kevin Reifsteck	National Security Council
Mr. Grant Schneider	National Security Council
Mr. Robert Strayer	Department of State
Ms. Bridgette Walsh	Department of Homeland Security

Other Attendees

Mr. Mark Bentley	Unisys Corporation
Mr. Bruce Byrd	AT&T, Inc.

Public Participants

Mr. Calvin Biesecker*	Defense Daily
Mr. Eric Geller	Politico
Mr. Zachary Israel	The Ferguson Group
Mr. Robert Mayer	USTelecom Association
Mr. Mark Rockwell	Federal Computer Week

Support Staff

Ms. Sheila Becherer	Booz Allen Hamilton, Inc.
Ms. Christina Berger	Booz Allen Hamilton, Inc.
Mr. Evan Caplan	Booz Allen Hamilton, Inc.
Ms. Laura Creel	Insight Technology Solutions, Inc.
Ms. Stephanie Curry	Booz Allen Hamilton, Inc.
Mr. Matthew Mindnich	Insight Technology Solutions, Inc.
Mr. Barry Skidmore	Insight Technology Solutions, Inc.
Ms. Aisha Toor*	Booz Allen Hamilton, Inc.

**Participated via teleconference*

Certification

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

Mr. John Donovan
NSTAC Chair