President's National Security Telecommunications Advisory Committee (NSTAC) Meeting Summary
May 6, 2021

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 May 2021 NSTAC Member Meeting was open to the public. She noted that no one had registered to provide comment during the meeting, but written comments would be accepted following the procedures outlined in the Federal Register Notice. Following roll call, Ms. Benevides turned the meeting over to Mr. John Donovan, NSTAC Chair.

Mr. Donovan welcomed the distinguished Government and industry partners in attendance, including: Mr. Jeffrey Greene, Acting Senior Director, Cyber Directorate, National Security Council (NSC); Mr. Brandon Wales, Acting Director, Cybersecurity and Infrastructure Security Agency (CISA), DHS; Mr. Michael Daniel, President and Chief Executive Officer, Cyber Threat Alliance; Mr. John Simms, Senior Technical Advisor, Office of the Chief Technology Officer, CISA, DHS; Mr. Scott Rose, Computer Scientist, National Institute for Standards and Technology (NIST); and Mr. John Kindervag, Senior Vice President of Cybersecurity Strategy and Group Fellow, ON2IT.

Mr. Donovan then reviewed the meeting agenda. He noted that the meeting would include: (1) opening remarks from the Administration and CISA on the Government's ongoing cybersecurity and national security and emergency preparedness (NS/EP) support efforts; (2) a keynote address from Mr. Daniel on ransomware's implications for national security; (3) a panel discussion on the NS/EP challenges to adopting zero-trust networking (ZTN); and (4) a deliberation and vote on the 2021 *NSTAC Report to the President on Communications Resiliency*.

Mr. Donovan also reviewed the outcomes of the February 10, 2021, NSTAC Member Conference Call (MCC). During the MCC, Ms. Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, NSC, offered remarks on the Administration's efforts to strengthen the United States' NS/EP communications posture. Acting Director Wales also spoke to CISA's strategies for securing the Nation's information and communications technology (ICT) ecosystem. Mr. Jeffrey Storey and Mr. Angel Ruiz, NSTAC Communications Resiliency (CR) Subcommittee Co-Chairs, then provided a progress update on the CR phase II study. Finally, NSTAC members deliberated, voted on, and unanimously approved the 2021 *NSTAC Letter to the President on NS/EP Communications Priorities*.

Mr. Donovan then invited Mr. Greene to provide opening remarks. Mr. Greene underscored his appreciation for the NSTAC's mission and charge, noting that he supported the committee

in its development of the 2014 *NSTAC Report to the President on the Internet of Things*. He stated that the Administration's cybersecurity approach is three-fold:

1. **Modernizing Cyber Defenses:** The U.S. Government is focused on transitioning from a proactive versus reactive cybersecurity posture. As a result, the Government is committed to investing in next-generation cybersecurity protection, breach prevention, and detection tools, rather than those centered solely on incident response. Mr. Greene stated that other prevention activities include security assessments, cyber hygiene, secure software acquisition, public-private information sharing, and modernizing federal information technology (IT) systems. He also encouraged the private sector to find ways to improve its quality control processes as this will ensure software security from development to deployment, as well as bolster the overall strength of the supply chain.
2. **International Leadership:** The U.S. Government must collaborate with its allies to respond to global adversaries who leverage ICT in a malicious manner. Mr. Greene explained that working with international partners will allow the United States to better protect its critical infrastructure and lead in standards development, both of which are key to promoting the Nation's cybersecurity.
3. **Private Sector Collaboration:** Promoting public-private partnerships and elevating the importance of robust information sharing mechanisms like the NSTAC are also important for improved cybersecurity posture. Through these partnerships, the U.S. Government can expand the development of network monitoring tools capable of detecting and preventing bad actors from gaining access to mission-critical IT systems.

Mr. Greene concluded by emphasizing the need for continued collaboration with the NSTAC and thanked the committee for its work on the Communications Resiliency report.

Mr. Donovan then turned the floor to Acting Director Wales. Acting Director Wales stated that CISA is pleased that the new Administration has continued to prioritize the Nation's cybersecurity. To this end, CISA is also working hard to "build back better" following a series of wide-scale compromises, like the SolarWinds and Microsoft Exchange Server breaches. He noted that achieving this goal requires strong collaboration between the public and private sectors at home and abroad. Acting Director Wales informed attendees that the President has nominated Ms. Jen Easterly, Morgan Stanley, for the CISA Director role. In response, CISA has started to engage Ms. Easterly on the agency's ongoing initiatives in anticipation of her confirmation.

Acting Director Wales continued that CISA recently concluded National Supply Chain Integrity Month, which focused on raising awareness of the role that trusted supply chains play in keeping the Nation safe, secure, and resilient. In the wake of recent high-impact cybersecurity incidents, the Government's work to secure the complex IT supply chain is crucial to securing critical infrastructure moving forward. Acting Director Wales stated that the NSTAC has provided key recommendations related to supply chain security in the past, including in the 2020 *NSTAC Report to the President on Software-Defined Networking* and the 2019 *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem*. He also noted that CISA continues to examine emergent supply chain risks

through the ICT Supply Chain Risk Management Task Force, which addresses salient issues pertaining to ICT supply chain security. In recent publications, the Task Force has provided important guidance on such areas as product evaluations, qualified bidder lists, and assurance, all of which are critical components to end-to-end supply chain integrity.

Acting Director Wales stated that CISA is working to provide guidance on transitioning legacy IT systems to more secure frameworks like zero-trust. Similarly, the NSTAC highlighted the need for modernizing Government IT systems in its 2017 *NSTAC Report to the President on Internet and Communications Resilience*. In conclusion, he complemented the committee for organizing an impactful agenda and expressed his thanks for the Communications Resiliency report.

Mr. Donovan thanked Acting Director Wales for his comments.

Keynote Address: Ransomware as a National Security Threat: Implications for NS/EP Communications

Mr. Donovan welcomed Mr. Daniel and invited him to provide his keynote address.

Mr. Daniel opened by noting that threats to critical infrastructure will continue to grow as "crimeware-as-a-service" becomes more widespread. He explained that ransomware attacks have increased in their severity over the last decade. To combat this threat, he called for Government to build: (1) a more comprehensive system of deterrence; (2) disruptive practices and processes; (3) more resilient infrastructure; and (4) greater options for victim recourse.

To accomplish these goals, Mr. Daniel proposed four areas of excellence in which the U.S. Government and industry could work together to mitigate the adverse effects of ransomware:

1. **Prioritization:** Mr. Daniel explained that, with proper prioritization, institutions will be better suited to pursue cyber criminals in a logical way. The Administration has begun this process through the establishment of a series of "cybersecurity sprints," which target specific improvements across each critical infrastructure sector. Part of prioritization is also modernizing corporate culture to the point where ransomware—and the methods to combat it—are engrained in workforce training.
2. **Resilience:** Mr. Daniel noted that, to ensure resiliency, organizations need access to a wider variety of tools to detect, respond to, and mitigate threats, like ransomware. As larger criminal organizations and nation-states continue to execute ransomware attacks, the threat to NS/EP communications will continue to grow. Thus, Mr. Daniel urged the telecommunications sector to find ways to optimize the defense of national communications infrastructure through target hardening and better education for their workforces.
3. **Collaboration:** Mr. Daniel stressed that collaboration within the communications sector is another key component for combating ransomware. Several new channels, such as a joint ransomware task force or private sector ransomware hub, could be useful in this regard. He

stated that mechanisms like these would raise the scope and scale of ransomware disruption.

4. **Creativity:** Mr. Daniel described how institutions should work to implement better methods to identify and prosecute bad actors executing ransomware attacks. As many countries provide a haven to ransomware criminals, the United States must devise new ways to hold them accountable. In addition, a creative approach towards making ransomware less profitable is key to long-term security and resilience.

Mr. Scott Charney, NSTAC Vice Chair, asked Mr. Daniel to confirm if the following three focus areas summarize his recommendations for combating ransomware: (1) better literacy in IT security; (2) consistent use of secure data backups; and (3) improved international relations to pursue cyber criminals. Mr. Daniel confirmed Mr. Charney's characterizations and added that cryptocurrency is the foundation of the ransomware market, which means that greater partnerships with the crypto industry will help combat this persistent threat.

Mr. David DeWalt, NSTAC Member, commented that small- and medium-sized businesses (SMB) are consistent targets for ransomware attacks. He highlighted the need to better educate SMBs, schools, hospitals, and similar organizations on the threat and how to respond. Mr. Daniel concurred with Mr. DeWalt's remarks, and further reiterated the importance of engaging smaller-scale and other, non-traditional soft targets.

Mr. Mark McLaughlin, NSTAC Member, asked if Mr. Daniel thought if any allies had a better ransomware response strategy than the United States. Mr. Daniel noted that the United States is still at the forefront in this area. He commented that criminals have traditionally targeted the United States given its economic prominence. Also, since the U.S. Government does not back insurance claims made against ransomware, the Government could explore ways to assist. He proposed the development of policies or regulations that encourage insurance providers to cover liabilities after an attack.

Hearing no further questions, Mr. Donovan thanked Mr. Daniel for his remarks.

Panel Discussion: The NS/EP Challenges to Adopting ZTN

Mr. Donovan turned the meeting over to Mr. Jack Huffard, NSTAC Member, to moderate the panel discussion on the NS/EP challenges to adopting ZTN.

Mr. Huffard began by introducing Mr. Kindervag, Mr. Rose, and Mr. Simms to the attendees. He then stated that ZTN is an architectural strategy for improving enterprise security that considers inherent trust to be a vulnerability. He noted that Mr. Kindervag developed the ZTN concept in his 2010 paper, *Build Security Into Your Network's DNA: The ZTN Architecture*. Similarly, Mr. Rose served as a co-author for NIST's 2020 Special Publication (SP) 800-207: *Zero-Trust Architecture*. Since then, both the public and private sectors have worked to adopt the ZTN framework and assess how it will impact their existing systems.

Mr. Huffard asked Mr. Simms to provide an overview of the Government's perspective on zero-trust. Mr. Simms stated that the 2015 Office of Personnel Management data breach made

Government leaders realize how vulnerable stored data is to exfiltration. After the breach, DHS determined that many departments and agencies (D/A) were storing high-value asset data on networks with limited security protocols. In response, DHS modernized the Trusted Internet Connections (TIC) Program to help federal D/As create modern network architectures that utilize multiple layers of security. He concluded that, while the TIC Program is effective, the SolarWinds attack highlighted the need for D/As to adopt zero-trust architectures to better secure their networks.

Next, Mr. Huffard requested that Mr. Kindervag discuss industry's lessons-learned from deploying ZTN. Mr. Kindervag defined zero-trust as a strategy that prevents unauthorized lateral movement on a network. In this context, trust on a network is both a vulnerability and a tool for exploitation. Once threat actors obtain trusted status on a network, they can then use that status as a platform for attack. To correctly implement zero-trust, Mr. Kindervag said that an organization needs to consider four design principles and implement five steps for deployment. He defined the design principles as: (1) determining what the organization is trying to achieve; (2) designing the core first and building the remainder of the network out from there, adding security controls in at each layer; (3) controlling access to data on a need-to-know basis; and (4) inspecting and logging all traffic in real-time and at all layers of the network stack. Similarly, the five deployment steps are: (1) defining what the network needs to do; (2) understanding what data transactions are needed to support the network's intended functions; (3) building the network to facilitate those operations; (4) creating a zero-trust policy; and (5) continuously monitoring and maintaining security.

Mr. Huffard asked Mr. Rose to outline SP 800-207's key findings and discuss how organizations can successfully adopt this guidance on NS/EP communications networks. Mr. Rose said that SP 800-207 had three intended purposes. First, the guidance seeks to help federal D/As understand the zero-trust concept and determine what capabilities are needed to recreate that environment on their networks. Second, SP 800-207 highlights existing efforts within Government that could help D/As design and successfully deploy ZTN approaches. Third, the document identifies gaps or interoperability issues that D/As might experience when leveraging ZTN models. Mr. Rose concluded that NIST considers SP 800-207 to be a baseline framework and not a complete roadmap to deploying ZTN models.

Mr. Huffard asked how Government and industry can successfully adopt ZTN. Mr. Kindervag said that organizations should start by defining the assets they need to protect and build a zero-trust security structure around them. To do this, organizations should first apply zero-trust principles to specific components instead of immediately converting their entire network to the new environment. Mr. Rose said that the ZTN designer should also consult with enterprise system users in order to understand how the network operates. This collaborative approach will ensure that the new zero-trust architecture does not interfere with current system functions.

Mr. Huffard asked what key challenges organizations will face when adopting ZTN. Mr. Simms stated that zero-trust is a strategy, not a tool. As a result, organizations will need to

take incremental steps to develop and enforce that strategy on their systems. Mr. Rose added that the need to retain legacy systems that are compatible with ZTN will be a significant hurdle to achieving a fully zero-trust environment. Mr. Kindervag added that many organizations are resistant to changing how their systems operate. That said, the zero-trust concept can seem like an overwhelming modification.

Mr. Huffard asked how deploying ZTN may differ between Federal Government and private sector enterprises. Mr. Kindervag said that private sector companies will adopt ZTN much faster than Government entities as industry has a financial incentive to do so. Mr. Rose remarked that D/As need to prioritize security in base system design instead of after deployment. Mr. Simms stated that D/As will need to establish long-term policies and maintain consistent leadership around the issue to make ZTN a reality.

Mr. Donovan thanked Mr. Huffard and the panelists for their contributions.

Deliberation and Vote: *NSTAC Report to the President on Communications Resiliency*

Mr. Donovan invited Mr. Storey and Mr. Ruiz to discuss the key findings and recommendations in the 2021 Communications Resiliency Report.

Mr. Storey noted that the subcommittee found that modern networking technologies will significantly increase the Nation's overall resilience, as well as position the economy to achieve operational efficiencies in next-generation technologies. He stated that the report also discussed how adversaries and a weakened ICT ecosystem will pose challenges to the United States' NS/EP communications resiliency in the next 8 to 10 years. Mr. Storey highlighted the importance of Government and industry adopting and mastering next-generation ICT to achieve national security, economic security, and emergency preparedness goals. To this end, the report complements the Administration's current cybersecurity priorities and efforts to establish the United States as a leader in the global ICT ecosystem.

Mr. Ruiz then outlined the report's key findings. Specifically, he noted the NSTAC discovered that:

- The increased density of wireless satellite and wireline networks has resulted in better service delivery and connectivity to a broader range of locations and devices;
- The increased integration of enterprises and customers into cloud/edge environments presents risks that will require more secure supply chains and enhanced partnerships between enterprises and suppliers;
- Quantum computing offers great potential in terms of network efficiencies, security, and encryption; and
- Public-private partnerships and standard bodies will be essential in ensuring that the United States continues to succeed in network implementation and overall resiliency.

Mr. Ruiz explained that the NSTAC's recommendations are presented in four major categories, including:

1. **Public-private planning, consultation, and risks assessments**, which helps to bolster resilience through stronger ties between industry and Government;
2. **Supporting the deployment of future networks**, which ensures users and architects alike benefit from safe, secure, and reliable technology solutions;
3. **Supporting the adoption of key technologies**, which guides the Administration in making informed, thoughtful decisions on cyber strategy and policy; and
4. **Utilizing testbeds to enable mastery of quantum and artificial intelligence technologies**, which promotes a more robust NS/EP posture in the face of emerging technological threats.

Mr. Ruiz and Mr. Storey then summarized the committee's recommendations within each category. Specifically, they noted the NSTAC recommends that:

- The U.S. Government should: (1) evaluate ways to strengthen NS/EP public-private partnerships both domestically and abroad; (2) create a whole-of-Nation strategy for next-generation Internet Protocol development; and (3) push forward a national strategy for cyber resilience on critical systems that addresses post-quantum cryptography.
- The Executive Branch should: (1) contract with a federally-funded research and development center to create and manage a quantum "sandbox," including a post-quantum cryptography testbed; and (2) coordinate with federal D/As to enhance awareness regarding quantum computing benefits.
- Government and industry should: (1) leverage and expand availability for quantum computing capabilities; and (2) research ways to mitigate near-future quantum computing threats.

Mr. Storey ceded the floor to Mr. Donovan to facilitate the deliberation and vote of the Communications Resiliency report.

Mr. Donovan thanked Mr. Ruiz and Mr. Storey for their overview. Hearing no questions from attendees, he made a motion to approve the report. Following this motion, NSTAC members unanimously approved the report for transmission to the President.

Mr. Donovan thanked the subcommittee for their contributions to the report. He also stated that he looks forward to seeing how the Government implements the recommendations contained therein.

Closing Remarks and Adjournment

Mr. Donovan asked Mr. Greene if he had any final remarks. In closing, Mr. Greene officially tasked the NSTAC with the "Enhancing Internet Resilience in 2021 and Beyond" study, which will be a multi-phased effort lasting 18 months total. During the study, he explained that the NSTAC would establish four separate subcommittees focused on: (1) software assurance; (2) zero-trust and trusted identity management; (3) the IT/operational technology convergence; and (4) increasing trust in ICT and services supply chains. The goal of the study will be to

provide the Administration recommendations on how the U.S. Government can overcome the challenges and embrace associated opportunities for long-term internet resiliency.

Mr. Donovan thanked Mr. Greene and noted that the topic merits the committee's expertise. He then accepted the new study tasking on behalf of the NSTAC.

Mr. Donovan asked Acting Director Wales to provide his closing remarks. Acting Director Wales stated that the NSTAC can provide timely, actionable expertise via this new study. In particular, he noted that the he looked forward to the committee's insights as to how Government—and CISA in particular—can better structure its approach to important NS/EP challenges in the future. He also thanked the CR Subcommittee for their efforts on the Communications Resiliency report. In particular, he underscored that CISA is eager to work on implementing several of the report's recommendations, including those that allow the agency to partner with other D/As focused on promoting resiliency in disaster (e.g., Federal Emergency Management Agency).

Mr. Donovan thanked NSTAC members and Government partners for the input they provided during the meeting, paying a special thanks to those who supported the development of the Communications Resiliency report. He also noted that, in the coming weeks, the NSTAC team will contact NSTAC members to identify volunteers to support the new study and schedule the phase I kickoff meeting.

Mr. Donovan announced that the next NSTAC meeting will be held via conference call on August 17, 2021. He then made a motion to close the meeting. Upon receiving a second, Mr. Donovan thanked participants and officially adjourned the meeting.

APPENDIX
May 6, 2021, NSTAC Meeting Participants List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corp.
Mr. William Brown	L3 Harris Technologies, Inc.
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	Communications Technologies, Inc.
Mr. Patrick Gelsinger	Intel Corp.
Ms. Lisa Hook	Two Island Partners, LLC
Mr. Jack Huffard	Tenable Holdings, Inc.
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	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
Mr. Christopher Young	Microsoft, Inc.
NSTAC Points of Contact	
Mr. Christopher Anderson	Lumen Technologies, Inc.
Mr. Jason Boswell	Ericsson, Inc.
Mr. Christopher Boyer	AT&T, Inc.
Mr. Jamie Brown	Tenable, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Ms. Cheryl Davis	Oracle Corp.
Mr. Thomas Gann	McAfee Corp.
Mr. Jonathan Gannon	AT&T, Inc.
Mr. Jonathan Goding	Raytheon Technologies Corp.
Ms. Kathryn Gronberg	CrowdStrike, Inc.
Mr. Robert Hoffman	Broadcom, Inc.
Ms. Ilana Johnson	Neustar, Inc.
Mr. Kent Landfield	McAfee Corp.
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Thomas Patterson	Unisys Corp.
Mr. Thomas Quillin	Intel 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.
Mr. Kent Varney	Lockheed Martin Corp.
Ms. Claire Vishik	Intel Corp.
Mr. Milan Vlajnic	Communications Technologies, Inc.

Other Attendees

Mr. Michael Daniel	Cyber Threat Alliance
Mr. John Kindervag	ON2IT BV

Government Participants

Ms. Sandy Benevides	Department of Homeland Security
Mr. Billy Bob Brown, Jr.	Department of Homeland Security
Ms. Desiree Chavis	Department of Homeland Security
Ms. Alaina Clark	Department of Homeland Security
Ms. DeShelle Cleghorn	Department of Homeland Security
Mr. Jonathan Dunn	Department of Homeland Security
Mr. Bruce Fitzgerald	First Responder Network Authority
Mr. Trent Frazier	Department of Homeland Security
Ms. Ashley Freitas	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. Jeffrey Greene	National Security Council
Mr. Robert Greene	Department of Homeland Security
Ms. Julia Hanson Takyi	Department of Homeland Security
Ms. Carole House	National Security Council
Ms. Helen Jackson	Department of Homeland Security
Dr. Sherry Lakes	National Security Agency
Mr. Jason Mayer	Department of Homeland Security
Mr. Michael Miron	Department of Homeland Security
Mr. Amit Mital	National Security Council
Ms. Renee Murphy	Department of Homeland Security
Dr. David Mussington	Department of Homeland Security
Ms. Tiffany Perry	First Responder Network Authority
Mr. Scott Rose	National Institute of Standards and Technology
Mr. Brian Scott	National Security Council
Ms. Katherine Siefert	Department of Homeland Security
Mr. John Simms	Department of Homeland Security
Ms. Brittany Trotter	Department of Homeland Security
Mr. Brandon Wales	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. Ryan Garnowski	Insight Technology Solutions, LLC
Ms. Laura Penn	Insight Technology Solutions, LLC
Mr. Barry Skidmore	Insight Technology Solutions, LLC

Public and Media Participants

Mr. William Barnett	Booz Allen Hamilton, Inc.
Ms. Mariam Baksh	Nextgov
Ms. Christina Berger	Booz Allen Hamilton, Inc.
Mr. Calvin Biesecker	Defense Daily
Mr. Jason Boose	Government of Canada
Mr. Christopher Castelli	Booz Allen Hamilton, Inc.
Mr. Aaron Edelstein	Tenable, Inc.
Ms. Leigh Francia	Morgan, Lewis, & Bockius, LLP
Ms. Sara Friedman	Inside Cybersecurity
Mr. Eric Geller	Politico
Mr. James Hayes	Tenable, Inc.
Mr. Jory Heckman	Federal News Network
Ms. Linda Johnson	Lumen Technologies, Inc.
Ms. Laura Karnas	Booz Allen Hamilton, Inc.
Mr. Aaron Kiesler	Lewis-Burke Associates, LLP
Ms. Jasmine Newby	Tenable, Inc.
Ms. Susan Nunziata	Tenable, Inc.
Mr. Scott Poretsky	Ericsson, Inc.

Certification

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

Mr. John Donovan
NSTAC Chair