President's National Security Telecommunications Advisory Committee (NSTAC)
Member Conference Call (MCC) Summary
February 10, 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 and welcomed participants. 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 that one member of the public—Mr. Kermit Kubitz—had registered to provide comment later on in the meeting. Similarly, Ms. Benevides explained that written comments would be accepted at any time through the procedures outlined in the meeting's Federal Register Notice. Following roll call, she turned the meeting over to Mr. John Donovan, NSTAC Chair.

Mr. Donovan opened the meeting and welcomed the senior Government partners in attendance, including Ms. Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, National Security Council (NSC); and Mr. Brandon Wales, Acting Director of the Cybersecurity and Infrastructure Security Agency (CISA), DHS.

Mr. Donovan then reviewed the meeting agenda. In addition to the public comment period, he noted that the February 10, 2021, NSTAC MCC would include: (1) remarks from Ms. Neuberger and Acting Director Wales regarding the Government's ongoing cybersecurity and national security and emergency preparedness (NS/EP) efforts; (2) an update from the Communications Resiliency (CR) Subcommittee; and (3) a deliberation and vote on the *NSTAC Letter to the President on NS/EP Communications Priorities* (NS/EP Communications Priorities Letter). Mr. Donovan also reviewed the outcomes from the last member meeting held on November 12, 2020. Specifically, he outlined the NSTAC CR Subcommittee's progress, as well as the Government's priorities and efforts regarding the information and communications (ICT) ecosystem. After providing this overview, Mr. Donovan invited Ms. Neuberger to provide her opening remarks.

Discussing Administration priorities, Ms. Neuberger stated that the Government is focused on improving ICT security after the SolarWinds attacks by using modernized defenses in cyberspace and defining measurable outcomes to reduce the risk of future attacks. The Administration is also working to: (1) promote international engagement, as foreign allies and partnerships are a critical component of ensuring network resiliency; and (2) address U.S. competition in cyberspace. Ms. Neuberger stated she looks forward to working with the private sector on these priorities moving forward. Mr. Donovan thanked Ms. Neuberger for her remarks and turned the meeting over to Acting Director Wales.

Acting Director Wales noted that the Senate had confirmed Mr. Alejandro Mayorkas, DHS, as the Secretary for Homeland Security on February 2, 2021. He expressed that Secretary Mayorkas' leadership will be beneficial to the Department, as he is already extremely engaged

in CISA's work and is seeking out ways to promote DHS' cybersecurity priorities with the new Administration. Acting Director Wales stated that CISA routinely leverages the NSTAC's recommendations in its work. He further remarked that the NS/EP Communications Priorities Letter highlights the NSTAC's intrinsic value and helps map out a path forward for collaboration between the committee and the Government in the immediate- and longer-term.

Acting Director Wales said that the Nation's coronavirus (COVID-19) response continues to be a top priority for the agency. To this end, CISA has supported the vaccine deployment nationwide by providing its expertise in risk analysis and threat mitigation.

As the Nation's risk advisor, CISA remains focused on its mission of protecting the ICT ecosystem and mission-critical supply chains. For example, Acting Director Wales called out the ICT Supply Chain Risk Management Task Force's 2020 *Year Two Report: Status Update on Activities and Objectives of the Task Force*, which summarizes the task force's progress in examining supply chain resiliency in the wake of COVID-19. He informed participants that, on February 4, 2021, CISA announced the six-month extension of the task force's charter. This extension—effective through July 2021—ensures continued collaboration between Government and industry on essential supply chain efforts. Specifically, in 2021, the task force will focus on ensuring software and hardware supply chain integrity, similar to the 2020 *NSTAC Report to the President on Software-Defined Networking*.

Acting Director Wales noted the January 19, 2021, release of the *National Strategy to Secure 5G Implementation Plan*. CISA has developed its own strategy for safeguarding fifth generation (5G) networks, which aligns with the White House's approach and larger implementation plan. He stated that CISA continues to review the NSTAC's previous recommendations on 5G to support its NS/EP communications efforts.

Mr. Donovan thanked Acting Director Wales for his remarks.

Status Update: NSTAC CR Subcommittee

Mr. Donovan invited Mr. Jeffrey Storey and Mr. Angel Ruiz, NSTAC Members and CR Subcommittee Co-Chairs, to provide an update on the subcommittee's phase II effort.

Mr. Storey explained that the purpose of the study is to conduct a broad, forward-looking examination of the resiliency of the Nation's ICT infrastructure 8 to 10 years into the future. He noted that the subcommittee leveraged information from the 2011 *NSTAC Report to the President on Communications Resiliency*, as well as its recent work on emerging technologies to scope the study. Currently, the subcommittee is focused on developing recommendations that can help position the U.S. ICT environment in a way that will support the country's national and economic security goals in the future. Mr. Storey then invited Mr. Ruiz to discuss the subcommittee's recent progress.

Mr. Ruiz stated that, since October of 2020, the subcommittee received over 30 briefings on a variety of topics including quantum computing, edge technology, and artificial intelligence. As

such, the subcommittee is using these inputs to build out the report outline. Mr. Ruiz noted that NSTAC members had the opportunity to provide direct feedback on the scope of the report during a recent subcommittee meeting. He thanked members for their insight and said this input will be helpful going forward.

Mr. Ruiz concluded that NSTAC members will deliberate and vote on the 2021 *NSTAC Report to the President on Communications Resiliency* during the May 2021 NSTAC Meeting.

Mr. Donovan thanked Mr. Storey and Mr. Ruiz for their remarks.

Public Comment Period

Mr. Donovan invited Mr. Kubitz to provide his comments.

Mr. Kubitz suggested that the NSTAC revisit the content in the NS/EP Communications Priorities Letter to:

- Address the recent SolarWinds compromise;
- Recommend the establishment of several multidisciplinary cyber institutes across the country;
- Outline cybersecurity best practices for Government, to include guidelines for protecting essential ICT networks and facilities;
- Prioritize and protect targets of potential cyber attacks in the public and private sectors;
- Identify available subject matter expertise in the public and private sectors capable of supporting NS/EP communications resilience; and
- Align NSTAC efforts with the National Infrastructure Advisory Council's recommendations on software, supply chain, and operational intelligence.

Mr. Donovan thanked Mr. Kubitz for his feedback.

Deliberation and Vote: *NSTAC Letter to the President on NS/EP Communications Priorities*

Mr. Donovan stated that, in December 2020, the NSTAC began drafting the NS/EP Communications Priorities Letter in order to: (1) explain the NSTAC's mission and expertise it can provide to the Administration; (2) summarize its recent work and recommendations; and (3) outline potential future studies the committee could pursue to advance the Nation's NS/EP priorities.

Mr. Donovan noted that, as the United States has become increasingly dependent on ICT for its economic continuity and security, it is challenged by a number of adversaries who have been able to compromise critical supply chains; steal intellectual property; interfere in elections; and make significant strides towards capturing global ICT market share. To help address these risks, NSTAC members regularly engage with Government counterparts on high-priority NS/EP communications topics to help inform policy initiatives. For example,

during the November 2020 NSTAC Meeting, members held a discussion on semiconductor supply chain issues from which several significant insights emerged. Mr. Donovan noted that this is a critical matter that requires further discussion.

Mr. Donovan stated that the NSTAC's previous reports contain untapped recommendations that can support the Administration's NS/EP efforts. In particular, he cited that:

- The 2017 *NSTAC Report to the President on Internet and Communications Resilience* offered several ideas to improve cybersecurity including accelerating the adoption of cybersecurity guidelines, promoting supply chain assurance, and raising the costs to cyber threat actors.
- The 2018 *NSTAC Report to the President on a Cybersecurity Moonshot* called for the U.S. Government to champion a whole-of-Nation effort to assure digital trust, safety, and resilience for all Americans, as well as provided actionable steps to organize, direct, resource, and empower these initiatives.
- The 2019 *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem* cited the Nation's growing critical dependencies on emerging technologies, and identified the need for a cohesive cross-agency strategic plan to address the issue of trusted manufacturers.

The letter also summarized several potential study topics, such as:

- The convergence of information and operational technologies, which would address the potential opportunities and security issues created by industry's efforts to use Internet of Things devices and 5G wireless connectivity to monitor, analyze, and manipulate industrial assets and data.
- An emerging technologies strategic assessment, which would consider how next-generation technologies are impacting the ICT ecosystem, the United States' position in the global marketplace, and what national policies the Government could introduce to promote U.S. leadership, competitiveness, and resilience.

Finally, Mr. Donovan noted that, in the letter, the NSTAC invites the President to attend the May 2021 NSTAC Meeting to discuss these issues and accelerate the process by which the committee can serve the Administration.

Mr. Donovan then opened the floor to comments. Ms. Neuberger said that the NSTAC is an excellent example of a successful public-private partnership. She asked for attendee insights on what challenges exist in fostering this type of collaboration and what might be done to resolve these issues.

Mr. Donovan remarked that the NSTAC is trying to create an agile study process to be more responsive to Administration priorities. Mr. Mark McLaughlin, NSTAC Member, added that the NSTAC is comprised of individuals whose expertise aligns well with the Administration's priorities. Further, he noted that the NSTAC previously developed a list of five criteria to ensure committee studies provide value to the Administration. These criteria dictate that NSTAC

studies should be Presidential, strategic, new, unique, and actionable. He maintained that these criteria have allowed for several NSTAC recommendations to become policy.

Ms. Renée James, NSTAC Member, stated that the NSTAC has considered conducting short-term and long-term studies in tandem to better meet the needs of the Administration. She highlighted that NSTAC members' direct engagement with the Government is critical to turning industry recommendations into policy.

Mr. David DeWalt, NSTAC Member, spoke to the risks posed to the NS/EP supply chain by foreign telecommunications service providers, noting the limitations in leveraging third-party components in support of mission-critical communications between Government and industry partners. He added that these risks are eminent dangers to the software ecosystem. As such, Mr. DeWalt suggested that the Committee on Foreign Investment in the United States and the Department of the Treasury conduct cyber audits on outsourced ICT contracts to combat threats posed by foreign suppliers.

Mr. Scott Charney, NSTAC Vice Chair, said that it is critical for the United States to understand how foreign countries are addressing cybersecurity threats. He noted that the close coordination between foreign Government and industry produces an advantage that will be difficult for the United States to overcome. Leveraging lessons learned and tools provided by global partners, the NSTAC and the Administration should work together to identify potential areas for partnership and a common set of objectives to confront known and emergent cybersecurity issues. As a result, this partnership could provide numerous benefits, as long as focus is maintained on ensuring U.S. competitiveness in the face of growing geopolitical tensions and new adversaries.

Ms. Neuberger reflected on how the NSTAC's almost 40-year tenure has allowed the committee to observe the evolution of technology, vulnerabilities, and international allies/adversaries. This experience has provided an in-depth knowledge and awareness of topics that require urgency. She stated that the NSTAC is an essential partner in supporting resilient and secure NS/EP communications. Therefore, the Administration will work with the committee to ensure that it can achieve its goal of producing impactful work on key cybersecurity and emerging technology challenges.

Mr. Donovan then made a motion to vote on the NS/EP Communications Priorities Letter. Members voted to unanimously approve the letter for transmission to the President.

Mr. Donovan thanked everyone who contributed to this effort.

Closing Remarks and Adjournment

Mr. Donovan thanked NSTAC members and Government partners for attending the meeting and supporting the development of the NS/EP Communications Priorities Letter. He also thanked the CR Subcommittee for its efforts. Likewise, Ms. Neuberger thanked attendees and noted that she looks forward to hearing more on potential NSTAC study topics and growing

the Administration's partnership with NSTAC and CISA. Acting Director Wales thanked NSTAC members for their feedback and reiterated the importance of public-private partnerships.

Mr. Donovan announced that the next NSTAC meeting will be held on May 6, 2021. Additional information on this meeting is forthcoming.

Mr. Donovan asked for a motion to close the meeting. Upon receiving a second, he thanked participants and officially adjourned the February 10, 2021, NSTAC MCC.

APPENDIX
February 10, 2021, NSTAC MCC Participant 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, LLC
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	Formerly of Neustar, Inc.
Mr. Jack Huffard	Tenable Holdings, 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. Stephen Schmidt	Amazon Web Services, Inc.
Ms. Kay Sears	Lockheed Martin Corp.
Mr. Gary Smith	Ciena Corp.
Mr. Jeffrey Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
Mr. Christopher Young	Microsoft Corp.
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.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	Lumen Technologies, 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. Ilana Johnson	Neustar, Inc.
Mr. Michael Kennedy	VMware, Inc.
Mr. Kent Landfield	McAfee, LLC
Mr. Sean Morgan	Palo Alto Networks, Inc.
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.

Government Participants

Mr. Dwayne Baker	Department of Homeland Security
Ms. Sandy Benevides	Department of Homeland Security
Ms. Alaina Clark	Department of Homeland Security
Ms. DeShelle Cleghorn	Department of Homeland Security
Ms. Deirdre Gallop-Anderson	Department of Homeland Security
Mr. Robert Greene	Department of Homeland Security
Ms. Helen Jackson	Department of Homeland Security
Mr. Enrique Matheu	Department of Homeland Security
Mr. Scott McConnell	Department of Homeland Security
Ms. Renee Murphy	Department of Homeland Security
Ms. Anne Neuberger	National Security Council
Mr. Brian Scott	National Security Council
Ms. Brittney Trotter	Department of Homeland Security
Mr. Christopher Visosky	Department of State
Mr. Brandon Wales	Department of Homeland Security
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.
Mr. Evan Caplan	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. David Aschkinasi	Law Office of David Aschkinasi, LLC
Ms. Christina Ayiotis	No Affiliation Provided
Mr. Frank Bajak	The Associated Press
Ms. Mariam Baksh	Nextgov
Mr. Reginald Barringer	CBS News
Ms. Christina Berger	Booz Allen Hamilton, Inc.
Mr. Calvin Biesecker	Defense Daily
Mr. Neil Cohen	Emerald Development Managers, LP
Mr. Thomas Conway	BlueVoyant, LLC

Mr. John Dermody	O'Melveny & Myers, LLP
Mr. Adam Dobell	Embassy of Australia
Ms. Sara Friedman	Inside Cybersecurity
Mr. Eric Geller	Politico
Mr. Marilu Goodyear	The University of Kansas
Mr. Joshua Grelle	Beacon Global Strategies, LLC
Mr. Peter Harter	The Farrington Group
Mr. Jory Heckman	Federal News Network
Ms. Kathryn Ignaszewski	IBM Corp.
Mr. Albert Kammler	Van Scoyoc Associates, Inc.
Ms. Laura Karnas	Booz Allen Hamilton, Inc.
Mr. Justin Katz	Federal Computer Week
Ms. Kirsten Koepsel	Self-Employed
Ms. Norma Krayem	Van Scoyoc Associates, Inc.
Mr. Kermit Kubitz	No Affiliation Provided
Mr. Thomas Leithauser	Wolters Kluwer N.V.
Ms. Flora Lethbridge-Çejku	Zeichner Risk Analytics
Mr. Robert Mayer	U.S. Telecom Association
Ms. Vonya McCann	Retired
Ms. Geneva Sands	CNN
Ms. Mary Saunders	American National Standards Institute
Mr. Aaron Schaffer	The Washington Post
Ms. Nicole Sganga	CBS News

Certification

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

Mr. John Donovan
NSTAC Chair