President's National Security Telecommunications Advisory Committee (NSTAC) Member Conference Call (MCC) Summary
August 17, 2021

Call to Order and Opening Remarks

Ms. Sandy Benevides, NSTAC Designated Federal Officer, Department of Homeland Security (DHS), 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 August 2021 NSTAC MCC was open to the public. She explained that one member of the public had registered to provide comment during the meeting, and 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 partners in attendance, including Mr. Jeffrey Greene, Acting Senior Director, Cyber Directorate, National Security Council (NSC); Ms. Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (CISA), DHS; and Mr. Kevin Stine, Chief Cybersecurity Advisor, National Institute of Standards and Technology (NIST). In reviewing the agenda, Mr. Donovan noted that the August 2021 NSTAC MCC would include: (1) opening remarks from the Administration and CISA regarding the Government's ongoing cybersecurity and national security and emergency preparedness (NS/EP) efforts; (2) a status update from Mr. Patrick Gelsinger, NSTAC Member and Software Assurance (SA) Subcommittee Chair, on the subcommittee's recent progress; (3) a public comment period; and (4) a fireside chat on the NS/EP impacts of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*.

Next, Mr. Donovan discussed the outcomes of the May 6, 2021, NSTAC Member Meeting. During the meeting, he noted that Mr. Greene commented on the Administration's efforts to strengthen the United States' NS/EP communications resiliency posture. Mr. Brandon Wales, Former Director, CISA, DHS, remarked on the agency's efforts to promote public-private partnerships across key technology areas, including zero-trust networking (ZTN) and software assurance. Mr. Michael Daniel, President and Chief Executive Officer, Cyber Threat Alliance, provided a keynote address on the implications of ransomware on national security. Mr. Jack Huffard, NSTAC Member, also facilitated a panel discussion on ZTN and its impact on NS/EP communications. Following the panel, NSTAC members deliberated, voted on, and unanimously approved the 2021 *NSTAC Report to the President on Communications Resiliency*. Finally, Mr. Greene officially tasked the NSTAC with its next study on "Enhancing Internet Resilience [EIR] in 2021 and Beyond."

Following this overview, Mr. Donovan invited Mr. Greene to provide opening remarks. Mr. Greene thanked NSTAC members and the SA Subcommittee for their efforts. He called attention to the President's recent appointments of Director Easterly and Mr. Christopher Inglis, National Cyber Director, Executive Office of the President, noting their extensive experience with cybersecurity and partnerships with the Government. Mr. Greene then discussed the impact of EO 14028 on industry's approach to software development. He also mentioned that, on July 28, 2021, the President signed the National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems, a memorandum that outlines actions for confronting threats posed to the systems that control and operate critical infrastructure. Mr. Greene explained that the Administration first formalized its critical infrastructure cybersecurity efforts in April 2021 with an electricity subsector effort, exemplifying the success of these kinds of public-private partnerships. Mr. Greene continued that the NSM has tasked CISA to work with NIST on developing performance goals for critical infrastructure by mid-September 2021 in order to determine which sectors rely most on control systems.

Mr. Donovan then turned the floor to Director Easterly. Director Easterly thanked the NSTAC for inviting her to participate in the MCC. She thanked Mr. Greene for his partnership and leadership and expressed her gratitude for participants' support of efforts to secure the Nation's critical systems. She then reviewed her key priorities as CISA Director, which include:

1. Moving CISA from a reactive posture to one that is proactive and resilient;
2. Empowering partners to defend themselves against emerging threats and collectively defend the Nation in cyberspace; and
3. Driving positive, sustainable, measurable change across the critical infrastructure at large while noting sectors' interdependency on each other.

To achieve these priorities, CISA will leverage the enhanced authorities it received from the Fiscal Year 2021 *National Defense Authorization Act* (FY21 NDAA), the *American Rescue Plan Act of 2021*, and EO 14028. Director Easterly extended thanks to Mr. Gelsinger and the SA Subcommittee for their efforts and future recommendations on how to promote security and integrity of the Nation's software supply chains, a central theme in Section 4 of EO 14028. Discussing EO 14028, she stated that the order focuses on "building back better" in several ways, including: (1) developing requirements for safeguarding federal networks; (2) encouraging information technology (IT) security providers to share threat intelligence; and (3) setting security standards for software vendors. As the Nation's risk advisor, CISA is key to implementing these policies.

Director Easterly noted that the EO also directs the Government to strengthen its IT security by implementing multi-factor authentication and zero-trust architectures on civilian networks, similar to what the NSTAC will study during phase II of the EIR study. She added that the NSTAC's previous recommendations on improving Government and industry coordination on cyber threats—particularly around the convergence of IT and operational technologies—was addressed in the EO. She commended the committee for its efforts to promote secure information and communications technology (ICT) supply chains and stressed the ongoing importance of the NSTAC's work.

As the Government continues to make progress in implementing EO 14028, Director Easterly stated that CISA will use this momentum to advance other critical infrastructure protection priorities. To this point, she discussed the launch of the Joint Cyber Defense Collaborative

(JCDC), which leverages CISA's new authorities in the FY21 NDAA to develop a joint cyber planning capability for U.S. critical infrastructure. She added that the JCDC intends to: (1) establish a common operating picture of the current threat environment; (2) develop comprehensive, whole-of-Nation plans against the most serious cyber threat; (3) exercise plans and determine where gaps exist; and (4) execute proactive cyber defense operations. As recommended in several NSTAC reports, CISA plans to leverage expertise across the critical infrastructure sectors to elevate the work of the JCDC, maximize CISA's footprint, and institutionalize partnership networks in the wake of high-priority threats.

Addressing the growing threat of ransomware, Director Easterly stressed that CISA remains vigilant in responding to these attacks and continues to leverage its partnership with the Federal Bureau of Investigation and the Multi-State Information Sharing and Analysis Center to stay aware of new tactics. She then discussed specific initiatives CISA has developed to help combat ransomware, to include introducing a Ransomware Readiness Self-Assessment and launching StopRansomware.gov, the first-ever central hub that consolidates resources from all federal agencies focused on reducing ransomware risk. She emphasized that partnerships between CISA and industry stakeholders are key to improving information sharing and bringing forth available expertise to meet emerging needs. In conclusion, she noted how she looks forward to collaborating with the NSTAC to develop a whole-of-Nation approach for mitigating emerging cybersecurity risks.

Mr. Donovan thanked Director Easterly for her remarks and voiced his gratitude for her willingness to engage the NSTAC as a partner in accomplishing CISA's goals. He acknowledged Mr. Inglis's attendance on the call, and thanked Mr. Wales for his leadership and support.

Status Update: NSTAC SA Subcommittee

Mr. Donovan invited Mr. Gelsinger to provide a status update on the NSTAC SA Subcommittee.

Mr. Gelsinger explained that the SA Subcommittee is charged with examining software assurance in the commercial ICT and services (ICTS) supply chain. Mr. Gelsinger explained that EO 14028 includes several new baseline security requirements for software sold to the Government. As such, the scope of EO 14028 poses significant implications for the NSTAC SA Subcommittee study and necessitates that the committee consider how its recommendations can support the order's implementation moving forward.

Since the May 6, 2021, NSTAC Meeting, the subcommittee has made significant progress in understanding the challenges associated with promoting software assurance in the ICTS supply chain by examining such topics as the software development lifecycle, role of cryptography, supply chain models, and standards. Throughout the course of the study, the subcommittee has applied its knowledge of technology to various aspects of software assurance and received briefings from experts in industry, academia, and Government.

Leveraging the data provided in these briefs, Mr. Gelsinger noted that the subcommittee has successfully developed an outline for the study and begun drafting the report.

Mr. Gelsinger stated that NSTAC members have provided invaluable insights to the study so far and will continue to have the opportunity to provide input on the subcommittee's efforts moving forward.

Mr. Gelsinger thanked the subcommittee for their support and expressed his eagerness to share the first draft of the report with NSTAC members in the coming weeks.

Hearing no questions, Mr. Donovan thanked Mr. Gelsinger for his comments.

Public Comment Period

Mr. Donovan welcomed Mr. Dana Goward, President and Director, Resilient Navigation and Timing (RNT) Foundation, and invited him to provide his remarks.

Mr. Goward stated that precise time has underpinned the Nation's information and telecommunications revolutions, making it a critical part of the technology infrastructure. He stressed the need for secure and resilient timing services across all critical infrastructure sectors. As such, he encouraged participants to work with the NSC, DHS, and Congress to convey the criticality of implementing a resilient national timing architecture. He noted that the Department of Transportation (DOT) needs additional funding to allow this to happen, as the DOT is the federal lead for position, navigation, and timing (PNT) requirements. Mr. Goward thanked participants for the opportunity to provide comments and yielded the floor to questions.

Mr. Matthew Desch, NSTAC Member, thanked Mr. Goward for his comments. He explained that Government has made significant strides towards standing up a national timing architecture, including EO 13905, *Strengthening National Resilience Through Responsible Use of PNT Services*. Mr. Desch agreed with Mr. Goward's statement regarding the need for resiliency and PNT but cautioned that there is no single solution for this complex issue.

Mr. Goward thanked Mr. Desch and stated that the RNT Foundation has recommended a multi-system architecture. He cited the foundation's white paper, *A Resilient National Timing Architecture*, which explains how a combination of systems can be used to address this challenge. He added that varied, widely accessible systems with no common failure modes will allow for a more secure Nation.

Hearing no further questions, Mr. Donovan thanked Mr. Goward for his comments.

Fireside Chat: The NS/EP Impacts of EO 14028

Mr. Donovan turned the meeting to Mr. Scott Charney, NSTAC Vice Chair, to facilitate a discussion on EO 14028, its NS/EP implications, and the impacts it poses on the NSTAC's ongoing EIR study.

After reviewing the intended outcomes of the session, Mr. Charney introduced Mr. Stine to the attendees. Mr. Stine underscored EO 14028's overarching theme on increasing trust and confidence in digital infrastructure. He noted that NIST has produced many resources that seek to leverage existing industry and Government standards, guides, and best practices for implementing the EO. Over the next several months, NIST will improve and expand on these resources to better meet the EO's specific requirements and the needs of software developers.

Mr. Charney noted that NIST's definition of critical software is broad. He asked if NIST has considered focusing the definition's scope on the software most important for supporting critical infrastructure security. Mr. Stine replied that NIST provided explanatory text with its definition, to include frequently asked questions and a preliminary list of critical software categories to help guide agencies conducting cost-benefit analyses for available security approaches. NIST also recommended that Government and industry use a phased approach to implement these software assurance guidelines, which would allow for the incremental fulfillment of the EO's tasks.

Mr. Stine said that NIST worked closely with CISA and the Office of Management and Budget (OMB) to develop the definition and maintain consistency with NIST, CISA, and OMB policies. He then referenced OMB's Memoranda M-21-30, *Protecting Critical Software Through Enhanced Security Measures*, which will provide agencies with specific information to assist in their implementation of secure software.

Next, Mr. Charney asked for Mr. Stine's input on the EO's timelines and the long-term processes necessary for achieving software security across the Nation's critical supply chains. Mr. Stine responded that Government and industry should use a phased approach beginning with fundamental practices, like analysis. He cited the 2016 NIST Internal Report to OMB on *Dramatically Reducing Software Vulnerabilities*, which offers recommendations on how to substantially reduce software vulnerabilities. Looking ahead, Mr. Stine said foundational resources will improve as Government and industry gain more information on security risks through the practical implementation of the EO's provisions. To this end, better tools and development methodologies will help improve software over time.

Mr. Charney noted that EO 14028 is heavily focused on security requirements. However, implementing software assurance measures can be time-consuming and costly, especially if added on top of existing regimes (e.g., Federal Risk and Authorization Risk Management Program). As a result, he asked Mr. Stine if NIST has considered how the EO's assurance requirements will be scaled to smaller companies and the open source community. Mr. Stine replied that NIST does not want to establish new or different compliance regimes. As such, companies will need to determine how to conform their capabilities to different requirements and demonstrate attestation. He continued that NIST is interested in partnering with industry to gather feedback on what artifacts and levels of attestation proof they can readily provide to those procuring their software. Mr. Stine argued that self-attestation should be considered a valid method for meeting the EO’s requirements. He also encouraged organizations to reuse artifacts and evidence of conformance from existing assurance regimes where possible.

Mr. Charney reiterated the NSTAC’s commitment to public-private partnerships focused on promoting better security. In light of the new EO, he asked if there are specific efforts the NSTAC should promote to help advance these strategic priorities. Mr. Stine replied that the EO focuses primarily on critical software, which could extend to hardware as well; thus, he would be interested to receive the NSTAC’s insights on this topic. Moreover, the NSTAC could help institutionalize existing security practices across the public and private sectors, as well as define how to ensure the order’s long-term success.

Hearing no further comments, Mr. Donovan thanked Mr. Charney and Mr. Stine for their input.

Closing Remarks and Adjournment

Mr. Donovan asked Mr. Greene and Director Easterly if they had any final remarks. In closing, Mr. Greene thanked participants for the discussion, and underscored his appreciation for Mr. Stine and NIST’s efforts on EO 14028. Director Easterly thanked participants and said she was eager to partner with the NSTAC moving forward.

Mr. Donovan thanked NSTAC members and Government partners for the input they provided during the meeting, paying a special thanks to Mr. Gelsinger for providing the SA Subcommittee update, and Mr. Stine and Mr. Charney for their participation in the fireside chat. He then announced that the NSTAC will hold its next meeting on November 2, 2021, and that more information regarding this engagement is forthcoming.

Mr. Donovan made a motion to close the meeting. Upon receiving a second, he thanked participants and officially adjourned the August 2021 NSTAC MCC.

APPENDIX
August 17, 2021, NSTAC Member Conference Call Participant 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	Communication Technologies, Inc.
Mr. Patrick Gelsinger	Intel Corp.
Ms. Lisa Hook	Two Island Partners, LLC
Mr. Jack Huffard	Tenable Holdings, Inc.
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. Jeffrey Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
NSTAC Points of Contact	
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.
Ms. Amanda Craig-Deckard	Microsoft Corp.
Ms. Cheryl Davis	Oracle Corp.
Mr. Jonathan Gannon	AT&T, Inc.
Ms. Katherine Gronberg	NightDragon Security, LLC
Mr. Robert Hoffman	Broadcom, Inc.
Mr. Kent Landfield	McAfee Corp.
Mr. Sean Morgan	Palo Alto Networks, Inc.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Charles Taylor	Raytheon Technologies Corp.
Mr. Kent Varney	Lockheed Martin Corp.
Dr. Claire Vishik	Intel Corp.
Mr. Milan Vlajnic	Communication Technologies, Inc.

Government Participants

Ms. Sandy Benevides	Department of Homeland Security
Ms. DeShelle Cleghorn	Department of Homeland Security
Mr. Antonio DaRosa	Department of Homeland Security
Ms. Jen Easterly	Department of Homeland Security
Mr. Trent Frazier	Department of Homeland Security
Mr. Joseph Galvin	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. Paul Gray	Department of Homeland Security
Mr. Jeffrey Greene	National Security Council
Mr. Robert Greene	Department of Homeland Security
Mr. Christopher Inglis	Executive Office of the President
Ms. Helen Jackson	Department of Homeland Security
Ms. Valerie Mongello	Department of Homeland Security
Ms. Renee Murphy	Department of Homeland Security
Mr. John O'Connor	Department of Homeland Security
Ms. Kate Schwartzer	Department of Homeland Security
Mr. Brian Scott	National Security Council
Ms. Katherine Siefert	Department of Homeland Security
Mr. Kevin Stine	National Institute of Standards and Technology
Ms. Megan Tsuyi	Department of Homeland Security
Mr. Bradford Willke	Department of Homeland Security
Mr. Scott Zigler	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. Stephanie Guzman	Booz Allen Hamilton, Inc.
Ms. Laura Penn	Insight Technology Solutions, LLC

Public and Media Participants

Mr. Drew Abrahams	Fox News Channel
Ms. Christina Berger	Booz Allen Hamilton, Inc.
Mr. Calvin Biesecker	Defense Daily
Mr. Christopher Castelli	Booz Allen Hamilton, Inc.
Mr. Matthew Eggers	U.S. Chamber of Commerce
Ms. Sharon Eshelman	Lewis-Burke Associates, LLC
Ms. Sara Friedman	Inside Cybersecurity
Mr. Eric Geller	Politico
Mr. Dana Goward	Resilient Navigation and Timing Foundation
Dr. Philip Grant	Booz Allen Hamilton, Inc.
Mr. Bart Gray	Oceus Networks, Inc.

Mr. Albert Kammler	Van Scoyoc Associates, Inc.
Ms. Laura Karnas	Booz Allen Hamilton, Inc.
Ms. Rebecca Kern	Bloomberg Industry Group
Mr. Tom Leithauser	Telecommunications Reports
Mr. Coleman Mehta	Palo Alto Networks, Inc.
Ms. Nicole Ogrysko	Federal News Network
Ms. Geneva Sands	CNN
Ms. Nicole Sganga	CBS News
Ms. Chelsea Smethurst	Microsoft Corp.
Ms. Liz Turrell	CNN
Ms. Rosie Vail	Paul, Weiss, Rifkind, Wharton, and Garrison, LLP
Mr. Vincent Voci	U.S. Chamber of Commerce

Certification

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

Mr. John Donovan
NSTAC Chair