President's National Security Telecommunications Advisory Committee (NSTAC)
Meeting Open Session Summary
November 2, 2021

Call to Order and Opening Remarks

Ms. Elizabeth Gauthier, NSTAC Alternate 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 meeting was open to the public. While no one had registered to provide comment, written comments would be accepted following the procedures outlined in the meeting's Federal Register Notice. Following roll call, Ms. Gauthier turned the meeting over to Mr. John Donovan, NSTAC Chair.

Mr. Donovan welcomed the distinguished Government partners in attendance, including: Ms. Alaina Clark, Assistant Director for Stakeholder Engagement, Cybersecurity and Infrastructure Security Agency (CISA), DHS; Mr. Jeffrey Greene, Chief, Cyber Response and Policy, National Security Council (NSC); Mr. John "Chris" Inglis, National Cyber Director, Executive Office of the President; and Mr. Rob Joyce, Director of Cybersecurity, National Security Agency (NSA).

In reviewing the agenda, Mr. Donovan 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) efforts; (2) a keynote address from Mr. Inglis on fortifying the Nation's cybersecurity; (3) an update on Administration actions to support NS/EP missions from Mr. Greene; (4) a deliberation and vote on the *NSTAC Report to the President on Software Assurance (SA) in the Information and Communications Technology (ICT) and Services Supply Chain* (SA Report) led by Mr. Patrick Gelsinger, SA Subcommittee Chair; and (5) an update on the NSTAC Zero-Trust and Trusted Identity Management (ZT-IdM) Subcommittee provided by Mr. Donovan and Mr. Mark McLaughlin, ZT-IdM Subcommittee Co-Chairs.

Mr. Donovan then asked Ms. Clark to provide her opening remarks. Ms. Clark expressed her appreciation for the NSTAC's insights concerning challenges presented by the rapidly evolving ICT ecosystem. She called attention to NSTAC recommendations that have been implemented by CISA and other Government agencies, specifically highlighting the 2017 NSTAC *Report to the President on Emerging Technology and Strategic Vision*, which underlined the need for the Government to develop a plan to modernize ICT network architectures in support of NS/EP missions. In response to this recommendation, CISA's Supply Chain Risk Management (SCRM) Task Force released two new products in September 2021. The first was the *Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information* report, which addresses challenges to and liabilities posed by threat information sharing. The second was the *Operationalizing the Vendor SCRM Template for Small and Medium-Sized Businesses (SMB)*, which serves as a resource to assist SMBs with mitigating ICT supply chain risks. Ms. Clark also highlighted

how the 2021 *National Defense Authorization Act* took actionable steps to reaffirm the whole-of-Nation moonshot strategy and the cybersecurity grand challenges program laid out in the 2018 NSTAC *Report to the President on a Cybersecurity Moonshot*.

Ms. Clark then reviewed CISA's current priorities, which uniquely align to the NSTAC's mission objectives. These priorities include:

- Attracting and retaining a world-class workforce;
- Implementing Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, through: (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;
- Securing cyber, physical, and communications critical infrastructure; and
- Building partnerships between Government and the private sector.

Ms. Clark also highlighted CISA's recent work to combat the ransomware threat, which includes: (1) disrupting ransomware operations; (2) taking the fight to the enemy; and (3) hardening at-risk targets. She also remarked how, in March, DHS began a series of 60-day sprints to strengthen cybersecurity across a range of issue areas, beginning with ransomware earlier this year.

Ms. Clark closed by reflecting on National Critical Infrastructure Security and Resilience Month. As the importance of cybersecurity and infrastructure has increased dramatically, she noted that the third phase of the "Enhancing Internet Resilience [EIR] in 2021 and Beyond" study on the convergence of IT and operational technology (OT) could not be timelier.

Mr. Donovan thanked Ms. Clark for her remarks. He then invited Mr. Greene to provide comment.

Mr. Greene welcomed Mr. Inglis to his first NSTAC meeting, underscoring the significance of having the National Cyber Director engaged with the private sector. He emphasized how the NSTAC's guidance complements the Administration's efforts to address emerging threats to the Nation's cybersecurity (e.g., SolarWinds compromise, ransomware). Mr. Greene then highlighted the release of the National Institute of Standards and Technology's (NIST) Special Publication 800-161 Revision 1 *Cybersecurity SCRM Practices for Systems and Organizations*. He closed by noting how the breadth of cybersecurity threats has added urgency to the creation of the Office of the National Cyber Director.

Mr. Donovan thanked Mr. Greene for his remarks.

Keynote Address: Fortifying the Nation's Cybersecurity Posture

Mr. Donovan invited Mr. Inglis to provide the keynote address.

Mr. Inglis explained that the different facets of Federal Government sometimes cause confusion on who is empowered to lead actionable change in this arena. As the Government's cybersecurity strategy is accomplished in partnership with industry, the NSC helps to facilitate the needed conditions for this strategy's success across a variety of domains. For this reason, Mr. Inglis maintained that it is appropriate that the NSTAC collaborates with the NSC.

Mr. Inglis stated that CISA is responsible for defending federal enterprises, as well as coordinating the protection of private sector critical infrastructure. He noted that the NSA's Cyber Collaboration Center: (1) underscores the importance for Government to develop relationships with specific critical infrastructure sectors; (2) helps to convey these sectors' defense strategies and needs; and (3) allows for the sharing of timely, granular, and actionable information between these sectors and with Government.

Mr. Inglis noted that it is impossible to discuss the topic of cybersecurity without first addressing threats. Government and industry should not just respond to threats. In fact, partners should establish proactive mitigation initiatives, while acknowledging the impact of present risks to their systems. He emphasized the importance of defending the National Critical Functions (NCF), and the data and systems used to support them. Mr. Inglis noted that defending NCFs – functions so vital that their disruption would have a debilitating effect on the United States' national security – is more challenging than defending technical infrastructures. Moreover, NCFs pose direct implications for system integration, collaboration, and user confidence across many sectors.

Mr. Inglis remarked that emerging cybersecurity strategies require addressing all individuals operating in cyberspace, not just IT specialists. Additionally, Government and industry should seek to lessen systemic risk by identifying the weakest links in the supply chain. Mr. Inglis further emphasized the importance of creating resiliency across technology, people, and policy/doctrine, as well as achieving heightened awareness to better defend the Nation's digital infrastructure.

Next, Mr. Inglis stated that ZT presumes the possibility of breach and penetration, which illustrates the need to punish or reward certain behaviors online. He stated that the Government can increase its responsiveness to malicious events by determining what is needed to increase resilience and establish a proactive defense.

Discussing the role of the National Cyber Director, Mr. Inglis stated that the position seeks to improve federal, state, local, tribal, and territorial governments' ability to better defend critical infrastructure. To this end, public-private partnerships are essential to implementing change in cyberspace. Citing the September 11, 2001, attacks, he noted how these events caused the United States to rethink homeland defense and how a foreign threat could lead to a domestic instantiation. In this instance, the Government did not adequately assess or integrate data provided by various intelligence streams to identify the threat beforehand. Mr. Inglis underscored the importance of cross-sector collaboration to compare information on perceived risks.

Currently, the private sector builds, manages, and develops most of cyberspace. As a result, Mr. Inglis noted that the partnership between the NSTAC and Government is meaningful in that it generates ideas on how industry can use Government resources and authority to support collective goals within cyberspace. He thanked the NSTAC for their work and turned the floor back over to Mr. Donovan.

Update: Administration Actions

Mr. Donovan invited Mr. Greene to provide an update on the Biden Administration's actions to strengthen the Nation's NS/EP and cybersecurity posture. Mr. Greene referenced a recent hack reported by Microsoft, noting that the successful employment of crude, unsophisticated tactics illustrates the need to improve the Nation's cyber defenses. The Administration's continued prioritization of cybersecurity has been reflected in recent legislative action, such as the *American Rescue Plan Act of 2021*, and EOs, like EO 14028. NIST, CISA, and the Office of Management and Budget (OMB) are working together to implement EO 14028's provisions, and Mr. Greene noted he is pleased with the progress to date. He highlighted the considerable private sector engagement on the effort, noting that NIST workshops on the EO have logged over 1,000 participants.

Next, Mr. Greene emphasized the need to shift the cost associated with cybersecurity from response and recovery to development. As such, the Federal Government should leverage its purchasing power to ensure that departments and agencies (D/A) procure only secure software and adopt security best practices enterprise-wide. Other priorities in this effort include: (1) ensuring complete and accurate system log files; (2) establishing the Cyber Safety Review Board to review and assess significant cyber incidents; and (3) ensuring that D/As follow a standard playbook for incident response.

Mr. Greene noted that, over the years, D/As have independently put significant effort into cybersecurity. In the past six months, EO 14028 has made great strides to shift these differing approaches into a unified methodology. Mr. Greene said that NIST guidance and definitions empower customers to make smart security choices. He continued that OMB and CISA have recently published three documents to encourage Government adoption of ZT architectures (ZTA), including: (1) OMB's Federal ZT Strategy; (2) CISA's ZT Maturity Model; and (3) CISA's Cloud Security Technical Reference Architecture. Similarly, improvements driven by EO 14028 will be reflected in the upcoming *Federal Information Security Modernization Act* report.

Beyond the Federal Government, the Administration is also working with the private sector to increase the cyber resiliency of the NCFs, an effort that began in August 2021 with natural gas pipelines. The Transportation Security Administration (TSA) issued requirements of critical infrastructure owners and operators to ensure that: (1) responsible cybersecurity officials are identified; (2) security architectures are reviewed annually; and (3) cyber resilience performance goals are established and voluntarily adopted. TSA will issue similar requirements for the other industries under their regulatory authority. He also noted that, at

present, Sector Risk Management Agencies are advising the Government on future sectors to examine; the water sector will be addressed next.

Mr. Donovan thanked Mr. Greene for his remarks.

Deliberation and Vote: *NSTAC Report to the President on SA in the ICT and Services Supply Chain*

Mr. Donovan invited Mr. Gelsinger to discuss the NSTAC SA Report's key findings and recommendations.

Following the official EIR tasking in May 2021, the NSTAC focused on examining SA in the ICT and services supply chain, which underpins the U.S. economy and national security. Mr. Gelsinger added that this is a timely and urgent study, as underscored by the provisions found in EO 14028.

In the last two decades, the United States has experienced significant changes in how software is designed, developed, procured, deployed, and managed across all aspects of the supply chain. Mr. Gelsinger cited one example of this change as the use of open-source software. Now, up to 70 percent of commercial software packages contain open-source components. Another example Mr. Gelsinger referenced is the use of distributed development, which requires new integration of third-party components. Likewise, the implementation of cloud deployment models has created new SA opportunities and challenges. Mr. Gelsinger said that these three examples are driving a dramatic change in how the United States builds, purchases, and manages software.

During the course of its study, the NSTAC realized that SA practices are well-defined, but unevenly practiced, and that the field would benefit from harmonizing efforts that address the urgency of the situation in clear, practical terms. For this, Mr. Gelsinger explained that considerable effort has been put into the development of new models, standards, and technologies to encourage SA. However, the NSTAC determined that such innovation should be adopted on a broader scale, with far greater consistency. Furthermore, Mr. Gelsinger noted that the NSTAC identified challenges to improving software supply chain security. For example, different stages of the software lifecycle are carried out by discrete stakeholder sets supporting development, procurement, and administration. As these stakeholders have differing tactical and local objectives, these varying priorities sometimes put them into conflict with each other. Other notable challenges to effective SA include:

- The complexity of the computing ecosystem;
- A lack of organic security and assurance education as a foundational part of competency and degree requirements;
- A limited understanding of the economic incentives for the extremely diverse global software development and deployment ecosystem;
- The fragmentation of the regulatory system; and

- A lack of uniformity and depth in existing standards and guidelines.

Mr. Gelsinger noted that one of the report's key recommendations is that the President establish a task force charged with defining a public-private initiative focused on key areas of SA and the software supply chain. Similar to the public-private effort on the NIST Cybersecurity Framework, such an initiative can address the fundamental misalignment of incentives, diversity of the assurance approaches, and complexity of the software supply chain.

In addition to the establishment of a task force, Mr. Gelsinger said that the report lists more specific recommendations along three broad topic areas, including SA, stakeholders, and external influencing factors.

- For SA, recommendations range from extending public-private partnerships, to investing in technology innovation, such as the use of artificial intelligence to help automate and streamline SA and supply chain processes.
- For stakeholders, recommendations focus on aligning incentives for developers, suppliers, and other stakeholders to become more proficient practitioners of SA.
- For external influencing factors, recommendations range from the task force previously described, to aligning training guidelines, and collaborating with states to integrate security education into K through 12 curricula.

Next, Mr. Gelsinger recognized the NSTAC's collaboration with a variety of partners on the study, to include NSTAC member companies who provided representation to the effort; Government officials who offered input, guidance, and clarification; a variety of key subject matter experts who shared their knowledge on this topic; and the CISA team for their assistance in the course of this work.

Mr. Gelsinger then ceded the floor to Mr. Donovan to facilitate the report deliberation and vote.

Mr. Donovan thanked Mr. Gelsinger for his commitment to and leadership of the study. He then asked participants for feedback. Mr. McLaughlin noted that this is the first time an NSTAC study has been completed in six months and asked for Mr. Gelsinger's insights into lessons learned from this effort. Mr. Gelsinger recommended picking a set timeline for completion, and clearly communicating expectations to ensure all parties are working towards a common goal.

Hearing no other comments, Mr. Donovan made a motion to approve the SA Report. Following this motion, NSTAC members unanimously approved the report for transmission to the President.

Mr. Donovan stated that he looks forward to seeing how the Government implements these recommendations.

Status Update: NSTAC ZT-IdM Subcommittee

Mr. Donovan informed attendees that phase II of the EIR study kicked off in August 2021. He further remarked that ZT is topical, relevant, and will underpin the United States' cybersecurity

strategy for years to come. He then invited Mr. McLaughlin to provide the update on the NSTAC ZT-IdM Subcommittee's progress to date.

Mr. McLaughlin stated that the subcommittee will finalize the report by February 2022. In the report, the subcommittee will: (1) include an overview of ZTA pillars; (2) propose a standardized definition for ZTA; (3) discuss existing policies impacted by ZTA; (4) explain best practices to drive ZT adoption; and (5) describe the baseline of the current ZT space. Mr. McLaughlin stated that recent subcommittee briefers represent federal D/As responsible for developing ZT guidance or are capable of sharing best practices from their own ZT implementations. Going forward, the subcommittee will pivot to industry briefings to identify lessons learned from the private sector that can be communicated to the Government.

Mr. McLaughlin stated that the subcommittee would appreciate NSTAC member recommendations for briefers who can discuss their experiences in implementing ZT. He then thanked the subcommittee and CISA staff for the work performed thus far.

Hearing no questions, Mr. Donovan thanked Mr. McLaughlin for his input.

Closing Remarks and Adjournment

Mr. Donovan asked Mr. Greene if he had any final remarks. In closing, Mr. Greene thanked Mr. Gelsinger for chairing the SA Subcommittee. He also thanked the NSTAC members for their efforts in developing the SA Report, running the ZT-IdM Subcommittee, and supporting the Government's NS/EP missions. Mr. Donovan thanked Mr. Greene and asked Ms. Clark to provide her closing remarks.

Ms. Clark underscored her appreciation to the NSTAC on their guidance on SA, ZT, and the upcoming work on the IT/OT convergence. She thanked Mr. Joyce, Mr. Greene, and Mr. Inglis for their partnership and participation, and the CISA team for holding the meeting in person.

After thanking Ms. Clark for her comments, Mr. Donovan also thanked NSTAC members and Government partners for the input they provided during the meeting.

Mr. Donovan announced that the next NSTAC meeting will be held via conference call on February 23, 2022, from 2:00 to 3:00 p.m. Eastern Time. He then made a motion to close the meeting. Upon receiving a second, Mr. Donovan thanked participants and officially adjourned the meeting.

APPENDIX
Open Session 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	Communications Technologies, Inc.
Mr. Patrick Gelsinger	Intel Corp.
Mr. Jack Huffard	Tenable Holdings, Inc.
Ms. Renée James	Ampere Computing, LLC
Mr. Mark McLaughlin	Palo Alto Networks, Inc.
Mr. Angel Ruiz	MediaKind, Inc.
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. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Ms. Cheryl Davis	Oracle Corp.
Mr. Thomas Gann	McAfee Corp.
Mr. Jonathan Gannon	AT&T, Inc.
Ms. Kathryn Gronberg	NightDragon Security, LLC
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. Kevin Riley	Ribbon Communications, Inc.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Robert Spiger	Microsoft Corp.
Mr. Charles Taylor	Raytheon Technologies Corp.
Mr. Kent Varney	Lockheed Martin Corp.
Dr. Claire Vishik	Intel Corp.
Mr. Milan Vlajnic	Communications Technologies, Inc.

Other Attendees

Mr. James Hayes	Tenable, Inc.
Mr. Gerald McLaughlin	Palo Alto Networks, Inc.

Government Participants

Ms. Alaina Clark	Department of Homeland Security
Ms. DeShelle Cleghorn	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. Jeffrey Greene	National Security Council
Mr. John "Chris" Inglis	Executive Office of the President
Ms. Helen Jackson	Department of Homeland Security
Mr. Rob Joyce	National Security Agency
Ms. Rachel Liang	Department of Homeland Security
Ms. Alexandra Martin	Department of Homeland Security
Ms. Erin McJeon	Department of Homeland Security
Ms. Celinda Moening	Department of Homeland Security
Ms. Katherine Siefert	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.
Ms. Susan Bowyer	Booz Allen Hamilton, Inc.
Mr. Kole Kurti	Insight Technology Solutions, LLC
Ms. Laura Penn	Insight Technology Solutions, LLC

Public and Media Participants

Ms. Mariam Baksh	Nextgov
Mr. Calvin Biesecker	Defense Daily
Mr. Christopher Castelli	Booz Allen Hamilton, Inc.
Mr. Justin Doubleday	Federal News Network
Mr. Matthew Eggers	U.S. Chamber of Commerce
Ms. Sara Friedman	Inside Cybersecurity
Mr. Eric Geller	Politico
Mr. Albert Kammler	Van Scoyoc Associates, Inc.
Ms. Norma Krayem	Van Scoyoc Associates, Inc.
Mr. Tim Starks	Cyberscoop

Certification

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

Mr. John Donovan
NSTAC Chair