President's National Security Telecommunications Advisory Committee (NSTAC) Member Conference Call February 23, 2022

Call to Order and Opening Remarks

Ms. Rachel Liang, Department of Homeland Security (DHS) and NSTAC Alternate 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 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. Liang turned the meeting over to Mr. John Donovan, NSTAC Chair.

Mr. Donovan noted that due to a scheduling conflict, he would provide opening remarks and Mr. Scott Charney, NSTAC Vice Chair, would facilitate the remainder of the call. Mr. Donovan then welcomed the distinguished Government partners in attendance, including: Mr. Trent Frazier, Deputy Assistant Director for Stakeholder Engagement, Cybersecurity and Infrastructure Security Agency (CISA), DHS; Ms. Elke Sobieraj, Director for Critical Infrastructure Cybersecurity, National Security Council (NSC); and Dr. Michelle Rozo, Director for Technology and National Security, NSC.

In reviewing the agenda, Mr. Donovan noted that the meeting would include: (1) opening remarks from the Administration and CISA leadership; (2) a status update on the NSTAC Information Technology and Operational Technology (IT/OT) Convergence Subcommittee; (3) a deliberation and vote on the *NSTAC Report to the President on Zero Trust and Trusted Identity Management* (ZT-IdM); and (4) a discussion on the NSTAC Enhancing U.S. Leadership in International Communications Technology Standards tasking.

Mr. Donovan then provided a summary of the November 2021 NSTAC Member Meeting, during which: (1) Mr. Jeffrey Greene, Chief, Cyber Response and Policy, Cyber Directorate, NSC, and Ms. Alaina Clark, Assistant Director for Stakeholder Engagement, CISA, DHS, remarked on the Government's collaboration with industry on key national security and emergency preparedness communication initiatives; (2) Mr. John "Chris" Inglis, National Cyber Director, Executive Office of the President (EOP), gave a keynote on fortifying the Nation's cybersecurity posture; (3) Mr. Greene provided an update on Administration efforts to fortify the nation's cybersecurity posture, efforts to address the emergent cybersecurity threats, and the importance of public/private partnerships; (4) NSTAC members voted to unanimously approve the *NSTAC Report to the President on Software Assurance in the Information and Communications Technology and Services Supply Chain*; and (5) Mr. Donovan and Mr. Mark McLaughlin, NSTAC ZT-IdM Subcommittee Co-Chairs, provided an update on the ZT-IdM Subcommittee. Mr. Donovan then turned the meeting over to Mr. Charney. Mr. Charney thanked Mr. Donovan and invited Mr. Frazier to provide his opening remarks.

Mr. Frazier highlighted the need to raise awareness regarding the importance of protecting critical infrastructure due to recent ongoing geopolitical tensions in Ukraine. He emphasized that CISA is focused on educating public and private sector partners on ways to protect infrastructure, focusing on four key tenants: (1) taking steps to reduce the likelihood of a damaging cyber intrusion; (2) taking appropriate measures to quickly detect potential intrusions and, where possible, report them to the appropriate authorities (both within CISA and within the Federal Bureau of Investigation's CyWatch program); (3) preparing to respond should an intrusion occur; and (4) maximizing their resilience should they be the victims of destructive cyber incidents. Mr. Frazier underscored that CISA is urging all cybersecurity and information technology (IT) personnel to review recent guidance on understanding and mitigating Russian state sponsored cyber threats to U.S. critical infrastructure. He recommended that organizations visit www.stopransomware.gov, a centralized whole-of-government website containing up-to-date information on ransomware attacks occurring throughout the nation and across the world.

Mr. Frazier underscored the NSTAC's dedication to CISA's mission and the vital role the NSTAC has played in providing the Government with insightful advice to improve the Nation's posture and help combat cyber threats. He noted that the 2021 *NSTAC Report to the President on Software Assurance in the Information and Communications Technology and Services Supply Chain* and the *NSTAC Report to the President on Communications Resiliency* are invaluable assets that continue to evolve CISA's approach to cybersecurity. He stated that CISA is closely following the progress of the "Enhancing Internet Resilience [EIR] in 2021 and Beyond" study and the Standards Subcommittee. Mr. Frazier affirmed that the NSTAC has demonstrated the ability to successfully address a variety of mission critical topics, and expressed his confidence that CISA and other government agencies would be able to leverage the NSTAC's recommendations in an actionable and insightful manner.

Mr. Frazier reviewed the ways in which CISA is implementing Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, including: (1) developing requirements for safeguarding federal networks; (2) encouraging IT security providers to share threat intelligence readily; and (3) setting security standards for software vendors. He emphasized that the EO will enable the Government to improve security practices for federal IT networks, while also providing a platform to review issues that the NSTAC has addressed in its previous studies and current efforts.

Mr. Frazier closed by extending his thanks to the ZT-IdM, Standards, and IT/OT Convergence subcommittees, as well as their respective chairs, for their efforts.

Mr. Charney thanked Mr. Frazier for his remarks and invited Ms. Sobieraj to provide comment.

Ms. Sobieraj stated that the EOP values the NSTAC's industry-based analysis on important topics and noted the urgency of strengthening the Nation's cyber defenses regarding recent geopolitical developments. She emphasized that securing the Nation's critical infrastructure requires a whole-of-Nation approach and that collaborative partnerships, like the NSTAC, are important. Ms. Sobieraj closed by thanking the NSTAC for their continued work on critical topics.

Mr. Charney thanked Ms. Sobieraj for her remarks.

Status Update: NSTAC IT/OT Convergence Subcommittee

Mr. Charney invited Mr. Huffard to provide an update on the subcommittee's progress.

Mr. Huffard noted that the IT/OT Convergence Subcommittee will develop a report that examines the key challenges of securing operational technology (OT) systems against threats that emerge from IT network connections and identifies emerging approaches to the increased OT resiliency to these threats (including through adaptations of IT security approaches to accommodate OT design constraints). He stated that recent attacks on critical infrastructure highlight the many challenges involved in securing OT, underscoring the difficulty in developing patches for, and deploying, industrial control systems and other technologies used in OT.

Mr. Huffard noted the timeliness of the subcommittee's efforts due to the 2021 National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. He stated that the IT/OT Subcommittee will focus on how the NSTAC can raise awareness on current IT/OT convergence best practices and highlight existing gaps. He noted that the subcommittee previously met with Mr. Greene and Ms. Sobieraj to discuss the Administration's goals for the study, and to help guide the subcommittee as they develop a plan of action for the report. Based on this discussion, Mr. Huffard believes the report should scope the challenge that should be addressed and include a series of policy recommendations to strengthen OT cybersecurity for the Federal Government as well as state, local, tribal and territorial governments, and private sector owners and operators of critical infrastructure. He noted that the study will focus specifically on the convergence of IT/OT for industrial or critical infrastructure, and that it will highlight what is and is not working from government, asset owners, and original equipment manufacturers' perspectives.

Mr. Huffard stated that the subcommittee is currently in the process of extending invitations to individuals to brief the subcommittee, and asked NSTAC members to provide recommendations for potential briefers or additional subcommittee members.

Mr. Charney thanked Mr. Huffard for his remarks.

Deliberation and Vote: *NSTAC Report to the President on Zero-Trust and Trusted Identity Management*

Mr. Charney turned the meeting to Mr. Mark McLaughlin, ZT-IdM Subcommittee Co-Chair, to discuss the key findings and recommendations in the *NSTAC Report to the President on Zero Trust and Trusted Identity Management*.

Mr. McLaughlin highlighted the timeliness of the ZT-IdM Subcommittee, noting that EO 14028 placed significant emphasis on zero trust and that the White House issued the first draft of the Federal Zero Trust Strategy mere weeks after the subcommittee commenced its efforts. He stated that the final Federal Zero Trust Strategy was released on January 26, 2022, and it laid out specific directives on how federal agencies must practically implement zero trust principles. He noted that the report proposes over 20 actionable recommendations for how the U.S. Government can effectively implement the Federal Zero Trust Strategy and foster a sustained institutionalized commitment to zero trust over the long term, both within the Federal Government and across the broader national ecosystem.

Mr. McLaughlin stated that the report concludes that the U.S. Government should be commended for its strategic emphasis on zero trust and that the Federal Zero Trust Strategy is well-grounded in many industry best practices. However, while the restrained scope of the Federal Zero Trust Strategy is appropriate, the report notes that zero trust risks becoming an incomplete short-term experiment rather than the foundation of an enduring, coherent, and transformative Federal Government strategy that can be measured for decades. This is why the subcommittee focused its recommendations on policy actions that can help institutionalize zero trust over the long term, beyond the two-and-a-half-year focus of the Federal Zero Trust Strategy. To accomplish this, the report notes that zero trust principles must be fully integrated into existing and new Federal Government structures, policies, and programs, and not be viewed as a new standalone initiative. Mr. McLaughlin emphasized that this would require significant leadership prioritization, funding, and the establishment of new governance and accountability mechanisms.

Mr. McLaughlin explained that the report's key recommendations fall into two categories: (1) actions the U.S. Government can take to influence effective zero trust implementation within the Federal Government; and (2) actions the U.S. Government can take to influence and incentivize zero trust adoption for non-Federal entities, including state, local, and critical infrastructure communities. For within the Federal Government enterprise, recommendations include: that the Federal Chief Information Security Officer, working through the Federal Chief Information Security Office Council, establish new oversight and governance mechanisms that helps agencies share best practices for zero trust maturity; and that CISA establish a Civilian Government Zero Trust Program Office as a way to empower and accelerate civilian agencies' zero trust adoption and complement what the Department of Defense has established for the defense enterprise. For incentivizing the adoption of zero trust outside the Federal Government, recommendations include: that National Institute of Standards and Technology partner closely with industry to undertake a multi-year effort to develop and mature zero trust standards and guidelines; and that the U.S. Government use federal security grant distributions to incentivize zero trust adoptions.

Mr. McLaughlin concluded by thanking NSTAC members, the ZT-IdM Subcommittee, and CISA's administrative staff for their contributions to the report. Mr. McLaughlin then ceded the floor to Mr. Charney to facilitate the report deliberation and vote.

Mr. Charney thanked Mr. McLaughlin for the report overview, and asked participants for feedback. Hearing no comments, Mr. Charney made a motion to approve the report. Following this motion, NSTAC members unanimously approved the report for transmission to the President.

Discussion: NSTAC Standards Subcommittee

Mr. Charney invited Dr. Rozo to provide comment on the Standards tasking.

Dr. Rozo thanked the NSTAC for researching the topic of standards, and for providing their expert insight into this critical problem. She underlined the U.S. Government's commitment to maintaining the integrity of, and trust in, international standards, and to strengthening the industry driven market-based approach to standards development. Dr. Rozo emphasized the need for partnership between industry and government to address the new challenges in the standards development landscape, particularly in regard to critical and emerging technologies. She stated that the number of standards activities and venues has increased rapidly, therefore there are more standards activities for the same number of experts to track.

Dr. Rozo underscored the People's Republic of China's (PRC) increased participation and coordination within and across standards development activities, noting its goal to become a global standards setter. She stated that the PRC's actions risk altering economic competitiveness in its favor, which may put U.S. industries at a disadvantage in global markets and could have national security implications. Dr. Rozo emphasized that the U.S. Government is focused on several priorities to ensure the U.S. remains a leader in international technology standards development, including: leading in research and development; advocating for open participation; removing barriers to participation in standards development activities; growing the talent for international standards development; and fostering strong public/private technology standards partnerships. Dr. Rozo closed by reiterating her appreciation for the NSTAC's focus on this topic.

Mr. Charney thanked Dr. Rozo for her insights.

Closing Remarks and Adjournment

Mr. Charney thanked participants for attending; Mr. Huffard, Mr. McLaughlin, and Dr. Rozo for providing updates on the subcommittees; and subcommittee working group leads, subcommittee members, and NSTAC support staff for their efforts in the studies. Mr. Charney then asked Mr. Frazier to provide his closing remarks.

Mr. Frazier underscored his appreciation for the NSTAC's ability to address issues through a multi-pronged approach and stated his belief that CISA and others in the Federal Government will be able to leverage the NSTAC's recommendations in an actionable manner. He emphasized the NSTAC's role in providing guidance on mission critical topics, such as zero trust and IT/OT convergence. Mr. Frazier thanked Ms. Sobieraj and Dr. Rozo for their input, and extended his appreciation to Mr. Donovan, Mr. McLaughlin, and the NTSAC ZT-IdM Subcommittee for successfully completing the report. Mr. Frazier also thanked Mr. Huffard and Mr. Dolan for their efforts with the IT/OT Convergence Subcommittee, and the Standards Subcommittee for their endeavors.

Mr. Charney thanked Mr. Frazier for his comments and invited Ms. Sobieraj to make her closing remarks.

Ms. Sobieraj thanked participants for attending the meeting and extended her thanks to the IT/OT Convergence Subcommittee and the Standards Subcommittee for their ongoing efforts. She also thanked the ZT-IdM Subcommittee for drafting the report.

Mr. Charney thanked Ms. Sobieraj for her comments. He reminded participants that the next NSTAC meeting will be held on May 24, 2022. He then made a motion to close the meeting. Upon receiving a second, Mr. Charney officially adjourned the meeting.

APPENDIX
February 23, 2022, NSTAC Member Conference Call Participant List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corp.
Mr. William Brown	L3Harris Technologies, Inc.
Mr. Scott Charney	Microsoft Corp.
Mr. Matthew Desch	Iridium Communications, Inc.
Mr. David DeWalt	NightDragon Security, LLC
Mr. John Donovan	NSTAC Chair
Dr. Joseph Fergus	Communications Technologies, Inc.
Mr. Patrick Gelsinger	Intel Corp.
Mr. Jack Huffard	Tenable Holdings, Inc.
Ms. Renee James	Ampere Computing, LLC
Mr. Mark McLaughlin	Palo Alto Networks, Inc.
Mr. Angel Ruiz	MediaKind, Inc.
Mr. Stephen Schmidt	Amazon Web Services, 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. Jamie Brown	Tenable Network Security, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. Thomas Gann	Trellix
Mr. Jonathan Gannon	AT&T, Inc.
Mr. Jonathan Goding	Raytheon Technologies Corp.
Ms. Kathryn Gronberg	NightDragon Security
Mr. Yoav Hebron	Cohere Technologies, Inc.
Mr. Robert Hoffman	Broadcom, Inc.
Ms. Ilana Johnson	Neustar, Inc.
Mr. Kent Landfield	Trellix
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Thomas Patterson	Unisys Corp.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Robert Spiger	Microsoft Corp.
Dr. Claire Vishik	Intel Corp.
Mr. Milan Vlajnic	Communications Technologies, Inc.
Government Participants	
Ms. DeShelle Cleghorn	Department of Homeland Security

Mr. Trent Frazier	Department of Homeland Security
Ms. Ashley Freitas	Department of Homeland Security
Ms. Deirdre Gallop-Anderson	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. John "Chris" Inglis	Executive Office of the President
Ms. Rachel Liang	Department of Homeland Security
Dr. Michelle Rozo	National Security Council
Ms. Elke Sobieraj	National Security Council
Mr. Scott Zigler	Department of Homeland Security

Contractor Support

Mr. Ed Hudson	Arcfield
Ms. Megan Keeling	Booz Allen Hamilton, Inc.
Mr. Santana King	TekSynap Corp.
Mr. Kole Kurti	TekSynap Corp.
Ms. Laura Penn	Edgesource Corp.
Ms. Dana Ripley	Arcfield

Public and Media Participants

Ms. Karin Athanas	Testing, Inspection, and Certification Council – Americas
Ms. Mariam Baksh	Nextgov
Ms. Julia Benbenek	Morgan, Lewis & Bockius LLP
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.
Ms. Sara Friedman	Inside Cybersecurity
Mr. Matthew Eggers	U.S. Chamber of Commerce
Mr. Eric Geller	Politico
Dr. Philip Grant	Booz Allen Hamilton, Inc.
Mr. Derek Johnson	Cyber Risk Alliance
Mr. Albert Kammler	Van Scoyoc Associates, Inc.
Mr. David Thornton	Federal News Network

Certification

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

Mr. John Donovan
NSTAC Chair