President's National Security Telecommunications Advisory Committee

President's National Security Telecommunications Advisory Committee (NSTAC) Member Meeting Summary December 1, 2022

Call to Order and Opening Remarks

Ms. Christina Berger, Cybersecurity and Infrastructure Security Agency (CISA) 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 meeting was open to the public. She noted that no one had registered to provide comment but that written comments would be accepted following the procedures outlined in the meeting's Federal Register Notice. Following roll call, Ms. Berger turned the meeting over to Mr. John Donovan, Palo Alto Networks and NSTAC Chair.

Mr. Donovan welcomed the distinguished 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); Mr. John "Chris" Inglis, National Cyber Director, Executive Office of the President (EOP); and Mr. Brandon Wales, Executive Director, CISA.

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 on a national cybersecurity strategy from Mr. Inglis; (3) a status update on NSTAC recommendations from Mr. Wales; and (4) an update on the NSTAC Strategy for Increasing Trust in the Information and Communications Technology and Services (ICTS) Ecosystem (Strategy for Increasing Trust) Subcommittee provided by Mr. Scott Charney, Microsoft, NSTAC Vice Chair and Strategy for Increasing Trust Subcommittee Chair.

Mr. Donovan then invited Ms. Neuberger to provide her opening remarks. Ms. Neuberger acknowledged the NSTAC's 40th Anniversary, which occurred on September 13, 2022. She underscored the significant contributions made by the committee throughout the years, noting that it is a prime example of a trusted public-private partnership.

Ms. Neuberger stated that there is direct alignment between the committee's work and the administration's priorities, to include efforts focused on improving the resilience of the nation's communication networks and enhancing U.S. competitiveness in international communications technology standards. She also referenced the NSTAC's current four-phased effort on "Enhancing Internet Resilience in 2021 and Beyond", emphasizing that the phases directly align with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, and the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*. Ms. Neuberger noted that the EOP is currently reviewing the recommendations provided in the phase III *NSTAC Report to the President on Information Technology and Operational Technology Convergence* (IT/OT Convergence Report). Ms. Neuberger then officially tasked the NSTAC with its next study, focused on addressing the misuse of domestic infrastructure by foreign malicious actors.

Mr. Donovan thanked Ms. Neuberger for her comments and accepted the tasking on behalf of the NSTAC. He then invited Mr. Inglis to provide his remarks.

Mr. Inglis thanked the NSTAC for its efforts and explained that he would be discussing important issues that have a significant impact on U.S. national security during his keynote address.

Mr. Donovan thanked Mr. Inglis for his comments. He then invited Mr. Wales to provide his remarks.

Mr. Wales recognized the NSTAC's 40th Anniversary, noting that it has advised seven presidents on national security issues since its inception. He also acknowledged the 2022 NSTAC IT/OT Convergence Report, stating that it is a catalyst for government activity. Mr. Wales concluded his remarks by explaining that he would provide an update on the government's implementation of recent NSTAC recommendations later in the meeting.

Mr. Donovan thanked Mr. Wales for his remarks.

Keynote Address: National Cybersecurity Strategy

Mr. Donovan then invited Mr. Inglis to provide the keynote address on the development of a national cybersecurity strategy.

Mr. Inglis outlined his keynote address, stating he would discuss the "why", "how", and "when" of the nation's cybersecurity strategy. He explained that the reason why the nation should implement a comprehensive cybersecurity strategy is simply because one is needed. Mr. Inglis added that there are cybersecurity threats against the United States and its inhabitants and that these attacks should be the focus of both government and citizens.

Mr. Inglis then explained the "how" and "when" of the cybersecurity strategy. He described how the government has taken steps to begin the process of rebuilding the country's cybersecurity infrastructure, stating this process began with two key pieces of legislation that have been passed into law—the Infrastructure Investment and Jobs Act and the Inflation Reduction Act of 2022. Mr. Inglis explained that these two laws are being utilized to rebuild both U.S. physical and digital infrastructure.

Mr. Inglis continued that to properly rebuild U.S. cybersecurity infrastructure, the nation must create a national cybersecurity strategy. He stated this new national strategy will allow the nation to define the problems it wants to resolve, as well as assign the appropriate people to accomplish its goals. Mr. Inglis noted that it is vital that this new national cybersecurity strategy be implemented across the whole of government as it will allow public and private entities to contribute to the defense of the United States.

Mr. Inglis stated that as part of the new national cybersecurity strategy, the United States must construct—from the ground up—defensive infrastructure based on the principles of the zero trust security model that is built on a resilient architecture with the agility to respond to a variety of threats. He stated that the government must assume that its systems are vulnerable yet defensible. Mr. Inglis conceded the complexity of this task and stated that to accomplish it, the government must harness the capabilities of public-private partnerships such as NSTAC.

Mr. Inglis said that government procurement of secure software should be included in the national cybersecurity strategy. He underscored that it should be easier for agencies to procure safer products.

Mr. Inglis then noted that the federal government should use all capabilities to repel cybersecurity threats. He underscored that the disruption of cybersecurity threats does not exclusively occur on a digital battleground that solely utilizes cybersecurity capabilities as a means of defense. Rather, the United States should include practical forms of deterrence utilized in other areas of international relations and diplomacy, such as economic sanctions.

Mr. Inglis explained that in order for a new cybersecurity strategy to be effective it must be built on three pillars, notably: (1) it must harness the collective forces and abilities of public-private partnerships; (2) it must directly invest in a national cybersecurity infrastructure that is defensible; and (3) people must be at the center of the plan (i.e., the government must invest in making the public more aware of cybersecurity threats and what their role is in disrupting them).

Mr. Inglis concluded his address by stating that the national cybersecurity plan is not yet complete and should not be viewed as such at this time. Rather, he noted that this was a starting point to rebuild the American cybersecurity infrastructure.

Mr. Donovan underscored the usefulness of the information provided. Mr. Charney asked Mr. Inglis if insurance companies are making progress in understanding and developing the cyber insurance marketplace, and Mr. Inglis responded in the affirmative.

Mr. Donovan thanked Mr. Inglis for his address.

Status Update: NSTAC Recommendations

Mr. Donovan invited Mr. Wales to provide a status update on the government's implementation of NSTAC recommendations.

Mr. Wales began by referencing the 2022 NSTAC IT/OT Convergence Report, which recommended that CISA issue a Binding Operational Directive (BOD) that would assist federal departments and agencies in maintaining inventory of their OT devices, software, systems, and assets. In October 2022, CISA announced BOD 23-01, Improving Asset Visibility and Vulnerability Detection on Federal Networks, with the purpose of assisting federal agencies in increasing visibility into their assets and relevant vulnerabilities.

Mr. Wales stated that the 2022 *NSTAC Letter to the President on Standards* recommended revising export controls to encourage standards participation. On September 9, 2022, the Commerce Department's Bureau of Industry and Security coordinated with the National Institute of Standards and Technology to issue an interim final rule, amending the rule dated June 18, 2020. These revisions are intended to alleviate export controls and compliance concerns (as they relate to the Entity List) and lessen any impediments to the involvement of U.S. companies in domestic and international standards activities.

Mr. Wales then covered government progress in implementing recommendations from the 2022 *NSTAC Report to the President on Zero Trust and Trusted Identity Management*, which recommended the government incentivize zero trust in federal grants funding for IT security modernization. On March 28, 2022, the government released the Fiscal Year 2023 (FY23) President's Budget, which supports funding to facilitate the ongoing transition to a "zero trust" approach and improve federal agencies' abilities to rapidly detect and respond to cyber threats. He also acknowledged the State and Local Cybersecurity Grant Program (SLCGP), which enables DHS to make targeted cybersecurity investments in state, local, and territorial government agencies, thus improving the security of critical infrastructure and resilience of the services that these agencies provide to their communities. He expressed that CISA anticipates measuring whether zero trust principles can be integrated into the SLCGP guidance for FY23 and beyond.

Mr. Wales then referenced progress made in implementing recommendations in the 2021 *NSTAC Report to the President on Communications Resiliency*. He stated the report recommended that the government develop a post-quantum cryptography transition framework for government systems that evaluates legacy systems, catalogs, and analyzes the risk of public-key cryptography in use for various classes of data, and defines guidelines for updating those systems to a minimum standard. On July 6, 2022, CISA announced the Post-Quantum Cryptography Initiative to unify and propel agency efforts to address threats posed by quantum computing and support critical infrastructure and government network owners and operators during the transition to post-quantum cryptography.

Finally, Mr. Wales stated that the 2020 *NSTAC Report to the President on Software-Defined Networking* (SDN Report) called for the Department of Defense (DOD) to develop use cases for SDN and related technologies, including fifth generation (5G), that can be adapted for the private sector. In June 2021, DOD, through its 5G-to-Next 5G Initiative, successfully developed a prototype delivering high-speed downloads and ultra-low-latency capability for logistics modernization.

Mr. Wales concluded his remarks by thanking NSTAC for its dedication in resolving and anticipating NS/EP communications challenges.

Mr. Donovan thanked Mr. Wales for the update.

Status Update: NSTAC Strategy for Increasing Trust Subcommittee

Mr. Donovan invited Mr. Charney to provide the update on Strategy for Increasing Trust Subcommittee.

Mr. Charney stated that this subcommittee represents the fourth phase of the "Enhancing Internet

Resilience in the 2021 and Beyond" study and is the capstone of the effort. He emphasized that the phase IV report will build upon the three prior phases, which focused on: (1) software assurance in the ICTS supply chain; (2) zero trust and trusted identity management; and (3) IT/OT convergence. Additionally, the NSTAC is focusing on a new issue of security assurance, which may progress the nationwide security efforts reflected in EO 14028. Mr. Charney stated that by reviewing the three prior interconnected reports, the NSTAC can determine whether it has covered the landscape presented, or if there are gaps in the recommendations. He stated that there is also an opportunity to identify recommendations that, if enacted, might advance all three prior areas of focus. Mr. Charney added that if the study reveals that certain recommendations apply to multiple cybersecurity focus areas, then NSTAC should identify them and recommend they be prioritized.

Regarding the new issue of security assurance, Mr. Charney explained that the subcommittee receives its guidance from the U.S government's efforts to supplement policies with more robust implementations. He underscored that as information and communications technologies become more critical to daily life, concern increases as to how security requirements are set, how compliance with those requirements is proven, and how the proof to the users and regulators is communicated.

Mr. Charney noted that the subcommittee is examining the way in which the federal government requirements have been promulgated, assurance has been proved, and compliance has been communicated. He stated that the goal is to learn from prior efforts and identify best practices that increase confidence in the assurance process. Mr. Charney explained that as the challenges are not limited to federal government procurement, the subcommittee is also examining the persistent challenge posed by an increasing number of sector-specific security requirements. He stated that the goal is to identify how the government can meaningfully streamline regulatory processes and promote cross-sector harmonization to ensure that assurances with security requirements is more effective and efficient.

Mr. Charney said that to achieve the study's objectives, the subcommittee is following a process which includes receiving briefings from the government, private sector, and other organizations to understand their challenges with security compliance, learn from their perspectives, and listen to their recommendations. He stated that the subcommittee is currently in the process of drafting the final report, which NSTAC members will have the opportunity to review in the coming weeks. He welcomed feedback from the NSTAC members on additional recommendations or information that should be included in the forthcoming report and noted that the report is scheduled to be deliberated and voted on during the February 2023 NSTAC Member Conference Call.

Mr. Charney concluded the subcommittee update by thanking the subcommittee members for their efforts. He expressed that the NSTAC looks forward to sharing the final report with the administration.

Mr. Donovan thanked Mr. Charney for the update.

Closing Remarks and Adjournment

Mr. Donovan thanked participants for attending the meeting. He also expressed his gratitude to the government partners for their insight and guidance; he thanked Mr. Charney and the Strategy for Increasing Trust Subcommittee for their efforts; and he acknowledged the hard work of the NSTAC members and staff.

Mr. Donovan then asked Mr. Inglis to provide his closing remarks. Mr. Inglis thanked the NSTAC and Strategy for Increasing Trust Subcommittee for their efforts.

Mr. Donovan then invited Mr. Wales to provide his closing remarks. Mr. Wales underscored the importance of the NSTAC and emphasized that the committee's efforts provide insights into salient NS/EP issues.

Mr. Donovan then invited Mr. Steve Kelly, Special Assistant to the President and Senior Director for Cybersecurity and Emerging Technology, NSC, to provide his remarks. Mr. Kelly thanked Mr. Charney for his leadership of the subcommittee and expressed anticipation of the NSTAC's next study.

Mr. Donovan thanked Mr. Kelly for his comments. He noted that the next NSTAC Member Conference Call will occur on February 21, 2023, from 3:00 to 4:00 p.m. Eastern Time.

Mr. Donovan then made a motion to close the meeting. Upon receiving a second, Mr. Donovan officially adjourned the meeting.

APPENDIX
December 1, 2022, NSTAC Meeting Participant List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corp.
Mr. Scott Charney	Microsoft Corp.
Mr. David DeWalt	NightDragon Security, LLC
Mr. Raymond Dolan	Cohere Technologies, Inc.
Mr. John Donovan	Palo Alto Networks, Inc.
Dr. Joseph Fergus	Communication Technologies, Inc.
Ms. Lisa Hook	Two Island Partners, LLC
Mr. Jack Huffard	Tenable Holdings, Inc.
Mr. Mark McLaughlin	Qualcomm
Mr. Angel Ruiz	MediaKind, Inc.
Mr. Gary Smith	Ciena Corp.
Mr. Jeffrey Storey	Lumen Technologies, Inc.
NSTAC Points of Contact	
Mr. Jason Boswell	Ericsson, Inc.
Mr. Jamie Brown	Tenable Holdings, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Ms. Cheryl Davis	Oracle Corp.
Mr. Ryan Gillis	Palo Alto Networks, Inc.
Ms. Kathryn Gronberg	NightDragon Security, LLC
Mr. Yoav Hebron	Cohere Technologies, Inc.
Ms. Ilana Johnson	Centergate
Mr. Sean Morgan	Palo Alto Networks, Inc.
Ms. Jennifer Raiford	Unisys Corp.
Mr. Kevin Reifsteck	Microsoft Corp.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Dr. Claire Vishik	Intel Corp.
Government Participants	
Ms. Christina Berger	Cybersecurity and Infrastructure Security Agency
Ms. DeShelle Cleghorn	Cybersecurity and Infrastructure Security Agency
Mr. Ben Deering	National Security Council
Mr. Trent Frazier	Cybersecurity and Infrastructure Security Agency
Ms. Elizabeth Gauthier	Cybersecurity and Infrastructure Security Agency
Mr. Steve Kelly	National Security Council
Mr. Chris Inglis	Office of the National Cyber Director
Ms. Alexandra Martin	Cybersecurity and Infrastructure Security Agency

Ms. Anne Neuberger	National Security Council
Ms. Alicia Romano	National Security Council
Mr. Brian Scott	Office of the National Cyber Director
Ms. Tanya Simms	Office of the National Cyber Director
Mr. Barry Skidmore	Cybersecurity and Infrastructure Security Agency
Ms. Elke Sobieraj	National Security Council
Mr. Phil Stupak	Office of the National Cyber Director
Mr. Parry VanLandingham	National Security Council
Mr. Brandon Wales	Cybersecurity and Infrastructure Security Agency
Mr. Scott Zigler	Cybersecurity and Infrastructure Security Agency

Contractor Support

Ms. Joan Harris	Edgesource Corp.
Ms. Laura Penn	Edgesource Corp.
Ms. Lauren Rousseau	Edgesource Corp.
Ms. Shiri Telfer	Edgesource Corp.
Mr. Jennifer Topps	Teksynap Corp.
Mr. Joel Vaughn	Teksynap Corp.

Public and Media Participants

Ms. Mariam Baksh	NextGov
Mr. Calvin Biesecker	Defense Daily
Mr. Christopher Castelli	Booz Allen Hamilton
Mr. Justin Doubleday	Federal News Network
Mr. Chris Frascella	EPIC
Mr. Eric Geller	Politico
Mr. John Hunter	T-Mobile
Mr. Albert Kammler	Van Scoyoc Associates, Inc.
Mr. Kent Landfield	Trellix
Mr. Charlie Mitchell	Inside Cybersecurity
Mr. Chris Riotta	FCW
Mr. Rashard Rose	CNN
Mr. John Sakellariadis	Politico
Mr. Tim Starks	Washington Post
Ms. Saundra Throneberry	Lockheed Martin
Mr. Samuel Visner	MITRE

Certification

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

Mr. John Donovan
NSTAC Chair