PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

MEMBER MEETING | MAY 16, 2023

Call to Order and Opening Remarks

Ms. Christina Berger, Cybersecurity and Infrastructure Security Agency (CISA) and Designated Federal Officer (DFO) for the President's National Security Telecommunications Advisory Committee (NSTAC), 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. Brandon Wales, Executive Director, CISA, to swear-in the new members.

Mr. Wales swore in the new NSTAC members, congratulated them on their appointment to the committee and turned the meeting over to Mr. Scott Charney, Microsoft, NSTAC Chair.

Mr. Charney welcomed participants, congratulated the new NSTAC members, and thanked Mr. John Donovan, Palo Alto Networks, for his contributions and time while serving as the NSTAC Chair. He then welcomed the 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); Ms. Kemba Walden, Acting National Cyber Director, Office of the National Cyber Director (ONCD); and Mr. Wales.

In reviewing the agenda, Mr. Charney 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 efforts; (2) a keynote discussion on implementing an Internet of Things (IoT) labeling scheme with Ms. Neuberger; and (3) an update on the NSTAC Addressing the Abuse of Domestic Infrastructure (ADI) by Foreign Malicious Actors Subcommittee provided by Mr. Stephen Schmidt, Amazon, and Mr. Hock Tan, Broadcom, NSTAC ADI Subcommittee Co-Chairs.

Mr. Charney then invited Ms. Neuberger to provide her opening remarks. Ms. Neuberger welcomed the new members and stated that the oath of office they recited reminds her of her relatives who immigrated to the United States seeking protections provided by the Constitution. She recognized that the rights and privileges enjoyed by American citizens are not present in many countries, and thanked the NSTAC members for contributing their skills, experience, and expertise, to ensuring that the American dream remains safe.

Ms. Neuberger then congratulated Mr. Charney on being appointed as NSTAC Chair and Mr. Jeff Storey, Lumen Technologies, for being appointed as NSTAC Vice Chair.

Ms. Neuberger emphasized the importance of NSTAC's contributions over its 40-year history, underscoring the significant contributions the committee has made in helping shape the Executive Office of the President's response to threats of national security, including the most recent *NSTAC Report to the President on a Strategy for Increasing Trust in the Information and Communications*

Technology and Services Ecosystem. She added that she looked forward to hearing the status update on the ADI Subcommittee during the meeting.

Next, Ms. Neuberger officially tasked the NSTAC with its next study on measuring and incentivizing the adoption of cybersecurity best practices and stated that she looks forward to hearing the recommendations provided by this study. Mr. Charney thanked Ms. Neuberger for her remarks and invited Ms. Walden to provide comment.

Ms. Walden congratulated Mr. Charney and Mr. Storey on their appointment as NSTAC Chair and Vice Chair and the new members on their appointment to the committee. She remarked that the advice and contributions the NSTAC provides to the president are invaluable and help inform the policymaking process. She noted that NSTAC's studies helped shape the National Cybersecurity Strategy (NCS) that was released in March, and that she expects NSTAC's contributions will continue to influence efforts to implement the National Cyber Workforce and Education Strategy portion of the NCS. She underscored that the point of the NCS is to remove the burden from people, communities, and small and medium businesses and shift it to those who are more capable of addressing the issues. Regarding mobilizing the strategy, she said ONCD is working with its department and agency partners to develop the implementation plan and expects it will be released by summer 2023.

Ms. Walden expressed that there is a shortage of available cybersecurity experts in the current workforce. She stated that efforts are underway to develop the national cyber strategy for workforce and education. Ms. Walden also stated that there are four pillars for increasing the nation's cybersecurity workforce: (1) equipping American consumers with foundational cyber skills; (2) transforming cyber education to include an IoT program, computational math, and digital resiliency; (3) strengthening the national cyber workforce; and (4) strengthening the federal cyber workforce.

Ms. Walden concluded by expressing her gratitude to the NSTAC members for their time and commitment to furthering the country's cybersecurity foundations. Mr. Charney thanked Ms. Walden for her comments and invited Mr. Wales to provide remarks.

Mr. Wales congratulated Mr. Charney on his appointment as NSTAC chair and expressed his thanks to Mr. Donovan for his time as chair championing the NSTAC's work. He also welcomed the new members and stated that it is a great honor to serve on a committee which has distinguished itself during its history as the central point of public and private sector collaboration at the highest levels of government.

Mr. Wales referenced the work underway to build a more sustainable cybersecurity framework for the nation, noting that the threats are enormous and playing catch-up to adversaries is not the way to succeed in achieving cybersecurity goals. He stated that transforming the current approach relies on members' roles on the committee, and more broadly, the role that the private sector plays in helping the country achieve the necessary level of cybersecurity.

Mr. Wales said that there are key principles which underlie efforts to develop a sustainable cybersecurity framework, with one being that technology should be secure-by-design and secure-by-default. Another principal Mr. Wales discussed is that accountability for cybersecurity needs to be borne by those best able to handle it, and that a core aspect of corporate leadership is the need to be held accountable and responsible for decisions which impact cybersecurity. Mr. Wales emphasized the importance of giving corporate leaders the appropriate tools to make those decisions and that there needs to be radical transparency from information technology (IT) products and service providers.

Mr. Wales listed several ways in which digital literacy contributes to improving security, noting that tools such as IoT labeling empower consumers to make more informed technological security decisions, whether they are individual consumers, large businesses, or small businesses. He called for greater investment in public awareness regarding threats and what people can do to stay safe and secure in a very complicated ecosystem. He said the key is to define expectations regarding the roles of consumers, businesses, and technology platforms in achieving a higher level of security.

Mr. Wales emphasized the importance of working together to create a cultural shift regarding the collaboration between government and industry. He said that collaboration has certainly been an enduring focus of CISA and the administration for the last two-and-a-half years, and for the NSTAC as well. He expressed looking forward to continuing to partner with the NSTAC members to achieve their shared goals.

Mr. Charney thanked Mr. Wales for his comments.

Keynote Discussion: Implementing an Internet of Things (IoT) Labeling Scheme

Ms. Neuberger began by expressing her desire to obtain NSTAC input on a key government initiative on IoT labeling that is under development. She said studies show that American consumers want to buy secure technology but lack the knowledge necessary to determine what is secure and what is not. Ms. Neuberger added that unsecure smart home electronics (such as televisions, thermostats, and home lock systems) represent an ever-increasing attack surface for malicious actors. To address this concern, Ms. Neuberger stated that the government is devising a voluntary secure labeling program currently known as Energy Star for Cyber.

Ms. Neuberger explained that like the Energy Star program that allows consumers to know a product is energy efficient, the Energy Star for Cyber program would provide consumers with the knowledge and satisfaction that a product offers certain baseline securities, and it is safe to purchase. She noted that the Energy Star for Cyber program would include a physical mark on the product to show that it complies with government security standards. Ms. Neuberger explained that the program will first focus on consumer electronics with the idea of keeping Americans secure at home while reducing the attack surface available to malicious actors. She noted that a future phase of the program could focus on industrial IT and IoT security.

Mr. Dave DeWalt, NightDragon Management Company, asked how well the government understands the cyber-literacy gap between what the public thinks they know about security and their true knowledge levels. Ms. Neuberger replied by likening the Energy Star and the Energy Star for Cyber programs. She asked if the consumer needs to know how the security works on the technical side or if they only need to know that the product they are purchasing is secure.

Mr. Steve Schmidt stated that it is easy for consumers to understand that purchasing an Energy Star product is more expensive up front but will save them money in the long term. He noted, however, that the security environment is more difficult to understand, especially if the device they purchase is being used to attack someone other than themselves. He stated that the Energy Star for Cyber program would need to find a way to link personal benefit to the individual making the purchase and not just to the collective benefit of surrounding infrastructure.

Mr. Jeff Storey noted that unlike sustainability or energy efficiency, cybersecurity is not static and is always evolving and what is secure today might not be secure in the future. Ms. Neuberger replied that to counter this problem, the Energy Star for Cyber program is considering adding a barcode that consumers could scan to show if a product is still secure.

Ms. Barbara Humpton, Siemens USA, explained that another complicating factor is that IT products operate within a connected ecosystem whereas energy efficient products do not. She stated that it is one thing to label the device itself as being compliant under Energy Star for Cyber, but another thing to understand how that device will operate within an architecture it does not control.

Mr. Mark Dankberg, Viasat, agreed with Mr. Storey that security is inherently transient and will continue to evolve. He explained that the devices such as home routers are often located in places that are not accessed frequently which could make it difficult for people to get to them. He also noted that a problem with the barcode solution is that it shifts responsibility to the owner of the home IT equipment to ensure it remains secure.

Mr. Charney agreed with Mr. Dankberg, stating it was already difficult enough to get people to change the batteries in their smoke detectors, let alone ensure their home IT infrastructure remains secure. He stated that the product should update itself and that homeowners should not be involved in that process. Ms. Neuberger agreed, stating that perhaps for a product to gain certification, it must be updated for life by the product manufacturer. Mr. Jack Huffard, Tenable Holdings, stated that as a producer of such home IT products, liability concerns will be an issue if purchasers will be required to update their own products.

Mr. DeWalt asked if Ms. Neuberger has considered the supply chain and how these products are manufactured. He stated that a company could produce hundreds of different versions of a product and that the manufacturer needs to be included in the program. Ms. Neuberger replied that this is a valid point, and that the security will need to be maintained all the way through the supply chain process.

Mr. Bryan Palma, Trellix, asked what the economic benefit would be for a company to take part in the program. Ms. Neuberger referenced a study by Carnegie Mellon University that showed consumers want to purchase secure devices. She stated that if the product was labeled as certified by the Energy Star for Cyber program, it should carry a market advantage over similar products.

Ms. Noopur Davis, Comcast, stated that it could be helpful and increase corporate participation if the program began with small, incremental steps instead of making large changes from the beginning. She said this would allow corporations to adjust their supply chains gradually and not require them to invest extensive capital at the beginning of the transition. Mr. Schmidt agreed with Ms. Davis, stating that incremental changes could be put in place while allowing time for corporate buy-in of larger, more substantial changes.

Mr. DeWalt noted that there is a small number of first-party IoT device manufacturers and that they have already built-in sensible security in their products. He explained that third-party manufacturers will be an ongoing issue as the devices are produced at low price points and sold quickly. He explained that those third-party devices cannot be updated and are poorly configured.

Mr. Brandon Wales, CISA, noted that many small businesses use small home office routers and other IoT devices. He noted that many of them would be interested in cyber insurance to protect against ransomware incidents. Ms. Neuberger agreed that this was a valid point.

Mr. Charney thanked Ms. Neuberger for facilitating the IoT labeling discussion.

Status Update: NSTAC ADI Subcommittee

Mr. Charney invited Mr. Schmidt and Mr. Tan to provide the update on the NSTAC ADI Subcommittee's progress to date.

Mr. Schmidt expressed his appreciation to his fellow co-chair, Mr. Tan, and the subcommittee working group leads. He noted the subcommittee is currently in the process of producing the initial outline and first draft of the report, acknowledging key inputs from various subcommittee members. He thanked Ms. Berger and the NSTAC team for their assistance.

Mr. Schmidt lauded the expert advice received from government, private sector, and civil society in crafting substantial briefings on the task at hand, which was initially assigned during the December 2022 NSTAC Member Meeting. He reminded participants that he and Mr. Tan provided an update on the study during the February 2023 NSTAC Member Conference Call, at which time they noted this topic was already a key focus for the private sector as well as the administration, including in

Executive Order 13984, *Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*, and the associated rulemaking process.

Mr. Schmidt also lauded the subcommittee for their diligent work in defining the project's scope, a task he had stressed during the subcommittee kickoff meeting in February 2023. He appreciated their efforts in identifying key issues for the subcommittee to consider using information from expert briefings.

Mr. Schmidt then shared highlights that have influenced the scope of the study, noting that one critical element was understanding how U.S. infrastructure would be defined in the context of Internet ecosystem companies. He continued that based on White House guidance and expert input, the current focus of the report is on virtual private server hosting providers, web hosting providers, and infrastructure service providers. He said the expert input received indicate these companies are seen as pivotal in combating domestic infrastructure abuse, being the first line of defense against malicious activity.

Mr. Schmidt then discussed observations from briefings, highlighting that U.S. virtual infrastructure is relatively inexpensive and easily accessible, making it an attractive target for malicious actors. He acknowledged the complex division of authority and resource allocation across different U.S. agencies, which can lead to dissimilar objectives. Mr. Schmidt also discussed the obstacles to information sharing despite the existence of laws designed to encourage it.

Mr. Schmidt briefly discussed the effectiveness of know-your-customer (KYC) requirements as a tool against abuse by foreign actors, mentioning that their efficacy in this context is not clear. He emphasized the insights gathered from briefings will inform the study's final report and its recommendations. Mr. Schmidt then invited Mr. Tan to provide remarks on the status of the report outline and drafting process.

Mr. Tan summarized the progress made, highlighting the commencement of the report's initial draft based on substantial information gathered. He also underscored the aggressive timeline in which to complete the report, and that the NSTAC can illuminate the issues and identify constructive, actionable recommendations to address them.

Mr. Tan then discussed the report outline, stating that it will begin with background and emphasize the need to clarify definitions and parameters, such as “abuse”, “malicious actors”, and “domestic infrastructure”. He also discussed the importance of differentiating between various domestic infrastructure providers based on their unique characteristics and other factors. Mr. Tan added that providers may not experience the same threats and challenges, and he underscored the need to ensure there is differentiation with respect to possible solutions the U.S. government and stakeholders should take.

Mr. Tan noted the report will also focus on the divergent goals and objectives within the U.S. government and stakeholders concerning domestic infrastructure threat management. He stated that understanding these differing viewpoints, rooted in law or established practices, will be crucial to addressing the task.

Mr. Tan stated that the report will also concentrate on the key issues identified from subcommittee briefings that will be the source of the report's findings and recommendations. These issues include governmental authorities and legal barriers that inhibit government agencies from acting effectively to achieve their goals; necessary resources; effective collaboration; and KYC approaches.

Mr. Tan noted the report would conclude with actionable recommendations for the president and his administration, aligning with the findings from key issues. The study aims to address critical issues to bolster domestic infrastructure security. Mr. Tan concluded by urging subcommittee members to engage actively during the final phase, contributing their unique perspectives and ideas.

Mr. Charney thanked Mr. Schmidt and Mr. Tan for the update.

Closing Remarks and Adjournment

Mr. Charney thanked participants for attending and providing input into the discussion, and Mr. Tan and Mr. Schmidt for providing an update on the ADI Subcommittee's progress. He then invited Ms. Neuberger to provide her closing remarks.

Ms. Neuberger thanked everyone for the excellent discussion and echoed Mr. Charney's sentiments regarding the subcommittee's work. She remarked that NSTAC provides the type of timely, productive reports needed to guide government policy. Mr. Charney thanked Ms. Neuberger and invited Ms. Walden to provide remarks.

Ms. Walden extended her thanks to Mr. Tan and Mr. Schmidt as well, noting the timeliness of the subject matter, and stated that she is looking forward to reading the resulting report, which should also inform implementation of the National Cybersecurity Strategy. She added that enabling the public and private sector to defend against or to prevent cyber actors from abusing U.S. critical infrastructure is important to defending U.S. infrastructure. Mr. Charney thanked Ms. Walden and invited Mr. Wales to provide his closing remarks.

Mr. Wales commented that Ms. Neuberger's keynote generated a fantastic discussion among the participants and that he looks forward to continuing to work with everyone.

Mr. Charney thanked Mr. Wales for his remarks. He stated the next NSTAC meeting will be a Member Conference Call to be held in August 2023. He then made a motion to close the meeting. Upon receiving a second, Mr. Charney officially adjourned the meeting.

APPENDIX

Participant List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corp.
Mr. Johnathon Caldwell	Lockheed Martin
Mr. Scott Charney	Microsoft Corp.
Mr. Mark Dankberg	Viasat
Ms. Noopur Davis	Comcast
Mr. Matthew Desch	Iridium Communications, Inc.
Mr. David DeWalt	NightDragon Management Company
Mr. Raymond Dolan	Cohere Technologies, Inc.
Mr. John Donovan	Palo Alto Networks, Inc.
Dr. Joseph Fergus	Communication Technologies, Inc.
Mr. Jack Huffard	Tenable Holdings, Inc.
Ms. Barbara Humpton	Siemens USA
Ms. Renee James	Ampere Computing, LLC
Ms. Kimberly Keever	Cox Communications
Mr. Kyle Malady	Verizon
Mr. Kevin Mandia	Mandiant
Ms. Maria Martinez	Cisco
Mr. Jeff McElfresh	AT&T Communications
Mr. Bryan Palma	Trellix
Mr. Neville Ray	T-Mobile
Mr. Angel Ruiz	MediaKind, Inc.
Mr. Stephen Schmidt	Amazon
Mr. Jeff Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
Mr. Corey Thomas	Rapid7
NSTAC Points of Contact	
Ms. Grace Arsenault	Rapid7
Mr. Chris Boyer	AT&T Communications
Mr. Rudy Brioche	Comcast
Mr. Jamie Brown	Tenable Holdings, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Mr. Matt Carothers	Cox Communications
Mr. Bruce Cathell	Viasat
Mr. Drew Colliatie	Siemens USA
Ms. Kathryn Condello	Lumen Technologies, Inc.
Ms. Cheryl Davis	Oracle Corp.

Mr. Jesse Freund	Amazon Corporate
Mr. Thomas Gann	Trellix
Ms. Katherine Gronberg	NightDragon Management Company
Mr. Robert Hoffman	Broadcom, Inc.
Mr. John Hunter	T-Mobile
Mr. Kent Landfield	Trellix
Mr. Sean Morgan	Palo Alto Networks, Inc.
Ms. Jennifer Raiford	Unisys Corp.
Mr. Kevin Reifsteck	Microsoft Corp.
Mr. Nick Saunders	Viasat
Ms. Jordana Siegel	Amazon Web Services, Inc.
Ms. Stephanie Travers	Lumen Technologies, Inc.
Mr. Thomas Quillin	Intel Corp.
Mr. Kent Varney	Lockheed Martin
Mr. Eric Wenger	Cisco
Mr. Michael Woods	Verizon

Government Participants

Ms. Christina Berger	Cybersecurity and Infrastructure Security Agency
Ms. DeShelle Cleghorn	Cybersecurity and Infrastructure Security Agency
Mr. Trent Frazier	Cybersecurity and Infrastructure Security Agency
Ms. Helen Jackson	Cybersecurity and Infrastructure Security Agency
Mr. Steven Kelly	National Security Council
Ms. Tanya Sims	Office of the National Cyber Director
Mr. Barry Skidmore	Cybersecurity and Infrastructure Security Agency
Ms. Elke Sobieraj	National Security Council
Ms. Marilyn Stackhouse	Cybersecurity and Infrastructure Security Agency
Mr. Mark Stidd	Cybersecurity and Infrastructure Security Agency
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. Jennifer Topps	TekSynap Corp.
Mr. Carlus Townsend	Edgesource Corp.
Mr. Joel Vaughn	TekSynap Corp.

Public and Media Participants

Ms. Lindsay Bednar	Amazon Web Services, Inc.
Ms. Katelyn Christ	Department of Commerce
Ms. Donna Dodson	EvolutionQ
Mr. Christopher Frastella	Electronic Privacy Information Center
Ms. Sara Friedman	Inside Cybersecurity

Ms. Deirdre Gallop-Anderson	Cybersecurity and Infrastructure Security Agency
Mr. Eric Geller	Politico
Mr. Albert Kammler	Van Scoyoc Associates
Ms. Norma Krayem	Van Scoyoc Associates
Mr. Tom Laeithauser	Telecommunications Reports
Mr. Sunjeet Randhawa	Broadcom, Inc.
Mr. John Sakellariadis	Politico
Mr. Christian Vasquez	Cyber Scoop

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

Scott Ch

Mr. Scott Charney
NSTAC Chair