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 stated that no one had registered to provide oral comment, but 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. Scott Charney, Microsoft, NSTAC Chair.

Mr. Charney welcomed distinguished government partners in attendance, including Ms. Caitlin Clarke, Special Assistant to the President and Senior Director for Cybersecurity and Emerging Technology, National Security Council (NSC); Mr. Nicholas Leiserson, Assistant National Cyber Director for Cyber Policy and Programs, Office of the National Cyber Director (ONCD); and Mr. Brandon Wales, Executive Director, CISA.

Mr. Charney then provided a summary of the May 2023 NSTAC Member Meeting. stating that the committee: (1) heard remarks from government partners on key national security and emergency preparedness initiatives relevant to information and communications technologies; (2) participated in a keynote discussion led by Ms. Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, NSC, on implementing an Internet-of-Things labeling scheme; and (3) received a tasking from the administration to conduct a study on measuring and incentivizing the adoption of cybersecurity best practices (M&I). Mr. Charney added that, following the May 2023 NSTAC Member Meeting, the Executive Office of the President (EOP) tasked the NSTAC with a study on securing next generation wireless telecommunications.

In reviewing the September 2023 NSTAC Member Conference Call agenda, Mr. Charney noted that, during the meeting, NSTAC members would: (1) hear opening remarks from the administration and CISA leadership; (2) deliberate and vote on the Draft *NSTAC Letter to the President on Securing Next Generation Wireless Telecommunications* (Draft Next Generation Wireless Letter); (3) deliberate and vote on the Draft *NSTAC Report to the President on Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors* (Draft ADI Report); and (4) receive a status update on the M&I Subcommittee.

Mr. Charney then invited Ms. Clarke to provide her opening remarks. Ms. Clarke expressed her excitement to participate in her first NSTAC meeting in a senior director role, adding that she has had the opportunity in her previous positions to be informed by the NSTAC's efforts. She also expressed her anticipation of the meeting's agenda, particularly the M&I study update, which she said is vital in helping to protect our nation's critical infrastructure and supports the administration's priority to secure it. Mr. Charney thanked Ms. Clarke for her comments and invited Mr. Leiserson to provide remarks.

Mr. Leiserson noted that he would provide a brief update on the National Cybersecurity Strategy Implementation Plan (Implementation Plan) on behalf of Ms. Kemba Walden, Acting National Cyber Director, ONCD. He explained that the Implementation Plan was released on July 13, 2023, and includes 69 initiatives related to 27 strategic objectives in the National Cybersecurity Strategy. A lead agency is responsible for executing each initiative and there are 18 different agencies spearheading at least one initiative. He added that all of the Implementation Plan initiatives are scheduled to be completed by fiscal year (FY) 2026.

Mr. Leiserson said the Implementation Plan is an iterative document and that NSTAC members can expect new versions to be updated and released annually. The president will also receive an annual report on progress for implementation. Mr. Leiserson mentioned that ONCD would welcome the opportunity to follow-up with NSTAC members as they desire on portions of the Implementation Plan, adding that the committee's products for the president can help inform future iterations. Mr. Charney thanked Mr. Leiserson for his comments and invited Mr. Wales to provide his opening remarks.

Mr. Wales expressed his desire to underscore one issue relative to Mr. Leiserson's discussion on the Implementation Plan. He noted that since the May 2023 NSTAC Member Meeting, CISA released its FY2024-2026 Cybersecurity Strategic Plan which organizes the agency's efforts under the guidance of the broader National Cybersecurity Strategy and focuses on three enduring goals: (1) address immediate threats; (2) harden the terrain; and (3) drive a more secure ecosystem.

Mr. Wales noted that CISA is working to accomplish its various responsibilities within the Implementation Plan, most prevalently in regard to National Cybersecurity Strategy Pillar One: Defending Critical Infrastructure. CISA has overall efforts designed to assist in gaining broader visibility into intrusions targeting the United States, advancing and promoting the adoption of strong security practices, and reimagining the possibilities and expectations for security-focused operational collaboration between industry and government. Mr. Wales stated that CISA is working with stakeholders to understand long-term cybersecurity planning and prioritization, adding that it is a shared responsibility, journey, and challenge that everyone must work toward together.

Finally, Mr. Wales underscored his enthusiasm to learn more about recent NSTAC efforts, including the Draft Next Generation Wireless Letter, the Draft ADI Report, and the NSTAC M&I study.

Mr. Charney thanked Mr. Wales for his comments.

Deliberation and Vote: *NSTAC Letter to the President on Securing Next Generation Wireless Telecommunications*

Mr. Charney then introduced Mr. Raymond Dolan, Cohere Technologies, and asked him to present the Draft Next Generation Wireless Letter.

Mr. Dolan thanked the NSTAC members and points of contact for their time and expertise toward producing the final version of the document. He explained that the topic of the Draft Next Generation Wireless Letter is complex and includes many facets. He noted that the breadth of NSTAC membership generated a broad range of perspectives which was a tremendous benefit and that the letter reflects those views as much as possible. He added that, throughout the development of the draft letter, the authors sought to integrate the views of all members and, when views diverged, the draft letter seeks to offer a fair compromise.

Mr. Dolan continued that the draft letter attempts to balance the goals of those primarily using licensed spectrum with those utilizing unlicensed spectrum. He said the draft letter provides a significant voice to both cellular operators that have spent hundreds of billions of dollars on spectrum licenses and technology providers that have invested heavily in Wi-Fi solutions. Mr. Dolan explained that the draft letter acknowledges the role of today's satellite networks and the likelihood of their increased importance moving forward. The draft letter also highlights the importance of the defense industry and its critical reliance on spectrum now and into the future, as well as the significance of U.S.-only spectrum and international spectrum decisions. He noted there is tension among constituencies as future spectrum is considered for allocation and said this is reflected in the draft letter in a fair and balanced manner.

Mr. Dolan commented that the draft letter addresses the technology issues that need resolution in order for the United States to secure a trusted and diversified supply chain for all wireless networks moving forward (particularly for cellular networks). He also noted that there are tradeoffs. Current suppliers are critical to running and expanding existing cellular networks and need to be supported going forward. At the same time, everyone acknowledges the need for new entrants to expand and diversify the supply chain and broaden the industrial base that can sustain the aggregate research and development needed to lead moving onward. Mr. Dolan concluded that the draft letter makes every effort to focus on the facts and provide actionable recommendations. This requires a balanced approach with policies that protect existing investments while incentivizing accelerated innovation.

Mr. Charney thanked Mr. Dolan and opened the floor for comments or questions from NSTAC members and government partners. Ms. Maria Martinez, Cisco, expressed her agreement with the need for a comprehensive spectrum strategy that enables effective access to mid-band spectrum, including Wi-Fi and licensed applications. She also noted her concurrence with the importance of ensuring that international standard-setting efforts are not politicized, adding that she supports the importance of developing incentives to enable American innovators to robustly participate in those efforts.

Mr. Johnathon Caldwell, Lockheed Martin, thanked Mr. Charney and Mr. Dolan for their work developing the draft letter. He expressed his support in the need for NSTAC to take a hard look at the key elements in securing next generation wireless capabilities and making balanced recommendations to the president. He underscored that it's never been more critical to ensure that the United States' national security capabilities are prominently accounted for in any

recommendation concerning the strategy for spectrum allocation. Mr. Caldwell added that the letter should elevate the coexistence of commercial and national defense equities. He said that the recommendations should acknowledge and account for adverse nations' attempts to shape the use of spectrum in their favor through international standards bodies.

Mr. Caldwell said the defense industry, major wireless carriers, original equipment manufacturers, and satellite operators are routinely collaborating on commercial wireless technologies and standards and solutions for national security needs. This includes informing an ongoing Department of Defense study known as "Partnering to Advance Trusted and Holistic Spectrum Solutions" which includes many key regulators like the National Telecommunications and Information Administration and Federal Trade Commission on spectrum sharing for next generation wireless. Mr. Caldwell explained that, once complete, it will be a powerful companion piece to a NSTAC recommendation. He said the United States is not just in a competition for fifth generation (5G) telecommunications and standards, and that the nation needs the ability to deploy next generation telecommunications of its own defense capabilities in addition to maintaining commercial leadership in wireless operations.

Ms. Noopur Davis, Comcast, expressed appreciation to Mr. Dolan and Mr. Charney for reflecting Comcast's views in the draft letter. However, she added that the company has continuing concerns that the draft letter does not include balanced references to both licensed and unlicensed spectrum.

Ms. Davis said that, as it is written, the draft letter continues to focus predominantly on 5G and sixth generation-licensed services while de-emphasizing unlicensed and sharing approaches that enable additional innovation and efficient use of spectrum. She noted that, despite these concerns, Comcast is satisfied with the draft letter.

Upon hearing no further comments, Mr. Charney made a motion to approve the report, which was seconded. Following the motion, the NSTAC members voted on approving the Draft Next Generation Wireless Letter for transmission to the president. 21 NSTAC members voted to approve the draft letter and one member, Mr. Caldwell, abstained from voting.

Deliberation and Vote: *NSTAC Report to the President on Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*

Mr. Charney invited Mr. Stephen Schmidt, Amazon, and Mr. Hock Tan, Broadcom, NSTAC Addressing the Abuse of Domestic Infrastructure (ADI) by Foreign Malicious Actors Subcommittee Co-Chairs, to present the Draft ADI Report.

Mr. Tan noted that the draft report outlines a number of relevant findings and actionable recommendations for the president to consider and implement. He reminded participants that the EOP tasked the NSTAC with the study at the December 2022 NSTAC Meeting. In response, the NSTAC established the ADI subcommittee to investigate and report on the voluntary actions that key internet ecosystem companies take to prevent or mitigate ADI by foreign malicious actors.

Mr. Tan said the EOP also requested the subcommittee investigate factors that are creating opportunities, challenges, and barriers—including financial, legal, technological, and human—that may be assisting or preventing public and private stakeholders from systematically addressing malicious actor ADI. The process the subcommittee undertook to produce the final draft report has led to several important findings and actionable recommendations that, together, can be instrumental in future government and industry efforts to address ADI.

Mr. Tan explained that scoping the effort was critical and led to several key findings. For example, the NSTAC had to carefully define what was meant by "abuse" and who was meant in defining "malicious actors." In the context of "cyber operations," this abuse could include everything from foreign-based nation-state activity to financially motivated cybercrime.

Mr. Tan said that subcommittee briefers consistently identified ADI as a significant issue. However, government briefers could not articulate with specificity: the type of abuse they were most concerned with or sought to address; the tactics of malicious actors; or where they had the greatest challenges. Industry briefers were clear that the techniques they employ are designed to prevent or mitigate all types of abuse. Mr. Tan said that both government and private sector briefers did not have a consistent answer as to whether it is possible to tell the difference between a foreign and domestic actor. This led to a key finding that there is no technical or consistent method to distinguish ADI between foreign and domestic actors with speed and accuracy at the macro level, especially for routine online business transactions. He stated that this is different than attribution after an event has occurred, which is more attainable, but also time consuming, costly, and labor-intensive. Given this finding, the guidance in the report is generally applicable to prevent all ADI, regardless of the malicious actors' country of origin.

Mr. Tan underscored that while the National Cybersecurity Strategy and Implementation Plan called for the prevention of abuse of U.S.-based infrastructure, U.S. government briefers did not articulate a clear overarching strategy with respect to addressing ADI. He noted that, absent such a strategy, there is an unintentional risk of overlapping and competing priorities and interests among the agencies with relevant responsibilities and a lack of unity of effort across the ecosystem. This can complicate government efforts to work with the private sector to address ADI.

Mr. Tan said that this led to another key finding which is the need for a multi-faceted strategy to combat ADI. While many efforts to combat ADI are currently in place or under development, a strategic, coordinated approach is essential to help unify these efforts.

Mr. Tan said a third key finding relates to Know Your Customer (KYC) requirements on infrastructure as a service provider that are being considered by the U.S. government. After numerous briefings over several months, the subcommittee found that KYC requirements alone are not likely to reduce ADI by malicious actors. However, given the existence of best practices already being utilized today by some infrastructure providers, the subcommittee established that development and use of such practices should be elevated and promoted, and should factor into how the Commerce Department considers the potential implementation of KYC.

Mr. Tan noted the final draft report also makes several findings on government collaboration with the private sector. First, focused information sharing and collaboration between the private sector and the government, as well as within the private sector, is needed to better understand the scope and scale of ADI and adequately address it. Second, the report identifies real and perceived barriers for private sector companies to share threat information with one another and the government. He said that such barriers include resource constraints, legal and reputational concerns, and privacy constraints from both domestic and international laws.

The last finding Mr. Tan discussed is the promise technology provides us to enhance our collective ability to combat ADI, such as through privacy-enhancing technologies that can support greater collaboration, particularly between companies. There is also potential for additional applications, such as artificial intelligence and machine learning, to boost the efficiency of efforts to detect, mitigate, and prevent or disrupt ADI.

Mr. Schmidt then explained that the subcommittee identified six actionable recommendations that flow directly from the report's findings, a few of which can be immediately implemented.

Mr. Schmidt noted that the first recommendation is for the president to direct ONCD to develop a strategy for combating ADI that recognizes the need for, and establishes, a long-term, multi-faceted approach to combat ADI as part of its implementation of the National Cybersecurity Strategy. He underscored appreciation of the inclusion of this issue in the National Cybersecurity Strategy but explained that there needs to be a more coordinated approach that is informed by data about the issue and the scale and extent to which malicious actors are abusing U.S. domestic infrastructure.

Next, Mr. Schmidt said the second recommendation is for the U.S. government, working through existing mechanisms such as CISA's Joint Cyber Defense Collaborative and National Security Agency's Cybersecurity Collaboration Center, to create an operational working group that includes relevant private-sector providers and key government representatives to focus on enhancing tactical, operational collaboration to address ADI. The goal is to engage subject matter experts (SME) from the government and the private sector and focus on how both can more effectively operationalize combatting ADI in real-time and identify opportunities for joint responsive action.

The third recommendation is in response to the report's finding regarding the important role technology can assume in providing the necessary tools to combat ADI. Specifically, NSTAC recommends that the U.S. government, through the National Institute of Standards and Technology and other relevant departments and agencies, conduct a pilot program to test the practical application of privacy enhancing technologies to accelerate the development of at-scale data sharing and analysis of threats to domestic infrastructure.

Mr. Schmidt said that the fourth recommendation focuses on the importance of best practices. NSTAC recommends that the U.S. government create a public-private task force to develop a framework that outlines best practices to mitigate ADI, including for managing reseller relationships.

This framework will serve as a guide to enhance security practices of technology providers across the ecosystem.

Mr. Schmidt explained that the fifth recommendation is designed to improve multilateral information sharing. Specifically, the NSTAC recommends that the U.S. government, working through relevant national security and law enforcement agencies, develop a strategy to share intelligence with international partners regarding U.S. government concerns about ADI, encourage joint operations, provide feedback to infrastructure providers, and facilitate collective defense.

Mr. Schmidt noted that the sixth recommendation in the report gets to an important legal milestone for information sharing. In just two years, the Cybersecurity Information Sharing Act of 2015 (CISA 2015) is scheduled to expire. This presents an opportunity to review and update this law to account for remaining barriers and further advance information sharing. Accordingly, the NSTAC recommends that the U.S. government work through CISA and the Department of Justice, in coordination with the private sector to develop a set of recommendations to update and enhance CISA 2015.

Mr. Schmidt explained that each of these recommendations on their own will improve government, industry, and civil society's overall ability to combat ADI. However, the overall impact will increase exponentially as collective recommendations are implemented.

Mr. Charney thanked Mr. Schmidt and Mr. Tan for their efforts and opened the floor for comments or questions from NSTAC members and government partners before proceeding to a vote to approve the report. Ms. Martinez thanked Mr. Schmidt and Mr. Tan for their efforts and expressed her appreciation for the opportunity for Cisco to provide input. She asked that the NSTAC continue to engage on this important topic.

Upon hearing no further comments, Mr. Charney made a motion to approve the report, which was seconded. The NSTAC members voted unanimously to approve the Draft ADI Report for transmission to the president.

Status Update: NSTAC M&I Subcommittee

Mr. Charney then invited Ms. Kimberly Keever, Cox Communications and NSTAC M&I Subcommittee Co-Chair, to provide an update on the study.

Ms. Keever said that the subcommittee was tasked with developing a report to advise the federal government on how it can measure the degree to which entities adopt cybersecurity best practices. She added that the committee was further tasked with developing recommendations on how the government can best incentivize adoption.

Ms. Keever noted that the M&I Subcommittee was formed in June 2023, and received its first briefing in late July 2023. She explained that the meeting cadence includes two subcommittee meetings (to include briefings) per week, along with weekly internal and working group lead discussions.

Ms. Keever said that NSTAC's work is vital to helping protect the nation's critical infrastructure and expressed appreciation to the subcommittee members for their commitment toward addressing the significant cybersecurity challenges facing multiple industrial sectors.

Ms. Keever said that in terms of scoping, the subcommittee decided against recommending any specific best practices as those vary from industry to industry. Rather, the subcommittee anticipates recommending methodologies that will apply broadly to cybersecurity measurement in general. It will recommend how to collect objective, quantifiable data and how to use that data in a mathematically sound manner that does not create perverse incentives.

Ms. Keever explained that several consistent themes are emerging from briefings to the subcommittee. She said that measurements must be quantitative, objective numbers rather than qualitative or subjective words. Ms. Keever said methodologies must be transparent, and that stakeholders must have a clear understanding of how measurements are taken and what steps can improve them. She also underscored that care must be taken to protect stakeholders' data. Information about a company's cybersecurity posture could be a roadmap for attackers if handled improperly. She explained that stakeholders respond better to rewards than punishments.

Ms. Keever said that, as the subcommittee drafts the report, it will provide an overview of specific issues as well as success stories and cautionary tales from SMEs. She closed by stating that she anticipates the subcommittee will release the final Draft M&I Report in February 2024.

Mr. Charney thanked Ms. Keever for the update.

Closing Remarks and Adjournment

Mr. Charney thanked: participants for attending; NSTAC members for providing input during the discussions; government partners for their insights; Mr. Dolan, Mr. Schmidt, and Mr. Tan for leading the development of their respective products; Ms. Keever for providing the M&I Subcommittee update; and the subcommittee working group leads, members, and the NSTAC team for their efforts.

Mr. Charney then asked if anyone else had any final comments they would like to offer. Hearing none, he stated that the next NSTAC meeting is scheduled for December 7, 2023. He then made a motion to close the meeting, which was seconded, and Mr. Charney officially adjourned the meeting.

APPENDIX

September 26, 2023, NSTAC Member Conference Call Participant List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corp.
Mr. Johnathon Caldwell	Lockheed Martin
Mr. Scott Charney	Microsoft Corp.
Ms. Noopur Davis	Comcast Corp.
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.
Ms. Lisa Hook	Two Island Partners, LLC
Ms. Barbara Humpton	Siemens USA
Ms. Kimberly Keever	Cox Communications, Inc.
Mr. Kyle Malady	Verizon Communications, Inc.
Mr. Kevin Mandia	Mandiant
Ms. Maria Martinez	Cisco Systems, Inc.
Mr. Jeffery McElfresh	AT&T Communications
Mr. Bryan Palma	Trellix
Mr. Neville Ray	T-Mobile US, Inc.
Mr. Angel Ruiz	MediaKind, Inc. and Nsight
Mr. Stephen Schmidt	Amazon
Mr. Jeffrey Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
Mr. Corey Thomas	Rapid7, Inc.

NSTAC Points of Contact

Mr. Christopher Anderson	Lumen Technologies, Inc.
Mr. Christopher Boyer	AT&T Communications
Mr. Rudy Brioché	Comcast Corp.
Mr. Jamie Brown	Tenable Network Security, Inc.
Mr. Matt Carothers	Cox Communications, Inc.
Mr. Bruce Cathell	Viasat
Mr. Drew Colliatie	Siemens USA
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. William Conner	Iridium Communications, Inc.
Mr. Jesse Freund	Amazon Corporate
Mr. Thomas Gann	Trellix
Ms. Katherine Gronberg	NightDragon Management Company
Mr. Yoav Hebron	Cohere Technologies, Inc.
Mr. Robert Hoffman	Broadcom, Inc.
Mr. Kent Landfield	Trellix
Mr. Sean Morgan	Palo Alto Networks, Inc.
Ms. Helen Negre	Siemens USA
Mr. Christopher Oatway	Verizon Communications, Inc.
Mr. Thomas Quillin	Intel Corp.
Ms. Jennifer Raiford	Unisys Corp.
Mr. Kevin Reifsteck	Microsoft Corp.
Mr. Nick Saunders	Viasat, Inc.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Ms. Stephanie Travers	Lumen Technologies, Inc.
Mr. Eric Wenger	Cisco Systems, Inc.
Mr. Michael Woods	Verizon Communications, Inc.

Government Participants

Ms. Christina Berger	Cybersecurity and Infrastructure Security Agency
Ms. Caitlin Clarke	National Security Council
Ms. DeShelle Cleghorn	Cybersecurity and Infrastructure Security Agency
Ms. Elizabeth Gauthier	Cybersecurity and Infrastructure Security Agency
Ms. Helen Jackson	Cybersecurity and Infrastructure Security Agency
Mr. Nicholas Leiserson	Office of the National Cyber Director
Ms. Valerie Mongello	Cybersecurity and Infrastructure Security Agency
Mr. Jonathan Murphy	National Security Council
Mr. Barry Skidmore	Cybersecurity and Infrastructure Security Agency
Mr. Wayne Rash	Cybersecurity and Infrastructure Security Agency
Mr. William Rybczynski	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 Poole	Edgesource Corp.
Mr. Nicholas Smith	TekSynap Corp.

Public and Media Participants

Ms. Lindsay Bednar	Amazon Web Services, Inc.
Mr. Raymond DeMeo	Virsec Systems
Mr. John Evans	Cayuga County, New York
Ms. Sara Friedman	Inside Cybersecurity
Mr. Tom Leithauser	Telecommunications Reports/Cybersecurity Policy Report
Mr. John Miller	Information Technology Industry Council
Mr. Steve Nelson	Goldman Sachs Group, Inc.
Ms. Amanda Olson	Southern California Edison
Ms. Erin Pattillo	Cybersecurity and Infrastructure Security Agency
Ms. Thais Price	Cybersecurity and Infrastructure Security Agency
Mr. Sunjeet Randhawa	Broadcom, Inc.
Mr. Ari Schwartz	Broadcom, Inc.
Ms. Kate Siefert	Cybersecurity and Infrastructure Security Agency
Ms. Suzanne Smalley	The Record
Mr. Tim Starks	The Washington Post
Mr. Christopher Whyte	Cybersecurity and Infrastructure Security Agency
Mr. Will Williams	Cybersecurity and Infrastructure Security Agency

Certification

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

Mr. Scott Charney
NSTAC Chair