Call to Order and Opening Remarks

Ms. Christina Berger, the President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Officer, Cybersecurity and Infrastructure Security Agency (CISA), called the meeting to order. She stated that the NSTAC is a federal advisory committee, governed by the *Federal Advisory Committee Act* and that the meeting is open to the public. She noted that no individuals registered to provide comment, but written comments would be accepted following the procedures outlined in the meeting's Federal Register Notice. Ms. Berger conducted roll call and handed the meeting over to Mr. Scott Charney, Microsoft and NSTAC Chair.

Mr. Charney welcomed distinguished government partners including Mr. Harry Coker, Jr., National Cyber Director, Office of the National Cyber Director (ONCD); Mr. Jonathan Murphy, Director for Critical Infrastructure Cybersecurity, National Security Council (NSC); and Mr. Brandon Wales, Executive Director, CISA.

Mr. Charney reviewed items from the December 2023 NSTAC Member Meeting, which included remarks from government partners on key national security and emergency preparedness initiatives. Specifically, Mr. Charney recalled that Ms. Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, NSC, discussed recent cyber incidents impacting the water and healthcare sectors that highlighted the continued threat against U.S. critical infrastructure. She explained that these incidents represented examples of attacks the administration is looking to defend against by establishing minimum cybersecurity practices for sectors. Lastly, Mr. Charney recalled that the administration tasked the NSTAC to conduct a study on Principles for Baseline Security Offerings from Cloud Service Providers and draft a letter to the president on industry views of dynamic spectrum sharing (DSS).

Mr. Charney then summarized the agenda for the March 2024 NSTAC Member Conference Call which included: (1) remarks from the administration and CISA leadership; and (2) the deliberation and vote on two NSTAC products, the *NSTAC Report to the President on Measuring and Incentivizing the Adoption of Cybersecurity Best Practices* and the *NSTAC Letter to the President on Dynamic Spectrum Sharing*.

Finally, Mr. Charney provided a brief update on the status of the upcoming NSTAC Baseline Security Offerings study. He stated that Mr. Kevin Mandia and Ms. Maria Martinez have agreed to co-chair and provide leadership for the NSTAC Baseline Security Offerings Subcommittee. He explained that the subcommittee will examine what principles should guide cloud service providers in determining whether a security feature should be included in cloud service offerings by default and what features should, pursuant to those principles, be provided to various categories of critical infrastructure stakeholders at no additional cost. Mr. Charney then introduced Mr. Coker and invited him to provide opening remarks.

Mr. Coker thanked Mr. Charney and said that he assumed the role of National Cyber Director only 13 weeks prior to the meeting. He expressed his appreciation of the committee's collaboration and

work to date, to include the NSTAC's reports on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem, Software Assurance, Zero Trust, and IT/OT Convergence.

Mr. Coker stated that in March 2023, the president released the National Cybersecurity Strategy (the Strategy), followed by the National Cybersecurity Strategy Implementation Plan (Implementation Plan) in July 2023. He explained that to date, the ONCD has completed more than 20 of the 69 initiatives in the Implementation Plan, has continued to work with cyber sector partners to continue driving progress, and will release an updated implementation plan by late spring or early summer 2024.

Mr. Coker thanked the NSTAC for their advice to the president and the Executive Office of the President. He shared his anticipation to hear and discuss the findings and recommendations of the NSTAC Measuring and Incentivizing Report and the NSTAC Dynamic Spectrum Sharing Letter, as well as his continued work with the NSTAC. Mr. Charney thanked Mr. Coker for his remarks and invited Mr. Brandon Wales to speak.

Mr. Wales thanked the NSTAC for their insightful work, making particular note of the NSTAC Measuring and Incentivizing Report. He stated that on February 7, 2024, CISA, in conjunction with the National Security Agency, Federal Bureau of Investigation, and other U.S. and international partners, issued a joint cybersecurity advisory warning of a shift in malicious cyber activity against the United States. The People's Republic of China state-sponsored cyber actors, including a group known as Volt Typhoon, are burrowing deep into U.S. critical infrastructure to launch destructive cyberattacks in the event of a major crisis or conflict with the United States and its allies. Volt Typhoon actors are pre-positioning themselves on information technology networks and possess capabilities to disrupt operational technology functions across multiple critical infrastructure sectors.

Mr. Wales recommended organizations take the necessary actions to detect if this activity is on their networks, apply mitigation practices to improve cybersecurity posture, and strengthen resilience to reduce impact of malicious activity. He stressed the imperative to identify ways to incentivize the adoption of cybersecurity best practices. Mr. Charney thanked Mr. Wales for his remarks and welcomed Mr. Matt Desch, Iridium Communications and Co-Chair of the NSTAC Measuring and Incentivizing Subcommittee, to begin his remarks on the findings and recommendations in the *NSTAC Report to the President on Measuring and Incentivizing the Adoption of Cybersecurity Best Practices*.

Deliberation and Vote: *NSTAC Report to the President on Measuring and Incentivizing the Adoption of Cybersecurity Best Practices*

Mr. Desch shared his appreciation for his fellow subcommittee co-chairs [Jack Huffard, Tenable and Kim Keever, Cox Communications] and the working group leads. He expressed his satisfaction of having three NSTAC members act as co-chairs for the study, allowing the subcommittee and report to benefit from additional leadership and more diverse opinions.

Mr. Desch stated that the report addressed challenges the United States faces regarding managing and incentivizing cybersecurity best practices on behalf of U.S. national infrastructure. Despite government, standards organizations, and other stakeholders creating numerous best practices and standards around cybersecurity, many organizations are either not adopting or are poorly implementing them. This increases the likelihood of threats and cybersecurity incidents with deeper impact. Additionally, he explained that a lack of consistent adoption and implementation of cyber best practices and standards is especially problematic as U.S. critical infrastructure entities face a significantly heightened threat landscape in the current geopolitical environment.

Mr. Desch noted that the NSTAC Measuring and Incentivizing Subcommittee received approximately 50 briefings from a wide range of government officials, critical infrastructure industry representatives, cybersecurity insurance carriers, cloud service and technology providers, consultants, trade associations, and think tanks.

Mr. Desch explained that the NSTAC Measuring and Incentivizing Report highlighted four key findings: (1) material gaps exist between the cybersecurity investments that organizations make based on cost-benefit analyses and the investments the federal government believes are required by those organizations to improve the security posture of the nation; (2) civil, criminal, and regulatory liabilities are creating disincentives for effective cybersecurity information sharing, and liability protections will be required to enable participation in effective information-sharing processes; (3) industry stakeholders have spent considerable efforts aligning their cyber programs with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and other international, consensus-driven standards, but duplication or conflict within various regulatory requirements continues to strain organizational cybersecurity budgets, resources, and priorities; (4) government and private sector have access to significant amounts of cybersecurity data that could be better utilized to help support more effective measurements and metrics.

The recommendations provided in the NSTAC Measuring and Incentivizing Report to address these key findings included the government should: (1) develop a strategy to make recommendations on impactful financial incentives, such as tax deductions or federal grants for organizations that adopt appropriate cybersecurity best practices; (2) develop a nationwide education and outreach program for critical infrastructure providers to increase the use of the many free services already offered; (3) connect liability reform and safe harbors to the sharing of threat, incident, and other information with the government for those organizations that can demonstrate they have adopted cybersecurity best practices; (4) require federal agencies to map any new proposed cybersecurity requirements to the NIST Cybersecurity Framework and that deviations should be explained and minimized; (5) establish a Cybersecurity Measurement Center of Excellence under the Department of Commerce to coordinate data collection and management; (6) develop a resource center to help organizations leverage the NIST Cybersecurity Framework to develop measurements and metrics tied to business outcomes; (7) establish virtual national cyber academies to provide free training in exchange for service as a lack of qualified personnel is often cited as a barrier to organizations adopting best practices; and (8) create a cybersecurity "Grand Challenge" for organizations to leverage next generation Artificial Intelligence and Machine

Learning capabilities to drive adoption and use of cybersecurity best practices and enable more efficient measurement. Mr. Desch explained that additional details can be found in the full report.

Mr. Charney thanked Mr. Desch for his efforts and opened the floor for comments or questions from NSTAC members and government partners.

Ms. Martinez stated that Cisco provided use cases describing the importance of this study and the negative real-world consequences that follow from failure to apply software patches. She then highlighted a specific concern listed in the report that if hardware, and/or software, are beyond the manufacturer's supported lifespan, they cannot be properly secured. She suggested a future study with more sustained attention to this matter be undertaken as many stakeholders have a role to play in this domain. She implored vendors to develop technology that is secure by default, and operators to take additional steps in applying known security patches while also replacing hardware that is past its lifespan and can no longer be secured. She emphasized that government must share known risks and mitigations with everyone, especially with key stakeholders.

Upon hearing no further comments, Mr. Charney made a motion to approve the *NSTAC Report to the President on Measuring and Incentivizing the Adoption of Cybersecurity Best Practices*. Following the motion, which was seconded, NSTAC members voted unanimously to approve the report for transmission to the president.

After the vote on the NSTAC Measuring & Incentivizing Report, Mr. Charney realized that he mistakenly skipped Mr. Jonathan Murphy during the opening remarks segment of the meeting. He then invited Mr. Murphy to provide his opening remarks.

Mr. Murphy thanked Mr. Charney for the opportunity to address the NSTAC and expressed his appreciation towards the NSTAC Dynamic Spectrum Sharing and the NSTAC Measuring and Incentivizing subcommittees for addressing crucial topics in the communication technology space. He also congratulated the NSTAC for the speed in which they accomplished the NSTAC Dynamic Spectrum Sharing Letter. He noted that the topics discussed by the NSTAC are supporting the priorities of the administration and its line of effort and will be valuable for the development of innovative government solutions. He stated that the administration's focus will remain on strategic challenges, and the administration will look for NSTAC's insight on these issues, which include incorporating operational resilience concepts into cybersecurity efforts and securing emerging technologies like artificial intelligence.

Mr. Charney thanked Mr. Murphy for his remarks. He then welcomed Mr. Jeff McElfresh, AT&T Communications and Co-Chair of the NSTAC Dynamic Spectrum Sharing Subcommittee, to begin his remarks on the findings and recommendations in the *NSTAC Letter to the President on Dynamic Spectrum Sharing*.

Deliberation and Vote: *NSTAC Letter to the President on Dynamic Spectrum Sharing*

Mr. McElfresh recalled that during the December 7, 2023, NSTAC Member Meeting, the committee discussed DSS and the critical role it plays both in enabling commercial wireless

services and supporting U.S. national security and defense systems. He explained that demand for spectrum is growing rapidly as more innovations occur in wireless and spectrum-dependent technologies. With this in mind, the NSTAC was tasked to provide perspective and recommendations on the implementation of DSS as referenced in the National Spectrum Strategy.

Mr. McElfresh noted that the National Spectrum Strategy recognized the importance of connecting all Americans to high-speed broadband, including through wireless investment and infrastructure deployment that requires predictable spectrum access. It also recognized that critical U.S. government services and missions rely on predictable spectrum access on the ground, in the air, at sea, and in space operations to protect national security.

Mr. McElfresh explained that the National Spectrum Strategy is the beginning of a "moonshot effort" to advance the state of potential dynamic forms of spectrum sharing in collaboration with industry with a goal to advance research, create investment incentives, and set forth measurable goals for advancing the state of technology for spectrum access. To accomplish this goal, the Strategy looked to establish a national testbed to support the next generation spectrum sharing. NSTAC encouraged the administration to review the record in the National Telecommunications and Information Administration proceedings as they develop the National Spectrum Strategy Implementation Plan.

Mr. McElfresh stated that the NSTAC Dynamic Spectrum Sharing Subcommittee kicked off in early January 2024, to provide consensus recommendations to the president on the implementation of the National Spectrum Strategy as it pertains to DSS. He highlighted that NSTAC members hold a wide range of perspectives on spectrum sharing.

Mr. McElfresh reviewed the key points and recommendations of the letter. He explained that the National Spectrum Strategy Implementation Plan should acknowledge that the need for spectrum is growing for both commercial wireless services and national security missions and therefore it is important that the National Spectrum Strategy Implementation Plan account for both use cases. He further explained that the National Spectrum Strategy Implementation Plan should establish aggressive timelines and ensure that necessary steps are taken to confirm the viability of these processes, while also preventing technical studies and testbeds from becoming an unnecessary source of delay. Investment in the commercial wireless ecosystem and federal national security technologies and capabilities require a strong knowledge of the spectrum access environment.

Mr. McElfresh continued that robust technical analysis is needed, and the administration must study both the operating environment and operating parameters. This should include information about the inputs and assumptions made in interference analyses and the technical parameters of federal capabilities to accurately assess the viability of varying commercial spectrum access frameworks.

Mr. McElfresh underscored the importance of the Department of Defense's (DoD) mission requirements but cautioned that all aspects of DoD's use of spectrum should not remain unchanged.

Effective sharing cannot exist when neither commercial systems nor federal systems are able to operate as needed due to a lack of consistent, reliable access to spectrum.

Mr. McElfresh stated that the National Spectrum Strategy Implementation Plan should also consider leading efforts to harmonize international standards around broader spectrum access. Previous efforts to address the feasibility of sharing included most recently the Emerging Mid-Band Radar Spectrum Sharing Feasibility Assessment and DoD's Partnering to Advance Trusted and Holistic Spectrum Solutions Task Group. He explained that the National Spectrum Strategy Implementation Plan can build upon these efforts while also including the interests of the communications and defense industries and other stakeholders.

Mr. Charney thanked Mr. McElfresh for his report on the letter's findings and recommendations and opened the floor for comments or questions from NSTAC members and government partners.

Mr. Kyle Malady, Verizon, commented on the many differing views on spectrum sharing in the NSTAC Dynamic Spectrum Sharing study and affirmed any effort to improve spectrum. He opined that spectrum must be made more available to the wireless industry without distracting from other ongoing efforts led by wireless industry for commercial use.

Upon hearing no further comments, Mr. Charney made a motion to approve the *NSTAC Letter to the President on Dynamic Spectrum Sharing*. Following the motion, which was seconded, NSTAC members voted unanimously to approve the letter for transmission to the president.

Closing Remarks and Adjournment

Mr. Charney thanked participants, government attendees, the NSTAC Measuring and Incentivizing Subcommittee co-chairs, the Dynamic Spectrum Sharing Subcommittee co-chairs, NSTAC members, and invited attendees for their participation.

He noted that NSTAC's efforts will help make America's cyber ecosystem more secure and expressed his appreciation to all the working group leads, the subcommittee members, and staff for their hard work in putting together the letter and report.

Mr. Charney stated that the next NSTAC meeting is scheduled for May 2024, and additional meeting information will be provided in the Federal Register. He then adjourned the meeting.

APPENDIX

March 7, 2024, 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.
Mr. Mark Dankberg	Viasat
Mr. Matthew Desch	Iridium Communications, Inc.
Mr. David DeWalt	NightDragon Management Company
Mr. Raymond Dolan	Cohere Technologies, Inc.
Mr. John Donovan	Palo Alto Networks
Mr. Joseph Fergus	Communication Technologies, Inc.
Ms. Lisa Hook	Two Island Partners, LLC
Mr. Jack Huffard	Tenable Holdings
Ms. Barbara Humpton	Siemens USA
Ms. Renée James	Ampere Computing, LLC
Ms. Kimberly Keever	Cox Communications
Mr. Kyle Malady	Verizon
Mr. Kevin Mandia	Mandiant
Ms. Maria Martinez	Cisco
Mr. Jeffery McElfresh	AT&T Communications
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
NSTAC Points of Contact	
Mr. Jason Boswell	Ericsson, Inc.
Mr. Chris Boyer	AT&T
Mr. Rudy Brioché	Comcast
Mr. Jamie Brown	Tenable Network Security, Inc.
Mr. Matt Carothers	Cox Communications
Mr. Bruce Cathell	Viasat
Mr. Drew Colliatie	Siemens
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. William Conner	Iridium Communications, Inc.
Ms. Cheryl Davis	Oracle
Mr. Tom Gann	Trellix
Ms. Katherine Gronberg	NightDragon Management Company

Mr. Robert Hoffman	Broadcom, Inc.
Mr. John Hunter	T-Mobile
Mr. Joel Johnson	Lockheed Martin
Ms. Sabeen Malik	Rapid7
Mr. Joel Max	Siemens
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Christopher Oatway	Verizon
Ms. Stacy O'Mara	Mandiant
Ms. Jeanine Pihonak	Unisys
Ms. Ista Pinon	Cisco Systems
Mr. Kevin Reifsteck	Microsoft Corp.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Thomas Quillin	Intel Corp.
Ms. Jennifer Warren	Lockheed Martin
Mr. Eric Wenger	Cisco Systems
Ms. Stephanie Woods	Lumen Technologies

Government Participants

Ms. Christina Berger	Cybersecurity and Infrastructure Security Agency
Ms. DeShelle Cleghorn	Cybersecurity and Infrastructure Security Agency
Mr. Harry Coker, Jr.	Office of the National Cyber Director
Mr. Trent Frazier	Cybersecurity and Infrastructure Security Agency
Mr. Deirdre Gallop-Anderson	Cybersecurity and Infrastructure Security Agency
Mr. Jonathan Murphy	National Security Council
Ms. Valerie Mongello	Cybersecurity and Infrastructure Security Agency
Ms. Janelle Pace	Cybersecurity and Infrastructure Security Agency
Ms. Erin Pattillo	Cybersecurity and Infrastructure Security Agency
Mr. Wayne Rash	Cybersecurity and Infrastructure Security Agency
Mr. Barry Skidmore	Cybersecurity and Infrastructure Security Agency
Ms. Marilyn Stackhouse	Cybersecurity and Infrastructure Security Agency
Mr. Joel Vaughn	Cybersecurity and Infrastructure Security Agency
Mr. Brandon Wales	Cybersecurity and Infrastructure Security Agency
Mr. Scott Zigler	Cybersecurity and Infrastructure Security Agency

Contractor Support

Mr. Mohammed Alian	TekSynap Corp.
Mr. Rodger Edmonds	TekSynap Corp.
Ms. Ashley Gaston	Edgesource Corp.
Ms. Joan Harris	Edgesource Corp.
Ms. Laura Penn	Edgesource Corp.
Ms. Jennifer Poole	Edgesource Corp.
Mr. Nicholas Smith	TekSynap Corp.

Public and Media Participants

Mr. Doug Brake	Cellular Telephone Industries Association
Mr. Howard Buskirk	Communications Daily
Mr. Justin Doubleday	Federal News Network
Mr. David Durcsak	General Dynamics Information Technology
Mr. Andrew Farquharson	Lockheed Martin
Ms. Sara Friedman	Inside Cybersecurity
Mr. Eric Geller	The Messenger
Mr. Matt Hayden	General Dynamics Information Technology
Ms. Katie Ignaszewski	IBM
Mr. Derek Johnson	Cyberscoop
Mr. Albert Kammler	Van Scoyoc Associates
Mr. Paul Kirby	TR Daily
Ms. Norma Krayem	Van Scoyoc Associates
Mr. Thomas Leithauser	Telecommunications Reports/Cybersecurity Policy Report/Wolters Kluwer
Mr. Jerry Markon	MeriTalk
Mr. Jamie Tarabay	Bloomberg News

Certification

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

Mr. Scott Charney
NSTAC Chair