Call to Order and Introductions

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 noted that the NSTAC is a federal advisory committee governed by the *Federal Advisory Committee Act* and the meeting was open to the public. She noted that no one had registered to provide comments from the Federal Register Notice (FRN) but that written comments would be accepted following the procedures outlined in the meeting's FRN. Following roll call, Ms. Berger turned the meeting over to Mr. Scott Charney, Microsoft, NSTAC Chair.

Mr. Charney thanked Ms. Berger, government officials, and participants for their attendance. He welcomed distinguished government officials 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. Harry Coker Jr., National Cyber Director, Office of the National Cyber Director (ONCD); and Mr. Brandon Wales, Executive Director, CISA.

Mr. Charney then provided a brief overview of the March 2024 NSTAC Member Conference Call. He explained that the committee heard from government partners on key national security and emergency preparedness initiatives and voted to approve the *NSTAC Letter to the President on Dynamic Spectrum Sharing* and the *NSTAC Report to the President on Measuring and Incentivizing the Adoption of Cybersecurity Best Practices*. Lastly, he announced Mr. Kevin Mandia, Mandiant, and Ms. Maria Martinez, Cisco, will lead the upcoming study on Principles for Baseline Security Offerings from Cloud Service Providers.

The meeting agenda for the May 2024 NSTAC Member Meeting Agenda, included: (1) remarks from government partners regarding ongoing efforts relevant to information and communications technologies; (2) an update on the administration's cybersecurity initiatives; (3) a keynote address from Mr. Coker; (4) an NSTAC recommendations update; and (5) an update from the NSTAC Principles for Baseline Security Offerings from Cloud Service Providers (Baseline Security Offerings) Subcommittee. Mr. Charney then turned the meeting over to Ms. Neuberger to provide opening remarks.

Ms. Neuberger thanked Mr. Charney, Mr. Jeff Storey, Lumen Technologies, NSTAC Vice Chair, and the NSTAC members for the previously held rich discussions and the value the NSTAC provides the administration. She also thanked the members for investing their time and that she looked forward to their continued partnership. Ms. Neuberger also commended Mr. Charney for his leadership as NSTAC Chair.

Mr. Charney thanked Ms. Neuberger and invited Mr. Coker to provide remarks. Mr. Coker stated that he was delighted to be there and that he looked forward to working with the NSTAC to address the many challenges confronting the nation. He stated that the nation has benefited from the NSTAC's work and expressed his gratitude to the members for their efforts.

Mr. Charney thanked Mr. Coker and invited Mr. Wales to give opening remarks. Mr. Wales highlighted CISA's recent roll-out of its Secure by Design pledge to help ensure that companies benefit from a more secure technology base and that it has been signed by over 100 technology companies. He also noted that CISA was still receiving comments to its Notice of Proposed Rulemaking (NPRM) that would require companies to report certain cyber incidents and ransomware payments. He encouraged more input to help shape the final rule. Mr. Wales then thanked the NSTAC for their support and strong collaboration.

Update on the Administration's Cybersecurity Initiatives

Ms. Anne Neuberger outlined the National Cybersecurity Strategy's three core components: (1) securing critical infrastructure; (2) enhancing the cybersecurity of hardware and software; and (3) investing in international partnerships to combat global cybersecurity threats.

In securing the critical infrastructure, the administration has transitioned from a voluntary cybersecurity framework to a mandatory framework that is more focused on critical services. She noted that progress has been made in sectors such as pipelines, airports, and rail systems, with a priority of securing water systems through Environmental Protection Agency enforcement actions and coordinated efforts against nation-state actors and other criminal threats. The administration has established the Crypto Information Systems Audit and Control Association to address ransomware threats and counter other illicit cryptocurrency activities.

She then turned to enhancing the cybersecurity of hardware and software, highlighting the U.S. Cyber Trust Mark Program. The administration established this program to provide companies with a way to demonstrate that their products meet cybersecurity standards that align with the Secure by Design principles advocated by CISA. This will provide consumers with a clear indication of cybersecurity standards in products ranging from baby monitors to routers. She explained that the Federal Communications Commission is facilitating the program and that the final rule for the program is expected to finalize soon, aligning with the end-of-year shopping seasons.

Turning to international partnerships, she stated that the administration's Counter Ransomware Initiative has expanded from thirty countries to more than sixty countries and focuses on policy and operational cooperation. Recent meetings like CYBERUK and the RSA Conference have driven further discussions on ransomware policies and collaboration with the insurance industry to incentivize better cybersecurity practices.

Finally, she highlighted the NSTAC's work on the Dynamic Spectrum Sharing Letter and acknowledged the holistic viewpoints provided by the committee in the document. She praised the members for their discussions and work to address the need to balance national security and commercial requirements in an increasingly congested spectrum environment. Mr. Charney thanked Ms. Neuberger and then turned the meeting over to Mr. Coker to provide the keynote address.

Keynote Address from the National Cyber Director

Mr. Coker stated that partnerships between the federal government, telecommunications industry,

and critical infrastructure providers are necessary to succeed in cybersecurity. He explained that ONCD works to implement the President's National Cybersecurity Strategy and is currently trying to solve three difficult problems: (1) protecting cyber infrastructure in space; (2) strengthening internet routing security; and (3) building a large and robust cybersecurity workforce.

He shared space system cybersecurity is of great importance in countering the significant threat the United States faces in attacks to critical infrastructure by adversaries. Targeting of critical infrastructure happens across all domains, and cyber is the preferred attack vector in space systems for America's adversaries. While adversaries pursue alternative means to disrupt satellites, attacks in the cyber domain are the first choice with the lowest barrier to entry.

He added that his time in the Navy and intelligence community working with space operations showed him how complex these environments are with engineering challenges, logistics concerns, bandwidth issues, and life cycle issues. Space systems often are designed to last eight to ten years and routinely outlive their lifespan, which means they may not be protected against evolving threats. Designing secure space systems is inherently difficult, and the consequences are challenging as the space environment and economy continue to grow at a breakneck pace.

Mr. Coker said ONCD, the National Space Council, NSC, and industry convened a Space Systems Cybersecurity Executive Forum at the White House to discuss the evolving risk landscape, and all agreed there is significant work to do. Following the Forum, key players from the public and private sector in the space economy met in multiple workshops, which revealed barriers companies face daily as they attempt to ensure cybersecurity was core to their space mission. ONCD partnered again with the National Space Council and NSC to lead a project on space-system cybersecurity. Discussions were held with government space-system operators to understand their policies and processes in implementing *Space Policy Directive 5—Cybersecurity Principles for Space Systems,* which outlined policy gaps, ensuring government leads the way in improving space cybersecurity.

Industry partners, as noted by Mr. Coker have repeatedly said cybersecurity requirements for space from federal mission owners vary significantly by agency and contract, which resulted in an inconsistent application of best practices across federal space missions, frustrating mission partners and preventing the United States from leading internationally. The U.S. government space systems were recently tasked with creating a minimum set of cybersecurity requirements that will form the basis of controls needed to combat the evolving threats, make it easier for companies supporting U.S. space missions, and lay the groundwork for future work that ensures commercial space is adequately protected.

Mr. Coker noted that the security and resilience of the Border Gateway Protocol (BGP) needs to be strengthened as BGP is one of the foundational protocols that enables over 70,000 independent networks to operate within the internet and is used to advertise Internet Protocol (IP) addresses to construct routes to reach them from anywhere in the world. BGP was not built with the security needed for today's internet ecosystem, and recently there has been an increase in BGP hijacks, which are often used to subvert foundational IPs, including domain-name systems and the web's public-key

infrastructure. BGP attacks seek to gather account credentials or install malware and have resulted in losses of millions of dollars.

Mr. Coker stated through the adoption of Resource Public Key Infrastructure (RPKI), BGP hijacking can become a thing of the past. Only recently has a majority of global internet addresses been registered in RPKI to allow internet service providers to filter false routing advertising and prevent hijacking attempts, although government lags in registering which is putting the United States in danger of disruption and espionage. A strategic objective calls for BGP as a key protocol to security, and interagency partners and the private sector are working on a roadmap to drive universal RPKI adoption. Additionally, the Department of Commerce signed contracts to register their address space and create Route Origin Authorizations (ROAs). These contracts are models for other agencies to follow and will pave the way to establish ROAs for federal networks.

Building the nation's cybersecurity workforce noted Mr. Coker is critical and the talent pool needs to be broadened. He noted that there are 500,000 open cyber jobs in the United States, and these jobs need to be filled to protect the country. Workers should be hired based on aptitude and skills, and The Office of Personnel Management is converting most federal technology employees to skills-based hiring.

Mr. Coker ended by saying investments in long-term cybersecurity and resilience need to be incentivized, and private and federal partners need to work together to drive coherence across the ecosystem. He stressed that private sector partners' expertise is critical to national security. Mr. Coker then turned the meeting back to Mr. Charney who invited Mr. Wales to provide an update on the progress of NSTAC recommendations.

NSTAC Recommendations Update

Mr. Wales provided an update on government actions that are aligned with past NSTAC recommendations. He began by praising the NSTAC for its exceptional track record, emphasizing that it is one of the most successful presidential advisory committees due to its impactful study topics and the dedicated efforts of its members.

He referenced the 2021 *NSTAC Report to the President on Software Assurance in the Information and Communications Technology and Services Supply Chain*. This report urged government agencies to prioritize purchasing software developed in accordance with the Supply Chain Risk Management Framework to ensure trustworthiness. In line with this recommendation, he noted that the Department of Defense, the General Service Administration, and the National Aeronautics and Space Administration issued a now-closed NPRM in October 2023 to standardize cybersecurity contractual requirements across federal agencies.

He highlighted CISA's collaboration with public and private sectors to continually provide upgrade guidance for software companies. In March 2024, CISA and the Office of Management and Budget released a Secure Software Development Attestation Form—a new requirement for government software providers. Additionally, CISA's Information and Communications Technologies (ICT)

Supply Chain Risk Management Task Force published a fact sheet to help organizations assess the security of their vendors when purchasing ICT hardware, software, and services.

He then discussed the 2022 *NSTAC Report to the President on Zero Trust and Identity Management*, which recommended establishing a Zero Trust Program Office within CISA. In March 2024, CISA established this office to provide comprehensive training on zero trust principles. The office serves as a central hub for interagency partners and the broader information technology community to develop guidance, services, tools, and performance measures.

He acknowledged that the 2023 *NSTAC Report to the President on the Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem* recommended speeding up the adoption and deployment of Post-Quantum Cryptography (PQC) through partnerships with the private sector and academia. CISA, the National Institute of Standards and Technology (NIST), and the NSA published a Cybersecurity Information Sheet on Quantum Readiness in August 2023 to help organizations transition to PQC standards. He added that NIST also released a draft publication in December 2023 on integrating quantum-resistant algorithms into existing security systems.

He then addressed the recommendations in the 2023 *NSTAC Report to the President on Mitigating Domestic Infrastructure Abuse by Foreign Malicious Actors*, which recommended development of a framework to prioritize domestic infrastructure abuse mitigation. The Department of Commerce issued a proposed rule in January 2024 requiring infrastructure-as-a-service providers to verify the identities of foreign entities. This rule aligns with the report's recommendations and aims to prevent foreign cyber actors from exploiting U.S. infrastructure. Additionally, in February 2024, President Biden issued Executive Order 14117: *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, to prevent the transfer of bulk sensitive personal and government-related data to countries of concern. Mr. Wales noted that this order is crucial for protecting American data from foreign exploitation.

Mr. Wales concluded by underscoring the NSTAC's pivotal role in advising on national cybersecurity defenses. He emphasized that the committee's recommendations have led to measurable improvements in cybersecurity and reflected the effective collaboration between government agencies and the broader cybersecurity community. Mr. Wales then turned the meeting back to Mr. Charney who invited Mr. Mandia and Ms. Martinez for the Baseline Security Offerings status update.

Status Update: NSTAC Baseline Security Offerings Subcommittee

Ms. Martinez and Mr. Mandia provided an update on the Baseline Security Offerings subcommittee's progress to date. Ms. Martinez began by stating that the subcommittee's task is to develop principles for baseline security offerings from cloud service providers. She said this involves the rational allocation of roles between cloud service vendors, customers, and users to manage specific risks effectively. She also underscored the need for rebalancing security responsibilities in the cloud as too much burden has traditionally been placed on users. She highlighted the importance of examining default settings in shaping the security posture of cloud

services and noted that the subcommittee has started identifying key issues and briefers to support this work. She also stated that the subcommittee aims to have a proposed set of recommendations for NSTAC members to review by the NSTAC by the August 2024 NSTAC Member Conference Call.

She acknowledged the tight timeline to complete the study but expressed confidence in meeting the deadline with the assembled team's support. She concluded by reiterating the importance of the study's scope around national security and thanked the subcommittee members in advance for their contributions. Ms. Martinez then invited the subcommittee's co-chair, Mr. Mandia, to provide remarks.

Mr. Mandia echoed Ms. Martinez's sentiments and provided additional details on the subcommittee's progress. He motioned that the subcommittee has established a regular meeting cadence to ensure consistent progress and has begun planning briefings to scope their efforts.

He outlined the initial steps for the subcommittee, including gathering inputs from industry experts, cloud service providers, government representatives, and key cloud service consumers ranging from enterprise to small and medium-size businesses. He stressed the importance of defining the scope to avoid overcomplicating the recommendations and staying focused on practical solutions.

Finally, he shared appreciation for the cooperation of the NSTAC members and their organizations, noting that the subcommittee would maintain their work pace through the summer to meet the study's deadline. He ended his remarks by expressing eagerness to advance the core principles for more consistent security applications and to identify default security capabilities for critical infrastructure sectors through the study. The co-chairs then turned the meeting back to Mr. Charney who invited Ms. Neuberger, Mr. Coker, and Mr. Wales to provide closing remarks.

Closing Remarks and Adjournment

Ms. Neuberger thanked the NSTAC members for joining the meeting and thanked Mr. Charney and Mr. Storey for their continued leadership. She noted that she has been a part of many public-private partnership efforts and said the NSTAC is particularly notable for the quality of its reports, the breadth of the members who participate, and how its recommendations have enhanced the government's policy and operational efforts. She concluded by saying that she looks forward to continuing to work with the NSTAC.

Mr. Charney thanked Ms. Neuberger and invited Mr. Coker to provide remarks. Mr. Coker said that he echoed Ms. Neuberger's remarks and expressed his personal gratitude to the NSTAC.

Mr. Charney thanked Mr. Coker and turned the floor to Mr. Wales for closing remarks. Mr. Wales thanked the participants for their time, energy, and expertise; emphasizing that it is needed and useful. He also thanked Ms. Berger and the NSTAC team for making the meeting possible.

Mr. Charney stated that the next member conference call is scheduled for August 2024 and further will be provided via the Federal Register Notice. He then 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. 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. Patrick Gelsinger	Intel Corp.
Ms. Lisa Hook	Two Island Partners, LLC
Mr. Jack Huffard	Tenable Holdings, Inc.
Ms. Barbara Humpton	Siemens USA
Mr. Kyle Malady	Verizon
Mr. Kevin Mandia	Mandiant
Ms. Maria Martinez	Cisco
Mr. Stephen Schmidt	Amazon
Mr. Jeffrey Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
Mr. Corey Thomas	Rapid7
NSTAC Points of Contact	
Mr. Christopher Anderson	Lumen Technologies, Inc.
Mr. Jason Boswell	Ericsson, Inc.
Mr. Christopher Boyer	AT&T Communications
Mr. Rudy Brioche	Comcast
Mr. Jamie Brown	Tenable Holdings, Inc.
Mr. Bruce Cathell	Viasat
Mr. Drew Colliatie	Siemens USA
Ms. Kathryn Condello	Lumen Technologies, Inc.
Ms. Cheryl Davis	Oracle Corp.
Mr. Thomas Gann	Trellix
Ms. Katherine Gronberg	NightDragon Management Company
Mr. Robert Hoffman	Broadcom, Inc.
Mr. John Hunter	T-Mobile
Ms. Ilana Johnson	Centergate

Ms. Sabeen Malik	Rapid7
Mr. Joel Max	Siemens USA
Mr. Sean Morgan	Palo Alto Networks, Inc.
Ms. Jeanine Pihonak	Unisys Corp.
Ms. Ista Pinon	Cisco
Mr. Thomas Quillin	Intel Corp.
Mr. Kevin Reifsteck	Microsoft Corp.
Mr. Nicholas Saunders	Viasat
Ms. Jordana Siegel	Amazon Web Services, Inc.
Ms. Jennifer Warren	Lockheed Martin
Mr. Adam Weller	Cisco
Mr. Eric Wenger	Cisco
Mr. Michael Woods	Verizon
Ms. Stephanie Woods	Lumen Technologies, Inc.

Government Participants

Ms. Caitlin Clarke	National Security Council
Mr. Harry Coker	Office of the National Cyber Director
Mr. Jon Murphy	National Security Council
Ms. Anne Neuberger	National Security Council
Mr. Brian Scott	Office of the National Cyber Director
Mr. Brandon Wales	Cybersecurity and Infrastructure Security Agency

NSTAC Support Staff

Mr. Mohammed Alian	Edgesource Corp.
Ms. Christina Berger	Cybersecurity and Infrastructure Security Agency
Ms. Ashley Gaston	Edgesource Corp.
Ms. Elizabeth Gauthier	Cybersecurity and Infrastructure Security Agency
Ms. Helen Jackson	Cybersecurity and Infrastructure Security Agency
Ms. Erin Patillo	Cybersecurity and Infrastructure Security Agency
Ms. Janelle Pace	Cybersecurity and Infrastructure Security Agency
Ms. Laura Penn	Edgesource Corp.
Ms. Jennifer Poole	Edgesource Corp.
Ms. Cheryl Santiago	TekSynap Corp.
Mr. Barry Skidmore	Cybersecurity and Infrastructure Security Agency
Mr. Nicholas Smith	TekSynap Corp.
Mr. Joel Vaughn	Cybersecurity and Infrastructure Security Agency
Mr. Scott Zigler	Cybersecurity and Infrastructure Security Agency

Public and Media Participants

Ms. Manali Basu	Office of the National Cyber Director
Ms. Cate Burgan	MeriTalk

Mr. Howard Buskirk	Communications Daily
Ms. Victoria Dillon	Office of the National Cyber Director
Mr. David DiMolfetta	Nextgov
Mr. Justin Doubleday	Federal News Network
Ms. Sara Friedman	Inside Cybersecurity
Mr. Eric Geller	Freelance Reporter
Mr. Johnathan Grieg	The Record
Mr. James Jackson	Cybersecurity and Infrastructure Security Agency
Mr. Albert Kammler	Van Scoyoc Associates
Mr. Matthew Kapko	Cybersecurity Dive
Ms. Katrina Manson	Bloomberg
Ms. Alexandra Martin	Department of Homeland Security
Mr. John Sakellariadis	Politico
Ms. Katherine Siefert	Cybersecurity and Infrastructure Security Agency
Mr. Timothy Starks	CyberScoop
Mr. Michael Stone	Department of Homeland Security
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