## Call to Order and Opening Remarks

Ms. Christina Berger, the President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Officer (DFO), Cybersecurity and Infrastructure Security Agency (CISA), called the meeting to order. 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 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. Scott Charney, Microsoft, NSTAC Chair.

Mr. Charney welcomed members and 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); Ms. Drenan Dudley, Acting National Cyber Director, Office of the National Cyber Director (ONCD); and Mr. Brandon Wales, Executive Director, CISA.

Mr. Charney reviewed items from the September 2023 NSTAC Member Conference Call (MCC), to include remarks from the government on key national security and emergency preparedness (NS/EP) initiatives relevant to information and communications technologies (ICT). During the meeting, the committee also voted to approve the *NSTAC Letter to the President on Securing Next Generation Wireless Telecommunications*, and the *NSTAC Report to the President on Addressing the Abuse of Domestic Infrastructure by Foreign Malicious Actors*. Additionally, NSTAC members received a status update on the NSTAC Measuring and Incentivizing the Adoption of Cybersecurity Best Practices (M&I) study.

The meeting agenda for the December meeting included: (1) opening remarks from the administration and CISA on the government's ongoing collaboration with industry on key NS/EP initiatives relevant to ICT; (2) an update on the administration's cybersecurity initiatives; and (3) an update from the NSTAC M&I Subcommittee.

Ms. Neuberger thanked attendees for their partnership to secure and improve the security of cyberspace and technologies that are relied upon daily. Each NSTAC member brings unique perspective to this committee for the companies they represent and their own professional experiences and knowledge. She shared her anticipation regarding the NSTAC's contributions on key critical policy initiatives and thanked Mr. Charney for his continued leadership as NSTAC chair.

For over 40 years, the NSTAC has served as a model for trusted partnership between government and the private sector. Throughout the NSTAC's history, significant contributions have shaped how the Executive Office of the President (EOP) views and executes national security policy related to cybersecurity, global communications, and the dependencies of critical infrastructure.

Looking ahead to priorities for 2024 to 2025, and areas for the committee to incentivize additional action, Ms. Neuberger officially tasked the NSTAC with its next study on *Principles for Baseline*

*Security Offerings from Cloud Service Providers (CSP)*. She underscored that many critical infrastructure sectors rely upon the cybersecurity and resilience of their third-party service providers. Cloud-based services enable better and more economical cybersecurity practices at scale and reviewed the federal government's push for widespread adoption of such services.

Ms. Neuberger encouraged the NSTAC to ensure the digital ecosystem's biggest, most capable, and best positioned actors assume a greater share of the burden for mitigating cyber risk. This new study will help identify steps to enable more security by default across cloud providers and recognized the obligation of cloud service providers to embed security offerings. Ms. Neuberger encouraged the NSTAC to share their recommendations on the topic in time to deliberate and vote during the next in-person meeting.

Next, Ms. Dudley expressed her honor to serve as the Acting National Cyber Director as the National Cyber Director nominee, Mr. Harry Coker, awaits his Senate confirmation. Ms. Dudley highlighted select ONCD key activities, explaining that it is focusing on enacting the President's National Cybersecurity Strategy (NCS), and within the NCS, the sixty-nine actionable individual initiatives part of the implementation plan. The team is currently advancing updates to the next iteration of the implementation plan, expected in spring 2024. This plan will include new initiatives as ONCD continues to implement the president's enduring and affirmative vision for cyberspace. ONCD is also implementing the National Cyber Workforce and Education Strategy. In line with the strategy, ONCD aims to match well-paying jobs with government and non-government organizations for required cyber talent.

Mr. Wales thanked Mr. Charney and Mr. Jeffrey Storey, Lumen Technologies, NSTAC Vice Chair, for their leadership, and thanked attendees for their hard work and cooperation. He addressed NSTAC's arduous work on cybersecurity goals and efforts to improve the nation's critical infrastructure and highlighted the shared goal of fortifying the nation's cyber defenses. Public and private partnership share an important responsibility to showcase collaboration and enhance cybersecurity. While the nation has made tremendous progress in 2023 in deterring and responding to recent and urgent security threats, there is more work to be done.

## Update: The Administration's Cybersecurity Initiatives

Ms. Neuberger underscored the importance of the committee's work and partnership. She recalled two recent incidents in which bad actors targeted the U.S. water sector by compromising Unitronics, a particular brand of operational technology, that is commonly used worldwide to utilize gaps in default password processes to gain access.

The second incident amounted to the third largest attack against a U.S. hospital chain in the past year, compromising another healthcare system via ransomware. The attack jeopardized healthcare delivery, shut down rural clinics, and forced diversions from emergency rooms by exploiting a known vulnerability more than a month after it was added to the known exploited vulnerability catalog.

Ms. Neuberger noted that the NSC works to defend against and mitigate such attacks. Like the Environmental Protection Agency— and in alignment with the current administration's strategy for implementing minimum cybersecurity practices across all critical infrastructure sectors in the country— the NSC works closely with the Department of Health and Human Services and the Centers for Medicare and Medicaid to go beyond the successful medical device requirements levied in 2023. The NSC aims to establish minimum cybersecurity practices for healthcare providers to ensure Americans can always rely on their local hospitals and local clinics.

## Status Update: NSTAC M&I Subcommittee

Mr. Jack Huffard, Tenable Holdings, provided the update on the NSTAC M&I Subcommittee's progress to date.

He said that while governments, organizations, and other stakeholders have created numerous cybersecurity best practices and standards, many entities are either not consistently adopting or are poorly implementing best practices and standards, increasing vulnerabilities and the likelihood of threats and cybersecurity incidents with deeper geopolitical impact.

Existing market forces have been insufficient to incentivize the adoption of these cybersecurity best practices and standards at the level needed to meet the evolving cyber-threat landscape and to strengthen U.S. NS/EP. The lack of consistent adoption and implementation of cybersecurity best practices and standards is especially problematic as U.S. critical infrastructure entities face a significantly heightened threat landscape in the current geopolitical environment. Given this dynamic and evolving backdrop, the administration tasked the NSTAC to develop a report with strategic recommendations on how the federal government can facilitate better measurement of cybersecurity within organizations, and how it can incentivize adoption of cybersecurity best practices in a scalable, repeatable manner.

The M&I study began its work in June 2023, and since July 2023, has received approximately 50 briefings from a wide range of experts, including government officials from various departments and agencies, industry representatives from multiple critical infrastructure sectors, cybersecurity insurance carriers, cloud service providers, cybersecurity consultants and technology providers, trade associations, think tanks, and experts on measurement science. Consistent themes from the briefings have informed the key findings highlighted in the draft report.

Key findings included: (1) that the federal government and the private sector collect and possess significant amounts of cybersecurity data that could be utilized to baseline and support more effective measurements and metrics; (2) cybersecurity measurements and metrics that are tied to business outcomes are more effective than those that are void of business strategy context; (3) strengthening the nation's cybersecurity depends on the ability of public and private sector decision makers to make risk-informed decisions on the most effective solutions available when allocating limited resources; (4) objective measurements—combined with poor metrics literacy lead to ineffective decision decision-making, improved metrics literacy, and a focus on leading versus lagging indicators—can strengthen cybersecurity prioritization; (5) private firms may hold data that can be used to forecast and measure best practice adoption; (6) duplication or conflict with

regulatory requirements can impose significant burdens on organizational cybersecurity budgets, resources, and priorities; (7) civil, criminal, and regulatory liability— as well as reputational challenges— are barriers to information sharing; (8) lack of qualified personnel as well as lack of resources to recruit and retain qualified personnel are barriers to both adoption and measurement of cyber best practices; (9) different types of hiring incentives may be more appropriate depending on the maturity and the resources of the entity that are being targeted; (10) the importance of transparency to improving secure software development processes and outcomes; (11) public and private sector organizations should be encouraged to leverage emerging technologies that level the playing field against attackers or give defenders an advantage; and (12) a healthy security workplace culture is a leading indicator of strong cyber security.

The subcommittee is developing specific recommendations to address the key findings. The recommendations will focus on: (1) a better understanding and leveraging of data the government and the private sector currently have available; (2) linking cyber measurements and metrics to business outcomes; (3) utilizing effective methodologies for measurements and metrics; (4) promoting secure software development practices; and (5) identifying incentives that improve best practice adoption and strengthen cyber workforces. The subcommittee intends to highlight recommendations from previous NSTAC reports, which should be implemented or accelerated to achieve these goals, such as those from the *NSTAC Report to the President on a Cybersecurity Moonshot* and the NSTAC "Enhancing Internet Resilience in 2021 and Beyond" study.

The subcommittee is tracking recent developments, such as the *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, to determine how the EO may inform the subcommittee's final report, or whether it should serve as the subject of future NSTAC studies. Mr. Huffard welcomed further input on the report and potential recommendations under consideration. He said the subcommittee will incorporate feedback as it is received to continue to refine and improve the final draft product.

The subcommittee will complete the briefing series and move forward in finalizing the report and recommendations in January 2024, for presentation during the February 2024 NSTAC MCC.

## Closing Remarks and Adjournment

Mr. Charney thanked participants, government officials, M&I Subcommittee co-chairs, NSTAC leadership, and invited attendees for their participation.

Ms. Neuberger reviewed that programs—such as U.S. Cyber Trust Mark— allow individuals to identify particular products built to standard and allow consumers to make product decisions accordingly. As consumers care about security when purchasing items, they know that these devices can be used to collect data that they may not want to be gathered. Individuals are also aware that these devices can also be utilized to potentially disrupt services at particular times.

Government and industry have an obligation to design practices that enable and incentivize secure by design features. Ms. Neuberger thanked government and NSTAC attendees for their discussion

on how such programs are scaled rapidly and effectively, and underscored the role that NSTAC companies have across their supply chains to help ensure that secure products are made available quickly and effectively. Ms. Dudley thanked attendees and underscored that their work helps improve government.

Mr. Wales underscored the importance of the recent NSTAC study and expressed appreciation to the NSTAC for their agility in assisting government in handling emerging cybersecurity challenges.

Mr. Charney stated that the next NSTAC MCC is slated for February 2024. 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. 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. Patrick Gelsinger | Intel Corp. |
| Mr. Jack Huffard | Tenable Holdings, Inc. |
| Ms. Barbara Humpton | Siemens USA |
| Ms. Kimberly Keever | Cox Communications |
| Mr. Kyle Malady | Verizon |
| Mr. Kevin Mandia | Mandiant |
| Ms. Maria Martinez | Cisco |
| Mr. Jeffery McElfresh | AT&T Communications |
| Mr. Bryan Palma | Trellix |
| Mr. Neville Ray | T-Mobile |
| Mr. Stephen Schmidt | Amazon |
| Mr. Jeffrey Storey | Lumen Technologies, Inc. |
| **NSTAC Points of Contact** | |
| Mr. Jason Boswell | Ericsson, Inc. |
| Mr. Chris Boyer | AT&T Communications |
| Mr. Rudy Brioche | Comcast |
| Mr. Jamie Brown | Tenable Holdings, Inc. |
| Mr. Matt Carothers | Cox Communications |
| Ms. Kathryn Condello | Lumen Technologies, Inc. |
| Mr. William Conner | Iridium Communications, Inc. |
| Ms. Cheryl Davis | Oracle Corp. |
| Ms. Katherine Gronberg | NightDragon Management Company |
| Mr. Robert Hoffman | Broadcom, Inc. |
| Mr. John Hunter | T-Mobile |
| Ms. Ilana Johnson | Centergate |

| | |
|---|---|
| Mr. Joel Johnson | Lockheed Martin |
| Mr. Kent Landfield | Trellix |
| Mr. Sean Morgan | Palo Alto Networks, Inc. |
| Mr. Christopher Oatway | Verizon |
| Ms. Stacy O'Mara | Mandiant |
| Mr. Thomas Quillin | Intel Corp. |
| Ms. Jennifer Raiford | Unisys Corp. |
| Mr. Kevin Reifsteck | Microsoft Corp. |
| Ms. Jordana Siegel | Amazon Web Services, Inc. |
| Mr. Eric Wenger | Cisco |

**Government Participants**

| | |
|---|---|
| Ms. Caitlin Clarke | National Security Council |
| Ms. Drenan Dudley | Office of the National Cyber Director |
| Mr. Trent Frazier | Cybersecurity and Infrastructure Security Agency |
| Ms. Laura Galante | Office of the Director of National Intelligence |
| Mr. Nick Leiserson | Office of the National Cyber Director |
| Mr. Jon Murphy | National Security Council |
| Ms. Anne Neuberger | National Security Council |
| Ms. Jessica Rosenworcel | Federal Communications Commission |
| Mr. Brian Scott | Office of the National Cyber Director |

**NSTAC Staff**

| | |
|---|---|
| Ms. Christina Berger | Cybersecurity and Infrastructure Security Agency |
| Ms. DeShelle Cleghorn | Cybersecurity and Infrastructure Security Agency |
| Ms. Elizabeth Gauthier | Cybersecurity and Infrastructure Security Agency |
| Mr. Wayne Rash | Cybersecurity and Infrastructure Security Agency |
| Mr. Daniel Bravo Requeno | Cybersecurity and Infrastructure Security Agency |
| Mr. William (Bill) Rybczynski | Cybersecurity and Infrastructure Security Agency |
| Mr. Barry Skidmore | Cybersecurity and Infrastructure Security Agency |
| Mr. Joel Vaughn | Cybersecurity and Infrastructure Security Agency |
| Mr. Scott Zigler | Cybersecurity and Infrastructure Security Agency |

**Contractor Support**

| | |
|---|---|
| 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. Howard Buskirk | Communications Daily |

| | |
|---|---|
| Mr. Justin Doubleday | Federal News Network |
| Mr. Chris Frascella | EPIC |
| Ms. Sara Friedman | Inside Cybersecurity |
| Mr. Eric Geller | The Messenger |
| Mr. Albert Kammler | Van Scoyoc Associates |
| Mr. Tom Laeithauser | Telecommunications Reports/ Cybersecurity Policy Report/Wolters Kluwer |
| Mr. Jake Nash | Wilkinson Baker Knauer, LLP |
| Ms. Marilyn Stackhouse | 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