



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 and welcomed all participants. She stated that the NSTAC is a federal advisory committee governed by the *Federal Advisory Committee Act* and that the meeting was open to the public. Ms. Berger then conducted a roll call and noted that one attendee from the public has registered to provide a comment during the meeting. She reminded participants to state their names before speaking and then turned the meeting over to the Mr. Scott Charney, NSTAC Chair, Microsoft.

Mr. Charney thanked Ms. Berger and the participants for their attendance. He then welcomed the distinguished government officials: 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. Nitin Natarajan, Deputy Director, CISA.

Next, Mr. Charney provided key takeaways from the August 2024 NSTAC Member Conference Call. He explained that the committee heard from government partners on initiatives addressing challenges within the Communications and Information Technology sectors. The participants also received a status update from NSTAC Members Mr. Kevin Mandia and Ms. Maria Martinez on the *NSTAC Principles for Baseline Security Offerings from Cloud Service Providers* (Baseline Security Offerings) Study. Lastly, the administration tasked the NSTAC to conduct a study on *National Preparedness for Post-Quantum Cryptography* (Post-Quantum Cryptography).

Mr. Charney then outlined the agenda for the November 2024 NSTAC Member Meeting. The NSTAC would: (1) receive an update on the administration's cybersecurity initiatives from Ms. Neuberger; (2) hear public comments; and (3) get a progress report from Mr. Mandia on the Baseline Security Offerings Study. Mr. Charney then invited Ms. Neuberger to provide her opening remarks.

Ms. Neuberger thanked the NSTAC for its contributions, highlighting the committee's 40-year legacy as a model for public-private partnership. She emphasized the escalating cybersecurity threats from foreign adversaries and the increasing convergence of cyber and physical attacks, particularly against critical infrastructure sectors like healthcare. Ms. Neuberger underscored the importance of driving down risks and noted the current Post-Quantum Cryptography Study's critical role in securing the nation's digital future. Ms. Neuberger then invited Mr. Coker to provide his opening remarks.



Mr. Coker thanked Ms. Neuberger and then followed with remarks on the expanding cyber threat landscape, including the challenges posed by state-sponsored actors, transnational criminal organizations, and other malicious cyber actors. He stressed the need for a whole-of-nation approach to cybersecurity, emphasizing the importance of protecting critical infrastructure and enhancing public-private collaboration. Mr. Coker highlighted several ongoing initiatives, including CISA's efforts to improve cyber risk capacity in its role as a sector risk management agency, as well as other focus areas to expand public-private collaboration and information exchange, enhance federal coherence in cyberspace, and foster a secure and resilient connected internet ecosystem.

Mr. Charney thanked Mr. Coker and invited Mr. Natarajan to give his opening remarks. Mr. Natarajan thanked Mr. Charney and Mr. Storey for their leadership of the NSTAC, also noting that the hard work of the committee members has helped to build resilience across the nation. He added that this work is more-critical than ever, pointing to the evolving threat landscape, including non-nation-state actors and the increasingly diverse victims such as schools and rural areas. Mr. Natarajan also previewed four of CISA's priorities for 2025: (1) countering threats from the People's Republic of China; (2) promoting secure by design principles; (3) addressing the risks and opportunities of artificial intelligence (AI); and (4) ensuring election security.

Mr. Charney thanked the speakers and transitioned the meeting to Mr. Neuberger for further updates on the administration's cybersecurity initiatives.

Update on the Administration's Cybersecurity Initiatives

Ms. Neuberger delivered remarks emphasizing four key government initiatives in telecommunications and cyber security beginning with the first initiative, the Federal Communications Commission's (FCC) Cyber Trust Mark program. Ms. Neuberger explained that this initiative is designed to serve as an "Energy Star for Cybersecurity," and will allow Internet-connected devices to earn government certification, indicating that they meet basic cybersecurity standards.

Next, Ms. Neuberger turned to the second initiative, highlighting the administration's ongoing collaboration with the European Union to establish mutual recognition of cyber security labels so that any products tested in the United States or Europe can be sold in both markets.

Ms. Neuberger then discussed the Counter-Ransomware initiative, launched in 2021 to combat the global ransomware threats. Originally involving 30 nations, this partnership has since expanded to 68 countries. She detailed a recent meeting which focused on disrupting criminal activities, implementing anti-money laundering measures for cryptocurrency, and leveraging AI to enhance overall cybersecurity.

Finally, Ms. Neuberger shifted to the fourth initiative, highlighting the administration's focus on securing emerging technologies by issuing the first National Security Memorandum (NSM) on AI: [*NSM-25: Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial*](#)



Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence. She also commended the National Institute of Standards and Technology for releasing post-quantum cryptography (PQC) algorithms and noted the importance of transitioning global infrastructure to PQC.

Ms. Neuberger concluded her remarks by focusing on communications resilience, stressing the critical need to address vulnerabilities in space-based infrastructure, submarine cables, and overseas communications systems. She referenced the strategic risk posed by state actors' repositioning efforts and targeted attacks, drawing specific lessons from recent incidents in Ukraine. To help address these risks, Ms. Neuberger tasked the NSTAC to conduct a study on *United States' Global Communications Resiliency – Risks and Mitigation Options* (2024 NSTAC Communications Resiliency). The purpose of the study will be to identify the points of interdependence and national security risks and make recommendations to improve the resilience of the communications sector.

Mr. Charney thanked Ms. Neuberger for providing the updates and for the new tasking. He then transitioned to the public comment period, inviting Mr. Zygmunt Lozinski, IBM Research, to speak.

Public Comment Period

Mr. Lozinski introduced himself and provided comments on the NSTAC Post-Quantum Cryptography Study. He first outlined IBM Research's dual mission: (1) to bring useful quantum computing to the world, and (2) to ensure the safety of quantum computing technologies. He noted that both IBM Research and Vodafone had contributed to the comment submission. Mr. Lozinski emphasized the transformative potential of quantum computing across industries such as pharmaceuticals, aerospace, and financial services. However, he underscored the associated risk: an advanced quantum computer could compromise public key cryptography, which underpins the security of digital infrastructure and telecommunications networks. He noted that the Post-Quantum Cryptography Study is addressing several topics, including: the implementation of cryptographic standards, the barriers to implementation, and additional policy opportunities.

Then, Mr. Lozinski stressed the importance of creating a coalition of U.S. telecom operators, vendors, and major customers to facilitate the transition to PQC. He also highlighted the need for a detailed timeline for the U.S. telecom sector's transition to PQC. This timeline would help operators and vendors establish requirements for critical technologies like 5G and align with emerging standards.

Mr. Lozinski noted that IBM Research has actively collaborated with various industry groups to address PQC. He cited the Global System for Mobile Communications Association's (GSMA) Post-Quantum Telecom Network Task Force—founded by GSMA, IBM, and Vodafone—which now includes over 60 members, including many U.S. operators. Mr. Lozinski also mentioned the Emerging Payments Association and the Canadian Forum for Digital Infrastructure Resiliency as valuable models for collaboration.



MEMBER MEETING | November 14, 2024

In closing, Mr. Lozinski commended the Post-Quantum Cryptography Study as a crucial initiative and thanked the committee for its leadership in this vital area.

Mr. Charney thanked Mr. Lozinski for providing his comments and invited Mr. Mandia to provide an update on the Baseline Security Offerings Study.

Status Update: NSTAC Baseline Security Offerings Subcommittee

Mr. Mandia began by expressing his gratitude to the subcommittee members and specifically acknowledged the contributions of the subcommittee's leads. He noted that the subcommittee has completed its data collection, having engaged with a broad range of stakeholders, including security experts, cloud service providers (CSPs), security vendors, and representatives from various industries. With the conclusion of these discussions, the subcommittee's focus has shifted toward synthesizing input and refining recommendations.

Mr. Mandia highlighted key areas of ongoing work, including improving transparency between CSPs and their customers, and refining the Shared Responsibility Model. He said this involves developing clear definitions, taxonomies, and baselines for security. Mr. Mandia also stressed the importance of striking the right balance: ensuring the subcommittee's recommendations are specific enough to be actionable while remaining flexible to encourage innovation and competition among CSPs.

Mr. Mandia informed the group that a draft of the subcommittee's report had already been shared with the NSTAC members, who provided valuable feedback. The subcommittee is now integrating these suggestions and preparing for a final draft review in December, which will be followed by a vote in February 2025.

Finally, Mr. Mandia reaffirmed the subcommittee's commitment to delivering actionable and impactful recommendations and thanked the NSTAC members for their continuous support and insight.

Mr. Charney commended Mr. Mandia for his leadership, describing the latest draft as a significant achievement in advancing the security framework for cloud technologies. He then invited government partners to share their closing remarks.

Closing Remarks and Adjournment

Mr. Coker expressed his gratitude to the NSTAC, commending the body for their work on critical initiatives such as the Post-Quantum Cryptography Study and the Baseline Security Offerings Study. He emphasized the significance of their contributions, stating the NSTAC's work is "valued and leveraged for national security" and closed by thanking them for their dedication.

Mr. Natarajan also offered his thanks, noting the importance of the NSTAC's work in shaping national cybersecurity policy. He shared that this would be his final NSTAC meeting and expressed his appreciation for the opportunity to collaborate with such a dedicated team.



PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE



MEMBER MEETING | November 14, 2024

Ms. Neuberger thanked both the members and the companies that have contributed to securing the nation's communications infrastructure. She highlighted that it has been a privilege to work with the NSTAC, noting that this was the final NSTAC meeting of the current administration. She closed by emphasizing the critical importance of the NSTAC's work and expressing her deep gratitude for the partnership.

Mr. Charney concluded the meeting by extending his appreciation to all participants and fellow members for their ongoing commitment to strengthening national infrastructure. He underscored the rewarding nature of the collaboration and acknowledged the collective effort in driving meaningful progress.

Mr. Charney reminded members that the next NSTAC Member Conference Call is scheduled for February 2025, with further details to 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. Matt Desch	Iridium Communications
Ms. Noopur Davis	Comcast
Mr. Dave DeWalt	NightDragon Management Co.
Mr. Raymond Dolan	Cohere Technologies, Inc.
Mr. John Donovan	Palo Alto Networks
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
Ms. Renee James	Ampere Computing
Ms. Kim Keever	Cox Communications
Mr. Kyle Malady	Verizon
Mr. Kevin Mandia	Google Cloud
Mr. Jeffery McElfresh	AT&T
Mr. Bryan Palma	Trellix
Mr. Neville Ray	T-Mobile
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. Rudy Brioché	Comcast
Mr. Jamie Brown	Tenable
Mr. Matt Carothers	Cox Communications
Ms. Kathryn Condello	Lumen Technologies Inc.
Mr. Thomas Gann	Trellix
Ms. Katherine Gronberg	NightDragon Management Co.
Mr. Robert Hoffman	Broadcom
Mr. John Hunter	T-Mobile
Ms. Ilana Johnson	Centergate



PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE



MEMBER MEETING | November 14, 2024

NSTAC Points of Contact (Cont.)

Mr. Ken Kaminski	Ericsson
Mr. Joel Max	Siemens USA
Mr. Sean Morgan	Palo Alto Networks
Mr. Chris Oatway	Verizon
Ms. Jeanine Pihonak	Unisys Corp.
Ms. Ista Pinon	Cisco
Mr. Tom Quillin	Intel Corp.
Mr. Kevin Reifsteck	Microsoft Corp.
Mr. Nick Saunders	Viasat
Ms. Jordana Siegel	Amazon Web Services
Ms. Jennifer Warren	Lockheed Martin
Mr. Eric Wenger	Cisco
Ms. Stephanie Woods	Lumen Technologies, Inc.

Government Participants

Ms. Caitlin Clarke	National Security Council
Mr. Harry Coker, Jr.	Office of the National Cyber Director
Dr. Ryan Donaghy	Cybersecurity and Infrastructure Security Agency
Ms. Carol House	National Security Council
Mr. Nitin Natarajan	Cybersecurity and Infrastructure Security Agency
Ms. Anne Neuberger	National Security Council
Mr. Brian Scott	Office of the National Cyber Director

NSTAC Support Staff

Mr. Mohammed Alian	TekSynap Corp.
Ms. Christina Berger	Cybersecurity and Infrastructure Security Agency
Ms. DeShelle Cleghorn	Cybersecurity and Infrastructure Security Agency
Ms. Jamie Fleece	Cybersecurity and Infrastructure Security Agency
Ms. Ashley Gaston	Customer Value Partners
Mr. John Holland	Edgesource
Ms. Janelle Pace	Cybersecurity and Infrastructure Security Agency
Ms. Laura Penn	Edgesource
Mr. William Rybczynski	Cybersecurity and Infrastructure Security Agency
Ms. Cheryl Santiago	TekSynap Corp.
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. Scott Zigler	Cybersecurity and Infrastructure Security Agency



PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE



MEMBER MEETING | November 14, 2024

Public and Media Participants

Ms. Cate Burgan	Meritalk
Mr. Ludovica Ciarravano	QTI Company
Mr. John Crossno	Rocket Software
Mr. David DiMolfetta	NextGov
Mr. Justin Doubleday	Federal News Network
Ms. Sara Friedman	Inside Cybersecurity
Mr. Eric Geller	Freelance Reporter
Ms. Katie Ignazewski	IBM
Mr. Albert Kammler	Van Scoyoc Associates
Ms. Stephanie Kiel	Google
Ms. Samantha Korta	Cybersecurity and Infrastructure Security Agency
Ms. Norma Krayem	Van Scoyoc Associates
Mr. Larry Lidz	Cisco
Mr. Zygmunt Lozinski	IBM Research
Mr. Joseph Menn	Washington Post
Mr. John Sakellariadis	Politico
Ms. Mary Schwartz	IBM
Ms. Katherine Siefert	Cybersecurity and Infrastructure Security Agency
Mr. Keelan Sweeney	Cybersecurity and Infrastructure Security Agency
Mr. Tim Starks	CyberScoop
Mr. Adrienne Winston	CNN



PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE



MEMBER MEETING | November 14, 2024

Certification

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

Mr. Scott Charney
NSTAC Chair