PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

MEMBER CONFERENCE CALL | FEBRUARY 21, 2023

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. While no one had registered to provide oral comment, 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. John Donovan, NSTAC Chair.

Mr. Donovan welcomed distinguished government partners in attendance, including Mr. Steve Kelly, Special Assistant to the President and Senior Director for Cybersecurity and Emerging Technology, National Security Council (NSC), and Mr. Brandon Wales, Executive Director, CISA.

Mr. Donovan noted that on February 3, 2023, the president announced his intent to appoint 12 new NSTAC members, underscoring that their expertise and experience will provide additional diverse viewpoints from the telecommunications industry. He added that the president also announced that Mr. Scott Charney, current NSTAC Vice Chair, will become chair and Mr. Jeffrey Storey, Lumen Technologies, will become vice chair. Mr. Donovan extended his congratulations and thanks for their willingness to serve.

In reviewing the agenda, Mr. Donovan noted that the meeting would include: (1) opening remarks from the administration and CISA leadership; (2) a status update on the NSTAC Addressing the Abuse of Domestic Infrastructure (ADI) by Foreign Malicious Actors Subcommittee; and (3) a deliberation and vote on the draft *NSTAC Report to the President on a Strategy for Increasing Trust in the Information and Communications Technology and Services (ICTS) Ecosystem* (Strategy for Increasing Trust Report).

Mr. Donovan then provided a summary of the December 2022 NSTAC Member Meeting, during which: (1) Ms. Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, NSC, tasked the NSTAC with a study focused on addressing the abuse of domestic infrastructure by foreign malicious actors; (2) Mr. Chris Inglis, National Cyber Director, Executive Office of the President, gave a keynote on a strategic approach for the next decade of cybersecurity; (3) Mr. Wales provided a status update on the government's implementation of NSTAC recommendations; and (4) Mr. Charney, Strategy for Increasing Trust Subcommittee Chair, provided a status update on the subcommittee's progress.

Mr. Donovan noted Mr. Inglis recently retired and expressed his gratitude for his partnership to the NSTAC and service to the nation. He then turned the floor over to Mr. Kelly to provide his opening remarks.

Mr. Kelly thanked Mr. Donovan and Mr. Charney for their continued leadership and expressed his enthusiasm for the president's announcement of new NSTAC members. He stated he was looking forward to the status update on the ADI Subcommittee and discussing the fourth and final phase of the "Enhancing Internet Resilience (EIR) in 2021 and Beyond" study. He noted that the topics closely align and support the priorities of the administration.

Mr. Kelly then introduced Mr. Rob Knake, Acting Principal Deputy National Cyber Director, Office of the National Cyber Director (ONCD), to provide remarks on recent updates within the office.

Mr. Knake reiterated that Mr. Inglis recently retired after 50 years of government service and announced that Ms. Kemba Walden has assumed Mr. Inglis' duties as Acting National Cyber Director.

Mr. Knake reported that developing the National Cybersecurity Strategy involved reviewing over a decade of NSTAC reports and recommendations, and that the strategy will be released soon. He added that he believes the committee will notice its work reflected in the strategy. Mr. Knake also expressed his anticipation in reviewing the draft Strategy for Increasing Trust Report and said the recommendations regarding regulatory harmonization align well with the overarching goals of the strategy. Mr. Knake thanked Mr. Kelly for being a valued partner on the development of the strategy and monitoring its progress through the NSC process over the last few months, and Mr. Kelly expressed his thanks for this partnership. Mr. Donovan thanked Mr. Kelly and Mr. Knake for their comments and invited Mr. Wales to provide his remarks.

Mr. Wales thanked Mr. Donovan and Mr. Charney for their leadership of the committee and for the continued efforts to support the nation's security and resilience of its information technology and communications infrastructure. He stated that there has been tremendous progress in many of these efforts over the past year.

Mr. Wales noted that there has been a more focused, robust collaboration between the public and private sector in deterring and responding to recent and emerging cybersecurity threats. To further these partnerships, CISA continues to partner alongside the cybersecurity community to cultivate a safe, secure cyber ecosystem. Mr. Wales cited three major efforts of this partnership, which he believes relates to several NSTAC recommendations. He stated that the first effort is focused on stopping the threat by working with CISA's partners to gain greater visibility into cybersecurity threats against the nation, the threat actors who wage those threat campaigns, and the country's own vulnerabilities. He said that CISA and its partners work together to coordinate disclosure and strive for mitigation of critical and exploitable vulnerabilities.

Second, Mr. Wales referred to "hardening the terrain," explaining that CISA and its partners achieve this by taking a holistic approach, examining risks and hazards to the cybersecurity landscape, and prioritizing those that are most systemic in nature. He stated that driving effective implementation of risk management frameworks and practices, and by providing state-of-the-art cybersecurity capability and services to public and private sector partners, is key to achieving this goal.

The third effort Mr. Wales highlighted is the attempt to drive security by default. He explained that this includes partnering with the broader community to drive development of trustworthy products and services and advancing the ecosystem to support network defenders. He underscored that driving security by default is critical as the path to a more secure cyber world starts with designing, engineering, and manufacturing products in alignment with cybersecurity best practices.

Mr. Wales then cited the Joint Cyber Defense Collaborative (JCDC) as an example of the public-private partnership that is currently in practice. He stated that CISA created the JCDC in 2021 and recently announced its 2023 planning agenda, the first of its kind to bring together the public and private sector to develop and execute cyber defense plans that achieve very specific risk reduction goals and enable more focused collaboration. He noted that the JCDC is currently focused on three areas: (1) systemic risk; (2) collective cyber response; and (3) high-risk communities. Mr. Wales stated that there are other topics to examine, including risks potentially posed by open-source software used in industrial control systems; supply chain risk for small and medium-critical infrastructure entities; work with the energy sector alongside the Department of Energy; and approaches to edge devices in the water sector.

Mr. Wales thanked the NSTAC for its efforts in producing the Strategy for Increasing Trust Report. Mr. Wales emphasized that the U.S. government, including CISA, is eagerly utilizing NSTAC reports to ensure that it leverages those recommendations to continue to advance the security of the ecosystem.

Mr. Donovan thanked Mr. Wales for his comments.

Status Update: NSTAC ADI Subcommittee

Mr. Donovan then introduced Mr. Stephen Schmidt and Mr. Hock Tan, Co-Chairs of the ADI Subcommittee, to provide an update on the study's progress.

Mr. Tan stated that the tasking is timely and important. He said that when Ms. Neuberger issued the tasking at the December meeting, the topic was already a key focus for the administration, including in Executive Order (EO) 13984, *Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*, and a related Department of Commerce rulemaking process. He remarked that the study could be a very wide-ranging topic, which is why it is important to properly scope the project.

Mr. Tan noted that the subcommittee will first review various factors that unintentionally aid and abet the ability of foreign actors to unleash cyber-attacks, citing the quality of technological infrastructure as one key factor. He continued that as enterprises and governments modernize their networks, they are seeing the continued adoption of Infrastructures-as-a-Service (IaaS), and Platform-as-a-Service (PaaS). He explained reports show that malicious actors are also leveraging IaaS and PaaS to their advantage, and the reduced barriers to delivery that these services bring to legitimate enterprises are doing the same for malicious actors. Mr. Tan stated that these services appeal to malicious actors due to their marketplace and feature-set popularity. He said these services also provide a degree of reputation and further allow attackers to blend in with legitimate network traffic more easily. He further noted that another well-known factor is that much of the internet ecosystem, including IaaS and PaaS vendors, are privately owned, operated, and based in the United States, but this can also serve as a cybersecurity advantage.

Mr. Tan said that discussing real-world experiences that U.S. based IaaS and PaaS vendors have had with malicious actors, whether they be foreign or domestic, will be essential to the subcommittee's briefings, findings, and recommendations. He emphasized that it is important for the committee to identify the additional needs of IaaS and PaaS vendors to eliminate malicious activities on their infrastructure, and by doing so, disrupt malicious actors, increase their cost, and decrease their effectiveness in compromising networks.

Mr. Tan stated that as the second focus, the subcommittee will examine the role of the U.S. government, as well as U.S. laws and regulations, in either aiding or slowing down proactive U.S. government interventions to prevent or respond to malicious attacks. He noted that the U.S. government depends on the private sector to initiate preventive actions and to share information to prevent or respond to an attack. He explained that in most instances, the first lines of response and defense to malicious attacks are voluntary actions or reactions by the private sector and that, because of this, the third focus area of the study will examine potential influences and incentives that might increase this private sector action.

Mr. Tan emphasized that completing the study will require the subcommittee to examine several legal, financial, technological, and operational sources, among other relevant materials and information. He stated that these sources include briefings from government experts and welcomed briefer suggestions from participants on government and industry subject matter experts. He underscored that the subcommittee would start preparing the first draft of the report in April 2023 so that it can be posted and made public in August 2023. He implored everyone to reach out to subcommittee leadership with ideas, questions, and recommendations. Mr. Tan then invited Mr. Schmidt to provide his remarks.

Mr. Schmidt thanked government colleagues from the NSC and CISA, as well as Mr. Donovan for his support and guidance. He also expressed his gratitude to Mr. Tan for his partnership to co-chairing the study.

Mr. Schmidt stated that the study is critical and important to the nation, and that he takes concerns raised by the U.S. government about the use of IaaS and PaaS for malicious purposes seriously. He stated the tactics, techniques, and procedures of malicious actors are constantly evolving and emphasized that companies must also constantly evolve to keep pace to mitigate any malicious activity. He expressed confidence that the study can help inform the government's rulemaking efforts.

Mr. Schmidt stated that a better understanding of the scope of the issue from the government's perspective will both aid the subcommittee's efforts and will shape the scope of the issue from the private sector's perspective. He said that it is imperative for the subcommittee to adequately define the scope at the outset to avoid including topics which fall too far outside the original core issues that prompted the tasking in the first place. He expressed that the private sector needs to have a better handle on what the government is most concerned about so it can consider what can be done to address these concerns and assess whether there are blockers that need to be removed. For example, there has been a significant focus on how government and industry partner to address cybersecurity issues, including on operational cooperation and information sharing via the JCDC. Mr. Schmidt said that to add more value to the work that has been done, the subcommittee needs to ensure they focus on the specific malicious activity included in the tasking.

Mr. Schmidt closed by saying that he believes the subcommittee can illuminate the issues at hand, and identify constructive, actionable recommendations to address them.

Status Update: NSTAC Strategy for Increasing Trust Subcommittee

Mr. Donovan invited Mr. Charney to present the Strategy for Increasing Trust Report. Mr. Charney explained that this report represents the fourth and final phase of the EIR study and builds upon the three prior reports focused on software assurance in the ICTS supply chain, zero trust and trusted identity management, and information technology (IT) and operational technology (OT) convergence. He explained that the subcommittee reviewed these prior reports to determine if gaps existed and to identify recommendations that, if enacted, might advance all three prior work streams. He said the subcommittee also focused on one new issue that could advance not only the prior recommendations, but security efforts more broadly. Mr. Charney stated that this issue relates to how cybersecurity requirements are promulgated, compliance is proved, and if proof of compliance is communicated to users and regulators. He noted that the subcommittee received 17 briefings from the government, private sector, and other organizations to understand their challenges with security compliance, learn from their perspectives, and listen to their recommendations.

Mr. Charney said that the draft report identifies seven key findings and seven actionable recommendations. For the purposes of this update, Mr. Charney focused on two areas: (1) the findings and recommendations originating from the review of the first three reports; and (2) the findings and recommendations related to the promulgation of security requirements and compliance. He explained that after reviewing the phase I, II, and III, reports and hearing from briefers, one fact proved consistent throughout: sustained effort, especially within the federal government, is required to research, deploy, and operationalize security technologies.

Mr. Charney said that due to a clear need to sustain security efforts over long periods of time, the report recommends three ways to integrate security efforts into existing government programs and the processes. First, government should improve procurement language to encourage vendor security best practices. Second, the government should enhance CISA's Continuous Diagnostics and Mitigation (CDM) program, to ensure sustained application of security best practices. Third, the government should maximize the use of automation and the reuse of evidence when assessing Federal Information Security Management Act (FISMA) compliance.

Regarding the first focus area, Mr. Charney explained that while the phase III study recommended that CISA work with the General Services Administration (GSA) to require enhanced procurement language for OT procurements, the subcommittee believes the recommendation should be more broadly applied, and that all ICT federal procurement preferences align with specifically articulated zero trust standards and best practices. He also said the report recommends that CISA, in consultation with private and public sector partners, should work with GSA to draft standard procurement language to help federal agencies sustain security improvements over time and that this language should achieve three objectives. Mr. Charney explained that these objectives are to: (1) require that software is developed and maintained according to the current National Institute of Standards and Technology (NIST) supply chain risk management and software assurance guidance; (2) prefer services provided by organizations that prioritize cybersecurity within their own enterprise environments by aligning with specifically articulated zero trust standards and best practices; and (3) prefer OT products and services that support asset inventory and that align where applicable with zero trust principles and other cybersecurity best practices.

Mr. Charney said that for the second focus area, while the phase II study specifically identified the value of aligning the CDM program with zero trust, the program could also be leveraged for other purposes, such as gathering accurate inventories and managing the distribution of software purchases. He said the CDM program should be used to achieve four goals: (1) incorporate OT technologies by performing continuous inventorying of OT devices, software, system, and assets; (2) categorize in software inventories, software provided by producers following NIST’s special publication 800-218, the secure software development framework; (3) include scanning and discovery of internet-accessible applications; and (4) provide continuous and dynamic asset mapping as part of CDM shared services, since static data poles will have limited utility in the constantly evolving IT environment.

Mr. Charney said that for the third focus area, both the phase I and phase III studies provided recommendations relevant to maximizing automation and reuse of evidence, as doing so allows compliance regimes to scale efficiently. He added that to promote this objective, federal shared services programs should work towards a consistent approach for assessing implementation of FISMA requirements, while giving special considerations to the issues raised in the NSTAC’s three prior reports.

Mr. Charney stated that implementing these recommendations of improving procurement language, enhancing CDM, and maximizing the automation and reuse of evidence, could help advance objectives identified in all three prior phases of the EIR effort.

Mr. Charney noted that after reviewing the challenges associated with the promulgation of security requirements and compliance, the subcommittee identified two critical findings from its briefings and research: (1) growing concerns about cybersecurity risks have caused requirements and assurance programs to dramatically increase domestically and internationally, sometimes diverting resources from improving security to proving compliance with overlapping, redundant, or inconsistent requirements; and (2) development of and alignment to consensus standards are critical for driving harmonization, which permits compliance activities to be done effectively and efficiently, and allows for compliance results to be used and reused globally. He then highlighted two specific recommendations from the report that responds to these findings.

The first recommendation is that the executive branch should establish a government office within CISA with the primary mission of driving regulatory harmonization. He noted that no such office currently exists, and there is a strong need for a group of individuals who have both an in-depth expertise on cybersecurity regulations, and a vision for how to use consensus standards to reduce existing cacophony, confusion, and costs. He explained that the responsibilities of this office should include establishing expertise on cybersecurity regulations across sectors and creating resources that regulators can use to more easily develop cybersecurity requirements that leverage consensus standards and should also provide technical assistance to regulators during the rulemaking process. He clarified by stating that the office would serve in an advisory and assistance capacity to other regulators and would not issue rules. He explained that instead, the office would institutionalize and expand upon existing harmonization efforts, such as the Cyber Incident Reporting Council, and the Cybersecurity Forum for Independent and Executive Branch Regulators.

The second recommendation is that the president should explicitly establish cybersecurity regulatory harmonization as a regulatory principle and require that cybersecurity requirements and rulemaking align to consensus standards. Mr. Charney explained that to achieve this, the report recommends that the president build upon EO 12866, *Regulatory Planning and Review*, which established the policies and processes for regulatory planning and review within the executive branch. He stated that as part of this effort, agencies issuing cybersecurity regulations should be required to document and explain how the cybersecurity requirements in their rulemaking align to consensus standards or explain why proposed requirements need to diverge. Mr. Charney noted that this documentation and analysis requirement is similar to the EO 12866 requirement that issuing agencies assess the potential costs and benefits of a regulatory action in support of the regulatory principle that regulations be designed in a cost-effective manner. He said that one challenge in adapting existing EO 12866 processes towards the goal of cybersecurity regulatory harmonization is that independent regulatory agencies are excluded from the EO's existing regulatory review requirements. Mr. Charney said that streamlining regulatory requirements, aligning them to consensus standards, and developing automated tools to prove compliance all improve security while reducing inefficiencies. He emphasized that the president should, at a minimum, encourage independent regulatory agencies to follow the government's approach towards regulatory harmonization.

Mr. Charney emphasized that the recommendations in the report, combined with earlier recommendations in phases I, II, and III, have the potential to advance the shared goal of improving the nation's cybersecurity.

Mr. Donovan thanked Mr. Charney for the update and opened the floor for comments or questions from NSTAC members and government partners before proceeding to a vote to approve the report. Mr. Wales asked for additional clarity on the subcommittee's rationale for recommending CISA have responsibility for establishing the new Office of Regulatory Harmonization.

Mr. Charney stated that recognizing that the responsibility for cybersecurity regulation is spread across the federal government, the subcommittee thoroughly considered where to base the focal point for this effort and concluded that the primary advantage of housing this effort in CISA is that most other departments, such as the U.S. Department of the Treasury or Health and Human Services, are primarily concerned with their respective verticals. He explained that by contrast, the new harmonization office would be focused on protecting critical infrastructures, giving it a broader cross-vertical perspective. He noted that CISA has established deep relationships with those horizontal providers of ICTs, whose products and services support a broad range of verticals. He also said that the proposed office would act in an advisory capacity to other regulators and would not impose regulation itself, which is consistent with CISA's existing interactions with regulators.

Mr. Charney continued explaining the subcommittee's rationale, noting they considered Department of Commerce, ONCD, and the Office of Information and Regulatory Affairs (OIRA) as other locations for the new office, as they could bring similar broad cross-vertical perspectives. He said they considered Commerce based on its standards expertise and its experience in implementing regulations in other contexts, but they believed CISA is a better fit because it currently undertakes similar cross-sector cybersecurity efforts, such as the Cyber Incident Reporting Council, and the Cross-Sector Performance Goals. He said they next considered ONCD based on its ability to have cross-agency visibility from the White House but believed that ONCD's focus on policy might make it more difficult for staff to develop and sustain in-depth expertise on this complex topic. He said that finally they considered OIRA based on its roles and responsibilities for regulatory review under EO 12866 but believed the specialized cybersecurity knowledge and expertise required would be more effectively developed and maintained within CISA.

Mr. Wales thanked Mr. Charney for the explanation. Upon Mr. Donovan's request for additional comments, Mr. David DeWalt, NightDragon Management Company, expressed his appreciation for the subcommittee's work on the report. Upon hearing no further comments, Mr. Donovan made a motion to approve the report. Following the motion, which was seconded, NSTAC members unanimously approved the report for transmission to the president.

Closing Remarks and Adjournment

Mr. Donovan thanked: participants for attending and providing input into the discussion; Mr. Tan and Mr. Schmidt for providing an update on the ADI Subcommittee; Mr. Charney for the development of the draft Strategy for Increasing Trust Report; and the subcommittee working group leads, members, and the NSTAC team for their efforts. Mr. Donovan then invited Mr. Kelly to provide his closing remarks.

Mr. Kelly thanked Mr. Charney for the update on the report, adding that he will be tracking NSTAC's progress on the ADI study topic.

Mr. Donovan thanked Mr. Kelly for his comments and invited Mr. Wales to provide his closing remarks.

Mr. Wales thanked the subcommittee for developing the report, adding that some of the recommendations will encourage action and inspire ideas or addressing important issues like regulatory harmonization, which he said he recognizes is a high priority issue for critical infrastructure community partners and the cyber private sector. He commented that the forthcoming ADI report will be of high interest given current awareness of adversaries' most recent activities and he is looking forward to seeing innovative ideas coming from the NTSAC to help in the future.

Mr. Donovan thanked Mr. Wales for his remarks. He stated the next NSTAC meeting will be held on May 16, 2023. He then made a motion to close the meeting. Upon receiving a second, Mr. Donovan officially adjourned the meeting.

APPENDIX

February 21, 2023, NSTAC Member Conference Call Participant List

NAME	ORGANIZATION
NSTAC Members	
Mr. Peter Altabef	Unisys Corp.
Mr. Scott Charney	Microsoft Corp.
Mr. Matthew Desch	Iridium Communications, Inc.
Mr. David DeWalt	NightDragon Management Company, LLC
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.
Mr. Mark McLaughlin	Qualcomm
Mr. Angel Ruiz	MediaKind, Inc.
Mr. Stephen Schmidt	Amazon
Mr. Jeffrey Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
NSTAC Points of Contact	
Mr. Jason Boswell	Ericsson, Inc.
Mr. Jamie Brown	Tenable Holdings, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Mr. Robert Hoffman	Broadcom, Inc.
Ms. Ilana Johnson	Two Island Partners, LLC
Mr. Sean Morgan	Palo Alto Networks, Inc.
Ms. Jennifer Raiford	Unisys Corp.
Mr. Kevin Reifsteck	Microsoft Corp.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Thomas Quillin	Intel Corp.
Government Participants	
Ms. Christina Berger	Cybersecurity and Infrastructure Security Agency
Ms. DeShelle Cleghorn	Cybersecurity and Infrastructure Security Agency
Mr. Trent Frazier	Cybersecurity and Infrastructure Security Agency
Ms. Elizabeth Gauthier	Cybersecurity and Infrastructure Security Agency
Ms. Helen Jackson	Cybersecurity and Infrastructure Security Agency
Mr. Steven Kelly	National Security Council
Mr. Rob Knake	Office of the National Cyber Director

Ms. Loran Lascar	Office of the National Cyber Director
Mr. Barry Skidmore	Cybersecurity and Infrastructure Security Agency
Ms. Tanya Sims	Office of the National Cyber Director
Mr. William Rybczinski	Cybersecurity and Infrastructure Security Agency
Ms. Elke Sobieraj	National Security Council
Ms. Marilyn Stackhouse	Cybersecurity and Infrastructure Security Agency
Mr. Brandon Wales	Cybersecurity and Infrastructure Security Agency
Mr. Scott Zigler	Cybersecurity and Infrastructure Security Agency

Contractor Support

Ms. Ashley Burrell	TekSynap Corp.
Ms. Joan Harris	Edgesource Corp.
Ms. Laura Penn	Edgesource Corp.
Ms. Jennifer Topps	TekSynap Corp.
Mr. Joel Vaughn	TekSynap Corp.

Public and Media Participants

Mr. Colin Alberts	Freedom Technologies, Inc.
Ms. Lindsay Bednar	Amazon Web Services, Inc.
Mr. Rudy Brioche	Comcast Corp.
Mr. Howard Buskirk	Communications Daily
Mr. Johnathon Caldwell	Lockheed Martin Space
Mr. Drew Colliatie	Siemens USA
Mr. Matt Carothers	Cox Communications
Mr. Mark Dankberg	Viasat, Inc.
Mr. Noopur Davis	Comcast Corporation
Ms. Sara Friedman	Inside Cybersecurity
Ms. Deirdre Gallop-Anderson	Cybersecurity and Infrastructure Security Agency
Mr. Eric Geller	Politico
Ms. Barbara Humpton	Siemens USA
Mr. John Hunter	T-Mobile US, Inc.
Mr. Albert Kammler	Van Scoyoc Associates
Ms. Karen Kaya	Crowdstrike
Ms. Kimberly Keever	Cox Communications
Mr. Matt Kostman	Zeichner Risk Analytics
Ms. Norma Krayem	Van Scoyoc Associates
Mr. Taylor Lamb	Morgan Lewis
Ms. Danouh Louis	Cybersecurity and Infrastructure Security Agency
Mr. Sean Lyngaas	CNN
Mr. Kyle Malady	Verizon Communications
Mr. Kevin Mandia	Mandiant Google Cloud
Ms. Maria Martinez	Cisco Systems, Inc.
Mr. Chris McCall	Siemans Corp

Mr. Jeff McElfresh	AT&T, Inc.
Ms. Helen Negre	Siemans USA
Ms. Stacy O’Mara	Mandiant Google Cloud
Mr. Bryan Palma	Trellix
Mr. Sunjeet Randhawa	Broadcom, Inc.
Mr. Neville Ray	T-Mobile US, Inc.
Mr. Rashard Rose	CNN
Mr. John Sakellariadis	Politico
Mr. Jeff Seldin	Voice of America
Ms. Suzanne Smalley	Reuters
Mr. Tim Starks	Washington Post
Mr. Corey Thomas	Rapid7, Inc.
Mr. Kent Varney	Lockheed Martin
Mr. Eric Wenger	Cisco Systems
Mr. Jeff Williams	TR Daily
Mr. Michael Woods	Verizon Communications

Certification

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

Mr. John Donovan
NSTAC Chair