Call to Order and Opening Remarks

Ms. Christina Berger, Cybersecurity and Infrastructure Security Agency (CISA)and NSTAC Designated Federal Officer, 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 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. Trent Frazier, Deputy Assistant Director for Stakeholder Engagement, CISA; Mr. Steve Kelly, Senior Director for Cybersecurity and Emerging Technology, National Security Council (NSC); and Ms. Kemba Walden, Principal Deputy National Cyber Director, Office of the National Cyber Director (ONCD).

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 Strategy for Increasing Trust in the Information and Communications Technology and Services (ICTS) Ecosystem (Strategy for Increasing Trust) Subcommittee; and (3) a deliberation and vote on the draft *NSTAC Report to the President on Information Technology and Operational Technology (IT/OT) Convergence* (IT/OT Convergence Report).

Mr. Donovan then provided a summary of the May 2022 NSTAC Member Meeting, during which: (1) Ms. Elke Sobieraj, Director for Critical Infrastructure Cybersecurity, NSC; Mr. Brandon Wales, Executive Director, CISA; and Mr. Neal Higgins, Deputy National Cyber Director for National Cybersecurity, ONCD, remarked on the government's collaboration with industry on key national security and emergency preparedness communications initiatives; (2) Mr. Mike Herrington, Section Chief, Executive Cyber Division, Federal Bureau of Investigation, provided a keynote speech; (4) NSTAC members voted to unanimously approve the *NSTAC Letter to the President on Enhancing U.S. Leadership in International Communications Technology Standards* (Standards Letter); and (5) Mr. Jack Huffard, Chair of the IT/OT Convergence Subcommittee Chair, provided an update on the subcommittee's progress. Mr. Donovan then turned the floor over to Mr. Frazier to provide his opening remarks.

Mr. Frazier stated that the nation's cybersecurity threat landscape continues to evolve and expand. He remarked that the recent joint cybersecurity advisory on North Korea's state-sponsored actors use of Maui ransomware to target healthcare and public health sector organizations highlights some of the tactics, techniques, procedures, and indicators of compromise that state-sponsored actors are employing broadly across U.S. networks to attack many critical infrastructure sectors and communities. He also mentioned that the advisory includes recommended actions organizations can take to mitigate the risks.

Mr. Frazier continued that CISA recently announced its Post-Quantum Cryptography Initiative, which has been established to unify and foster various efforts within the agency and in partnership with the National Security Agency. He stated that CISA, in close coordination with DHS and the Department of Commerce's National Institute of Standards and Technology (NIST), is working to support critical infrastructure and government network owners and operators during the transition to a post-quantum environment. Mr. Frazier explained that quantum information science is an interdisciplinary field that studies the impacts of quantum physics properties on information science. Those properties increase computational power and the speed with which one executes the kinds of computations that classical computers could never achieve. He underscored that these properties also expose users to an increasing number of risks specific to the communications that are most relied upon and found on current networks. Mr. Frazier stated that, as this technology advances over the next decade, quantum computing is increasing those risks to encryption methods that are widely used for technology customer data, to complete transactions across businesses and industries, and to secure communications.

Mr. Frazier noted that a recent NIST announcement highlights that the institute has chosen the first group of cryptographic algorithms, and is a key milestone to identify a new standard to replace the current quantum vulnerable cryptography. He noted that NIST is not expected to publish the standard for use by commercial products until 2024, but CISA recommends organizations start preparing for this transition by following the Post-Quantum Cryptography Roadmap. He said that some of the planned efforts by the Post-Quantum Cryptography Initiative will address how CISA will approach the threat presented by quantum computing, including assessing quantum vulnerabilities across U.S. critical infrastructure by evaluating risks in the 55 national critical functions. Mr. Frazier closed by thanking Mr. Huffard, Chair of the IT/OT Convergence Subcommittee, and Mr. Scott Charney, NSTAC Vice Chair and Chair of the Strategy for Increasing Trust Subcommittee, and the respective subcommittees for their efforts.

Mr. Donovan thanked Mr. Frazier for his comments. He then invited Mr. Kelly to provide his remarks.

Mr. Kelly acknowledged the president's receipt of the Standards Letter and underscored appreciation for the committee's insights and recommendations on how to assure that U.S. interests are protected and that the widely accepted principles for the development of international standards are followed. He stated that the administration is working on the next round of proposed future study topics for the NSTAC to address, and the prioritized list will be shared with the committee in the coming weeks for further discussion and refinement.

Mr. Kelly concluded his remarks by noting that recent topics the NSTAC is addressing, such as increasing trust in the ICTS ecosystem and IT/OT convergence, closely align and support the administration's priority to secure the nation's critical infrastructure.

Mr. Donovan thanked Mr. Kelly for his comments and invited Ms. Walden to provide her remarks.

Ms. Walden thanked the NSTAC for its continued efforts and contributions, and thanked Mr. Donovan and Mr. Charney for their leadership. She noted the government's need for industry's perspective and experience in critical areas and highlighted that the NSTAC is a key contributor to enhancing its understanding of many complex issues. She said that the ONCD is currently working collaboratively with the NSC, other executive offices of the president, the interagency, and the private sector to draft the national cybersecurity strategy which will build on the president's broader vision for building a better America. She said that the goal of the strategy is to align policy choices with digital aspirations to build a durable cyber-secure foundation for the administration's goals. She continued that the strategy will build on government work that has been accomplished over the past 19 months, to include Executive Order (EO)14028, *Improving the Nation's Cybersecurity*, and other efforts and initiatives, such as the NSTAC IT/OT Report. Additionally, the strategy will lay out the administration's near-term investments in cybersecurity alongside the more deliberate, confirmative long-term construction of a secure digital future.

Ms. Walden asserted that the recent NSTAC studies are prime examples of how the committee is providing valuable contributions to inform strategy and policy development. She stated that ensuring the security of the nation's critical infrastructure will always be a paramount goal and that these studies are timely and are addressing key areas of concern.

Ms. Walden mentioned that ONCD and its government partners continue to focus on effective collaboration to achieve the most robust information sharing. She also emphasized the need to leverage government's unique authorities where appropriate. Ms. Walden concluded by noting that that the advice, counsel, and recommendations the NSTAC provides to the president continue to be especially important contributions to U.S. national security policy and development.

Mr. Donovan thanked Ms. Walden for her remarks.

Status Update: NSTAC Strategy for Increasing Trust in the ICTS Ecosystem Subcommittee

Mr. Donovan invited Mr. Charney to provide an update on the subcommittee's progress to date.

Mr. Charney noted that the strategy for increasing trust in the ICTS ecosystem is the topic of phase IV and the capstone of the "Enhancing Internet Resilience in 2021 and Beyond" study. He explained that this phase will build upon the NSTAC's prior three reports, which focus on software assurance in the ICTS supply chain, zero trust and trusted identity management, and IT/OT convergence. Additionally, this phase will focus on one new issue, improving security assurance, which might dramatically move forward the nationwide security efforts reflected in EO 14028.

Mr. Charney noted that phase IV presents an opportunity to review the previous three reports and determine whether the topics have been adequately addressed or if there are gaps that should be further explored. He said that phase IV also presents an opportunity to identify recommendations that, if enacted, might advance all three prior focus areas.

Mr. Charney said the guidance on phase IV was derived from the U.S. government's efforts to supplement policies with more robust implementations. He noted that as information and communications technologies become more critical to people's daily lives, setting security requirements, proving compliance with those requirements, and communicating that proof to users and regulators is of critical concern. Mr. Charney has asked the subcommittee to focus on the issue of improving security assurance, as the way in which requirements have been promulgated and assurance has been approved and communicated has not worked well and can be improved.

Mr. Charney stated that the subcommittee is currently extending invitations to potential briefers from the government, the private sector, and other organizations to understand their challenges with security compliance, learn from their perspectives, and listen to their recommendations. He welcomed additional recommendations for potential briefers from the members. In closing, Mr. Charney expressed his appreciation to the subcommittee, and thanked Mr. Donovan for the opportunity to brief the NSTAC. Mr. Donovan thanked Mr. Charney for his comments.

Deliberation and Vote: *NSTAC Report to the President on Information Technology and Operational Technology Convergence*

Mr. Donovan welcomed Mr. Huffard to discuss the key findings and recommendations of the report.

Mr. Huffard said that critical infrastructure in the U.S. faces a significant heightened threat landscape and the importance of securing IT and OT systems, including those in converged IT/OT environments, has become a national security imperative. For example, in 2021 a hacker leveraged a known vulnerability in the IT system at a water treatment plant in Oldsmar, Florida in an attempt to manipulate the level of sodium hydroxide in the water supply. The Colonial Pipeline also faced a ransomware attack in 2021 and was forced to halt pipeline operations for six days, disrupting 45% of the fuel use on the East Coast in the United States. Mr. Huffard added that shortly after the launch of the study, Russia invaded Ukraine, which significantly heightened geopolitical tensions. By extension, these have then increased the threat of dangerous cyberattacks against critical infrastructure in countries that support Ukraine, including the United States.

Mr. Huffard then explained that the NSTAC was tasked with developing a report to examine the key challenges of securing converged OT systems against threats that emerge from IT network connections. The committee was also asked to identify emerging approaches to increase OT resiliency to these fronts. He said that the subcommittee distilled briefings into three phases: (1) government entities and policymakers; (2) critical infrastructure owners and operators of converged IT/OT environments and original equipment manufacturers; and (3) cloud service providers, integrators, and cybersecurity vendors. In all, the subcommittee received more than 30 briefings from subject matter experts which contributed significantly to the NSTAC's report.

Mr. Huffard then shared some of the study's key findings. First, he noted that the convergence of IT and OT systems is not a new issue and is one that has been happening for decades. He added that the convergence of IT and OT has created clear and present cyber exposure challenges that require

attention. Mr. Huffard stated that as a whole, the nation's stakeholders have access to the technology and knowledge to secure these systems but has not prioritized the resources required to implement appropriate solutions. For the second key finding, Mr. Huffard expressed that in contrast to the cybersecurity attacks on IT systems, the outcomes of successful OT attacks include the potential to impact human safety and damage physical equipment by taking any industrial processes OT equipment supports offline for extended time periods. The third key finding was that, even in 2022, many organizations lack visibility into their complete OT environments, including IT/OT interconnection and supply chain dependencies. For the fourth key report finding, Mr. Huffard stated that silos exist between IT and OT personnel within organizations, creating an opportunity to bring them into a more unified structure to better manage shared responsibilities to secure converged environments. The final key finding Mr. Huffard discussed is that cybersecurity is rarely required in public and private OT requests for proposals and procurement policies.

Mr. Huffard noted that the IT/OT Convergence Report includes 15 presidential, strategic, and actionable recommendations to address many of the challenges that were raised in the briefings the subcommittee received and the research conducted. He added that of these 15 recommendations, the subcommittee identified three which are critically important for the president to implement to provide immediate improvement to the cybersecurity posture of U.S. government owned and operated OT systems with relatively low risk. He continued that these recommendations can also serve as a model for critical infrastructure owners and operators.

Mr. Huffard then reviewed the three critical recommendations. First, CISA should issue a binding operational directive requiring executive civilian branch departments and agencies to maintain a real-time, continuous inventory of all OT devices, software systems, and assets within their area of responsibility, including an understanding of any interconnectivity to other systems. Once agencies clearly understand the vast interconnected nature of their OT devices and infrastructure, they can then make risk-informed decisions about how to prioritize their IT, OT, and cybersecurity resources. Second, CISA should develop guidance for procurement language on OT products and services that require the inclusion of risk-informed cybersecurity capabilities for products and services that support converged IT/OT environments, including for supply chain risk management. CISA should then work with the General Services Administration to require the inclusion of risk-informed cybersecurity capabilities and procurement vehicles for federal government. Finally, the NSC, CISA, and the ONCD should prioritize the development and implementation of interoperable, technology-neutral, vendor-agnostic information sharing mechanisms to enable the real-time sharing of sensitive, collective defense information between authorized stakeholders involved in securing critical infrastructure in the United States. Mr. Huffard asserted that these recommendations, coupled with the other 12 in the report, can greatly improve the nation's critical infrastructure cybersecurity posture.

Mr. Huffard concluded by thanking the subcommittee for their efforts. He also thanked the NSTAC team and CISA for their support in coordinating subcommittee activity. Finally, Mr. Huffard thanked Mr. Donovan and Mr. Charney, as well as the members of the NSTAC, for the opportunity to chair

the study.

Mr. Donovan thanked Mr. Huffard for the update and for chairing the study.

Mr. Donovan then made a motion to approve the IT/OT Convergence 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; Mr. Charney for providing an update on the Strategy for Increasing Trust Subcommittee; Mr. Huffard for the development of the IT/OT Convergence Report; and the subcommittee working group leads, members, and the NSTAC team for their efforts. Mr. Donovan then asked Mr. Frazier to provide his closing remarks.

Mr. Frazier thanked the IT/OT Convergence Subcommittee for their efforts and acknowledged that this is an area that the CISA Director has expressed considerable interest. He added that CISA anticipates reviewing the recommendations in the IT/OT Convergence Report and finding ways that principals within the agency can not only support their implementation but learn from them and improve operations.

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

Mr. Kelly expressed his thanks to Mr. Huffard and Mr. Charney for their leadership of the subcommittees. He thanked the NSTAC for its contribution to the security of the nation and stated that he looks forward to continuing to work with the committee moving forward.

Mr. Donovan thanked Mr. Kelly and invited Ms. Walden to make her closing remarks.

Ms. Walden reiterated her appreciation for the IT/OT Convergence Report and said that ONCD will review the recommendations and work to implement them.

Mr. Donovan thanked Ms. Walden for her comments. He reminded participants that the next NSTAC meeting will be held on November 10, 2022. He then made a motion to close the meeting. Upon receiving a second, Mr. Donovan officially adjourned the meeting.

APPENDIX

August 23, 2022, 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 Security, LLC
Mr. Raymond Dolan	Cohere Technologies, Inc.
Mr. John Donovan	Palo Alto Networks, Inc.
Dr. Joseph Fergus	Communications Technologies, Inc.
Mr. Patrick Gelsinger	Intel Corp.
Ms. Lisa Hook	Two Island Partners, Inc.
Mr. Jack Huffard	Tenable Holdings, Inc.
Ms. Renee James	Ampere Computing, LLC
Mr. Angel Ruiz	MediaKind, Inc.
Mr. Jeffrey Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
NSTAC Points of Contact	
Mr. Jason Boswell	Ericsson, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Ms. Cheryl Davis	Oracle Corp.
Ms. Kathryn Gronberg	NightDragon Security
Mr. Yoav Hebron	Cohere Technologies, Inc.
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Kevin Reifsteck	Microsoft Corp.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Dr. Claire Vishik	Intel Corp.
Mr. Milan Vlajnic	Communications Technologies, Inc.
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. Steve Kelly	National Security Council
Ms. Alexandra Martin	Cybersecurity and Infrastructure Security Agency

Ms. Elke Sobieraj	National Security Council
Ms. Kemba Walden	Office of the National Cybersecurity Director
Mr. Scott Zigler	Cybersecurity and Infrastructure Security Agency

Contractor Support

Mr. Santana King	TekSynap Corp.
Ms. Laura Penn	Edgesource Corp.
Ms. Shiri Telfer	Edgesource Corp.
Ms. Jennifer Topps	TekSynap Corp.
Mr. Joel Vaughn	TekSynap Corp.

Public and Media Participants

Mr. Mitchell Berger	Department of Health and Human Services
Mr. Howard Buskirk	Communications Daily
Mr. Christopher Boyer	AT&T, Inc.
Mr. Mark Coldiron	Department of Defense
Mr. Ben Deering	National Security Council
Mr. Nzinga Dyson	Louis-Burke Associates LLC
Ms. Sara Friedman	Inside Cybersecurity
Mr. Eric Geller	Politico
Ms. Sheryl Goldberg	Zeichner Risk Analytics
Mr. John Hewitt Jones	FedScoop
Mr. Albert Kammler	Van Scoyoc Associates
Ms. Alexandra Kelly	Nextgov
Mr. Kent Landfield	Trellix
Mr. Tom Leithauser	Telecommunications Reports
Mr. Mike Maier	Readiness Resource Group
Mr. Jacob Nash	Wilkinson Barker Knauer, LLP
Ms. Shannon O'Keefe	Motorola Solutions, Inc.
Mr. Sunjeet Randhawa	Broadcom, Inc.
Mr. Jake Seaboch	Department of Defense
Ms. Makenzie Shellnutt	NTCA-The Rural Broadband Association
Mr. Samuel Wish	Department of Defense

Certification

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

Mr. John Donovan
NSTAC Chair