President's National Security Telecommunications Advisory Committee (NSTAC) Member Meeting Open Session Summary
May 24, 2022

Call to Order and Opening Remarks

Ms. Christina Berger, Department of Homeland Security (DHS) 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. 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. John Donovan, Palo Alto Networks and NSTAC Chair.

Mr. Donovan welcomed the distinguished Government partners in attendance including Mr. Brandon Wales, Executive Director, Cybersecurity and Infrastructure Security Agency (CISA); Ms. Elke Sobieraj, Director for Critical Infrastructure Cybersecurity, National Security Council (NSC); Mr. Neal Higgins, Deputy National Cyber Director for National Cybersecurity, Office of the National Cyber Director (ONCD); and Mr. Mike Herrington, Section Chief, Cyber Division, Federal Bureau of Investigation (FBI).

In reviewing the agenda, Mr. Donovan noted that the meeting would include: (1) opening remarks from the administration and CISA on the Government's ongoing cybersecurity and national security and emergency preparedness efforts; (2) a keynote address from Mr. Herrington; (3) a deliberation and vote on the *NSTAC Letter to the President on Enhancing U.S. Leadership in International Communications Technology Standards* (Standards Letter) led by Mr. Raymond Dolan, Cohere Technologies and Standards Subcommittee Chair; and (4) an update on the NSTAC Information Technology and Operational Technology (IT/OT) Convergence Subcommittee provided by Mr. Jack Huffard, Tenable Holdings and IT/OT Convergence Subcommittee Chair.

Mr. Donovan then invited Mr. Wales to provide his opening remarks. Mr. Wales expressed his appreciation for the NSTAC's insights which have been instrumental in the national effort to enhance cybersecurity. He highlighted his appreciation for the committee's work on the 2022 *NSTAC Report to the President on Zero Trust and Trusted Identity Management* (ZT-IdM Report), underscoring that identity management has been at the center of almost every cyber incident. Mr. Wales also thanked the committee for its current efforts focused on IT/OT convergence as it directly addresses critical national security priorities across the Government to secure essential critical infrastructure targeted by malicious cyber actors and nation states (e.g., China).

Mr. Wales also referenced current CISA efforts that utilize insights and advice from the NSTAC, to include implementing Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*; and improving supply chain security. He also referenced recent efforts that CISA has undertaken to prepare the nation for potential retaliation from the Russian

government in response to the unprecedented sanctions and unity of effort western countries have enacted due to its unprovoked invasion of Ukraine. Mr. Wales said that these efforts exemplify how the government and industry can collaborate together to ensure they are partnering in a unified way to protect essential infrastructure. Mr. Wales closed by thanking the NSTAC for their efforts and continued partnership.

Mr. Donovan thanked Mr. Wales for his comments. He then invited Ms. Sobieraj to provide her remarks.

Ms. Sobieraj expressed her gratitude to the NSTAC for its continued work on the "Enhancing Internet Resilience (EIR) in 2021 and Beyond" study and noted how it has been implemented in phases in a timely way to meet the requirements of EO 14028 and the administration's priorities. Ms. Sobieraj continued that the ZT-IdM Report is on its way to the President. She added that the administration is considering how to build the report's recommendations into existing and future efforts as it works to transform the federal government's adoption of cybersecurity zero trust architecture.

Ms. Sobieraj closed her remarks by thanking Mr. Dolan and Mr. Huffard for their leadership on their respective subcommittees. Ms. Sobieraj underscored that it is imperative that government and industry collaborate to strengthen cybersecurity and national security.

Mr. Donovan thanked Ms. Sobieraj for her comments. He then invited Mr. Higgins to provide his remarks.

Mr. Higgins remarked that the NSTAC's ability to conduct timely studies and provide recommendations to the President reflects the committee's dedication to national security. He noted how the NSTAC's current EIR study provides insights on key issues that assist both government and industry.

Next, Mr. Higgins mentioned that ONCD was formally established in July 2021 with the swearing in of its Director, Mr. Christopher Inglis. He also noted that it was the one-year anniversary of EO 14028 and that the ONCD is overseeing its implementation.

Mr. Higgins stated the recent Russian invasion of Ukraine has resulted in an increased global cyber threat level, and both government and industry must stay vigilant and continue their work to fortify collective cyber defenses. He underscored that one significant area of focus for government is moving beyond information sharing to public-private collaboration. He then highlighted two initiatives: (1) CISA's Joint Cyber Defense Collaborative (JCDC); and (2) the National Security Agency's (NSA) Cybersecurity Collaboration Center. The JCDC has private sector partners working with CISA and Federal Government cybersecurity partner agencies to understand and respond to national cyber threats. The Cybersecurity Collaboration Center is a partnership between NSA and private industry to address foreign cyber threats to national security systems, the Department of Defense (DoD), and the defense industrial base.

Mr. Higgins explained that federal experts and technology companies must collaborate to create a safer and more stable digital ecosystem. He noted that Americans must do their part to create a safer ecosystem by using difficult passwords, multi-factor authentication (MFA), and other simple measures that can stop a significant percentage of malicious cyber activity.

Mr. Higgins continued that Director Inglis recently provided ways to improve cybersecurity in the future and reiterated them to participants. He noted that one way to create a more secure cyberspace is to expand the focus beyond operators and end users to those who build and deploy the hardware and software that comprise the internals of critical systems. Mr. Higgins added that as end users, all individuals need to take the simple steps to secure systems (e.g., personal devices, enterprise networks, etc.). Another way to enhance cybersecurity is for developers and companies with expertise and resources to build security into all of their products. Mr. Higgins continued that to help improve cybersecurity, the Government must: provide better intelligence that industry can utilize; develop MFA or implement zero trust architectures; and leverage authority to enhance cybersecurity broadly. He concluded that the private sector must meet baseline security requirements and participate in the national collective defense, providing more transparency into cyber incidents and the security of the supply chain. He closed his remarks by stating that he anticipates the NSTAC's input regarding future challenges and opportunities.

Mr. Donovan thanked Mr. Higgins for his remarks.

Keynote Address

Mr. Donovan invited Mr. Herrington to provide the keynote address.

Mr. Herrington noted that 2021 was a landmark year for cybersecurity due to the large volume of cyber-attacks. He stated that in the past few months the FBI has been warning private industry partners and the public about malicious cyber activity from Russia. Mr. Herrington referenced Russia's history of using poorly controlled damaging attacks that could spread beyond their intended targets. For example, in 2017 Russia used Petya malware that was presented as ransomware to infect Ukrainian software. Its purpose was to cause destruction with no capability for victims to pay a ransom or recover information. Mr. Herrington stated that although Russia's target was Ukraine, the malware spread globally causing billions of dollars in damage.

Mr. Herrington explained that Russian cyber actors are also known to gain unauthorized access to sensitive or secret information from victims and then publicly release it through proxies with no direct ties to the Russian government. These leaks are designed to cause confusion among the targeted audiences. He said that the FBI remains concerned that Russian cyber criminals will target U.S. critical infrastructure with ransomware attacks which is why it remains focused on the threat emanating from Russian intelligence services. The FBI is using all of its available tools to identify and disrupt cyber threats to Ukraine, U.S. allies, and U.S. networks.

Mr. Herrington said that since the beginning of 2022, the FBI has disseminated hundreds of intelligence reports to provide its partners with key cyber intelligence about Russian cyber threats. The FBI has shared operational reports with foreign partners, including Ukraine, and continues providing support through its cyber assistant legal attachés overseas.

Mr. Herrington stated the FBI provides threat overviews to its partners, and individualized threat warnings. For example, in April 2022 the FBI conducted a successful court authorized operation that removed malware known as Cyclops Blink from a botnet's command and control devices. This removed the Russian Federation's Main Intelligence Directorate's (GRU) control over thousands of infected devices worldwide. The GRU began building this malicious botnet in 2019 and implanted Cyclops Blink malware on thousands of devices from WatchGuard technologies. Over several weeks the FBI worked closely with Watchguard and analyzed the malware as the company developed detection tools and remediation techniques. Before the technical disruption, the FBI, CISA and the United Kingdom's National Security Cyber Centre released an advisory identifying Cyclops Blink malware as a replacement for the virtual private network filter malware which was exposed in 2018.

In May 2022, the FBI and CISA attributed cyber-attacks that occurred in February 2022 against Cycom networks to Russian state sponsored malicious cyber actors. In March 2022, the FBI and CISA provided warnings about threats to Cycom network providers and customers before issuing an update advisory in May 2022 to coincide with messaging regarding the U.S. Government's attribution of these attacks.

Mr. Herrington said that in March 2022 the Department of Justice unsealed indictments following two separate criminal investigations involving Russian government actors. In coordination on those indictments, the FBI and its domestic and international partners executed a whole-of-government effort revealing Russian computer network operations against the global sector, specially targeting the U.S., its western allies, and foreign countries with whom Russia had sought economic, military, or strategic alliances.

Mr. Herrington said that cyber adversaries have also obtained an increasing capacity for stealth in the recent years, facilitating more persistent comprehensive access to U.S. networks. He stated that unfortunately these rapidly changing technical threats will increasingly challenge the FBI. He said that over the next five years, disruptive virtual asset innovations and blockchain technology, decentralized finance, and central bank digital currencies will very likely create unprecedent financial conduit for illicit actor exploits. This will significantly limit U.S. law enforcement's ability to identify illicit actors, track funds, and compel the production of financial records. Mr. Herrington said the FBI will use existing laws to prosecute crimes.

Mr. Herrington noted that the top U.S. adversaries also include the cybercriminal actors who callously infect systems in hospitals, the energy sector, emergency services, and other critical infrastructure with ransomware. Thus, effectively holding the stability of society hostage in pursuit of financial gain. He explained that cybercriminals knowingly target these sectors

because the catastrophic impact or disruption often forces victims to pay increasingly outrageous sums to resume operations.

Mr. Herrington noted that many skilled foreign cyber criminals targeting the United States maintain mutually beneficial relationship with countries that offer safe haven or benefit from their activity. For example, in 2021 the Justice Department unsealed an indictment against actors who worked on behalf of North Korea's premier intelligence agency, the Reconnaissance General Bureau, and served as a revenue generator for the Democratic People's Republic of Korea. These entities collaborated with the cyber criminals to funnel hundreds of millions of dollars of illicit profits to the North Korean regime.

Mr. Herrington then provided an overview of the United States' top nation-state adversaries. He said that China and Russia pose particularly capable and sophisticated espionage and cyber-attack threats. China, Iran and North Korea all continue to carry out sophisticated intrusions targeting U.S. victims. He said that China cyber actors continue to aggressively conduct cyber operations to gather foreign intelligence; policy information; and sensitive business, commercial, and proprietary information from U.S. officials.

Mr. Herrington stated that in 2020, the FBI became aware that certain U.S. companies who have operations in China were being targeted through Chinese government mandated tax software. The businesses had to use certain government sanctioned software to comply with the value added tax system and other Chinese laws.

Mr. Herrington explained that Russia will continue to remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Russia continues to target critical infrastructure in the United States and allied and partner countries. He said that SolarWinds is a recent reminder that Russia is not afraid to conduct massive hacks to obtain its goals.

Mr. Herrington stated that Iran is increasing its expertise and willingness to conduct aggressive cyber operations, which makes it a significant threat to the security of U.S. and allied networks and data. Iranian cyber actors conducted multiple operations surrounding the 2020 U.S. presidential election, including sending threatening emails to intimidate U.S. voters and targeting voter registration data in U.S. state election sites. In 2021, the FBI, Department of Justice, Department of State, and Department of the Treasury Office of Foreign Assets Control announced a series of coordinated U.S. actions in identifying Iranian cyber actors who participated in operations targeting this election.

Mr. Herrington stated that North Korea's cyber program has become an increasing espionage, theft, and attack threat, noting that its cyber capabilities have increased in recent years. North Korea has conducted espionage operations against a range of organizations including media, academia, defense companies, and governments in multiple countries. He noted that North Korea poses a cyber threat to financial institutions as well, explaining that cyber actors have conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars. They have done this using malware,

ransomware, and e-skimming to target Automated Teller Machines, cryptocurrency exchanges, financial services companies, and online gambling and e-commerce payment platforms. Mr. Herrington said that North Korean cyber actors used this malware to steal $6 million worth of cryptocurrency from a U.S. financial services company in August of 2020.

Mr. Herrington said that the FBI seized $6.1 million in ransomware profits from an account in cryptocurrency exchange that held proceeds from several cyber-attacks against U.S. victims using REvil ransomware. In February 2022, the FBI seized RaidForums, a prolific site marketing cybercriminal services and trafficking in stolen information. Mr. Herrington stated that the seizure came two weeks after the United Kingdom arrested the forum's operator. Also in February 2022, the FBI made the largest financial seizure in the Justice Department's history recovering more than $3.6 million in bitcoin that was stolen in 2016.

Mr. Herrington underscored that the FBI is building strong relationships with its private sector partners that are based on trust and that today's cyber threats and attacks have become increasingly larger and demand concerted and sustained efforts from everyone.

Mr. Herrington concluded that not every cyber-attack can be stopped, but through government and industry partnerships risks and threats can be minimized. The FBI wants all corporations to think about viewing the bureau as an indispensable ally in working towards collective security.

Mr. Donovan thanked Mr. Herrington for his address.

Deliberation and Vote: *NSTAC Letter to the President on Enhancing U.S. Leadership in International Communications Technology Standards*

Mr. Donovan invited Mr. Dolan to discuss the key findings and recommendations of the NSTAC Standards Letter.

Mr. Dolan said that during the November 2021 NSTAC Meeting, participants had a robust discussion focused on standards due to the increase in the frequency of cyber-attacks and geopolitical and economic competition. Concerns with security resiliency, interoperability, and other critical communications technology issues have caused governments, industry, and users to focus more intently on recognizing the role that standards play to help address these concerns.

Mr. Dolan stated that one primary concern the committee had was the continued actions of some governments and organizations to significantly increase participation in standards bodies to promote technical approaches or government philosophies that are counter to U.S. values. In January of 2022, the NSTAC was tasked with developing a letter to the President outlining its recommendations on how government and industry can work together to preserve the widespread use of the industry driven standards development model, and at the same time enhance U.S. competitiveness through effective participation in global standards bodies.

Mr. Dolan explained that the NSTAC's primary objectives were to obtain an understanding of the concerns around standards bodies and the extent to which the bodies have been impacted by efforts to influence the standards process to achieve national objectives. He said that the Standards Letter's key findings and recommendations were derived from briefings provided by government, private sector, academia, and standards development organizations.

Mr. Dolan then reviewed the letter's key findings, noting that industry-led standards play a vital role in ensuring U.S. technology leadership. He explained that open markets enable U.S. technology to promulgate around the world and that past U.S. policy has specifically encouraged the adoption of global standards to ensure access to markets and the necessary scale to drive more vibrant information communications technology supply chain.

Mr. Dolan continued to the next key finding, which is that technology shapes international standards. He explained that for the United States to lead in standards, it must increase investments in emerging and foundational technologies and bring those technologies to standards bodies to promote standardization.

The next key finding Mr. Dolan discussed is that there is no evidence of security vulnerabilities being inserted into products through the standards process. He explained that standards by their nature are open and transparent, which inherently minimizes this risk, although security issues may arise when products include functionality above and beyond the standards.

Mr. Dolan said that the next key finding is that there is not a one size fits all approach to standards. He explained that as there are thousands of standards development organizations, one cannot assume that experience in one entity is indicative of all.

Mr. Dolan concluded by referencing the final key finding, which is that standards bodies include rules promoting balance to ensure that no one region or country dominates the development of standards. He underscored that there remains a need to make strategic investments to bolster participation in standards.

Next, Mr. Dolan explained that the letter offers several recommendations for the Government to implement which are organized in order of priority based on ability to be implemented immediately versus those that are ongoing and longer term.

He stated that the Government should revise export control rules to encourage standards participation. There have been a series of revisions made to the U.S. Export Administration Regulations (EAR) over the past three years that have created uncertainty around companies' participation in standards bodies. He noted that while the Bureau of Industry and Security made attempts to clarify the EAR, in particular revised guidance issued in 2020, there remains concerns and the administration could provide further clarity on this issue to confirm that standards development activities are acceptable under the EAR.

Mr. Dolan said that the government should make structural changes in areas such as visas to establish the United States as a venue of choice for hosting standards meetings. He explained that one way to increase U.S. participation in standards is to host more standards meetings in the United States as this reduces costs to companies and helps bring more robust participation. However, for the U.S. to host more meetings, it must remove obstacles to the entry of foreign participants.

Next, Mr. Dolan said that the government should make investments in emerging and developing technologies which serve as the underlying foundation for U.S. leadership in standards development. Fundamental investment in foundational and emerging technologies is critical to U.S. leadership and standards.

Mr. Dolan continued that the government should ensure the continued independence of industry-led standards development bodies, noting that the majority of ICT standards are developed by industry-led standards organizations. The U.S. should look for opportunities to sustain and enhance that model, which has served its interest well for years.

Mr. Dolan said the United States should look to reform the International Telecommunication Union (ITU), which is the predominant government-led standards organization. The United States should continue to promote its own or allied leadership at the ITU and collaborate with the ITU in attempts to reform the ITU to be a more effective venue. Mr. Dolan continued that a key aspect of reform is to establish more liaison relationships between the ITU and several industry-led standards organizations to prevent the duplication of efforts or more favorable outcomes for certain entities.

Mr. Dolan concluded the key recommendations by stating that the U.S. government should work with industry to develop programs to encourage a more standards savvy U.S. workforce. The U.S. government should also collaborate with industry to ensure robust U.S. standards participation by leveraging the U.S. government's convening capabilities and, through incentives, bolster participation in standards development processes.

Mr. Donovan thanked Mr. Dolan for the update and asked participants for feedback. Mr. Mark McLaughlin, Qualcomm, asked if a large number of representatives from one country can sway outcomes in standards bodies. Mr. Dolan replied that although there are some standards bodies that are one person, one vote, there are many standards bodies that vote by organization.

Mr. Perter Altabef, Unisys, thanked Mr. Dolan and the subcommittee for their efforts.
Mr. Donovan asked if the size and maturity of an organization affects its ability to contribute to standards bodies. Mr. Dolan replied that in his personal experience he has not seen size or maturity affect an organization's ability to participate, but that he would review this further.

Hearing no other comments, Mr. Donovan made a motion to approve the Standards Letter. Following this motion, NSTAC members unanimously approved the letter for transmission to the President.

Status Update: NSTAC Information Technology and Operational Technology Convergence Subcommittee

Mr. Donovan invited Mr. Huffard to provide the update on the NSTAC IT/OT Convergence Subcommittee's progress to date.

Mr. Huffard stated that the subcommittee kicked off in February 2022 and that shortly thereafter Russia launched its invasion of Ukraine, fundamentally changing the security environment in both the physical and cyber realms and significantly raising the importance and relevance of the EIR study. He said that U.S. critical infrastructure is facing a pointedly heightened threat landscape and the importance of securing IT/OT systems, including those in converged environments, has become even more of an imperative. For example, in April 2022 CISA released NSA's *Stop Malicious Cyber Activity Against Connected Operational Technology* guidance to help IT/OT converged organizations prepare for potential threats.

Mr. Huffard explained that phase III of the EIR study will culminate in a report to examine the key challenges of securing OT systems against threats that emerge from IT network connections and to identify emerging approaches to increase OT resiliency to these threats. He noted that briefings to the subcommittee were organized into three phases: (1) government related entities (e.g., NSC, CISA, Department of Defense); (2) asset owners/operators of IT/OT entities as well as original equipment manufacturers (OEM); and (3) vendors/suppliers/integrators that provide cybersecurity products and services for IT/OT convergence. Mr. Huffard explained that the subcommittee is currently transitioning to phase III briefings.

Mr. Huffard then remarked that the subcommittee has noted a number of consistent themes emerging from the briefings, to include:

- The challenge of securing connected legacy OT equipment;
- The importance of breaking down silos that exist between personnel in the IT and OT teams within organizations;
- The need for manufacturers to "build in" rather than "bolt on" security;
- The benefits of incentivizing cybersecurity in public and private sector procurement;
- The benefits of flexible, outcomes-oriented government policy and regulations; and
- The need for stronger cybersecurity education and training for the critical infrastructure workforce.

Mr. Huffard stated that as the subcommittee drafts the report, it will provide OT specific issues and a description of the challenges encountered by a range of stakeholders, including federal,

state, and local government entities; regulated and unregulated industry sectors; and OEMs and OT cybersecurity vendors. It will also highlight existing best practices and frameworks that address IT/OT convergence challenges. Finally, it will work to develop recommendations for the respective stakeholder groups and recommendations that are applicable across the entire cybersecurity ecosystem. Mr. Huffard concluded the IT/OT update by expressing his appreciation for the subcommittee's efforts.

Mr. Donovan thanked Mr. Huffard for the update.

Closing Remarks and Adjournment

Mr. Donovan thanked: participants for attending; government partners for their insights; Mr. Dolan and Mr. Huffard for their leadership of their respective subcommittees; and the subcommittee working leads.

Mr. Donovan asked Mr. Wales to provide his closing remarks.

Mr. Wales thanked Mr. Herrington for his briefing and the NSTAC for its current IT/OT convergence efforts. He stated that he looks forward to the transmittal of the Standards Letter to the President so the Government can begin to develop policies to leverage the NSTAC's recommendations for further progress. He emphasized the importance of long-term change in the approach to international standards bodies and the impact on the dynamic nature of the U.S. industry challenges.

Mr. Donovan thanked Mr. Wales for his comments. He then invited Ms. Sobieraj to provide her closing remarks.

Ms. Sobieraj thanked the NSTAC for its insights and underscored how partnerships like this allow for the government to keep ahead of the evolving threat landscape.

Mr. Donovan thanked Ms. Sobieraj for her comments and invited Mr. Higgins to provide his closing remarks.

Mr. Higgins thanked the members of the committee and noted the President anticipates receiving the Standards Letter. He also thanked the IT/OT convergence for their continuous efforts.

Mr. Donovan thanked Mr. Higgins for his comments.

Mr. Donovan made a motion to close the meeting. Upon receiving a second, Mr. Donovan officially adjourned the meeting.

APPENDIX
May 24, 2022, NSTAC Meeting 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.
Ms. Lisa Hook	Two Island Partners, LLC
Mr. Jack Huffard	Tenable Holdings, Inc.
Ms. Renée James	Ampere Computing, LLC
Mr. Mark McLaughlin	Qualcomm
Mr. Angel Ruiz	MediaKind, Inc.
Mr. Jeffrey Storey	Lumen Technologies, Inc.
Mr. Hock Tan	Broadcom, Inc.
NSTAC Points of Contact	
Mr. Christopher Anderson	Lumen Technologies, Inc.
Mr. Jason Boswell	Ericsson, Inc.
Mr. Christopher Boyer	AT&T, Inc.
Mr. Jamie Brown	Tenable Holdings, Inc.
Mr. John Campbell	Iridium Communications, Inc.
Ms. Kathryn Condello	Lumen Technologies, Inc.
Ms. Cheryl Davis	Oracle Corp.
Mr. Ryan Gillis	Palo Alto Networks, Inc.
Ms. Kathryn Gronberg	NightDragon Security, LLC
Ms. Ilana Johnson	Neustar, Inc.
Mr. Kent Landfield	Trellix
Mr. Sean Morgan	Palo Alto Networks, Inc.
Mr. Thomas Patterson	Unisys Corp.
Mr. Tom Quillen	Intel Corp.
Ms. Jordana Siegel	Amazon Web Services, Inc.
Mr. Robert Spiger	Microsoft Corp.
Dr. Claire Vishik	Intel Corp.
Mr. Milan Vlajnic	Communications Technologies, Inc.
Government Participants	
Ms. Christina Berger	Department of Homeland Security
Ms. Alaina Clark	Department of Homeland Security

Ms. DeShelle Cleghorn	Department of Homeland Security
Ms. Elizabeth Gauthier	Department of Homeland Security
Mr. Mike Herrington	Federal Bureau of Investigation
Mr. Neil Higgins	Office of the National Cyber Director
Ms. Helen Jackson	Department of Homeland Security
Mr. Brian Scott	Office of the National Cyber Director
Mr. Barry Skidmore	Department of Homeland Security
Ms. Elke Sobieraj	National Security Council
Mr. Brandon Wales	Department of Homeland Security
Mr. Scott Zigler	Department of Homeland Security

Contractor Support

Ms. Bianca Berrios	Teksynap Corp.
Mr. Santana King	Teksynap Corp.
Ms. Laura Penn	Edgesource Corp.
Ms. Shiri Telfer	Edgesource Corp.
Mr. Brian Weingast	Edgesource Corp.

Public and Media Participants

Ms. Catherine Abramson	Department of Homeland Security
Mr. George Bamford	Department of Homeland Security
Ms. Manali Basu	Federal Bureau of Investigation
Mr. Calvin Biesecker	Defense Daily
Mr. Billy Bob Brown, Jr.	Department of Homeland Security
Mr. Bruce Byrd	Palo Alto Networks, Inc.
Mr. Andrew Clos	Department of Homeland Security
Mr. Matthew Eggers	U.S. Chamber of Commerce
Mr. Chris Frascella	EPIC
Ms. Ashley Freitas	Department of Homeland Security
Ms. Sara Friedman	Inside Cybersecurity
Mr. Joseph Fryday	Sagen
Ms. Dierdre Gallop-Anderson	Department of Homeland Security
Mr. Eric Geller	Politico
Mr. Albert Kammler	Van Scoyoc Associates, Inc.
Ms. Norma Krayem	Van Scoyoc Associates, Inc.
Mr. Tom Leithauser	Telecommunication Reports
Ms. Katherine Moore	Department of Homeland Security
Mr. Jake Nash	Wilson/Barker/Knauer LLP
Mr. Randall Palmer	Government of Canada
Mr. William Ryan	Department of Homeland Security
Ms. Katherine Siefert	Department of Homeland Security
Ms. Kendall Smith	Federal Bureau of Investigation
Mr. Keelan Sweeney	Department of Homeland Security
Mr. Will Williams	Department of Homeland Security

Certification

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

Mr. John Donovan
NSTAC Chair