NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

QUARTERLY BUSINESS MEETING AGENDA

June 13, 2019
12:15 PM – 3:00 PM
Microsoft Studio H/1022-Chinook Facility
3850 148th Avenue NE, Redmond, WA 98052

I. OPENING OF MEETING — *Ginger Norris,* Designated Federal Officer (DFO), President's National Infrastructure Advisory Council (NIAC), Department of Homeland Security (DHS)

Ms. Ginger Norris, Cybersecurity and Infrastructure Security (CISA), Department of Homeland Security (DHS) and Designated Federal Officer (DFO) for the President's National Infrastructure Advisory Council (NIAC), called the meeting to order and welcomed participants.

II. ROLL CALL OF MEMBERS — *Ginger Norris,* DFO, NIAC, DHS

Ms. Norris then called roll of all present at the meeting. She stated that the NIAC was established under Section 10 of Executive Order (EO) 13231, *Critical Infrastructure Protection in the Information Age,* and the President's National Security Telecommunications Advisory Committee (NSTAC) was established by EO 12382, *President's National Security Telecommunications Advisory Committee*. Both advisory councils were most recently renewed by EO 13811, *Continuance of Certain Federal Advisory Committees*. Ms. Norris stated that it was important to note that while both the committee and council are meeting here together, they are doing so under the authority of their individual EO as outlined above. Ms. Norris stated that both the NIAC and NSTAC have a mandate to provide the President; the Secretary of Homeland Security; and other relevant agencies with advice on security of critical infrastructure and communications systems supporting the public and private sectors. During their combined history of 55 years, the two advisory bodies have collectively provided countless, publically available, in depth studies, resulting in hundreds of recommendations to the President that have helped identify and reduce complex risks for cyber and physical systems that operate critical processes. Ms. Norris then gave a few instructions for the public comment period and informed that, at that time, no written public comments. Ms. Norris then introduced Ms. Renée James, NSTAC Chair, to provide opening remarks.

NIAC MEMBERS PRESENT IN PERSON:
Ms. Constance Lau, Dr. Beverly Scott, Mr. Robert Carr, Mr. J. Richard Baich, and Mr. Georges Benjamin.

NSTAC MEMBERS PRESENT IN PERSON:
Mr. Peter Altabef, Mr. David DeWalt, Mr. Raymond Dolan, Dr. Joseph Fergus, Ms. Lisa Hook, Ms. Renée James, Dr. Kevin Kennedy, Mr. Stephen Schmidt, Ms. Kay Sears, and Mr. Christopher Young.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Ms. Jan Allman, Mr. Rand Beers, General Albert Edmonds, Mr. William Fehrman, Ms. Margaret Grayson, Mr. George Hawkins, Ms. Joan McDonald, Mr. James J. Murren, Mr. Carl Newman, Mr. Keith T. Parker, and Mr. James Reid.

NSTC MEMBERS ATTENDING VIA CONFERENCE CALL:
Mr. Mark McLaughlin

NIAC MEMBERS ABSENT:
Chief Rhoda Kerr, Mr. William Terry Boston, Mr. Ben Fowke, Mr. Thomas Noonan, and Mr. Michael J. Wallace.

NSTAC MEMBERS ABSENT:
Mr. John Donovan, Mr. Scott Charney, Mr. William Brown, Mr. Robert Carrigan, Mr. Matthew Desch, Dr. Thomas Kennedy, Mr. Angel Ruiz, Mr. Gary Smith, and Mr. Jeffrey Storey.

SUBSTANTIVE POINTS OF CONTACT PRESENT:
Mr. Scott Seu with Ms. Constance Lau
Mr. Peter Grandgeorge with Mr. William Fehrman
Mr. Charles Durant with Mr. William Ferhman
Mr. Frank Prager with Mr. Benjamin Fowke
Mr. Robert Carr
Mr. Chris Boyer with Mr. John Donovan
Mr. John Campbell with Mr. Matthew Desch
Ms. Katherine Condello with Mr. Jeffrey Storey
Ms. Amanda Craig-Deckard with Mr. Scott Charney
Mr. Thomas Gann with Mr. Christopher Young
Ms. Katherine Gronberg with Mr. David DeWalt
Mr. Kent Landfield with Mr. Christopher Young
Mr. Sean Morgan with Mr. Mark McLaughlin
Mr. Tom Patterson with Mr. Peter Altabef
Ms. Jordana Siegel with Mr. Stephen Schmidt
Ms. Lynn Star with Mr. Angel Ruiz
Mr. Kent Varney with Ms. Kay Sears

SUBSTANTIVE POINTS OF CONTACT OBSERVING VIA CONFERENCE CALL:
Mr. Theodore Basta with Dr. Beverly Scott
Ms. Ilana Johnson with Ms. Lisa Hook
Mr. Nathaniel Millsap with Ms. Jan Allman

OTHER DIGNITARIES PRESENT:
Ms. Miriam Baksh, Inside Cybersecurity; Ms. Sandy Benevides, Department of Homeland Security (DHS); Mr. Michael Boyle, Westin Building Exchange; Dr. Thomas Donohue, Formerly of NSC; Ms. Ashley Dutta, National Bureau of Asian Research; Ms. Emily Early, DHS; Mr. Steven Harris, DHS; Mr. Dean Hullings, ForeScout Technologies, Inc.; Dr. Galen Hunt, Microsoft Corporation; Ms. Helen Jackson, DHS; Mr. Christopher Krebs, DHS, Cybersecurity and Infrastructure Security Agency (CISA); Mr. Daniel Kroese, DHS; Ms. Kayla Lord, DHS; Mr. Patrick Massey, DHS; Ms. Valerie Mongello, DHS; Ms. Mary Beth Muong, NCSC; Mr. Christopher Nissen, MITRE Corporation; Ginger Norris, DHS; Mr. Harvey Rishkof, iCloud; Ms. Jodie Ryan, Verizon Media; Ms. Anita Patanker-Stoll, National Security Council (NSC); Mr. Grant Schneider, NSC; Mr. William Schrier, Department of Commerce (DOC); Ms. Constance Taube, National Counterintelligence and Security Center (NCSC); Ms. Traci Silas, DHS; Ms. Eleanor Watson, CBS News; and Mr. Bradford Willke, DHS.

III. OPENING REMARKS AND INTRODUCTIONS

Constance H. Lau, NIAC Chair

Renée James, NSTAC Chair

Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency (CISA) (Invited)

Grant Schneider, Senior Director, National Security Council (NSC)

Ms. James introduced herself and Ms. Connie Lau, NIAC Chair. Ms. James thanked the participants for attending, noting this was the first joint meeting between the NIAC and NSTAC. Ms. James also recognized the government stakeholders attending the meeting, including: Mr. Grant Schneider, Senior Director for Cybersecurity Policy, National Security Council (NSC); Mr. Christopher Krebs, Director, CISA; Mr. Bradford Willke, CISA; and Ms. Constance Taube, Deputy Director, National Counterintelligence and Security Center. Ms. James then asked Ms. Lau, Mr. Schneider, and Director Krebs if they would like to provide any opening remarks.

Ms. Lau thanked the participants for attending the meeting and stated that the NIAC was pleased to participate in the first joint meeting between the two advisory councils. She stated that while the councils have different focus areas and different types of membership, the

NIAC is very encouraged by the two councils being able to exchange ideas and see the possibility of great collaboration and coordination between the two councils going forward. The presentations and discussion will be very enlightening for everyone and will allow both the NIAC and NSTAC to see the different perspectives on the issues they study.

Mr. Schneider expressed his excitement to do this joint meeting and how this meeting would allow information to be shared across NIAC and NSTAC. He believes that as technology continues to evolve and as there is a convergence on information technology (IT) and operational technology (OT) systems and capabilities, these two groups will have a lot of shared risks, vulnerabilities, and interdependencies. He then provided an update on the Administration's efforts to operationalize the *National Cyber Strategy of the United States,* including efforts to implement NIAC and NSTAC recommendations. He also summarized the recent EOs that the President has signed, including: EO 13865, *Coordinating National Resilience to Electromagnetic Pulses;* EO 13859, *Maintaining American Leadership in Artificial Intelligence;* EO 13870, *America's Cybersecurity Workforce*; and EO 13873, *Securing the Information and Communications Technology and Services Supply Chain*.

Director Krebs stated that the Joint NIAC NSTAC Meeting was a priority of his and that it was critical for both groups to meet and exchange ideas on issues that impact both groups in order for them to provide proper strategic guidance to the Administration. He added that the recommendations made by the NIAC and NSTAC contributed greatly to the development of EO 13865, *Coordinating National Resilience to Electromagnetic Pulses*. They are looking to integrate the recommendations and advice from these key groups into administrative action and policy. They are also finding that the recommendations from the groups are manifesting in legislative action as well. Director Krebs highlighted the importance of awareness, security, partnerships between groups like the NIAC and NSTAC. He closed his remarks by thanking Microsoft for hosting the meeting, and welcoming the members of both advisory councils.

IV. DISCUSSION: ADVANCING RESILIENCY AND FOSTERING INNOVATION IN THE ICT ECOSYSTEM

David DeWalt, NSTAC Member and Subcommittee Chair

Ms. James introduced Mr. David DeWalt, NSTAC Member and Advancing Resiliency and Fostering Innovation in the Information and Communications Technology (ICT) Ecosystem Subcommittee Chair. Mr. DeWalt thanked everyone attend the joint QBM for their support of the subcommittee, the NSTAC members for their support, and Ms. Katherine Gronberg, NSTAC Point of Contact, and Mr. Dean Hullings, Advancing Resiliency and Fostering Innovation in the ICT Ecosystem Working Group Co-Leads for their leadership of the subcommittee. Mr. DeWalt stated that the purpose of his discussion was to create a dialogue between the NIAC and NSTAC on the *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem* and solicit as much input as he can get from NIAC and NSTAC on the report that they will be presenting in August. He noted that the challenge that was asked of the subcommittee was really two-part: (1) advancing resiliency

in the ICT Ecosystem and (2) fostering innovation in this ICT ecosystem, which is equally if not more important. There has been a tremendous amount of technology innovation occurring in our ICT ecosystem, but these innovations has brought a lot of potential vulnerabilities to the ICT ecosystem with it. These vulnerabilities are increased even more by a foreign dependence on critical pieces of that ICT ecosystem on potentially adversarial nations, which creates higher risks and possibility of exploitation. He noted that the study began in September 2018, and the subcommittee had received over 30 briefings by subject matter experts from both the public and private sector. Mr. DeWalt added that the NSTAC voted to approve the *NSTAC Letter to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem* in April 2019.

Mr. DeWalt stated that the ICT ecosystem subcommittee felt three items were critical to the study: (1) determining what technologies are most important to the ICT ecosystem; (2) how to determine trustworthiness of these technologies; and (3) how to encourage diversifying vendors. He also said that it is important to discuss how to encourage innovation around national security and emergency preparedness (NS/EP) capabilities that interlocks the public and private sector.

Mr. DeWalt stated that the *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem* focuses what technologies matter most, which lead the subcommittee to look into the 5G infrastructure, and he asked members of the NIAC and NSTAC what other technologies the ICT ecosystem report should address. Mr. Robert Carr, NIAC Member, noted that the NIAC's report on *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation* considered utilizing ham radios for communication when all other technologies fail. He also said the weaponization of the Internet of Things (IoT), for example the sewage plants, and thinking about all of the possible things being connected to the internet now and the enemies trying to do harm with those things. In addition to this, expanding the minimum security standards implemented by credit card companies might be worth discussing in the ICT ecosystem report. Ms. Kay Sears, NSTAC Member, mentioned that the ICT ecosystem subcommittee should consider the resiliency efforts undertaken by the Department of Defense (DOD). She said that a layered architecture, where multiple platforms can perform the same task, increases the survivability and resiliency of military systems, so if there is a failure in one platform, it does not bring down the entire system. Mr. Stephen Schmidt, NSTAC Member, suggested that the NSTAC subcommittee analyze back up communication technologies as recovering from a power outages and other systemic failures are dependent on the telephone system. He stated that we need to go back to something that was followed in the 50s and 60s and establish a very distinct, defined secondary communication path for critical components of government communication, and we need to shift to a realization that government communication, while important, it not the key. We need to figure out how to make sure we have the lights on.

Mr. DeWalt stated that industry needs to implement certifications and standards for devices entering networks. He stated that we need a better environment to trust the devices coming in and discuss what kinds of ways we can create a mechanism for this. For example, he

commented on how people used to know a device was trustworthy based on the company who made it and that company's certifications. He asked what certifications, standards, and mechanisms could we deploy to ensure that the devices coming into the ICT ecosystem can be trusted. There should be a way to create fast and sufficient models for this. Being able to note which companies are creating devices that are trusted is vital. Ms. Lau said that it is critical to determine what companies and components can be trusted, especially for critical infrastructure. These types of certifications are even more valuable for small and medium players who might be equally critical to nation's defense. Dr. Thomas Donahue, formerly NSC, said that there are already existing certification processes and compliance models for operational environments. However, not many are striving for the highest certification level, and there is actually only one product that has ever met the highest certification level, and also there is the issue of member taking people who are using uncertified products with them, causing a huge implementation problem. There is a compliance problem as well, where a person only thinks of compliance and does not understand the risk that are happening in an operation environment. Mr. Christopher Young, NSTAC Member, said that industry needs a consistent model for trust, and it is important to consistently assert machine identity and test the trust model. Mr. J. Richard Baich, NIAC Member, stated that industry and Government need to establish baseline security standards before Government tries to set policy. Acceptable practices must be set and a definition on what is good enough needs to be established before policies and standards can be put forward.

Mr. DeWalt said that Government should review the vulnerabilities of devices critical to the ICT ecosystem, creating a risk rating on a couple of levels that will give some guidance on the potential risks. Director Krebs stated that security is a positive differentiator on the consumer side. He noted that the United Kingdom has an IoT code of practice and said it is important to analyze how the United States can adopt this practice. He suggested bringing in some members from the National Economic Council (NEC) and other, more economic sided administrators to participate in this conversation at the next NSTAC meeting. He added that increasing vendor diversity has been discussed as well as developing and supporting champions and asked the participants to consider what needs to be done to achieve this goal and boost allies in this. Ms. Beverly Scott stated that along with trust and standards, another important partner to have is organized labor. In her sector, 80% of North America are represented by Unions with people like-minded, and they participate in apprenticeship programs and training programs, which are joint activities. When intuitional knowledge transfers, certifications, etc. are discussed, the organized labor workers for are a critical of this for many of the sectors.

Mr. DeWalt stated that the ICT ecosystem subcommittee is investigating how the private and public sector can align their priorities to improve innovation. He added that improving education is needed in order to develop technology faster to lessen the dependency on foreign nations. Mr. DeWalt asked what the government can do to incentivize companies to help improve ICT education. Ms. Lau mentioned that the Hawaii Department of Education has been experimenting with work-based education, and particularly in the cyber area where everything cannot be learned in school, these programs are creating the awareness, giving

students the opportunity to enter the workplace and see these areas in action, and providing them with internships. She noted that, when the students graduate, they have some of the skillsets that can be used in the cyber workforce. Ms. Lau said that retired military personnel from the intelligence community could be employed in the private sector as they possess valuable cyber skills and experience. Mr. Baich shared the option of creating an online consumer level certification that gives people something. Mr. Baich said that certifications can be an easy baseline for developing a culture of security. He also noted that in Charlotte, North Carolina, the Federal Bureau of Investigation has partnered with Microsoft to create a cybersecurity camp for children. With all of the different efforts out there, it would be interesting to inventory and figure out what are the best recommendations. Mr. Baich stated that it is important to make people aware of the Government cybersecurity educational opportunities and scholarships that are currently available. It is also very important to get the word out to individuals about the opportunities that are there for them. Ms. James states that access to capital is very important for innovation, especially in ICT. There is some intersection between technologies that are critical to our infrastructure and the sanctity of RND efforts in some of these areas. She commented that this in combination with how we think about an economic program that fosters innovations specific to those critical functions would be very interesting on the innovation side. She also stated that if we want more resiliency, then there needs to be more diversity of vendors, which means that we need a mechanism to ensure that people able to invest. She stated that we need to think about the economic part of it relative to our resiliency. She wanted to highlight what Direct Krebs had previously stated about identity. She stated that in a world where there is so much that could happen she thinks that the "no good" is quite important and we should look at it for a construct for how we go forward. Direct Krebs stated that we have to look at what the coalition of the aligned interest looks like and how we drive these. He went on to say that we need to know how to drive those coalitions when we know that there are players in the market and produce competition with them. Ms. James states that we need to think of innovation and critical functions as technology and human resource.

Mr. DeWalt stated the aligning of industry and Government efforts is a great idea. He noted that the ICT ecosystem subcommittee will review a draft of the *NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem* the week of June 18, 2019, and thanked the NIAC and NSTAC for their input.

V. KEYNOTE SPEAKER — *Dr. Galen Hunt,* Microsoft Corporation

Ms. James introduced Dr. Galen Hunt, Microsoft, who spoke about making IoT safe in today's interconnected society. Dr. Hunt discussed the Microsoft Xbox, noting that the product's chip-laden composition was both exciting and terrifying because it has a programmable microcontroller (MCU),or a single chip computer, and a radio on the same chip for a price target that is about two dollars. Although this resulting connectivity affords many benefits, it also presents malicious actors with opportunities to hack everyday products. Dr. Hunt

underscored that virtually any device with a MCU can connect to the internet and be an IoT device. With the prevalence of MCU-enabled devices in society, Dr. Hunt stated that securing IoT devices is critical.

Dr. Hunt described the Mirai botnet attack, where hackers accessed over 100,000 IoT devices by exploiting weak, fixed passwords given to the devices and initiated a distributed denial of service attack that disabled the internet across the entire East Coast of the United States. Dr. Hunt noted that, should a similar attack occur in the future, the Internet may be permanently damaged. He stated that industry must find a way to build devices affordably with enough security to connect to the internet but not present opportunities to malicious actors.

Dr. Hunt stated there are seven properties a device needs in order to be considered highly secure. These properties include: (1) hardware security that protects its identity and software integrity; (2) multiple layers of defense against cyber-attacks; (3) restricted access to its security features; (4) the ability to be updated after it is deployed; (5) using certificates instead of passwords for trusted user authentication; (6) it can report failures and anomalies to the manufacturer; and (7) its software can be updated automatically.

Central to these seven properties is that hardware and software must work together to provide device security. Dr. Hunt stated that fixing bugs quickly and automatically is critical to maintaining security. He noted that hackers often exploit bugs in devices that have not been regularly updated. In order to ensure that all of the devices are up-to-date, it requires three things: (1) a cloud where those updates can be stored and communicated to the device, (2) a software that can take this update and robustly and reliable apply it to the device, and (3) a hardware capability called *Roll-back Protection*, which prevents hackers from being able to trick the device into rolling back from the updated version of software to a past, vulnerable version.

However, he stated that meeting the seven properties is very expensive and very difficult, and one of the reasons for this is because it requires three classes of expertise that normally do not reside in the same enterprise. These three classes of expertise are engineers, security, and logistics and operations. Not many organizations have all three of these skillsets to the level required to address nation-state hackers or financially motivated hackers.

Mr. DeWalt said that home routers are one of the greatest IoT vulnerabilities and asked what Microsoft is doing to secure these devices. Dr. Hunt noted that securing end devices that connect to a network is a critical element in securing home routers, but added that router security features must be based on the environment in which they operate. He noted that establishing trust between devices is critical to operating in an environment in which organizations must assume the network is hostile. Mr. Baich asked if quantum computing poses a threat to device security. Dr. Hunt said that quantum poses a real threat to security and that it is important for organizations to develop strong cryptography for their devices and systems before quantum computing becomes a reality.

Ms. Sears asked if consumers or manufacturers should be responsible for device security. Dr. Hunt said that there were differing perspectives on the issue of responsibility across the world. In Europe, the attitude has been to build security into every device. In the United States, consumers are generally aware that they need to secure their devices, but are not sure how. In Asia, and China in particular, the primary focus is on price and that many consider security the Government's responsibility. The last question asked to Dr. Hunt was how he thought about the heterogeneity in this device ecosystem, as this can be one of the enemies of the model. Dr. Hunt responded that heterogeneity is necessary for innovation. From a security the standpoint, the 7 properties can be used by any company and are a minimum bar of security for device connectivity. However, there is still a need for heterogeneity in the ecosystem that Microsoft is building. They have created heterogeneity in three places: (1) IP Block can be licensed to any silicone partner, (2) uses a lynx operating system because it is open source, and (3) the cloud.

In closing, Dr. Hunt reiterated that the only way to ensure that connected devices can be trusted is for them to maintain a high level of security. Ms. James thanked Dr. Hunt for his remarks.

VI. PANEL DISCUSSION: THE ASYMMETRIC ERA AS A DRIVING NEED FOR A NEW SECURITY AND ECONOMIC STRATEGY

Mr. Bradford, Willke, Assistant Director (Acting) for Stakeholder Engagement Cybersecurity and Infrastructure Security Agency

Mr. Christopher Nissen, MITRE Corporation

Mr. David DeWalt, NSTAC Member

Ms. James introduced Mr. Bradford Willke to moderate the panel discussion on the Asymmetric Era as a driving need for a new security and economic strategy. Mr. Willke began by explaining that the intent of the panel discussion is to address asymmetric threats and the need for the United States to take a more proactive approach to defending U.S. infrastructure both at home and abroad. He then introduced the panelists, including Dr. Thomas Donahue, formerly of the National Security Council, and Mr. Christopher Nissen, MITRE Corporation.

Dr. Donahue stated that the day-to-day espionage efforts against U.S. companies by criminals and hacking groups do not pose a major threat. He said that the real threat to the United States is that nation-state adversaries are infiltrating the U.S. infrastructure as part of a broader effort to prepare the battlefield for the worst case scenario. He noted that U.S. national defense and emergency preparedness capabilities rely heavily on a global communications network and said that the Government must build resiliency into these systems as they will be attacked and eventually fail.

Mr. Nissen stated that MITRE began studying asymmetric warfare between global powers because it was clear that America's adversaries did not believe they could defeat the U.S. military through kinetic warfare and were now taking on an asymmetric warfare tactic, leading us into a new era of warfare. He noted that, during and after the Cold War, the United States had strategic nuclear deterrence and a centralized industrial base that was too dominant to be overcome by conventional means. After looking at past warfare failures with our adversaries, Mr. Nissen said that adversaries have decided the best approach to fighting a war with the United States is to attack it in a manner to which the U.S. military is not prepared to respond. The U.S. is still in a defensive state against this warfare, and it needs to get into an offensive position, and the U.S. needs to learn to fight asymmetrically.

Mr. Willke asked what type of organizational structure within the Government would be best suited to addressing supply chain security issues. Dr. Donahue stated that the Government needs a sustained, focused effort with urgent timelines to address the issue. The U.S. is not taking an intensive, focused approach and working towards a synchronized, single objective. Instead, it is doing things in little bits and piece and not as a whole. He said that agencies are not coordinating their efforts to address cybersecurity issues. He noted that the Government devoted four percent of its annual budget to the Apollo program, which had a specific goal, a specific purpose, and the support of the entire Government. By comparison, U.S. cybersecurity efforts are diffuse, unorganized, and are significantly underfunded. Dr. Donahue also noted that the Government must improve public-private partnerships so that information can be shared sooner and the Government and industry can actively coordinate and respond to cyberattacks as they are occurring.

Mr. Willke asked if the United States has lost the drive to innovate. Dr. Donahue stated that the United States is good at innovation, but that it lacks focus. He said the Government and industry know how to coordinate on innovation but that they are not using the tools or knowledge available to them. There is a lack of urgency and push for regulations and standards, and there needs to be organization and a decision to do this process better if the U.S. wants to see improvement. Mr. Willke asked how the Government could drive innovation and more effectively coordinate with its allies on cybersecurity. Mr. Nissen said that litigations, legislation protections, tax incentives, no or low cost loans (which are being used in Hawaii), a recognition that this problem is bigger than cyber, and the form of supply chain being used should be looked at in order to properly adjust risk.

Mr. Nissen stated that the United States and its allies should look beyond cybersecurity and address threats to the entire supply chain. This entire vector comes down to why the U.S. should accept third party risks. Mr. Nissen stated that the Government and private sectors should be making acquisitions not just based on cost, schedule, and performance, but also on security. He said that the U.S. supply chain is unsecure because security is not a priority for most corporations. Mr. Nissen suggested that the Government make supply chain security the fourth pillar of acquisition and recommended creating a supply chain intelligence center to actively assess and mitigate these threats. Dr. Donahue noted that the Government does not have situational awareness of current cybersecurity threats and does not know where our

strategic adversaries are and to what extent these adversaries have penetrated U.S. critical infrastructure. He said that cyber-attacks are a tool of warfare, and that the Government needs to develop a means to respond to it. The kinetic eliminate is also being used against the cyber realm. Mr. Nissen added that China's attacks on U.S. infrastructure violates the Geneva Convention because such attacks primarily target civilians. He stated that this needs to be studied and that there needs to be penalties put in place to combat this.

Mr. Willke asked how the United States and its allies could address the insecurities in existing 4G and 5G infrastructure. Mr. Nissen stated that the U.S. should begin to look at the spectrum in a new way and no longer as those for or against the U.S. He also emphasized that application creators need to start taking some accountability and responsibility for the applications they are creating. Mr. Wilke stated that there is value in public discourse about this topic. Dr. Donahue stated that there needs to a push for greater interoperability between old and new technology, so that countries can correct previous mistakes. He said that the Government also needs to recognize that infrastructure and communications companies are not operating in open markets, and that the Government should consider establishing an industrial policy to protect key industries and manufacturing capabilities in the United States and European Union. He also stated that the U.S. needs to build trusted relationship with other countries and needs to compete with these companies not exclude them. The U.S. needs to provide helpful advice to build relationships and help other overseas companies with their activities. He also stressed that the U.S. needs to look at its relationship with China with a non-adversarial view in order to find a way to co-exist with them within the market place.

Mr. Peter Altabef, NSTAC Member, asked if it was possible for the Government to have a coordinated, whole-of-nation effort like the Apollo program today. Mr. Nissen said that establishing effective industrial policy would be paramount to making such an effort work, finding strategic ways to buy risk down, such as creating franchises across U.S. or co-ops across super vertical where resources can be pulled. There is a lot that can be down if the right people get together. Dr. Donahue stated that the Government could use its development of stealth technology as a model. He said that the Government invested in researching and developing stealth technology and then provided it to industry to incorporate into new aircraft. Mr. Nissen added that the *Defense Production Act of 1950* should be relooked at and gives the Government wide authority to establish industrial policies, but that the Government chooses not to use them. He said that the U.S. needs to seriously look at how they leverage these authorities because they are a fulcrum for how to engage with industries and the vast ecosystem out there. He said that the Government and industry also need to do a better job of educating the public on the risks that currently exist in the U.S. supply chain. The vast majority of small companies think that international productions are cheaper because the cost of labor is less but do not have a clue that when they buy these cheaper products that those companies are buying access into them, and this is pivotal to why the U.S. needs better to provide better risk information.

Director Krebs thanked the panelists for their comments. He added that the majority of CISA's work will focus on issues beyond cybersecurity, including supply chain issues and hybrid threats.

VII. CLOSING REMARKS AND ADJOURNMENT

Constance H. Lau, NIAC Chair

Renée James, NSTAC Chair

Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency (CISA) (Invited)

Grant Schneider, Senior Director, National Security Council (NSC)

Ms. James invited Mr. Schneider to provide any closing remarks and thoughts.

Mr. Schneider thanked the NIAC and NSTAC members for attending the meeting and for their participation in their respective committees. He also thanked Ms. Lau, Ms. Scott, and Ms. James for their leadership and thanked Microsoft for hosting the event. He also stated that Mr. John Donovan, AT&T, had been named as the next NSTAC Chair and that an official transition will take place at the next NSTAC meeting.

Director Krebs thanked Ms. James for her leadership of the NSTAC. He added that he looks forward to working with Mr. Donovan. Director Krebs stated that the NIAC and NSTAC are two key national assets that continue to provide strategic guidance and direction to the Administration as it works to improve the Nation's national security.

Ms. Lau thanked the NSTAC for allowing the NIAC to participate in the meeting. She added that there are many areas where the councils can collaborate. She stated that the United States is a nation of innovation and that it is crucial to have strong partnerships between the Government and industry. Ms. Lau stated that the next NIAC meeting will take place on August 15, 2019, in the Washington, D.C. area, and invited NSTAC members to attend.

Ms. James said that the NSTAC will hold a member conference call on August 28, 2019. Ms. James then adjourned the meeting.