NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

QUARTERLY BUSINESS MEETING AGENDA

August 15, 2019
2:00 PM – 4:00 PM
The United States Naval Academy
Laboon Religious Conference Center
566 Brownson Rd., Annapolis, MD 21402

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 was most recently amended and continued under EO 13811, *Continuance of Certain Federal Advisory Committees,* in October of 2017. She stated that the NIAC is composed of members appointed by the President and includes senior executives with expertise throughout the critical infrastructure sectors as identified in Presidential Policy Directive 21, *Critical Infrastructure, Security, and Resilience.* During its nearly 18-year history, the NIAC has conducted and completed over 30 in-depth studies, which resulted in more than 300 recommendations to the President, such as how to improve intelligence information sharing across government and industry and how to identify and reduce complex cyber risks for cyber physical systems that operate critical processes, all of which have been made available to the public. Ms. Norris then gave a few instructions for the public comment period and informed that, at that time, no written public comments. Ms. Norris call to order the Quarterly Business Meeting for the NIAC and turn the meeting over to the NIAC Chair, Ms. Constance Lau to provide opening remarks.

NIAC MEMBERS PRESENT IN PERSON:
Ms. Constance Lau, Dr. Beverly Scott, Mr. Robert Carr, Mr. J. Richard Baich, and Dr. Georges Benjamin, Mr. William Boston, Mr. Robert Carr, Mr. Benjamin Fowke, Ms. Joan McDonald, and Mr. Michael J. Wallace.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Ms. Jan Allman, General Albert Edmonds, Mr. William Fehrman, Ms. Margaret Grayson, Chief Rhoda Kerr, and Mr. James Reid.

NIAC MEMBERS ABSENT:
Mr. Rand Beers, Mr. George Hawkins, Mr. James Murren, Mr. Thomas Noonan, Mr. Carl Newman, and Mr. Keith Parker.

SUBSTANTIVE POINTS OF CONTACT PRESENT:
Mr. Scott Seu with Ms. Constance Lau
Mr. Charles Durant with Mr. William Fehrman
Mr. Frank Prager with Mr. Benjamin Fowke
Mr. William Lawrence with Mr. Michael J. Wallace
Mr. Nathaniel Millsap with Ms. Jan Allman

SUBSTANTIVE POINTS OF CONTACT OBSERVING VIA CONFERENCE CALL:
Mr. Theodore Basta with Dr. Beverly Scott

OTHER DIGNITARIES PRESENT:
Ms. Emily Early, DHS; Mr. Steven Harris, DHS; Ms. Helen Jackson, DHS; Mr. Christopher Krebs, DHS, Cybersecurity and Infrastructure Security Agency (CISA); Ginger Norris, DHS; Mr. Mark Harvey, National Security Council (NSC); Mr. Ed Canuel NSC; Ms. Sara Mroz, NSC; Ms. Traci Silas, DHS; and Mr. Bradford Willke, DHS.

III. OPENING REMARKS AND INTRODUCTIONS

Constance H. Lau, NIAC Chair

Beverly A. Scott, NIAC Vice Chair

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

Mark Harvey, Senior Director for Resilience Policy, National Security Council (NSC)

Ms. Lau welcomed everyone to this NIAC Quarterly Business Meeting (QBM) and thanked those who were remotely attending by phone, those from the White House, those from DHS, and those who were members of the public for attending this meeting. She then invited Dr. Beverly Scott to provide any opening remarks.

Dr. Scott added her welcome to all those attending the NIAC QBM and stated that she was looking forward to the panelist as the NIAC does their best work with strong information and with staying as up-to-date as they can on the different sectors across the national infrastructure critical areas.

Ms. Lau then invited CISA Director Christopher Krebs to give any welcoming remarks, and she stated that CISA is the support agency for the NIAC. Director Krebs mentioned that it was great to be back with the NIAC and that it had been a very packed summer in terms of discussion on what both the NIAC and the President's National Security Telecommunications Advisory Committee (NSTAC) can do. He mentioned how the Joint NIAC-NSTAC meeting in June 2019 started these conversations. He stated that recent works in progress within the Administration can be seen through Acting Secretary McAleenan, who has sent out to the White House the *Risk Assessment of Telecommunication and Supply Chain Infrastructure* that was required by the recent Executive Order. He then announced the 2nd Annual National Cybersecurity Summit that CISA would be hosting on behalf of the Executive Branch on September 18th, 19th, and 20th, and he stated that the information shared would be directly relevant to the NIAC. He explained that the topics included: Industrial Control Systems and Operational Technology, Election Infrastructure, Challenges Associated with State, Local, and Tribal Territorial Governments, and Emerging Technologies and the Associated Risk Mitigated Challenges. He said that the NIAC members would be directly informed about this Summit.

Ms. Lau then invited Mark Harvey, who is the Special Assistant to the President, the NSC's Senior Director for Resilience Policy, and the principle contact with the White House for the NIAC, to share any opening remarks he had. Mr. Harvey thanked everyone for coming to the NIAC QBM and expressed how helpful it is to hear the private sector perspectives on security and resilience for critical infrastructures. He said that this private sector engagement helps to shape the critical infrastructure and build resilience into it. He stated that there are several different investments being made by the federal government to rebuild communities that have been struck by natural disasters within the last 2 years and that they are trying to update the transportation infrastructure across the country. He emphasized that all of these major investments give the opportunity to build in resilience as there are more infrastructure projects across the country. He said that having an active dialogue and identifying best practices with the NIAC has led to several efforts that have mitigated disruption to the American people. Ms. Lau thanked Mr. Harvey for his interest in their perspectives and commented that the NIAC would love to ensure that the private sector is present and considered when a policy is made for the United States (U.S).

IV. APPROVAL OF JUNE 2019 MINUTES

Constance H. Lau, NIAC Chair

Ms. Lau called to order the approval of the Joint NIAC-NSTAC meeting minutes from the June 2019 QBM. She asked if there were any changes or corrections to those minutes. With none recommended, Ms. Lau announced that the Joint NIAC-NSTAC meeting minutes would be approved and circulated.

V. PANEL DISCUSSION: INTRODUCTORY REMARKS

Constance H. Lau, NIAC Chair

Chris Boyer, Assistant Vice President, AT&T

Chris Colbert, Chief Strategy Officer, NuScale Power

Tom Farmer, Assistant Vice President, Security at the Association of American Railroads

Morgan O'Brien, Chief Executive Officer, Anterix

Robert Walters, Vice President of Construction and Engineering, Davidson Water, Inc.

Ms. Lau stated that the NIAC was very fortunate to have several wonderful subject matter experts and speakers who have tremendous knowledge and insights into the area of resiliency and security. She then introduced each panelist, thanked them for being at the QBM, and opened the discussion.

Mr. Boyer began the introductions. He stated that he was from AT&T and handles all of the cybersecurity policy portfolios there. He shared a few initial thoughts on Information Technology (IT)/Operational Technology (OT) convergence. He stated that as they start to incorporate the internet of things (IoT) and are connecting more and more things to the internet and deploying a bigger sensor network to help with operational technology, there are two effects:

1) An increase to the threat landscape and the management of these risks. This is a critical issue for AT&T as they work to protect their network assets and to ensure the reliability and integrity of the network and its availability.
2) A lot of large commercial entities that are deploying these technologies incorporate an IT technology into their operational environment. These companies are a large part of the community AT&T service, and AT&T works to help these companies deal with these challenges as they move forward. They also work with individual customers to help them deal with these challenges.

Mr. Colbert then introduced himself as the Chief Strategy Officer for NuScale Power. He stated that he has an Electrical Engineering Degree from Massachusetts Institute of Technology and a Master of Business Administration from the Walter A. Haas School of Business. He has spent 20 years doing fossil and electrical work both domestically and globally and has spent time developing a new technology called the Small Modular Light-Water Reactor (SMR). He shared that the benefits of this reactor are that it is about $1/20^{th}$ of

the size of a large reactor and brings many attributes with it, which are beneficial for resiliency and reliability. First, he stated that the design does not need external power to safely shut down and does not need power to operate, allowing their plant to be safe. Second, he commented that because it does not need external power, it can remain on the grid during events and can provide power to first responders. It also has a high resilience to natural events. Finally, to the aspect cybersecurity, he mentioned that early on NuScale utilized digital implementation of the analog systems that exist in the nuclear plants, and this means that their plants cannot be hacked because they have not gone to a CPU based technology system. He stated that they are using a technology that is separated from the rest of the plant systems so that no one can get into it or change the program. He mentioned that they are working to ensure that neutrons or radiation are not released into the environment by increasing the resiliency standpoint, which will allow them to power technology that will protect the environment and the rest of the plant from threats and attacks.

Tom Farmer then introduced himself as the Assistant Vice President of Security at the Association of American Railroads and said that he was privileged to represent the North American Railroad Industry, which is comprised of the seven major fairgrounds and Amtrak. He stated that the growth in their security program is driven by people who place an importance on both cyber and physical security within the threat elements and time/information sharing. He stated that this group has held a cybersecurity focus since 1981 and explained that the cooperation and fostered relationship that began in 1981 has continued through today. He stated that they operate in the Unified Security Plan. He shared that after the September 11th terrorist attack, they focused on terrorist prevention and came together to develop a 4-tiered, low-level approach that was based on flight intelligence and deployment incidents. He went on to state that over the years they have tested this plan and adapted it to integrate the cybersecurity portion.

He explained that, as the panel looks at the question of what the biggest risk and opportunity of convergence is, he wanted highlight that the Rail Industry's Positive Train Control (PTC). He stated that for the first time the Rail Industry will have an opportunity to have train controls computerized, which will change their operational approach but will allow the operations of the train to be slowed down and will function as a prevention tool. He mentioned that any change to the management frame in reference to how IT is utilized is an opportunity to come together and to build focused creative solutions to any deep threats. He believes that too often focus is put on placing the responsibility on the developer, on the organization with the old systems, or on the physical side when it should be on getting organizations to have the amenities they need to be protected. He stated that there have been opportunities to change how the threat is considered within potential targets.

Morgan O'Brien introduced himself and stated that this would be his 39th year in the wireless business. He then provided background on Anterix to help build a strong understanding as to why he was serving on the panel. He mentioned that Anterix is a public company operating in the spectrum space and added that they have acquired a nationwide spectrum position. He

explained that within the last five years Anterix has been going through a process with the Federal Communications Commission (FCC) that will help to make spectrum useable for private broadband implementations and this can be used for cybersecurity and other electrical grid and critical infrastructure purposes. He shared that for years critical infrastructure industries, specifically the electrical industry, have relied heavily on wireless communications in order to do many functions, including critical life functions. He stated that there is nothing new about spectrum or private radio systems because they is historic, but what has change is that the grid modernization, which has made the grid function as more of a 2-way rather than 1-way system. He explained that the architecture required for this had previously been used in back offices, but now, with the new grid modernization, it had been moved front and center so that broadband private radio spectrum could be made useable for all of the various elements of the modernized grid, which allows for operational awareness, control, and all the other big data aspects.

He stated that, in a world where public and private are going to be necessary to solve the arising challenges facing the grid and grid security resiliencies, there is an urgent public sensitivity. He emphasized that with FCC action he believes Anterix will be able to provide foundational private spectrum that facilitates the next generation grid connectivity and provides greater security, resilience, and operational control to the industry. He shared that the private industry is not looking for government mandates but for incentivization and popularization of these new technologies that are the very infrastructure of the grid.

Robert Walters stated that he works for Utility at Davidson Water and is the chair of the Water Sector Coordinating Council. He stated that the greatest risk in IT/OT convergence is that the IT and OT staff do not collaborate to secure their systems. He added that neither group is an expert in the other's systems, and he believes that convergence will open up new vectors, allowing attacks on one through the other. He shared that the greatest opportunity is the opportunity to build security practices into these unified systems as the convergence happens, and he emphasized that getting security practices right the first time will save operators time and money by mitigating the likelihood that expensive or labor-intensive solutions will need to be deployed later. He then gave an example of this within the Water Utilities in the U.S. He stated that there are about 50,000 public water suppliers, and out of that, about 80 percent serve under 3,300, which means that the majority of these public water suppliers are small water systems. However, he explained that there are about 400 systems that are large systems and serve about 90 percent of the population, and a lot of these systems are idle and are not interconnected. He stated that the smaller systems will often contract out the IT and OT, using different contractors.

VI. PANEL DISCUSSION: Q&A — *Constance H. Lau*, NIAC Chair

Chris Boyer, Assistant Vice President, AT&T

Chris Colbert, Chief Strategy Officer, NuScale Power

Tom Farmer, Assistant Vice President, Security at the Association of American Railroads

Morgan O'Brien, Chief Executive Officer, Anterix

Robert Walters, Vice President of Construction and Engineering, Davidson Water, Inc.

Ms. Lau began this discussion by referencing what Mr. Walters had stated in closing his introduction. She said that the point he raised is evident in all sectors, stating that the electric companies have companies in all different sizes. She asked him to speak on what his views were on IT/OT convergence and if he saw it as a different issue based on the size of its members. She added that she would also like to hear the opinions of Mr. Farmer and Mr. Colbert concerning this question as they are both owners and operators of infrastructure.

Mr. Walters stated that he did see IT and OT as being different. He said that the larger systems that serve the larger U.S. population are more of a target than the smaller systems because of their notoriety, their financial systems, and their port, which makes them a bigger IT/OT target. However, he restated that the smaller systems are not as much of a target because their size places them more under the radar. However, he stated that the smaller water suppliers who serve a facility that is a target are at risk of becoming a target themselves.

Mr. Colbert stated that because NuScale is a relatively new company, it does not have a product in the field yet and is considered more of a design space with its first plan to become operational in 2026. He explained that due to this they consider everything as being IT. However, he emphasized that they still separate systems that are used for Accounting, Human Resources, and other business type systems from the systems that are used for Design, Validation, and Demonstration of the Safety and Performance. He also stated that they have two types of OT: 1) for the safe shutdown and prevention of any kind of radioactive release to the public and 2) for the systems that are used for normal operational plans but are not critical to the first function. He added that these are completely separate systems and that there is no communication between the two.

He stated that for the safety side, they are using Field-Programmable Gate Arrays (FPGAs), an older technology that he has used since the 1980s, and that this technology is very well-known and robust. He explained that NuScale's first step was to demonstrate the process and put together a report that described the system for the Nuclear Regulatory Commission (NRC). He stated that getting digital controls approved by the NRC is very difficult and can be a challenge. However, NuScale submitted their report and had it approved within 18 months because of the robustness of the design, and since then, they have prototyped various portions of open module protection systems that work in the plant protection systems and safety information display systems, using this technology to demonstrate how it works and its robustness. He stated that they have questioned whether they should extend their protection to the rest of the plant at the same level as the cyber protection and added that they are looking to see if they can implement their technology to provide both cyber security and obsolescence protection. He said effectiveness and cost will impact these next steps.

Chris Boyer added that there is a lot of variability in terms of the capability of going up and down the spectrum. He stated that in cyber security resiliency it will vary some, but a lot of the threats and risks that they see are in bigger carries. However, the smaller carries could be at risk if they serve military bases or other facilities that could potentially be impacted by an adversarial attack. He referenced some work he had with the FCC back in 2013 and 2014 where they took the Network Information System (NIS) and conformed it to the communication industry. He shared that they then released a report that held the framework profile they had created for each of the segments of the industry and also looked specifically at smaller and midsize carriers, recognizing that the capabilities and investment resources they may have might differ from larger carriers.

Tom Farmer stated that the Rail Industry has a signification concern toward its protection. He stated that there are many different organizations that work together to make the Rail Industry work, and they must think about the railroads working as a whole rather than look at their organizations individually. He mentioned that railroads in general need to be protected so that smaller railroads are not at risk of being exploited due to having less resources and a smaller staff. He stated that a lot of smaller railroads are the ones that move dangerous commodities through metropolitan areas and that these smaller railroads are part of the supply chain transportation. He stated that this was the reason they focused on insuring the elevation of cyber security awareness within the industry.

He explained that it is important in the Rail Industry to know what is going on and to think about how they can transform a bad experience into good growth. He stated that they work with DHS and CISA that ensure that the good work done by them is broken down into an understandable way for the industry recipients. He shared that they work to distribute only relevant information and to educate everyone in the industry on what will impact them. He stated that they focus on what they can learn from adversary experiences and noted that they especially want to look at the attacks that their analysts see most often and at what holes are in the system. He stated that they need to get the adversaries to raise their game by closing any open risks they may have and emphasized the importance of looking into what potential risks

are being indicated through the developing threats that have already occurred and of being a forward thinker about how these potential risks and how to prevent them.

Mr. Ben Fowke complimented the work that Mr. Colbert and NuScale have done and stated that this work is essential for achieving a carbon free future at a reasonable price. He commented that the FPGAs interested him and asked if Mr. Colbert could elaborate on the air gap process.

Mr. Colbert stated that all communication can be viewed point-to-point, one directional, and that there is no communication coming from the other systems, discussing the relied upon safety signals for the reactor trip and the dedicated systems, such as the Nuclear Power Source (NPS), the market protection system, and the plant protection system. He stated for the safety function of the plant, if they take away power, the plant goes into a safe condition. He shared that this is because of how they designed their SMR, creating it with simplicity in mind and eliminating about two-thirds of the components found in large reactors, which allowed for the ability of setting valves in one safe position and not needing to reposition it. He explained that this allows for long-term safe cooling shutdown when the power is removed and that this has been validated by the NRC, who approved their topical report. He shared that this means they do not need any 1E electrical power for the plant because they don't have any loads that require that level of power supply and because there is no power needed to safely shutdown the plant.

Mr. Fowke asked if the plants would continue to be air gapped when the they become operational and are on the grid receiving signals from the grid operator. Mr. Colbert responded that at this moment all nuclear plants do not have automatic generation control, but it would be simple to get operational control in the future. He said that because of the margins they have in the plan, loss of power would still safely shutdown the plant, and the plant would remain that way indefinitely. However, he stated that this is different than making the plant operational in the event of a large systematic problem, which is why they are looking into whether or not they should take their FPGA architecture and design philosophy and move them over to the rest of the plant in order to provide the same level of resilience.

Mr. William Boston then posed a question to Mr. Walters about what Mr. Walters saw as the biggest cyber and physical risks to the Water Industry and what actions were being taken to prevent these risks from endangering the population. Mr. Walters replied that he felt that the biggest risk was accidentally creating new vulnerabilities through a lack of asset management, risk management, and vulnerability management. He went on to explain that these risks can be created through remote access protocols or through the adoption of IoT components from vendors that do not have a process for identifying and patching vulnerabilities.

He stated that last October Congress passed an American Water Infrastructure Act that will require utilities to do an assessment, to have a utilities emergency response plan to address scenarios where communications are compromised, to have regular training, and to have exercises that improve communication internally and between organizations. He went further to explain that emergency response operations also require operational coordination ahead of

the incident so that response partners can anticipate a plan for utilities and access the facilities following the loss of remote access compacity. He stated that for systems that serve over 100,000 of the population, these risk and resiliency assessments will be due March 2020. He also stated that the following 18-months are stage by size and that 6-months after that they will have to update their emergency response plan, which will have to be certified by the regulators at the Environmental Protection Agency (EPA). He shared that this assessment will go into detail about natural and manmade hazards and will be a much more comprehensive risk assessment, requiring a higher degree of cyber than what had been previously required. He explained that this will be an opportunity for utilities to look at themselves and measure how things can be made better and how they can be more resilient. He stated that this American Water Infrastructure Act assessment is to be looked at every 5 years.

Dr. Scott commented to Mr. Farmer that the implementation of PTC across the transportation sector was massive, and she asked him what he thought the biggest lessons learn were. Mr. Farmer provided some background on PTC by sharing about an accident that occurred in the Los Angeles area where a train collided with another train. He stated that this accident showed the need to be able to prevent these types of collisions and that they decided to use technology for this.

He mentioned that during 2007-2008, there was a mandate to the Rail Industry to develop train systems that would enhance safety and provide open source equipment and capabilities. He stated that today PTC is installed and functioning well in about 90 percent of the areas that they are required to meet. He explained that they are required to put PTC in trains that transport security sensitive materials, dangerous commodities, and passengers and that they believe by the year 2021 they will have installed the PTC system in all trains. He stated that the challenge with PTC is that it is a good concept but there isn't a good understanding of what it would be needed to make it happen or what it would cost. He stated that to make this system function effectively, the Rail Industry invested 15-billion dollars.

He then explained that PTC was developed with cyber threats in mind based on the information that was already circulating about adversarial attacks. Though, he mentioned that no matter how good the cyber protection is as cyber threats evolve those protections must evolve as well. He said that this is why threat analysis is so important. He suggested that one area for improvement is how the information is packaged and delivered. He said that the way information is shared now is not understood by many private sector companies, and he recommended that the protective measures are highlighted and what is most effective is showcased so that they are better understood. He also recommended establishing five things that companies could do to help manage threats. He said the advisories should be organized as a short summary of the threat and the measures that are most conducive for dealing with this threat. He emphasized that whether a company is a potential target or has a connection to a potential target this will help people better know the right actions to take.

Mr. Michael Wallace asked Mr. Boyer about the Global Policy for AT&T. He stated that because the NIAC is about U.S. National Security, he was interested in knowing what policy AT&T had towards serving the U.S. National Security interest over other countries or Global

National Security interests. Mr. Boyer stated that AT&T is part of the National Security Telecommunications Advisory Committee (NSTAC). He went on to explain that his current CEO, John Donovan, is the NSTAC chair and works with the White House and DHS on a variety of National Security issues. He also stated that 90 percent of AT&T's business is U.S. based, and most of who they serve internationally are U.S. multinationals, which is mostly U.S. corporations. He said that although they operate in other countries, they are sensitive to U.S. National Security issues and that this awareness is engrained into their amenities.

Mr. Wallace ask Mr. Boyer to further explain how AT&T thinks about vulnerabilities that stand to be introduced to the system due to providing services in many countries around the world. Mr. Boyer explained that AT&T treats the global networks as if these are an untrusted network and run them through several security gateways. He explained that some places are owned and operated by AT&T and some are worked through third party companies, but if it is an untrusted network, they can connect to an outside network through a security gateway, making it harder for outside networks to introduce security risks into the network.

Director Krebs asked Mr. Boyer if could speak to AT&T's efforts to develop global markets for trusted supply chain commodity issues. Mr. Boyer stated that this was a huge issue right now, especially with 5G and the radio part of the network. He said that there are not many suppliers in radio materials, and he expressed that they have been taking an active role in trying to build a more robust supply chain and have been working to create a scale for this supply chain and opportunities for new entrance into the domestic space, which could allow new players into the market.

Director Krebs than asked Mr. Colbert about the NuScale Digital Control System (DCS) and whether it was proprietary or customizable. Mr. Colbert stated that they are looking into whether they should do this because they are looking to prevent more than just radioactive release. He stated that they currently are conducting a study to ensure that the assets are available during emergency situations, to see how feasible this is, and to discover the cost it would take to implement this. He said that they are about five months away from deciding whether or not this is a viable option for them.

Ms. Lau asked Mr. Colbert if the nuclear plants needed to be connected to air gap since they connect with the many competitive markets on generation sites. Mr. Colbert responded that there are information systems that may be connected but the OT that is used for plant protection and to prevent a release of radioactive material into the environment are independent from this. He stated that they are considering whether they want to have an automatic function for what they currently have an operator do. He said that the NuScale technology can go from 0 to 100 percent power through steam by-pass and that this doesn't impact reactor power, so he believes this particular function should be allowable. He said that the technology they are using is now being implemented for the FPGA technology within medical isotope factories, showing that this technology is making its way into other areas of the economy.

Mr. O'Brien was asked to give more information about the cyber security aspect improvements and technology. He stated that they were proposing to make Spectrum available as a landlord not a carrier, which would be available for 4G technology that would have the latency and bandwidth characteristics that are necessary for IP basic communications on next generation connectivity. However, he stated that they have not received FCC approval to move their spectrum to broadband but are expecting this approval soon. He shared that they are already in discussion on ways that cyber security controls can be place into critical systems and stated that they are not suggestion that the amount of spectrum they are proposing to lease to the critical infrastructure players will allow them to do everything for the IoT or smart city. Instead, he said that it is a limited high-quality spectrum that has good propagation penetration characteristics that will lend itself to wide area systems. He shared that they had the opportunity to go into the National Renewable Energy Lab (NREL) and discuss how this spectrum could help them. He said that within the next few weeks they were on track to test the spectrum and use cases that have critical control units to the grid.

He also explained that they are working with large utilities in California who are struggling to create wildfires mitigation plans, which helps to make the abstract more real. He said that these companies have absolute requirements to distribute, throughout the network, the new sensors that are available globally and to have falling line inductor protection, which requires lines that have fallen to be deactivated before they hit the ground. He said that having wireless data use in utilities would allow for absolute control over the model these companies use and would help reduce the chance of wildfires in California.

Ms. Joan McDonald asked Mr. Farmer and Mr. Walters to speak on three points: 1) do their smaller entities have cyber risks, 2) do they know about these risks, and 3) how do they educate, train, and communicate to these smaller organizations. Mr. Farmer said that every organization has cyber risks but the risks that the Rail Industry is most concerned about are those with short-line railroads that interchange and regularly transact business with major freight railroads. He stated that one of the improvements made after 9/11 was to expand the scope of participation, which now includes more than 130 short-line railroads that share changes with hazardous materials, and the improved communication with them. He said that they manage a railroad network with a range of physical and cyber security resources and work with other government authorities, like DHS and the Transportation Security Administration, to ensure that they know the current threats and where their focus should be. He said that they get awareness messages that show useful information for railroads of all sizes and that this gives the railroad industry a collective knowledge that they can grow from.

Mr. Walters responded that there are number of organizations that work with the small systems. He also informed the NIAC that there are about 40,000 small water systems that serve about 3,300 or less, and a lot of these are not heavily reliant on the internet, and he shared that cell phones or radios would be used for different facilities to talk with each other; however, in very small water systems, they would do it manually. He said that only ten percent of the population is served by these small water systems. He shared that it is the larger water systems that would impact most of the population and whose IT/OT systems would be more susceptible, and because of this, the American Water Works Association (AWWA)

offers a tremendous amount of training and has developed guidance manuals and standards for these systems. In addition, he stated that the National Rural Water Association (NRWA), who is funded by grants given from EPA and the U.S. Department of Agriculture (USDA), also provides training and technical assistance to smaller utilities, adding that the people who work these smaller utilities may wear many hats in the towns where they live.

Mr. Farmer added that phishing emails are something that they are proactive in identifying and sharing information about industry wide. He stated that in the past 5 month they have been fact reporting and producing advisory information, and they are looking for ways to share this information with the government and other cross sectors, so that this information can get into the right hands and the right action can be taken against these phishing threats.

Director Krebs added that the critically important element to understand is that the adversaries look at the sectors as landscapes in front of them, which means that the adversary often ends up in places that they didn't anticipate and takes this to their advantage to move up the supply chain. He mentioned a campaign that CISA has been working on where they found that the adversary had started a construction company, worked through a heating and air conditioning company, and made its way to an engineering company. He emphasized that it is critically important to take the elements that have been seen in the rail sector and push it out across all sectors, avoiding stove piping information. He stated that information sharing has involved into actionable compromise and that it is less about the single indicator and more about strategic intelligence. He agreed that there should be five best practices provided to the private sectors along with the threat lay-down and stated that this is about operationalizing the partnerships.

Mr. J. Rich Baich asked whether the panelist knew the standards that would enable them to protect their organizations. Mr. Boyer responded that there are a lot of standards that AT&T uses. He went on to explain that AT&T has a Security Policy program, which holds the different standards that are applied across the business. He stated that standards are not a 100 percent guarantee against cyber-attacks but do provide a narrowed scope for cyber-attacks outside of these standards. Mr. Colbert stated that their safety standards generally come out of the *NRC 10 CFR 50* and the guidance within that. He went on to explain that the non-safety side does not have any standard panels but has a large resource working within it to protect the public and the asset.

Mr. Farmer stated that they evaluate their posture, draw lessons from those evaluations, and set these as priorities for further efforts. He said that they preform penetration testing to test the operations on their infrastructure, to see if there are any vulnerabilities, and to address them. He also stated that they have developed a procurement guide to help when talking with vendors. He explained that they have modeled their information sharing effort based on Hawaii and that they have been sharing with the NRC and with other cross sectors. He stated that they are looking at what tactics are being used most often, what vulnerabilities are being exploited, what protective measures are often found to be lacking, and what indicators were they developing. He said that looking at these four categories from a strategic outlook helps them narrow the risk window.

Mr. O'Brien stated that they were in a different category because they are a landlord of Spectrum and, therefore, a facilitator. He said that having private, stand-alone facilities that are not connected to the internet and are built with the security design that their customer desires produces heightened standards and roles and provides greater security. Mr. Walters stated that he believes that ISACs and sector coordinating councils go a long way to help facilitate government and industry collaboration. He explained that government, industry, and larger manufacturers can also be more vocal about the need for the industry to ensure that security is baked into products. He shared that CISA has been more proactive in providing threat notifications and non-regulatory guidance and added that DHS can also support the security activities of critical infrastructure operators by designating more information as sensitive but unclassified (SBU) or by more aggressively facilitating applications for security clearances. He explained that the biggest barriers are a lack of understanding about how to address threats and the cost of security relative to an organization's ability or willingness to pay. He said that DHS and the Idaho National Laboratory could support the adoption of solutions by testing them and publish research findings and recommendations. He also expressed that utilities, specifically the smaller companies, do not know about the support that they have, and he explained that email phishing is a huge vulnerability that is not realized by these utilities. He stated that more education is needed to reduce this risk.

Mr. Boyer added that one of the problems they have is pushing this information out to their suppliers and ensuring that their suppliers are following those standards. He said that this is a huge issue for all industries to look at and that supply chain is a very complex challenge. He said that the biggest challenge is the complexity of the environment, which is getting even more difficult with the entrance of IT/OT, and better security needs to be added into devices when they are manufactured. He stated that this is an industry wide challenge.

Mr. William Fehrman asked the panelist to speak on what impacts, concerns, or risks they had about the move to 5G. Mr. Boyer stated that 5G is critically important to AT&T and that the 5G architecture moves the security structure in the right direction. He shared that they believe 5G will be more secure than any previous network; however, he stated that the challenge will be the growth of the threat surface. Mr. Colbert stated that because NuScale is not using any wireless communications within the plant protection systems at this time they do not have any technology that 5G impacts. Mr. Farmer explained that they see 5G as a step in the right direction and that a lot of their business is being designed and developed with 5G in mind. He said that the communication aspect of it is very beneficial. Mr. O'Brien stated that 5G could bring enormous capabilities and powers to Spectrum and their target customers. Mr. Walters mentioned that the biggest broadband users in the water utilities are the video cameras used and the data feed these cameras produce. He stated that 5G will help them monitor tanks, reservoirs, etc., and will help with the video data produced.

Mr. Boston asked if the local fibers would be able to help industries secure critical infrastructure. Mr. Boyer stated that he was unsure if he could answer Mr. Boston's question but that with the 5G built there would be more cell sites required, which will require more

fibers needed; however, he is unsure about how this would impact the security of the critical infrastructure.

Ms. Lau asked the panelist to briefly discuss the security aspect of the Cloud. Mr. Boyer explained that what has been done in the Cloud is being put into the network, which will allow core functionalities to become virtual machines that run on commodity-based hardware that is deployed into IT services. He stated that this allows them to scale the network to meet demands, which creates flexibility in the network. He shared that this is something that is going to be required for AT&T because of the amount of data that runs through the company. Mr. Walters added that the Cloud is not like by every IT worker, and that the personality of the IT/OT personnel really impacts the acceptance of the Cloud and how successful it is.

VII. CLOSING REMARKS AND ADJOURNMENT

Constance H. Lau, NIAC Chair

Beverly A. Scott, NIAC Vice Chair

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

Mark Harvey, Senior Director for Resilience Policy, National Security Council (NSC)

Ms. Lau thanked the panelist for attending the NIAC's QBM and participating on the panel. She invited Dr. Scott to provide any closing remarks and thoughts.

Dr. Scott thanked the panelist for sharing and stated that the information was very helpful.

Director Krebs added that the information about the technology and where things were going was very interesting, and that they are trying to adopt the mentality shared throughout the panel. He stated that the next generation deployments must be secured by design and that the panelist really helped with understanding this.

Mr. Harvey shared that the panelist helped to show the relentless march forward in adopting technology into design and in the operation of critical infrastructure across the board. He said that it is very clear that the lexicon must change as emerging technology come out. He added that today was a great start to this discussion about how to update the lexicon and how to understand, measure, and manage the risks within this space.

Ms. Lau closed by stating the partnership between the private sector and government is critical. She stated that there are programs that the government has to help companies and wished that there had been time to note some of them. She then thanked everyone for attending the NIAC QBM and stated that the next NIAC QBM would be on December 12th, 2019, in Washington, D.C, followed by a February 28th, 2020, NIAC QBM in Hawaii.