NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

QUARTERLY BUSINESS MEETING MINUTES

May 8, 2017
1:30 PM- 4:30 PM EDT
US Access Board
1331 F Street Suite 800
Washington DC, 20004

I. OPENING OF MEETING

Ginger Norris, Designated Federal Officer (DFO), National Infrastructure Advisory Council (NIAC), Department of Homeland Security (DHS)

Ms. Ginger Norris, NIAC DFO, opened the meeting and welcomed all in attendance.

II. ROLL CALL OF MEMBERS

Ginger Norris, DFO, NIAC, DHS

Ms. Norris called roll of all present at the meeting. Ms. Norris described the responsibility and duty of the NIAC Members in their service to the President and how they are regulated by the Federal Advisory Committee Act (FACA). She also presented a brief history of the Council's work. She instructed the process of public comments, and reminded those who wish to make a public comment after the meeting that they can email such comments to the NIAC inbox (niac.niac@hq.dhs.gov). Public comments are accepted for thirty days after the meeting.

NIAC MEMBERS PRESENT IN PERSON:
Ms. Joan McDonald, Mr. Michael Wallace, Ms. Constance Lau, Dr. Beverly Scott, Ms. Cristin Dorgelo, Mr. Keith Parker, Ms. Jan Allman, Mr. Robert Carr, Ms. Amy Pope, Mr. Dan Tangherlini, Ms. Margaret Grayson, and Chief Rhoda Kerr.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
General Albert Edmonds, Ms. Diana Perreiah, Mr. George Hawkins, Mr. Georges Benjamin, Mr. Dhanurjay Patil, Mr. William Terry Boston, and Mr. James Reid.

MEMBERS ABSENT:
Mr. Rand Beers, Mr. James Murren, Mr. Carl Newman, Mr. Charles Ramsey, Ms. Christina Goldfuss, Mr. Dan Utech, Mr. Thomas Noonan, and Mr. Ben Fowke.

SUBSTANTIVE POINTS OF CONTACT PRESENT IN ARLINGTON:
Ms. Rivka Tadjer with Mr. Robert Carr
Ms. Bianca Mallory with Dr. Beverly Scott

Ms. Saba Long with Mr. Keith Parker
Mr. Frank Prager with Mr. Ben Fowke
Mr. Nathaniel Millsap with Ms. Jan Allman
Mr. Jonathan Reeves with Mr. George Hawkins

SUBSTANTIVE POINTS OF CONTACT OBSERVING VIA CONFERENCE CALL:
Mr. Scott Seu with Ms. Constance Lau

OTHER DIGNITARIES PRESENT:
Ms. Stephanie Morrison, NSC; Ms. Monica Maher, NSC; Ms. Heather King, NSC; Mr. Rob Joyce, NSC; Mr. David Hess, DHS, NPPD; Mr. Robert Kolasky, DHS, NPPD; Mr. Chris Krebs, DHS

III. OPENING REMARKS AND INTRODUCTIONS

Constance H. Lau, NIAC Chair

Elaine Duke, Deputy Secretary, DHS (invited)

David Hess, Senior Official Performing the Duties of the Under Secretary, National Protection and Programs Directorate (NPPD) (invited)

Robert Kolasky, Acting Deputy Under Secretary, NPPD (invited)

National Security Council

Ms. Constance Lau, NIAC Chair, welcomed everyone to the QBM. She welcomed members from the National Security Council (NSC) and members from DHS, and thanked them for participating in the meeting. Ms. Lau welcomed Mr. Rob Joyce, the Special Assistant to the President and the Cybersecurity Coordinator for the White House. She also welcomed Mr. Chris Krebs, the Cybersecurity Advisor to Secretary John Kelly.

Mr. Joyce thanked the NIAC Members. He noted as he looked to trend lines, threats to critical infrastructure are at the top of the list in terms of the cyber aspects of his work. He said the trend lines are not good and are headed in the wrong direction. He believes it will be governmental public-private partnerships (P3s) that help reverse that trend and make it so critical infrastructure can be defended, as well as made resilient. Because of the threats being faced, he thinks the nation must have the best possible defenses and be prepared should they ever fail. They need to be able to find penetrations and ensure those penetrations create minimal damage and defenses are resilient and can be restored. Mr. Joyce said in his new role he was able to review the Working Group's Cyber Scoping Study, taking a look at some of those serious cyber threats the nation is facing in critical infrastructure. He noted that it resonates with him and some of what he said is consistent with the points the Working Group is trying to make and that critically, severe, and urgent action is required. He said he is "right there with [the NIAC]." Mr. Joyce thanked the Members for the time they volunteer to build relationships and advise the government. He does not think in general, those who are not sophisticated and initiated really understand the interrelationships between all the different sectors' critical infrastructure. He noted a fault in one will likely cascade into another sector. He said those are the reasons that makes the government investment into this effort so important and he hopes it is part of the motivating factor in bringing the Member's companies and networks to the same table. Mr. Joyce said he interacts often with the Homeland Security Advisor, Mr. Tom Bossert, who has a passion for this topic as well. He recalled how Mr. Bossert has said "we need to move beyond lip service between public-private partnerships." Mr. Joyce has been talking to his team on the NSC and other partners within government and they are working on the tasking he hopes to deliver to the NIAC to depict where they think the NIAC would be most valuable in advising the Federal government. He acknowledged the Cyber Executive Order (EO) would be coming soon, but it is up to the President to release that when he chooses. Mr. Joyce noted he cannot speak about the EO, but he instead provided a list of his priorities. His three major areas of focus are as follows:

1. Inside the government, the networks are operated for the people. When there are compromises of the nature of the Office of Personnel Management (OPM) or a breach at the Social Security Administration (SSA), or the Internal Revenue Service (IRS). The consequences would be heinous. He said, "we have that data on behalf of and for the public, and so we have a huge responsibility to defend it." He noted they push hard in modernizing and protecting Federal networks.

2. Critical Infrastructure. He noted this is where the NIAC's expertise is important. There is a focus on improving P3s and looking to and enabling the information sharing and the efforts advancing the security of critical infrastructure to include making sure there is adequate planning. The government performs exercises and plans for the worst in the area of cybersecurity, but Mr. Joyce noted he does not feel comfortable with the playbooks set in place to prepare for cyber emergencies. Also, within the critical infrastructure area, Mr. Joyce says our country needs to better understand the nuances of the various sectors. Each sector has its own unique issues, as well as strengths and abilities to maneuver in responding to cyber threats. Some sectors do not have the agility, due to regulation or the nature of their infrastructure, like other sectors might. He recommended figuring out how they all interrelate.

3. International partnerships. He noted in the NIAC, the Electrical Sector (where the US shares a common grid with Canada) is an important place. Mr. Joyce said the US has great partners in Canada, as well as other international partners in critical infrastructure. He said the US has to have strong international partnerships, looking for like-minded countries that can build the common norms for a free and open internet. It will help the country do deterrence work and set the expectations of what is reasonable in cyber space, ensuring the rules of laws in the physical space also apply in cyber space. Deterrence is vital to not permit other countries to hold the US at risk in cyber space. One of the places adversaries would look to do that is in critical infrastructure. This takes offensive work, international norms, and efforts with like-minded partners, as well as strong defensive reaction.

Mr. Joyce said under all those priorities is the need for workforce. He said government, private sector, and academia do not have the minds or capacity to address all problems, so that work force needs to be built. He noted and apologized that he would have to leave around 2:15 pm to meet with Vice President Michael Pence.

Mr. Krebs gave opening remarks and noted that Mr. Joyce is well known within the cybersecurity arena and informed everyone Mr. Joyce was named in an article as one of the top five people in cybersecurity in D.C. Secretary Kelly was also included on that list, who was unable to attend the QBM, due to overseas travel. He told the Members the Deputy Secretary also sends her regrets for not being able to attend. Mr. Krebs said he is honored to sit at "this part of the table." He mentioned he may have worked with some of the Members in the past when he worked for DHS previously. He served in the Office of Infrastructure Protection (IP) and was an advisor to the Assistant Secretary at the time. During that time, Mr. Krebs worked on a number of NIAC issues, as well as the National Security Telecommunications Advisory Committee (NSTAC) and the Homeland Security Advisory Council (HSAC) issues. He said he is familiar with the value of work produced by such groups. In addition, he sees the value of P3s and the role they have in standing up the National Infrastructure Protection Plan (NIPP). In his current role as Senior Counselor to the Secretary, he covers cybersecurity, critical infrastructure, and resiliency issues. When he breaks that down in terms of the DHS work chart, he said he generally advises the Secretary on issues relating to the National Protection and Programs Directorate (NPPD) and the Federal Emergency Management Agency (FEMA) issues. He helps Secretary Kelly understand the unique additives on contributions that NIAC can make as he works through understanding how to approach his priorities. Mr. Krebs hoped everyone saw Secretary Kelly's speech at George Washington University, where he made his first policy statement. Secretary Kelly is interested in countering the terrorist threat and countering the transnational criminal organization threat. He is focused on many cyber areas, including securing the ".gov" traditional DHS mission, in addition to working with the critical infrastructure community. He said they are thinking more broadly about addressing systemic risks. He believes the NIAC will see how DHS plans to counter those in the Cybersecurity Executive Order (EO). Mr. Krebs reiterated Mr. Joyce's sentiments about not discussing the EO. The Secretary has mentioned the reorganization of NPPD, which is a priority of his to ensure it has the resources, capabilities, and personnel it needs to focus on the highest priority: cybersecurity and critical infrastructure issues. Secretary Kelly will be engaging with industry about this matter in the coming weeks and months, and asking for insight on how to best approach the issue and organize customer service equities. Mr. Krebs mentioned they are engaging with a number of the issues coming out of the White House, like the Office of American Innovation (OAI), in providing cybersecurity technical expertise. He thanked the Council for having him and said he looked forward to participating in the day's discussions.

Mr. David Hess thanked the NIAC Members for their hard work and dedication. He said the Council is a great resource to DHS and they look forward to strengthening their partnership. Mr. Hess added he was joined by Acting Deputy Under Secretary Robert Kolasky and they look forward to the meeting's conversation.

IV. Approval of February 2017 Minutes

Constance H. Lau, NIAC Chair

Ms. Lau asked for a motion to approve the final draft of the February 2017 QBM minutes, as amended for non-substantive changes. All Council Members present unanimously approved the minutes.

V. Final Report of Future Focus Working Group

Joan McDonald and Mike Wallace, Working Group Co-Chairs

Ms. Lau explained that the Future Focus Working Group chaired by Ms. McDonald and Mr. Wallace had organized into two work streams with Ms. McDonald heading the work stream charged with strengthening the NIAC study process and charting future topics and Mr. Wallace heading the work stream to scope a study on cyber security. She further explained that Mr. Wallace would start with an update on the cyber scoping report that had been delivered at the February 16th QBM.

Mr. Wallace apologized for any redundancy in his presentation, for he was drawing from the same slide deck as the February 16th QBM. He noted the comments made in the opening remarks resonated with the observations and recommendations of the Working Group. Drawing from a few of the slides (linked below), Mr. Wallace summarized what was reported in February, as well as updated the Council on the activities of the Working Group since the last QBM.

Mr. Wallace went through the NIAC Cyber Scoping Study Working Group slide deck, which is publically available on the NIAC website and linked here: Cyber Scoping Study Working Group Slide Deck.

Information provided by Mr. Wallace, not included in the slide deck:

- The NIAC does not see itself having a long-term role in cybersecurity.
- He noted the Working Group has held off on submitting recommendations to the President until the cybersecurity Executive Order comes out.

Mr. Wallace also presented an additional slide of a draft private-public structure for securing U.S. cyber infrastructure. He noted the Working Group developed the new slide in the morning prior to the meeting. He said the notion is whether one thinks about triaging or long-term, the question is then how to bring “real” P3s together. Mr. Wallace read through the details of the chart, which includes a Senior Advisory Group, an Executive Steering Group, and a Technical and Operational Staff. He noted the Working Group created this chart to show their view of how to bring P3s together in a workable way. He also said it could be used to “triage” what he thinks needs to be done immediately and could further inform a draft project plan to develop a broader approach for finding a new direction of tackling cybersecurity for the whole country. Mr. Wallace said the Working Group expects this draft structure will be molded and guided by the anticipated executive order. He said the firm views the Working Group is offering by putting the chart forward are as follows:

- Recommend P3s resemble this chart.
- Staffing at third level is critical.
- Quick-turn actionable outcomes are only possible through a project management type approach.

Ms. McDonald thanked Mr. Wallace, the Working Group, Ms. Norris, and the team and said she had enjoyed Co-Chairing the study. She reiterated from the February QBM that the first work stream was charged with strengthening the NIAC study process and to chart future topics. Ms. McDonald went through a shortened NIAC Future Focus Study slide deck, which is publically available on the NIAC website and linked here: Future Focus Study Slide Deck. The full slide deck is linked here: Full Future Focus Study Slide Deck.

Information provided by Ms. McDonald, not included in the slide deck:

- Key takeaway is that the NIAC is viewed as an independent voice on cross-cutting critical infrastructure issues, whose studies are seen as valuable, influential, and with objective insights.

VI. OPEN DISCUSSION AND PUBLIC COMMENT

Ginger Norris, DFO, NIAC, DHS

Mr. Kolasky began the discussion by talking about the new slide added within Mr. Wallace's presentation on executive collaboration. He said work has been done through the Electric Sector Coordinating Council (ESCC), and the Financial Services Sector Coordinating Council (FSSCC); some of the sector-specific groups have come together to strengthen public-private operational collaboration and executive involvement. He asked Mr. Wallace if he thought those were examples of where they need to go cross-sector, or if he is recommending something fundamentally different.

Mr. Wallace told Mr. Kolasky it is different. The NIAC is taking it to a new and higher executive level. He did not want to diminish the work of the Sector Coordinating Councils (SCCs) and the Government Coordinating Councils (GCCs), but he said that has been happening for a long time and it does not always address the major questions or tackle the highest priorities. He noted they are not in a position to be able to make those judgments in a robust sort of way for the country. He said the NIAC's view is if one looks at the chart and it says there is a financial services sector CEO, then perhaps the FSSCC determines who that should be. He added the ESCC could then determine who the electricity representative should be. Mr. Wallace reiterated it is a different and much higher executive framework in a tiered structure and in a project management-type mode, where those sectors are working on a common focus (in a triage sense) on what might be addressed first. Then in the parallel path, the suggestion is a different approach for cyber security for the whole nation needs to evolve, although he acknowledged that is a very big task and will take longer. Mr. Wallace added that may not be best accomplished through an SCC/GCC structure, because it is a different structure that levers off the resources in those groups.

Ms. Lau added that in many ways it builds off of what the Council has been repeatedly saying about executive level engagement. She added it is not only about executive level engagement, but additionally involves bringing all the right people to the table to cut across some of the tangled structure of Federal agencies involved in cyber as shown in one of Mr. Wallace's slides to really make major change in how the nation approaches cyber. She said it is where the NIAC thinks the key parties need to be involved to resolve the issue.

Mr. Kolasky appreciated their clarification and noted it is a question the Federal government has been grappling with. There is a question of incrementally making progress toward the end state or wondering if there has to be something that skips a generation of progress or turns the government in a different direction. He also wondered what the Federal levers are that make that happen. In terms of improvement, Mr. Kolasky noted there is better executive engagement than before, better information sharing, and more is being done to reduce risks. He understands the urgency by which the Working Group Members look and say, "that's great, but the problem is getting worse too." He told them he hears the call for something new and said they need to figure out what executive action could get us there, other than with a resource injection.

Mr. Wallace said the Working Group wants to recommend a bold new approach, because while the country is making progress incrementally, "we're losing the game." He said the risk is growing every day, because adversaries, threats, and vulnerabilities are moving away faster than the nation's ability to catch up. Mr. Wallace also included a two-track approach in his presentation. One triage addresses those things that are most important for most sectors, with the greatest threats to the economic and security viabilities most at risk; parallel to that is a focus on how to consider options to reframe cybersecurity for the country. He noted everything is being kept general, as to not get ahead of the EO. The NIAC is trying to voice that they think this is a viable process approach to the right answer. It will involve bringing a lot of the right people in along the way, with a project management definitive decision structure that brings private sector and public sector together at the highest level. Resources are important, without sufficient resources at the third level, the executives will not be supported adequately to make the necessary decisions. Mr. Wallace said within his own work, "[his] decisions are only as good as the resources, the analysis, the support, the critical challenges that all take place before it gets to my desk." He added generally executives will default to making no decision, because they lack the adequate basis to understand things. He said it is a decision-making process, a buildup of information and it is a level of engagement appropriate for the CEO (to meet quarterly), appropriate for the next level down (meeting about monthly), with thoroughly informed staff. He said these are not bottom line "worker bees", these are mid and upper-level managers who are able to do the work that needs to be done to deliver options up the chain. He repeated the Working Group is suggesting a bold approach that is different, and not just injecting resources.

Mr. Keith Parker made a comment about how large companies have a responsibility, and he thinks even in this anti-regulatory environment it should be recognized that their impact could have a significant disruptive consequence on the nation's infrastructure and security. He said he would be interested to hear a perspective on small companies, or perhaps if someone who develops an app, such as Waze. He said in the wrong hands it could be greatly disruptive, one way is if a terrorist is trying to maximize causalities by getting the most people into a centralized location and causing harm. He asked should the responsibility of firms (not necessarily big firms) be more regulated in this era of what could happen to the nation if something is suddenly in the wrong hands.

Ms. Heather King thanked the Working Group for the thought and ideas put into their presentations. She said she is thinking about how to have companies or organizations that have more similarities with one another, in terms of size and scope across sectors. She asked, "how do we encourage that cross collaboration?" She noted Mr. Parker brought up an important point about small businesses. In terms of processing this, she thinks this is an organizational structure for bringing together executive representation across various sectors, up to the President. Ms. King asked the Council how to bring leaders across industry to collaborate and work with one another that are more similar with an organization in one sector that is a smaller business, with another organization that is also smaller in different sector. She agreed the tiered organization is managing up to the President, but then she wondered about approaching cross collaboration differently in terms of building deeper relationships across the sectors.

Mr. Wallace told Ms. King the Working Group had the same conversation. Their notion is that while it is impossible to do everything, the priority should be "the most important thing." They believe what is most important is the triage. He said if they just do a broader approach then they may be successful two years from now, but lose the opportunity to make a real difference six months from now. Contrastingly, if they pursue a six month goal, then he said they do not answer the kind of question Ms. King and Mr. Parker asked. Mr. Wallace asked hypothetically, "so then what about the broader infrastructure and how everything gets done?" He suggested from the Working Group Members' experiences, when one solves a complex problem, typically the result also includes gaining insights about how to work together with those that helped, or how to function and organize one's self to solve other problems, broader problems or more difficult problems. Mr. Wallace described it as a learning experience from which a lot of input will be gained and taken aboard. He said the NIAC could help, but perhaps the people listed on that chart can become self-learning. He reiterated that the Working Group does not believe this chart holds the answer, but the whole notion is to focus and accomplish an outcome with senior leaders and then learn from that experience for the future or more broadly.

Mr. Kolasky said part of what Mr. Wallace was describing is risk identification done more quickly. Whether it is small or not, he said if a company has presented something that could be compromising, it could also present a bigger risk to the entire system. He said if that happens, no matter what size the company, it presents some level of systemic risk. Mr. Kolasky said he would speak for himself, but the last thing he would want is for something to very quickly become a dynamic risk and then possibly need more government regulations immediately within the agency. He said that is not going to solve the problem. Mr. Kolasky believes it is more important to recognize the risk, start to address the risk, and then manage the risk without rushing to a solution. He said he thinks the process the Working Group laid out provides that.

Ms. Dorgelo thanked the Working Group for their great work. She said it has been great to see where they have come since the February QBM. She provided three points: 1) She is interested in potential future topics and cybersecurity, in terms of having a follow-on discussion on what the healthcare sector is facing. She noted that topic was only starting to be analyzed by the last administration. She said information technology risk will dramatically shift in the coming years as precision medicine and vast data source of genetic sequencing and other personal information about patients is put online. Ms. Dorgelo said that data can become a much more attractive target for breaches and the implication of that is significant. She said she agrees with the four areas that were called out in the private-public structure chart around electricity and communications being cross-cutting issues. She noted that the healthcare sector is facing a chance to build right as they engage in data process from the start. This is less of a question of triage now, more of a question of building right from the beginning as precision medicine grows. She made the point she would like considered both in the cyber piece, but also when looking at future potential topics for NIAC to dive deeper into. She encouraged the Working Group to have a follow-up discussion on this topic with Mr. DJ Patil, whom she says is very knowledgeable on the topic. 2) The second point she described was related to structure. She wondered what role is designated for senior technical and scientific leaders of such corporations and agencies. She added knowing from a policy point of view, it has been helpful to have the science and technology industry at the table to inform the discussions. She said she is curious about what role they could play in these bodies and what representation they could have. Ms. Dorgelo provided an example: a Chief Technology Officer (CTO) or a Chief Innovation Officer of these corporations could have a voice. 3) Her last point suggested there may be private sector representatives on the Defense Innovation Board, United States President's Council of Advisors on Science and Technology (P-CAST), once reconstituted would be beneficial to have a discussion with this body to share ideas on this structure, given that they operate in those roles and have experts like Mr. Eric Schmidt and Mr. Reid Hoffman on the Defense Innovation Advisory Board. She said they would appreciate a dialogue with this body about this potential structure. Ms. Dorgelo thanked the Working Group again for their hard work.

Mr. Krebs said the work was impressive and shows a lot of critical thinking about a number of problems seen over the past several years. While he just recently returned to government from the private sector, he noted the findings were spot on with the Information Technology (IT) sector he was in. He added that he thought they “nailed” the population. Although, he wondered where the IT sector fit in. Mr. Krebs said when dealing with a cybersecurity issue, particularly from a risk mitigation perspective, the sector brings a certain set of experiences and expertise to help address the problem and he is interested in hearing where the Working Group sees them fitting in.

Mr. Wallace told Mr. Krebs when they mention telecommunications, they are including communications and information technology.

Mr. Krebs thanked Mr. Wallace for the clarification. One way he is thinking about the broader set of issues is by talking within the context of addressing large scale systemic risks. He asked what serious issues need to be addressed. He said from the government perspective and working with industry, the question is how to create market conditions and incentives to get best practices picked up more broadly and quickly. Mr. Krebs suggested an example could be the ability to pivot as quickly as possible to address certain applications if something were compromised. On the overarching approach to NIAC studies going forward, he believes the NIAC "got it right." He agrees that a quicker, iterative, and more measurable approach is key. He added that after an eighteen-month study cycle, the opportunity is already gone. Mr. Krebs believes quick-hitting, cyclical reports would be very helpful to the Secretary, in particular. After working on a number of NSTAC reports he said he understands how much time and effort they take and thanked the Members and their staff.

Ms. King said the NSC is thinking about the conceptual framework and how it relates to P-CAST, NIAC, NSTAC, and the enduring security framework. She said they have many different advisory groups and are considering how everything relates and conceptually comes together. She noted they spend a lot of time discussing the different work streams. Ms. King said once the President makes a decision, the NIAC can anticipate that there will likely be a similarity in taskings between themselves and NSTAC. She said the NSC hears from many sectors that there are other key people that may not be CEO-level, but could be the CIO or CTO and have a huge role within their sector. The NSC is interested in how the framework relates to those very important, non CEO-level leaders.

Ms. Lau told Ms. King that was the reasoning behind the NIAC recommendations changing from CEO-level leadership to senior-level/executive level. This permits flexibility, because the sectors and titles differ. Ms. Lau provided an example that in the Transportation Sector there may not even be a CEO, instead there is a general manager. She said the point was to ensure those individuals who can allocate resources were present. Ms. Lau stressed the Council wants action, but that is only possible with resource allocation.

Dr. Scott said that while technical expertise is extremely important, those individuals who are framing policy and directing resource allocation are those that are truly needed. Dr. Scott added that the Working Group is very cognizant and had a round discussion this morning about the differences between sectors.

Ms. Lau thanked Mr. Krebs for his very specific feedback and urged the NSC to do the same, especially since the Council receives its tasking from them. She added that her understanding is it can come from any department, but must come through the NSC. To the extent that they have very specific questions they would like assistance from the NIAC, the more focused the questions are, the easier it is for the NIAC to respond in a timely manner.

Ms. King thanked Ms. Lau for her helpful feedback. She said the NSC took the recommendations that came out of the NIAC's last study that was just briefed. She added that she hoped the Working Group will see a much more focused tasking moving forward, upon any decision-making made by the President.

Ms. Lau stated she would like to make some comments as a CEO, as opposed to the NIAC Chair. She said Mr. Parker knows the Working Group talks a lot about small companies, and having herself come from a small company and representing one, she always wants to make sure that is front and center in all of the NIAC's views as well. On the cyber side, she mentioned as Mr. Wallace pointed out, they are trying to look for what is most critical for the nation. Ms. Lau referred to the Electric Sector, small companies have been benefiting through the larger companies' work. She pointed out they now have a cyber mutual assistance group that has been stood up. She said because of the recognition, some of the large companies have the capabilities to analyze and counter or cease an attack, should one occur. She said if information sharing networks can be built within an industry, small companies can join. As of today, she believes 80% of the electric gird is represented in the cyber mutual assistance group. It is modeled after their regional mutual assistance group that came up around physical disasters like hurricanes or other storms. If any one company is attacked, regardless of size, there is now a network where all cybersecurity experts within the electric companies can immediately go for assistance from other companies. This can also include the creation of preexisting agreements, as far as cost sharing, depending on whose resources are actually used to facilitate mutual assistance. Ms. Lau said that is a good example of how large companies can help, a trickle-down effect can help smaller companies as well. She added then, the issue must be attacked on multiple levels, so it is not only at the attack level. Ms. Lau said a lot can be done by getting greater cyber awareness and cyber hygiene, which is included in much of the work DHS does. She explained NIAC is helpful in the areas that cross over, where it cannot necessarily be addressed within a single agency. Ms. Lau made one other comment to Ms. King on resource allocation. She believes much of what Mr. Wallace presented does not necessarily require additional resources. She clarified that the Working Group is saying they need resources to address this issue, but the resources actually already exist within the agencies and companies. She referenced when the ESCC was revamped; a lot of the companies involved committed resources. They did not increase resources, because it was a matter of resource allocation and prioritization within the companies. She believes there are likely existing resources that should address these issues, but they need to be prioritized so they get allocated to the cyber issues.

Mr. Terry Boston made a comment, referencing his work on both Hurricane Katrina and Sandy. He said the mutual assistance program in the Electric industry was very effective. Unfortunately, he said the resource allocation is not strong in the case of cybersecurity. He said 6,500 electrical workers were called during both events. Mr. Boston added that the defense industry that supports the Department of Defense has huge resources and he suggests the NIAC start thinking about how there are individuals trained in cybersecurity that could aid industry in the critical infrastructure area. Those individuals are often well-trained and have the appropriate clearance level that could work on Emergency Medical Services' supervisory control and data acquisition systems (SCADA) and communications systems.

Ms. Lau thanked Mr. Boston for his comment and added that is what the Working Group would hope to do with respect to cyber, is draw both from private sector and government. She said there absolutely would be more opportunity to discuss and ask some questions. She reminded everyone the slide is just a draft to identify who the key people are that would be necessary to bring to the table. She thinks the Working Group would say though that adding others may dilute the focus. She said there are some very strong thoughts behind this particular slide and they are happy to discuss those in other meetings as well. Ms. Morrison thanked Ms. Lau.

There were no further questions or public comments. Ms. Norris provided a reminder that written comments can still be submitted for consideration of the Council through www.regulations.gov.

Public comments are accepted for thirty days after the meeting.

The Council voted upon and unanimously approved the Working Group's report from both work streams, including the addition of the draft slide: Private-Public Structure for Securing U.S. Cyber Infrastructure.

VII. Critical Infrastructure Presentation

Ronald Hahn, Executive Vice President, AECOM

Ms. Lau introduced Mr. Ronald Hahn and he thanked the Council for inviting him to speak.

Mr. Hahn explained that AECOM is a very large, multi-million dollar, Fortune 250 company. He said his job in the resiliency, recovery, security aspect of that can be challenging. He noted security and resiliency tend to be an afterthought. In the conceptual stage of construction, and sometimes not even in the design stages, he does not think there is much thought into making a structure secure and resilient. Oftentimes, he said he is brought in while construction is underway to help companies figure out how to make a structure secure. Mr. Hahn said it is easier to "design-in" security. The second aspect he does not believe is usually considered is what he calls, "converge resiliency". Mr. Hahn describes this as looking at digital, physical, and wireless domains in an integrated fashion. He saw components of this in the NIAC's Water Sector Resilience Report. A second endeavor AECOM has tried to overcome is being able to not just secure data, but move it wherever and whenever necessary. Mr. Hahn discussed how oftentimes larger companies tend to break down into silos. He said he can always find an individual at a given company who is in charge of digital security, but never someone in charge of wireless security.

Mr. Hahn referenced the NIAC's first recommended future focus study topic, asking the question of how to incorporate resiliency into Federal planning and capital programs. He noted that any Federal capital program is going to be designed and built by an institute similar to AECOM. Mr. Hahn recommended advising building in resilience at the conceptual stage. He thinks the security on physical issues is great, such as preparing for a hurricane. He does not believe the country has the same capabilities on digital terrain. He believes they are national level issues that need to be executed at the state and local levels. In order to get to those stages, the country needs to figure out who has responsibility and what tools and resources are available. He noted it is difficult to draw boundaries along a digital environment. Mr. Hahn stressed the urgency of understanding the physical and logical boundaries. He said he completely agrees with the NIAC's recommendation of a P3 and also believes it needs to be improved, but the government side "does not know how to do it." In addition, he supported the inclusion of insurance, because it is currently an ineffective risk transfer for most companies in cybersecurity. The policies are not broad enough, but he also noted that no one knows how to categorize it enough to drive actuary tables.

Moving forward, Mr. Hahn recommended the NIAC consider leveraging captives. He believes they are a great tool for transferring risk, or improving and incentivizing better cybersecurity framework and practices. Then, instill best practice methodology. On the Federal side, there are ways to create tax incentives and other things that would encourage companies to drive better practices. He noted the CEO drives resources. Mr. Hahn admitted that while he can drive a compelling argument, he cannot make a decision for the entire company. He thinks the construct the NIAC came up with is important because of that top CEO tier. Mr. Hahn also agreed with the NIAC's assertion that while the cyber community is making progress, it is still not keeping up with the threat.

Mr. Hahn discussed the amount of data available in the world, data centers, and the movement of data. From a resiliency side, he is looking at a concept called, "integrated data delivery of the edge" of moving data centers out to substations and having that data localized. He said they can be used to drive costs out of the direct power. He also suggested housing data in utilities, which would make it more resilient, reduce costs, and improve services. Mr. Hahn believes consequences to adversaries needs to be more significant and more expensive.

Mr. Hahn believes resiliency and security should be a requirement at the "front end". He said he is trying to incorporate this into AECOM with dual-use technologies, which also become revenue streams. The challenge he sees with the private sector is viewing security as a cost, because it takes away from the "bottom line." He said they have to drive incentives and think about them at the concept phase of development. He believes a cultural change is required to get ahead of the curve, without it he believes the country will struggle. Mr. Hahn's last point was how much he appreciated the mention of ports, because there is so much dependence in ports. He thanked the Council for having him.

Mr. Parker asked Mr. Hahn from his perspective as a "bigger player", if he believes there should be a certain level of compliance met by companies and compared it to requirements set by the automotive industry.

Mr. Hahn liked his comparison and noted that technology is closer to autonomous vehicles than one would think. He said when it comes to those kinds of vehicles, the question Mr. Parker posed becomes incredibly important. Cars are required to pass safety inspections, but he said resiliency also needs to be a standard. He stressed that the country has to view safety and security as an integrated requirement.

Mr. Parker continued that the car industry is well-regulated and asked if there should be different avenue checkpoints to ensure the creators of software are making sure the software cannot be used in malicious ways.

Mr. Hahn said there is no simple solution of "one policy fits all." He thinks it needs to be analyzed through a sector by sector approach of what requirements are out where and what framework will be used. He provided an example of the healthcare industry where doctors are using technology (such as an iPad) to directly interact with patients. He said it would not be difficult for an adversary to cheaply and quickly compromise and disrupt service to hospitals, with a delayed time of potentially five days before they were even able to identify the problem. Mr. Hahn said Wi-Fi is one of the easiest systems to conduct electronic attacks against. He continued that there is no policy for that and barely an understanding of when a system has been compromised. He went back to his health industry example and explained that the doctor he talked to said people might die if that were to happen. Mr. Hahn said he was not sure if there was a universal answer, but believes there should be a better understanding of the capabilities of an adversary and if something could be put in place to avoid a disaster.

Dr. Scott said when one defines infrastructure, there are three dimensions- physical, cyber, and workforce. She asked when companies do asset management, should there be a minimum requirement of updating all software. She suggested that the “basics” may be more profound than they imagine. She referenced the effort, “See something, say something” and compared its use to cybersecurity and said she did not think anyone had conceptualized something equivalent for cyber risk.

Mr. Kolasky asked Mr. Hahn how he has avoided the argument that thinking about cybersecurity on the front-end slows down the development process of infrastructure.

Mr. Hahn told him the cultural change is ongoing. Thinking about it on the front-end is unfamiliar and challenging. He said he and his CEO constantly remind their team the challenge is innovation typically does not come out from the industry that is leading. Those who are the best may have little reason to change, but that is also a quick road to irrelevancy. He said it is more expensive to work differently. He does not believe it is slower to incorporate cybersecurity into the front-end, because the end goal is always completing the project. Mr. Hahn said it is more expensive and time consuming to correct mistakes, rather than just building in cybersecurity from the beginning. He believes if it is built into the front-end, the project can be built more effectively, more efficiently, and faster. The cultural change comes from companies not being used to performing in that order.

Ms. Lau added that all industries are being changed by technology, but she agreed with Mr. Hahn that many innovators come from outside of industry. Critical infrastructure mainly focuses on safety and security, but she said innovators do not think that way.

Mr. Patil asked Mr. Hahn if he had any comments about the increasing shift to artificial intelligence and the manipulation of data and the impact that has.

Mr. Hahn said machine learning tools are incredible and if they are brought into the front-end, they can be very powerful and effective, but much more challenging to leverage if brought in after the fact. Looking at data manipulation and data analytics, he believes it can be applied to discover new ways to generate revenue, which is what matters on the commercial side. He said there are areas to leverage that technology to change the way resiliency and security is seen and to improve the customer’s experience (or whatever service being provided) and to implement good procedures, but not be viewed as a cost.

Mr. Patil thanked Mr. Hahn for his explanation. He asked what happens to infrastructure when people start to manipulate it. He provided an example of body cameras and the possibility of using technology to show something completely different than reality or create distrust within the system. He wondered if the community was beginning to not just consider the breach of activities, but adversaries undermining them.

Mr. Hahn said whether data is exploited, manipulated, or denied; all three of those realms should be considered. He said as new technologies emerge, the ways in which it could be compromised also must be considered. Mr. Hahn said while he does not have an answer, he does know that adversaries will be analyzing new technology to discover how to use it to their advantage. To mitigate threats, he suggested industry be thinking in the same manner as new technology advances.

VIII. New Business

Constance H. Lau, NIAC Chair

No recommendations of new business.

IX. Closing Remarks

Constance H. Lau, NIAC Chair

Elaine Duke, Deputy Secretary, DHS(invited)

David Hess, Senior Official Performing the Duties of the Under Secretary, NPPD (invited)

Robert Kolasky, Acting Deputy Under Secretary, NPPD (invited)

National Security Council

Ms. Morrison announced this was her last QBM and thanked the Council and Ms. Lau and Dr. Scott for their leadership. She said the recommendations the NIAC make directly contributes to the critical infrastructure security and resilience and helps inform the President, Federal departments, and agencies. She noted it was National Public Service Recognition Week and wanted to thank the Council for the service they provide to the American public. They help contribute to the overall national security. She also recognized the DHS staff that supports the NIAC. Ms. Morrison said as she returns to her day job as a Coast Guard Commander, she will be taking those lessons learned with her.

Ms. Lau thanked Ms. Morrison on behalf of the Council for being their liaison to the White House.

Mr. Kolasky said he hopes the Council recognizes that the administration level within DHS is committed to continuing to work with the NIAC. He said he is happy that while the administration has changed, the importance placed on the mission of critical infrastructure security and resilience has not, which has been made clear by the White House involvement and questions by Secretary Kelly. With NPPD, he said they will continue to do the things he thinks DHS owes the NIAC, be effective stewards to make sure the NIAC's work gets done in a way that can serve the broader inter agency role and purpose and help to get policy context and interworkings of government context that will help keep recommendations relevant. Then, once those recommendations come, work with NSC to ensure there is a policy process and follow-up process to drive implementation. He sees DHS as a facilitator to make sure the work completed meets the needs of the administration and NIAC is being treated professionally. He said he looks forward to continuing to work with everyone.

Ms. Lau thanked Mr. Kolasky for ensuring the work of the Council continued through the administration transition.

Dr. Scott thanked everyone that supports the NIAC and said it is an honor for them to serve.

X. ADJOURNMENT *Constance H. Lau,* NIAC Chair

There being no further business, Ms. Lau adjourned the quarterly business meeting.