NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

QUARTERLY BUSINESS MEETING AGENDA

September 16, 2016
1:00 PM –4:00 PM EDT
1310 N Courthouse Road, Arlington, VA 22201
Department of Transportation, 3rd floor

I.	**OPENING OF MEETING**	*Ginger Norris*, Designated Federal Officer (DFO), National Infrastructure Advisory Council (NIAC), Department of Homeland Security (DHS)
II.	**ROLL CALL OF MEMBERS**	*Ginger Norris*, DFO NIAC, DHS
III.	**OPENING REMARKS AND INTRODUCTIONS**	*Constance H. Lau*, NIAC Chair *Caitlin Durkovich*, Assistant Secretary for Infrastructure Protection, DHS *Suzanne Spaulding*, Under Secretary, National Protection and Programs Directorate (NPPD) *Stephanie Morrison*, Director, Critical Infrastructure Protection Policy, National Security Council (NSC) (invited)
IV.	**APPROVAL OF JUNE 2016 MINUTES**	*Constance H. Lau*, NIAC Chair
V.	**PERSPECTIVES ON CYBER SECURITY AND FUTURE FOCUS AREAS**	*Suzanne Spaulding*, Under Secretary, National Protection and Programs Directorate (NPPD) *Elena Kvochko*, Technology and Cyber Security Strategy Implementation Executive at Barclays

	PERSPECTIVES ON CYBER SECURITY AND FUTURE FOCUS AREAS *Continued*	*Stephen E. Flynn*, PhD Professor of Political Science Professor of Civil and Environmental Engineering (affiliated) Director, Center for Resilience Studies Co-Director, George J. Kostas Research Institute for Homeland Security Northeastern University
VI.	**Status Update on Past NIAC Recommendations**	*Nancy J. Wong*, Former NIAC DFO
VII.	**Status report of New Working Group**	*Joan McDonald and Mike Wallace*, Co-Chairs of Future Focus Study Working Group
VIII.	**Open Discussion and Public Comment**	*Ginger Norris,* DFO, NIAC, DHS
IX.	**Closing Remarks**	*Constance H. Lau*, NIAC Chair *Caitlin Durkovich*, Assistant Secretary for Infrastructure Protection, DHS *Stephanie Morrison*, Director Critical Infrastructure Protection Policy, NSC
X.	**Adjournment**	*Constance H. Lau*, NIAC Chair

NIAC MEMBERS PRESENT IN ARLINGTON:
Mr. Jack Baylis, Dr. Georges Benjamin, Senator Jeff Bingaman, Mr. Robert Carr, General Albert Edmonds, Mr. Ben Fowke, Mr. George Hawkins, Ms. Constance Lau, Ms. Joan McDonald, Mr. James Murren, Mr. Keith Parker, Dr. Beverly Scott, Mr. Michael Wallace

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Ms. Jan Allman, Ms. Peg Grayson, Ms. Diana Bolt Perreiah, Mr. Jim Reid

MEMBERS ABSENT:
Mr. Rand Beers, Mr. David Grain, Mr. Philip Heasley, Mr. Bruce Rohde, Mr. Tom Noonan

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

SUBSTANTIVE POINTS OF CONTACT OBSERVING VIA CONFERENCE CALL:
Mr. Nathaniel Millsap with Ms. Jan Allman

OTHER DIGNITARIES PRESENT:
Ms. Suzanne Spaulding, NPPD, DHS; Ms. Caitlin Durkovich, IP, DHS; Ms. Stephanie Morrison, NSC; Ms. Monica Maher, NSC, Ms. Amy Rosenband, NSC

I. OPENING OF MEETING

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

II. ROLL CALL OF MEMBERS

Ginger Norris, DFO NIAC, DHS

Ms. Norris opened the meeting and called the roll. She reminded everyone that this meeting is open to the public and to exercise care on matters that are sensitive. Ms. Norris then gave a brief history and overview of the NIAC. The Council provides the President, the Secretary of Homeland Security, and other leadership advice on matters of security and critical infrastructure that support both the public and private sector. Ms. Norris then informed the attendees that the floor would be open for public comment during part six of the agenda as explained in the Federal Register Notice. She asked anyone who would like to make a public comment to submit a request to the Secretariat staff. Ms. Norris then turned the meeting over to Ms. Constance Lau, NIAC Chair.

I. OPENING REMARKS AND INTRODUCTIONS

Constance H. Lau, NIAC Chair

Caitlin Durkovich, Assistant Secretary for Infrastructure Protection, DHS

Suzanne Spaulding, Under Secretary, National Protection and Programs Directorate (NPPD)

Stephanie Morrison, Director, Critical Infrastructure Protection Policy, National Security Council (NSC) (invited)

Ms. Lau welcomed everyone to the NIAC's third quarterly business meeting (QBM) of 2016. She then announced that the NIAC will not be having a fourth quarter meeting because of the Administration Transition. She said they do have a Working Group that has taken up the latest tasking from the White House and they will continue working at full speed until the next QBM. She then welcomed two new members of the NIAC, George Hawkins who is the General Manager of DC Water and Sewer Authority, as well as Jeff Bingaman who is a former United States Senator from New Mexico. The Council is also expecting a third new member, Rand Beers, who is a former Under Secretary of the National Protection and Programs Directorate at DHS. Ms. Lau then welcomed Ms. Stephanie Morrison who is the NIAC's liaison to the White House and Ms. Caitlin Durkovich who is the Assistant Secretary for Infrastructure Protection at DHS. She said they are also expecting Under Secretary Suzanne Spaulding. Ms. Lau also welcomed the former DFO Ms. Nancy Wong and announced that Ms. Ginger Norris would now be taking full DFO responsibilities and will no longer be the alternate.

Ms. Lau said at the NIAC's last meeting, which took place in Los Angeles, they approved the Water Study with minor edits to the draft. The report is now on the NIAC's website. She said they have also received their next tasking from the White House, which is a future focus study. They will look at what topics the Council should look at in the new Administration, specifically a cyber study that would be done in 2017. This Study will be Co-Chaired by Ms. Joan McDonald and Mr. Michael Wallace. She said they will give a briefing at part 7 of the agenda. This meeting is the official kick off of the Working Group and they expect to complete the study in May 2017. She said that at the meeting there will be three presentations on cyber security as part of this study. She announced that other members who would like to join the Working Group are still welcome. She then turned the meeting over to Dr. Beverly Scott, Vice-Chair, who welcomed everyone and said she was looking forward to the study. Ms. Lau then invited Assistant Secretary Caitlin Durkovich to give opening comments.

Ms. Durkovich thanked the Members of the NIAC for their participation in this important Council and the great work they are doing and have done over the years. She said her office takes the reports and recommendations of the Council very seriously and looks for how they can be implemented. The reports also inform their strategic thinking for policy efforts. She said she had the privilege of swearing in two new Members earlier in the day and is delighted to see the Council grow. She thanked Ms. Morrison for helping to get the NIAC up to its full membership capacity. Ms. Durkovich then said that this would be her last NIAC QBM since she will be leaving her office on January 21, 2017. She said it has been a great seven years and they have accomplished a lot. She thanked the Council for the privilege of working with them on the topic of infrastructure security and resilience. She said she thinks the timing of this Future Focus Study is right given all the work that has been done over the past seven years, and how they can continue to evolve the reports and recommendations. She thanked Ms. McDonald and Mr. Wallace for their leadership on this study.

Ms. Durkovich then said she would like to briefly comment on the Strategic Infrastructure Executive Council report (March 2015) because she knows there is a lot of interest in how the Federal government is working to implement that recommendation. She said two QBMs ago, she gave advice on how to move forward based on the success of bringing the Electricity Sector to the table. She said she thinks having industry self-organize and then bring itself to government counterparts to build that trusted relationship and start developing the work plan is the best course of action. She said that it is happening, which she has verified through talking to industry representatives. She said she continues to advocate raising awareness about this report and recommendation at every opportunity she has. She said it is important to understand how these lifeline functions intersect and the importance to elevate the conversation to create frameworks for security and resilience of these lifeline sectors.

Ms. Durkovich then commented on the Water Sector Resilience Report. She said it was great to go to Los Angeles and it was a great meeting overall. She said she felt that the NIAC leaving Washington DC was great and she recommends that they continue to do that. She said the report is currently sitting on Secretary Johnson's desk and it will be signed and transmitted to the President very shortly. She said they have already begun conversations with the Environmental

Protection Agency about doing an exercise similar to "GridEx" in the Water Sector to test some of NIAC's recommendations. They plan to do that in spring 2017. She said she was looking forward to the guest speakers at the QBM and hearing from them about the future studies. She said the degree to which NIAC can continue to provide recommendations on critical infrastructure to the new Administration is very important. She said over the past four years, she has learned there is not one department, agency nor jurisdiction that owns infrastructure. She said she would recommend the Council identify who they see as taking the lead in implementing their recommendations, which the Water Study did a great job of. She said the diverse and diffuse nature of infrastructure development makes it complicated.

Ms. Durkovich also applauded the Council for looking at cyber.. Though there are a lot of groups and committees focusing on cyber, she said the events that happened in the Ukraine in December 2015 where there was a remote attack on the power system that resulted in the power grid being impacted underscores how cyberattacks can affect the physical functioning of critical infrastructure. She said another conversation they have been having is how to evolve the infrastructure workforce. She said in the rush to digitation, they cannot take out the human element. It is very important to the resilience of critical infrastructure. She feels how they talk about that moving forward is important as well. She thanked the NIAC for coming together for meetings on a quarterly basis and the work they do in between meetings while juggling their full time jobs. She said working with them has been one of her greatest privileges.

Ms. Lau thanked Ms. Durkovich for her remarks as well as her work in getting the Council's recommendations accepted. Ms. Lau then invited Ms. Stephanie Morrison to make opening remarks. Ms. Morrison welcomed the newest members of the NIAC and thanked Ms. Durkovich and Ms. Lau. She thanked Mr. Baylis for his leadership on the Water Report. She said it was a fantastic product and looks forward to exploring those recommendations further. She then introduced two of her colleagues at the NSC, Amy Rosenband who is the Director of Hazard Mitigation and Risk Reduction Policy and Monica Maher who is the Director of Cyber Security Policy. Ms. Morrison said she is looking forward to working with the NIAC on their next study. She then turned the meeting back to Ms. Lau.

VI. APPROVAL OF JUNE 2016 MINUTES

Constance H. Lau, NIAC Chair

Ms. Lau said the minutes from the June 2016 meeting had been distributed to the Council and could also be found in their folders. She said that there are some typographical errors that need to be fixed. She asked if the Council Members have any substantive changes to the minutes. There were none. The Council voted to approve the minutes.

VII. PERSPECTIVES ON CYBER SECURITY AND FUTURE FOCUS AREAS

Suzanne Spaulding, Under Secretary, National Protection and Programs Directorate (NPPD)

Elena Kvochko, Technology and Cyber Security Strategy Implementation Executive at Barclay’s

Stephen E. Flynn, PhD
Professor of Political Science
Professor of Civil and Environmental Engineering (affiliated)
Director, Center for Resilience Studies
Co-Director, George J. Kostas Research Institute for Homeland Security
Northeastern University

Ms. Lau said the next agenda item is to obtain perspectives on the upcoming Working Group report. The speakers represent government, the private sector and academia. The first speaker was Dr. Stephen Flynn from Northeastern University. He said critical infrastructure is something that they all share a passion for. He said that while he and the Members have had the opportunity to watch infrastructure be built up, children are watching it fall. He gave examples of power outages, bridge collapses, levee failures, etc. He said what is so important about the NIAC is the need to look at the cross-cutting nature of infrastructure. He said there is not one place to go to in the US government to address this, but the NIAC has served an important role in raising awareness of interdependencies and he looks forward to their future focus of integrating cyber throughout. He said his focus is on resilience, particularly the functions that infrastructure provides. He said resilience is a continuity of function in the face of risk. He said he had read an article that in the post-World War II era, Americans became convinced they could eliminate risk if they put enough money, intellect and muscle at it. He said one of the downsides is that they stopped being good at dealing with risk as it manifests itself. He said risks are a fact of life and they need to be able to adapt and recover to risks when it manifests. He said what they do before events happen, as well as post-event recovery are elements of resilience. He said adapting is very important for when things “go bump in the night”. Dr. Flynn said he is a retired Coast Guard Officer and often looks at things from a security perspective. He said when he looks at resilience and security, they have moved away from the concept of a threat centric approach to a resilience centric approach. Dr. Flynn said we largely approach critical infrastructure in the post 9/11 world by getting over a threat. He said they have to be prioritized by what is threatened and that is based primarily on intelligence. Next they have to prioritize whether or not it is vulnerable and consequential if it was hit. If that is the case, it becomes a priority. He said if they take the basic distillation of having the intent to cause harm and having the capacity to cause harm, they can make decisions. For example the French have nuclear weapons, but no intent to use them so they are not a threat. Threats are when intent and capability come together. He said critical infrastructure is threatened because “it is easy to do and you get a big bang for your buck”. That is what motivates an asymmetric threat against infrastructure. He proposed moving toward a resilience centric approach which looks at what it is truly critical, lower its vulnerability and lower its consequence if it is hit. If something is harder to compromise, they need more capability, meaning less people can do it. If it is hit, “it is a fizzle not a bang”, which takes out the consequence which results in taking out the intent. Therefore, there could be deterrent value in investing in resilience. He said the key is that they could drive the threat down by investing in resilience in infrastructure. He gave an example of the Oak River chemical supply that took out water for 300,000 people in 2004. He said that it had been missed that there were very nasty chemicals right next to the fresh water supply that had a containment wall that was not in very good shape. They had no intelligence to tell them anyone was targeting such systems, but he said if they had inventoried what is critical, vulnerable, and consequential, it would have been spotted and safe guarded. The resilience-centric range is there. Another miss was Hurricane Sandy. Governors and Mayors were very concerned that there would not be enough gas at the gas pump, but there were bigger problems with Sandy. The problems with Sandy were that the metro-NY area uses about 42 million gallons of fuel every day, 60% comes in by port, 20% by pipeline and 20% by refineries. When Sandy hit, the port was closed. There was major damage to two refineries in Newark, and the one in Philadelphia was shut down. The pipeline lost power in the compressor station and was damaged, so that supply was lost too. Initially, no one had that big picture. He said New York is the number one target for terrorist attacks, yet the fuel supply issues were only discovered because of a hurricane. He said infrastructure is not being looked at as a system of interdependencies in advance.

Dr. Flynn said he has yet to meet people who are against resilience. He has asked if people are not against resilience, why is the country not resilient. It is because there are barriers to getting there. He said that should be a focus of effort rather than looking at infrastructure and giving reports, he said they should look at why there is not investment. He said first there is the problem of overconfidence. Americans are very confident in the country’s ability to manage crises. He said there is complacency and it is fueled by the desire to reassure the public. He said they need to “walk a line” between panicking and being “adult-like” and talking about it. The challenge of building and investing is because a lot of people dismiss the risk, an example is climate change. In addition, avoiding costs is always a goal, but infrastructure has costs. He said there is clearly a lack of an integrated approach, resilience work has been largely sector specific. He has been in a number of academic settings dealing with this and talking to the national labs. He said they do not want to talk about interdependency until they have a complete understanding of every sector, and then never get around to talking about interdependency. He said the other scenario is hazard groups who see risk before they see interdependency. They feel that they need a complete understanding of various disasters such as hurricanes, before they talk about infrastructure and interdependencies. He said especially in a post 9/11 world, all threats become “road maps to bad guys”. He said in reality people are not applying resources and effort into problems they are not aware of. He said incentives are in the opposite direction of resilience. He said in the context of bringing more efficiencies and bringing costs down, they are struggling. However the transfer of risk is where there is mastery, such as buying insurance. This approach of “don’t blame me” needs to be wrestled with so they can come to a point of establishing standards that can be promoted. He said these are the areas that need to be focused on.

Dr. Flynn said the next problem is organization, noting that the NIAC is one of the few groups that weave everything together to see the big picture. He said it needs to be replicated at the metro-regional level. Taking it on at the national level is too abstract, and does not take into account that the power grid is North American and not just for the USA. This also applies to ports, which are connected to other ports overseas. These are examples of the multi-jurisdictional nature of infrastructure and the government goes with that. He said most infrastructure systems fall into multiple jurisdictions, but all the sectors have different jurisdictions. For example, the water system in Boston has a 60 mile radius, but with power, it goes into Canada, while transportation also involves Rhode Island and New Hampshire. He said largely the response has been to do studies, but he said action will not come out of these studies if it is not recognized that governance frameworks do not work the way infrastructure works today, especially when it comes to interdependency. Lastly he said that academia and the workforce are not educating and training people the way they need to. He said academia wants to stay in its stovepipes despite this being an interdisciplinary challenge.

To conclude his presentation, Dr. Flynn described an experience he had in which he received funding to examine the flooding in South Carolina last year. He said there would have been a common outcome if he went to Baton Rouge, LA last month. He said about six weeks after the SC event, he went down and spoke with state and city officials in the metro-Columbia area. He told them that he thought that they had a water shed infrastructure program that failed under this deluge, but they did not even know they had a water shed infrastructure system until it failed. They thought they had a water treatment plant, dam, etc. They did not see it as a system until Mother Nature pushed water through the water shed and impacted the infrastructure sectors. He said this is a system they have to organize, which is not a science or engineering challenge. Before he went down to SC, he researched how many dams were in the state. He could not find an answer. When he went to the SC office that oversees dam safety, they did not know either and relied on media estimates. Most of the dams are privately owned and there are no regulation requirements. Therefore, they were not aware of the dams until they started to fail in many instances. He said they cannot get their arms around infrastructure without mapping out what it is. The direct impact on this is they do not know where the resources are. Lakes could have been lowered with 24 hours' notice, but there was no communication. During an event they need to prioritize capabilities where there would be the most cascading effects, but the emergency manager does not even know where they are. After the event, they need to decide what is most important to focus on for recovery, but they do not know what is most important ahead of time. He said these are warning signs from Mother Nature saying that infrastructure should be understood as an integrated system and be organized in dealing with that. He suggested that this should be a key focus for the NIAC. He said he wishes the country was better at doing things before things go "bump in the night". The country has mastered responding, but infrastructure will abate because of these disasters. Disasters command attention and resources. He said that the country could rebuild better and smarter, and while it is not the best strategy to let things fail before they are made right, it creates the opportunity when they fail to draw attention to the challenges that were revealed. However, there is no organization to do that, "humpty dumpty" is just put back together again, placed back on the wall and hope it will never happen again. The focus of resilience is thinking about the recovery the morning after. Currently, when FEMA responds to a disaster with Stafford checks, and someone says they want to build something better, there are no criteria or tools to do that. He said it should be a focus that when things break to use it as a time to invest smarter, and have those tools and criteria available for communities to rebuild and go forward. He reiterated that he would like the NIAC to go forward with this, and thanked the Council for their time.

Ms. Lau then opened the meeting for any questions for Dr. Flynn. Mr. Parker said that this fall there will be over $200 million in tax measures to increase public transportation for cities around the country. He asked if Dr. Flynn views that as cause for concern or celebration. Dr. Flynn said that the fact that is happening at the local and state level is hopeful because democracy works best from the bottom up. He said the fact that these are Federal impacts is a continued worry, but the fact that some communities living with failing systems are willing to pay more is important. He said at the national level, this is a security imperative similar to how President Eisenhower made the case for building the national highway systems. He said if they are truly worried about the asymmetric threat and terrorists, this is another reason to step up to the plate. The primary reason is that it is necessary for the economy and the way modern societies work. He said an additional case could be made, that the NIAC could enforce, is that their mission was largely impacted by the security protection imperative. He said he hopes that even those who are wary about making those investments share the view that security and safety is a core function of government. Senator Bingaman then asked Dr. Flynn if he could elaborate on the distinction between resilience and sustainability. Dr. Flynn said they are very closely related. He said engineers define resilience as designing things to withstand a risk, while sustainability is about recovery and adaptation. Neither want the system to fail. They are complementary, with resilience as overarching while sustainability is an important element where they deal with the interface between the natural environment and the built environment. Sustainability gives a lot of guideposts, but the overarching priority for societal resilience involves building individual community resilience, infrastructure resilience, networks and systems and largely national resilience as a key element. It is an ambitious agenda on the resilience side. In addition, there is a competitiveness issue as well. At the end of the day people have a choice of where they will invest and where they will live, and if risk is the constant in the 21st century, people will gravitate to the communities that are most resilient. In terms of security, this is how communities lose people. He gave an example of Seattle, which has earthquakes but is also the headquarters of Microsoft and Amazon. He asked if they would stick around after an event if the country cannot get itself back together in 3-4 months. If there is not knowledge-based capital for recovery, people will leave. Dr. Flynn concluded his presentation and Ms. Lau thanked him.

Ms. Lau then introduced the next speaker, Ms. Elena Kvochko, who will be giving a private sector perspective. She is head of global security strategy and implementation at Barclays, which is an international banking and financial services company. Ms. Kvochko thanked the NIAC for the invitation and said it was a big honor to share Barclays' perspective and to hear from the Council. She said it has been impressive to see the government collaborate with the private sector on cyber security. She said Barclays is a global financial institution with 15 million clients, 130,000 employees and operates in 50 countries. She said financial services is one of the oldest industries, but also one of the most disruptive industries. Barclays Bank is 325 years old.

In terms of the meeting topic, Ms. Kvochko said that for a lot of the threats in the landscape, despite significant progress to address them, most companies are still relying on their own cyber security controls. However, Barclays is not only investing in the cyber security controls of their clients, and partners, but also the ecosystem and they are sponsoring research efforts, academia and other various institutions. Barclays is eager to engage in forums to advance the agenda on issues of cyber security. She said for many years, while infrastructure was built, most of the priorities were made on openness and functionality and security has been left behind. This understanding is now changing and there are efforts to "go back in time" and fix the technical deficit that companies have. In addition, the rise of cloud computing, people bringing in their own devices, and increasing reliance on third party vendors and suppliers dramatically changed the infrastructure ecosystem. She said the threats now differ greatly from the traditional threats they have gotten used to. She said in a traditional understanding, a threat is something they would expect the government to protect them from and rely on law enforcement institutions, however that does not work with cyber threats. Anyone who has access to the internet can perpetrate a cyber threat. In addition, crimes that were previously linked to certain geographic areas now no longer have those limits. She also said until now there have not been any international norms or guides of how to deal with these threats. Everyone is on their own. She said lastly there is the topic of "crime as a service". The financial sector has been the backbone for a lot of industries, and the attacks on the financial sector can have cascading consequences for all other sectors as well. She said they have seen an increase in the sophistication of threats against financial institutions. Personally identifiable information is matched together from data on social media through data dumps and big data analytics and is used to design and target attacks. As organizations harden their perimeter, there have been more cases of employees inside the network becoming threats. Whenever a cyber-attack is designed, profit and risk are taken into consideration. Right now cyber-crime remains a very low risk, high profit effort. There are a lot of incentives for many individuals to join the field, but Barclays hopes to work with the government to reshape those incentives.

In terms of what an institution can do to mitigate this threat, Ms. Kvochko said they focus on several areas. First is a robust cyber security strategy that lays out what they will do in a case of a breach, instead of reacting to what has happened already. She said it is also important for all institutions to do business securely which is very expensive and likely a roadblock. There is increasing spending across the industry. Companies face challenges in hiring qualified staff with the right expertise as well as investing in the skills of current employees. She said they are also focusing on education and awareness, not only of their own employees but everyone who touches their network such as stakeholders, vendors, suppliers, etc. Lastly she said it is important not to look at security separately but integrate it into core business operations. This means that if a private company is launching a product, they do not wait until the end to test it and mitigate the results and potential vulnerabilities. A company would design the process in a way that security is baked in from the beginning. Engineers, project managers, designers, etc. would be prepared.

Ms. Kvochko said at Barclays, they are trying to treat security holistically. In the past security was very siloed. There was a cyber security team, physical security team, resilience team, investigations team, and an intelligence team. All were functioning on their own. However, they realized as a global company in order to connect their systems, they needed to make sure that they are all connected. They were all brought together under one security function where it is harmonized and has common data and a common platform for everyone to function together. Therefor, if something happens, it can be handled by another part of the organization. She said Barclays is one of the first companies to take this holistic approach and they look forward to providing an update on how it goes. She said in addition there is an increased use of data analytics and automation technology from the attackers' side that they feel they need to match on the defenders side as well. She said for large companies, it is difficult to keep up with the alerts and potentially emerging incidents, some of which are false positives. She feels investing in automated systems that can function with limited supervision would be the direction the industry is going. They will be focused on technologies such as machine learning and artificial intelligence in the next few years. She emphasized that overall Barclays feels it is important to treat security holistically, and in addition to that financial services and banking is very dependent on the mechanisms of trust. If they do not maintain security and privacy of data for all of the customers, they are not able to maintain trust. Now, the main product that they sell to customers is trust, which means they have to prioritize security and privacy alongside convenience and functionality. Ms. Kvochko said to conclude, they are looking forward to partnering with the government. In terms of the scope of NIAC's study design, she said some areas they would like to get more help from the government is in incentives, exchanging actionable information, and be more engaged with the staff of other institutions. They are looking forward to the partnership as well as sharing what they have done to deliver this holistic cyber security service.

Ms. Kvochko then opened it up to questions. Ms. Lau asked Ms. Kvochko where she has seen government sharing be useful in information sharing and what parts of government they are getting that information from. Ms. Kvochko said a lot of the information they get is from their own network, but they also partner with law enforcement agencies to investigate certain cases. They would like to see more collaboration with the government on trying to predict what will hit companies as opposed to what has hit companies. Mr. Parker said that when they do the study that Dr. Scott had said that the NIAC should ask companies to be forthcoming about breaches or attacks. He asked Ms. Kvochko if there should be incentives for the private sector to be more forthcoming about breaches or attacks they have suffered. He said there could also be punitive measures to force them to disclose attacks and breaches. Ms. Kvochko said that she believes every company that operates in the financial space already has huge incentives to do their business securely because now customers leave if there is a problem. This is a new shift. She said in the past there was an erroneous assumption that as long as you reimburse your customers then they do not care about the breaches. However, now they do care where their personal information goes and what happens to it. These incentives are business driven. Many industries have already experienced large breaches and are trying to align punitive side with business side. Mr. Parker gave an example of the automobile industry, if the company knows they have a safety problem, they are required to bring that information forward. He asked if all private sector companies be forced to report breaches to some centrally located place so they can learn from each other. Ms. Kvochko said that is already the case in all the regulated industries. If they know of vulnerabilities, they disclose them. In terms of industries that are currently not regulated, she said it is difficult. She believes that they do share this information already, but in small circles such as companies, partners and suppliers. However, there are also a lot of changes in the third party liability side. Providers to large institutions are required to disclose this type of information. She said while this might not be the case yet in smaller companies and companies that are not currently regulated, she thinks they would benefit if this was implemented as well. Mr. Parker said if a company is forthcoming and their customers find out about it, there is an embarrassment. But if they do not bring the information forward, then other companies are more vulnerable because they cannot learn.

Ms. Spaulding felt that Mr. Parker made a very good point. She said NPPD has been working for a number of years on projects promoting a more robust cyber insurance market. They quickly realized bringing insurers and academics together allows a paucity of information that would allow insurers to understand how to build and price products. This is due to companies not being required, as well as a stigma attached. NPPD has developed a Cyber Incident Data Analysis Working Group, which has come up with the concept of a third party depository, where private sector companies could anonymously send a broad range of information. The working group has worked through what is the information that would be valuable and created a template of what should be sent to the depository. The depository would send in information about the incidents, without attribution to the victim. Ms. Spaulding said she hopes it will be available to the public. She said there is thinking going on, but it does not get to liability, incentives, shareholders etc. In addition, NPPD has established the sharing of cyber-threat indicators with anonymous and automated technology and protocols, sharing specific cyber incidents that others can use to protect themselves. It becomes the “see something, say something” of cyber. It would be similar to a BOLO alert, and everyone would know to be on the lookout for a certain IP address, for example. Mr. Parker said he thought that would be extremely useful to share the experiences of others in a safer place. He said in his industry (public transit), no one wants to confess that they have been breached. Ms. Spaulding agreed that it was critical.

Mr. Wallace asked if Ms. Kvochko if she could suspend any concern about liability issues, legal issues, privacy issues, are there any technologies or processes that could be more helpful in providing resiliency to Barclays’ assets. Ms. Kvochko said she thinks this is the way they should be looking at the future and the development of those technologies. She said looking at the past, there were a number of technologies that had a huge impact on security and resilience organizations, such as encryption tools. She said going forward, Barclays is placing a lot of emphasis on technologies such as artificial intelligence and machine learning. Companies are looking at those areas of how they use technology to augment cyber incident response to help manage the number of alerts. She thinks the second area with a lot of potential in the coming years is behavioral analytics, by distinguishing normal vs. abnormal behavior in a credible manner, will help organizations a lot. In terms of where they could collaborate better, she feels that information sharing could be a powerful area to work on, but it has to be actionable, close to real time, and it has to be specific. Otherwise the information can be overwhelming. In the financial services industry, they know that if a certain malware or tool was used to attack a bank one day, it will likely be used again the next day. She believes that is likely the case across other industries and sharing information openly would be helpful. Mr. Wallace clarified that mega data analytics is capability Ms. Kvochko believes could be helpful that they do not currently have to its fullest extent. He also asked if that could go to machine-to-machine actions to reduce the sense of threats, malware, vulnerabilities, etc. The analytics would find it and the machine-to-machine mutes it. Ms. Kvochko said that automatic remediation is the goal. Mr. Fowke said he is familiar with the financial industry's use of machine-to-machine communication software called Soltra Edge. Ms. Kvochko said she thinks it is one of many tools they have to consider, but there is no standard yet. She knows that a number of companies are working in this area, but it is hard to link the data formats because they are stored in different formats and locations. However there are now fusion databases that link all sources from different areas to try to devise insights and use them in operations and response. There are not a lot of standards in the field because it is fast developing, but investors are also looking at it.

Mr. Hawkins said he is hearing two different approaches that are somewhat in conflict. The first is that "we ought to be more common, more connected, have better practices, not do different things and be in silos." However, the security personnel at his organization (DC Water) say the opposite, "we want to be a silo, so if someone attacks the person next to us, we do not want to be connected to them, we want to be able to isolate an island and protect ourselves." One person has suggested ensuring all the analog switches still work so if all the computers go out, the plant can still run. He said they could have the best practice and spend less with everything being connected, but that means one attack that would be relevant to just one place, becomes relevant to all the places. He asked Ms. Kvochko if she was worried about connecting everything despite the fact that silos cause isolation. Ms. Kvochko said there are two important controls that need to be in place. The first is network segregation which means that if someone connects to the corporate network in one place, it does mean they can get connected anywhere. The second is management policy. It has to be tailored to the roles and responsibilities of the people who are managing and have access to various assets as opposed to everyone having access to everything. She said on the one hand, they need to have the ability to clear the data and link the incidents for this holistic perspective of security, but it does not mean they open up everything to everyone. Proper controls must be in place. Large companies have over one hundred controls on the network and end points at all levels of application. Mr. Hawkins said he understood. Ms. Maher said finance and water are two different industries. She feels that few industries can isolate themselves the way water and nuclear can. For other industries, the business model is built on being interconnected, having those technologies and also having all those threat and access vectors as a result. However, it is "woven into the fabric of all their business processes". She said she thinks it is great if they can still isolate, but she would not underestimate the points that they might have, where they actually touch some level of connectivity to other networks, through the internet. She said a lot of people are not aware that isolation is an easier capability or proposition than it used to be. Ms. Kvochko said she also thinks that many companies have their own separate networks for incident response and security communications. However, she reiterated that it does not mean everyone has access to everything, it is role based.

General Edmonds said that one size does not fit all. Now everybody is mobile and has their own device that they want to plug in and connect to the Wi-Fi. Therefore, he said they have to have security adept at different ways and times. He said it is a continuous process. Security and cyber-security is not an "end game", it is constant. With sensitive systems, there needs to be detection in place at all times and have a plan in place in case there is a hacking. There needs to be a plan to continue to operate, a plan to recover, and a strategy to detect who the hackers are so it can be reported to the FBI. Ms. Kvochko agreed. Ms. Lau said that Ms. Kvochko comes from an industry that has large organizations with many resources as well as many smaller organizations. She asked Ms. Kvochko how much she worries from a total system perspective about some of the smaller organizations and their level of cyber security and whether or not there should be programs that help them as well if they need it. Ms. Kvochko said she would answer in her personal view, not as a representative from Barclays. She said she thinks it is very hard to build a holistic security team. Barclays has 800 people working on cyber-security. However, for smaller companies, it is neither possible nor necessary to approach cyber-security in this way. She said many smaller companies may want to consider outsourcing their security team to manage risk and take care of their assets. She said she believes that it is necessary, but it is too cumbersome to build from scratch if it is not already in place. She said in terms of smaller companies being providers to larger companies, there are a number of security requirements that are imposed on those providers and they have to be met. In the past, she has seen that very often when the contracts are made, vendors or supplies would answer a “yes or no” question of whether or not they had a security program in place. If they answered yes, they were in compliance. That is no longer the case because suppliers to large institutions have to look in detail at their access policies, data retention policies, etc. They have to look closely at how they are managing their security, which is a big development in the field. Ms. Lau asked if there were any other questions. There were not and Ms. Kvochko’s presentation was concluded.

Ms. Lau then announced that the next speaker would be Undersecretary Suzanne Spaulding from DHS. Ms. Spaulding thanked the members for their hard work and said the Council’s value is very unique. Ms. Spaulding said she would be speaking about how NIAC can continue to have an impact and make sure that the time they are giving is being well used. She is supportive of the Council looking at what they should be doing differently and how they can continue to contribute. She said the expertise and insights that the NIAC Members bring are unique and there is no way NPPD can do their mission without that input. She said she is grateful they are putting time into this and appreciate the conversation that they will be having. She said she had an impressive list of all of the NIAC’s reports since 2004 and she feels the issues and topics areas they have tackled is prescient. She said would be asking her team to go back and pull all the recommendations to go back and see how they are doing, which can help inform the NIAC’s discussion especially in terms of why some recommendations have not gotten much traction. She said her team will do the same because the NIAC’s time is too valuable to provide insights and not see it get traction. She said much of what the NIAC has contributed has been very valuable and it has informed NPPD as they have gone forward and generated new program activity, making a significant difference. She said for example, in the NIAC’s sector specific studies, they built on the foundation of work they have done previously where they looked at things like regional resilience, cyber and physical convergence, and intelligence driven activities, as well as how to bring CEOs to the table. She then welcomed the new members and is excited about the areas of expertise they will be bringing to the table.

Ms. Spaulding said she would be discussing work being done at the Federal government, specifically Presidential Policy Directive (PPD) 41. She said the Federal government realized that there is not a clear picture of how the Federal government is organized to respond to significant cyber incidents. There is law enforcement, intelligence, DHS, etc. but no clarification on who does what. The President directed that they come together and put down on paper how the government was going to be organized to respond to a significant cyber incident. PPD-41 says there will be three concurrent lines of activity when there is a significant cyber incident. The first is asset response, led by DHS. Upon request, DHS would come in when there is a significant cyber incident and help figure out what is going on in the system, get the adversary out, and help rebuild the system more securely. This activity will often involve other Federal departments and agencies, particular sector specific agencies (SSAs). For example, a problem with a power substation would likely involve the Department of Energy. The second line of activity would be a threat response lead by the FBI. They will be identifying the malicious actors, and figure out how to go after the malicious actor. DHS and the FBI will work together to identify other potential victims who may be implicated by this. The FBI would be from a law enforcement perspective and DHS from preventative perspective. The third area of response is intelligence. That will be led by the Cyber Threat Intelligence Information Center (CTIIC). They will lead in making sure the intelligence community comes together to help provide a broader intelligence context to both of the other activities. To make sure all 3 are coordinated and working well together, there are two agency bodies: The Cyber Security Response Group and The Unified Coordination Group. One is primarily Federal employees, and the other brings in the private sector. It is at the White House level, bring the threat response, intelligence response and asset response together so everyone has transparency on what the others are doing. She said that is summary of PPD-41 and how the Federal government will be organized. As part of that a document, the President said he wanted a national cyber incident response plan (NCIRP) that the private sector will be a critical part of, in 180 days. A few months before the PPD was signed and published, NPPD started interacting with the private sector on this topic because they knew it was coming and there would be a short turn around. They discussed how they would work together and how the private sector would plug into all of those activities happening at the Federal level including what the private sector should and would be doing for incident response. There is representation from all 16 critical infrastructure sectors. She believes a draft will be ready by the end of September. They will then get some additional input and comments, and the end of October is the due date. She said in terms of planning, that is what is happening in cyber incident response at the Federal level.

Ms. Spaulding said they are also very busy looking at voting infrastructure in the run up to the election. They are looking at how to define election infrastructure, what the risks are, as well as the vulnerabilities and what type of assistance can be offered to states and localities. NPPD has been reaching out to states to make sure they are aware of what they can offer such as remote cyber hygiene scans that can be done on public facing parts of the network. Parts of the network and voter registration databases are often public facing. By remotely scanning, they can give states and localities very fast advice on vulnerabilities, system configuring issues, patching issues, etc. and then give remediation. The fix can be made before November. NPPD is also offering onsite vulnerability assessments and doing “red teaming” to see how far they can get into the system. However, those assessments are much more resource intensive and only a few can be done. They are focused on trying to enhance confidence in the election infrastructure from a cyber security perspective in November as well as a longer term effort. As more states look to update their technologies, and look to the potential of online voting, the inevitable and inherently unescapable vulnerabilities need to be assessed. Ms. Spaulding then invited Ms. Maher to speak about their efforts. Ms. Maher said NPPD has been issuing best practices and there are some additional ones that went out to the states providing information on not just securing voting and other election systems, but also making sure they are aware about the most recent threats such as ransomware or how to plan for potential attacks and continuity of operations. She said she hopes this is a great assistance to states in both the short term and long term to secure their systems. Ms. Spaulding said Secretary Jeh Johnson has been out publicly saying it would be extremely difficult and highly unlikely that a malicious actor could change the outcome of a national election through exploiting vulnerabilities in that election infrastructure on a national level because it is so diverse. She said "if you have seen one system, you have seen one kind of machine, they are all different." They have different security measures and audits in place. However, they are worried that a malicious actor could get into a state's voter registration database and potentially manipulate, delete, or deny access to data and cause disruptions on Election Day, then publically announce what they did to cause doubt in the public's mind about the reliability of the outcome of the election. She said that is the bigger concern and a big part of what they are investing in, if those types of claims are made to be able to help inform the American public on what is and is not feasible.

Ms. Spaulding closed by saying she was so glad to hear Dr. Flynn's and Ms. Kvochko's presentations. She said she endorses nearly everything that Dr. Flynn has said over the years. She said the resilience based approach, rather than the threat based approach, forces them to ask, "Where does it matter?" which she believes the NIAC has embraced. She said one of the reasons the NIAC's expertise is so valuable is because they are focused on "real world" consequences. She informed the NIAC that the Senate has passed a Continuing Resolution. She added that DHS has been working to transform NPPD to bring greater unity and effort across physical and cyber, implementing many recommendations that the NIAC has made. She said everyone at NPPD needs to understand the central mission of strengthening the security and resilience of the nation's critical infrastructure, both physical and cyber. She informed the NIAC that they are trying to get a single sentence in the Continuing Resolution that will change NPPD's name to Cyber and Infrastructure Protection Agency, but they need permission from Congress. She then thanked the NIAC for their great work and opened it up to questions. General Edmonds said in the President's cyber plan, there was a mission to increase the number of Federal response teams. He asked Ms. Spaulding for a status update on that. Ms. Spaulding said it is in the President's budget request and they are hoping Congress will appropriate funds to do that. In the meantime, they recognize that demand for their services is going to continue a lot faster than Congress will act. She said they are looking at ideas such as putting together inter-agencies, if DHS resources are exhausted under DHS leadership to help meet the needs. They have been looking at using the National Guard to help supplement those capabilities in the event of a wide scale need. She reiterated that it is still in the budget and they are fighting for it.

Dr. Flynn then thanked Ms. Spaulding for all she has done, noting much progress has been made. He asked her to talk about the regionalization effort. Ms. Spaulding said Ms. Durkovich has been driving regionalization for quite some time. In the proposed plan for standing up the first operational component since DHS was created, which would be the "Cyber and Infrastructure

Protection Agency". Beyond the name change, there is an effort to stand up this agency within DHS and a big part of it was to focus on regional operations. NPPD is still considered a headquarters component of DHS. However, NPPD is engaged in operational activity across the country regarding 9,000 federal facilities. There are 120 PSAs, 120 chemical inspectors, 5 cyber-security advisors, and lots of other operational activity across the country. Operational activity takes place in communities and regions across the country, not at headquarters. To do that, NPPD is setting up regional offices. They are starting the effort with the Office of Infrastructure Protection (IP), because they cannot do more than that without congressional authorization. Ms. Durkovich has recently hired regional directors for each of the FEMA regions. These directors are new positions whose job is to pull together all the field forces in those regions in a more cohesive and coordinated way. There was a pilot project in Atlanta (Region 4), which has been very successful. The people engaged are very excited about the unity of effort to pull the various expertise from NPPD and bring them together to meet the needs of the region. Ms. Kvochko asked as they are setting up these new offices, what the best way is for the private sector to collaborate. Ms. Spaulding said there are a number of ways to do that. If the focus is on what the regional employees in the area can do to plug into the program and take advantage of what may be coming out of the program, but also help and be full partners, it would be through the regional directors. They can be reached through Ms. Durkovich's office as well as the National Infrastructure Coordinating Center (NICC). If the private sector, for example, wants to be more involved on a national level to contribute best practices in regions across the country, then they should come in at the IP headquarters level. In terms of cyber, NPPD is working closely with some major banks on a series of initiatives that will take advantage of the resources that the largest banks and financial services companies to help with intelligence sharing, information sharing, and develop things that can be shared across the entire sector. Ms. Kvochko thanked Ms. Spaulding.

Ms. Maher added that she would encourage everyone to enquire about automated indicator sharing (AIS) because that is a free service at DHS that recently stood up. At the tactical level, she thinks it is important to look at AIS. She compared it to a "neighborhood watch" where the indicators are coming in at machine speed and the system will only continue to improve and show more value as more people participate and put in what they are seeing on their networks. Whether they are seeing suspicious activity, or known malicious activity, it is a good service to participate in. Personal company data is not being inputted. They feel this is an important initiative everyone should plug into. Ms. Spaulding said this is machine-to-machine. The product Sultra builds on this notion, technology and formats that DHS developed for this. Congress passed a law that gives liability protections to companies that share this information with the NCCIC, DHS's cyber operation center. It can be shared with information sharing and analysis organizations or directly with the NCCIC. It is shared in a format that is machine readable and happens in a matter of seconds. DHS then has the obligation under the law to get it out in real time to everyone who is on this "network of networks". For example, companies may share with an information sharing and analysis center (ISAC) and then the ISAC is sending those indicators to DHS. An adversary today can reuse the same internet protocol address for malicious activities over and over again for years. This is because sharing is not done effectively and efficiently. The idea is that if an adversary tries to get into a system, whether or not they succeed, the attempt is captured by intrusion detection technology and shared right away with everyone. The goal is to make sure the adversary can only get away with something once. That would be a huge advancement. It is all anonymous and she encouraged everyone to sign up. Ms. Lau asked how information is given to specific companies if it is anonymous. Ms. Spaulding said right now it is given back to everyone who signs up for AIS, sends in their indicators and receives all the indicators that everyone is sending. Each company receives more benefit than what they are putting in. Ms. Allman commented that the FBI has been sending out unclassified notifications and information on an ongoing basis as well. Ms. Spaulding said DHS and the FBI often put out joint advisories, bulletins and alerts that are usually a lot more narrative that provide broader context. It may not be in real time, they might wait until a number of incidents seem to reveal a trend and they will put out an advisory. However, sometimes the advisories that go out are just indicators. DHS and FBI have been sharing indicators for many years. This is the first time for receiving and sending in milliseconds in machine readable format. Ms. Spaulding then concluded her presentation.

VI. STATUS UPDATE ON PAST NIAC RECOMMENDATIONS — *Nancy J. Wong,* Former NIAC DFO

Ms. Lau said the next item on the agenda is also related to the work of the Future Focus Working Group. She is pleased to welcome the NIAC's former DFO, Nancy Wong who has spent quite a bit of time on these studies that NIAC has done in the past. She has aggregated them to look at what recommendations have actually been implemented or partially implemented, as well as insights gained from the study process. Ms. Wong thanked Ms. Lau and said it was a delight to work for the NIAC. She said in the briefing they will see the type of impact that a council of this stature and expertise has provided to the nation. When the NIAC first started, the mission was unformed and ill-understood. The original purpose of the NIAC was cyber, which has now come full circle. This Council was established as a result of the President's Commission on Infrastructure Protection and Presidential Decision Directive 63. The Council was intended to provide an insight into what the government did not know. She said, "It didn't know, what it didn't know". This is a shared commission that requires the insights and understandings of the owners and operators at the strategic level to inform policies that were useful and actionable to get the nation where it needed to be.

Ms. Wong said her tasking was to share a high level summary of the list of all the recommendations from 2004-2015. The NIAC delivered 26 studies in that time period. It composed 265 recommendations. Some of the recommendations were extremely complex, so part of the work the DFO had to do was decompose some of the recommendations so that they could be tracked in terms of implementation. The topics encompassed the entire range of critical infrastructure issues. At the beginning, the NIAC's mission was so little understood that it was very important to get the insights of the Council in order to identify where some of the critical issues were. The White House requested the Council to make a recommended agenda to the White House on topics it should take on, and the White House would then prioritize and task out the recommended topics. The topics encompass the entire range of critical infrastructure issues, which the Federal government has been addressing over time. It included cyber, physical and workforce security strategies. In terms of workforce, there was a very extensive study that was done by the Council in 2006 which contained very detailed recommendations. She said she would discuss why some of the detailed recommendations are hard to implement because of the evolving nature of the issue.

Ms. Wong said public-private partnerships (PPPs) are required through the Council's scope of work, as well as the intelligence and information sharing. The entire range today is called the National Preparedness Goal (NPG). She said she believed that the NIAC's input had influence on how the mission of the NPG was put together. The NIAC's reports and studies have covered prevention, protection, consequence mitigation, response and recovery, as well as what constitutes "resilience". For a very long time, resilience has been inherent from recommendations from the private sector as a risk mitigation approach. This is the insight that councils like the NIAC provides. She said in the real world, this is what is done to reduce risks and it is not necessarily about protection, but about resilience. That is because it is not the job of owners and operators to predict what potential threats could hit them. They have to assume that unpredictable things can happen to them, and at a minimum they need to be able to respond and recover, which is part of resilience. The studies have also really focused on risk management and effective practices. One of the studies related to how government and private industry interact to determine roles and responsibilities and when incentives work and when they do not and when regulation is necessary. She said they have to work up to regulation because they do not know about the issue or the risk to make it effective.

Ms. Wong said from the Federal Advisory Committee Act (FACA) perspective, the definition of implementing recommendations is that a recommendation is fully implemented when it is accepted. Implementation can take years. Partially implemented is when a recommendation is accepted for partial implementation. That may be when the Council makes recommendations to multiple parties and only a few of those parties choose to accept the recommendation. This input provides some lessons learned for how the Council could make recommendations in the future. There are reasons why some recommendations are not implemented. An agency needs to justify, by providing a rational and a reason, for not implementing or accepting the recommendation. Lastly, there are recommendations under review. It can take a long time for an agency to work through what it is going to accept and actually commit to implementing the recommendation.

Ms. Wong said 194 out of 265 recommendations were fully implemented, which is about 73%. She said this is an astounding level of implementation. It reflects how integral the Council's recommendations, advice and the work it has done in terms of the evolution of the mission itself. Therefore, in terms of impact, she said this Council has made an impact. Ms. Wong said that 16 recommendations were partially implemented. The majority of those were when the recommendations went to multiple agencies and not all of them accepted. Six percent of the recommendations were not implemented. Under review, all the recommendations from 2004-2008 are closed out. There are a few outstanding recommendations from 2009. The rest are all from recent recommendations the Council has made. Some of the recommendations tend to be fairly complex in terms of implementation requirements with involvement from multiple agencies so it takes some time to analyze what it will take to implement those recommendations. She said they are seeing that with the 2015 recommendation of the Strategic Infrastructure Executive Council. It requires many parties because it would be a cross-sector and crossdependency council. There are 39 outstanding recommendations, in addition to the recommendations that came out in the 2016 Water Sector report.

Ms. Wong said in summary, this Council's implementation rate is close to 80%, which she described as astounding. The feedback she received indicated that this was very unusual for a Council at this level. She said Al Berkley, a former NIAC chair, informed her that at the time between Administrations in 2008-2009, the Obama Transition Team had called him and shared with him that based on their evaluation and analysis of the NIAC, they considered it a top three presidential advisory council in terms of productivity and usefulness. Ms. Wong said, the Council will likely again be evaluated by the new Administration's transition team. She said her observations from evaluating and looking at all the recommendations is that NIAC's advice is pretty far-sighted. Ms. Wong said she identified some issues and risks, as well as proposed approaches to address them. She said they were proposed years before they were recognized as issues and as legitimate approaches to getting them implemented. An example of those came from the reports on insider threat, the convergence of physical and cyber issues, and cross-sector dependencies. She said the recognition of lifeline sectors is a key piece in terms of prioritization, came out of the NIAC. She said the emergence of lifeline sectors came as a result from a recommendation of the NIAC.

Ms. Wong said the NIAC advice has been impactful with a relative high acceptance rate. She said when looking at other reports and studies by other councils, it is apparent that the NIAC studies are extensively researched. The data collected is from a wide range of resources and perspectives. It is one of the few councils where DHS has funded the research resources, based on the request of the Council to make recommendations based on data and not just their own opinions. As a result, there is a lot of credibility for the recommendations of this Council beyond the Federal government, such as in academia and state and local government. She said when she was DFO, the NIAC had received feedback that state and local governments want to see NIAC recommendations as soon as they are available. Ms. Wong said based on her review of the recommendations, what makes a recommendation effective has evolved over time. When the Council was first established and focused on cyber, there were premier cyber security experts on the Council. They were able to focus on the taskings that came out of the White House on very specific topics. They created a whole body of work in the commercial industry on where to focus, vulnerabilities, and how to measure vulnerabilities. As the Council evolved into more policy and strategy work, it started to learn to focus recommendations so they were more actionable. The recommendations in 2005-2006 were much more general and more a matter of interpretation of what the Council's intent was. However, the recommendations were of such quality and so important to the mission's evaluation itself, the majority of them were accepted so that some focus could be put on using recommendations to evolve the mission. Ms. Wong said a lesson learned that has evolved over the last five years is understanding and incorporating required precursors as recommendations to achieve a specific identified outcome. She said that occurred in the 2015 transportation study in terms of discussions that occurred during the Council. It was such a major issue and they needed to decide how they could make a difference. The decision was to address what they could at the time. She said Dr. Scott and Ms. Lau were very focused on what could be addressed incrementally to get it started because this topic is so big. Those recommendations are more actionable than those that are too broad. Ms. Wong said another lesson learned was holding the right people accountable, who actually had the authority and ability to get things done. She believes this will continue to emerge overtime as recognition of the Council grows and the potential time required to implement recommendations. Some of the later reports also included milestones to recognize progress. Ms. Wong said she thinks this input might be useful to the current Working Group as the Council moves forward. She then opened it up to questions.

Ms. Kvochko asked how the Council will work during the transition. Ms. Wong deferred to the current DFO, Ms. Norris. Ms. Norris said the Council functions continue during an Administration change. That is why it is important that the NIAC is beginning this study now so that they can carry that through and when the new Administration is in place, they will have the opportunity to look at the recommendations the NIAC makes in terms of future focus areas, how they might study cyber, and ways they can make their recommendations more impactful. Mr. Hawkins said that he has only read one NIAC report, which was on his industry (water). He said he was fascinated to see that for NIAC, implementation equals acceptance. He said that is very different than what he is judged on. His board does not want to know if he wants to do something but whether or not it is actually done. He said he understands with so many recommendations, many of which are broad and all over the government, that they could not possibly implement all of them. He suggested for the next study to do an audit, and take a few of them and go deep to see whether the agencies who accepted actually delivered. Ms. Wong said that for all the recommendations before 2009 she followed up to see if implementation was actually completed. The recommendations before 2009 the recommendations that have been marked “implemented”, have actually been implemented. She said for example in 2006, the Council made some recommendations that required policy and strategy changes. She said it takes a long time to change a major strategy or policy. She referenced how a White House Liaison reported to the Council that when he was writing PPD-21, it takes so long for a policy change to occur that he had incorporated a bunch of recommendations that were accepted but still outstanding, or still under consideration. All of those recommendations are now closed out because they are incorporated. Ms. Wong validated that it happened. She said there are certain national strategies that get revised every five years. In order for strategy or policy to change, it can take five years to get implementation to occur. Ms. Wong said that she has seen that the Council has evolved to asking for speakers to come to QBMs. She recommended inviting speakers from various agencies to come and report the status of implementation of the recommendations. This would allow for a continuing flow if information on whether or not the recommendations were implemented, or are still under consideration and why. Ms. Wong said she understood Mr. Hawkins’ perspective that for owners and operators it is all about outcomes and results, which is why it is important to understand the lengthy government processes to get things done. She concluded that even though it does take a while, they eventually do get there. Ms. Lau thanked Ms. Wong.

VII. STATUS REPORT OF NEW WORKING GROUP

Joan McDonald and Mike Wallace, Co-Chairs of Future Focus Study Working Group

Ms. Lau said they will now be hearing the first briefing to the full Council from the Future Focus Working Group. She said many of the Members who are not Working Group Members had observed a Working Group meeting earlier in the day, but were asked to save their input for the QBM. She requested input from the Members after the briefing by Ms. McDonald and Mr. Wallace. Mr. Wallace thanked Ms. Lau, as well as the guest speakers. He said the comments from Dr. Flynn, Ms. Kvochko, Ms. Spaulding, and Ms. Durkovich had all been very helpful, and Ms. Wong crystalized it. Mr. Wallace explained that he and Ms. McDonald were co-chairs of the Working Group and would be "tag teaming". There have been two Working Group meetings. In the first meeting, Ms. McDonald and Mr. Wallace decided to bifurcate the study between the tasker that dealt with the NIAC recommendations and process for future studies, and the request for scoping a cyber study. They decided that Ms. McDonald will take the lead on the NIAC study, and Mr. Wallace will take the lead on cyber. However, they are cooperating and collaborating on behalf of each other through the whole thing. There are currently six other members on the Working Group. He thanked them for volunteering to be part of the process. The White House indicated how they would like to divide it out, with the first parts on the NIAC and future focus, and the third on cyber. Mr. Wallace said he would start with the cyber piece. He said the Working Group attended a meeting at the NSA at the Secret level to get a grounding on the backdrop of the cyber study. That led to many questions and thoughts on how to go forward. They then had a two hour Working Group meeting directly before the QBM which focused on both parts of the study. He said his briefing will on what they are going to do and how they are going to do it.

In terms of, "what", Mr. Wallace said they have six framing questions that have been broken out. He said the notion of cyber is huge and they need to figure out what NIAC can do to contribute to what has already been done in this very dynamic area. It is also a very serious area and they are not taking it as an academic study. There is critical infrastructure that is vulnerable and open to attacks. Referencing Dr. Flynn, he said "they have the capability, they just do not have the intent". He hopes it stays that way, while they continue to work to improve the posture within the country. He said, "To what extent is cyber security a concern to critical infrastructure?" remarking that they all can answer that. He said the Working Group would focus on what assets are really important from the point of view of cyber security vulnerabilities. They are then going to look at the roles and responsibilities of various government groups in the private sector. He said they talk about an "umbrella" where all this exists. There are a lot of groups and agencies, ISACs, private sector, the intelligence community, etc. involved. It has all come about in a very constructive way as more and more challenges, as well as opportunities to optimize have been identified. However, he feels they are finding themselves at a point where they have evolved, but they never decided where they want to go and be. He said roles and responsibilities are shifting and resources are being added, moved and pulled away as the country tries to find the right overall alignment. There are a lot of efforts that are underway. The Working Group has decided that they will probably look back no more than three years to studies and reports that have been done, because anything beyond that is too dated. They are also aware of new studies that will be coming out by the end of 2016. He said it precludes them getting down a path where they would be making suggestions to remake things in an unhelpful way. He said they will be scoping a roadmap for cyber study as opposed to "a study to scope a study". The three questions involve the situational analysis and what exists today. Next they will address the questions of what are the greatest and most urgent cyber challenges, which they will collect data through interviews. The next question is, "what are the gaps in cyber risk reduction?" He said there are touchpoints and interface handoffs, some of which are efficient and some of which are not. There may also be some gaps in what are perceived to be interfaces and handoffs between government and private sector and vice versa. Next, they will look at in a very broad sense, suspending all that exists at the moment (such as financial and liability issues), and no restrictions existed, how they would think about optimally going about protecting critical infrastructure using their knowledge and capabilities. He said they would not be solving that problem, just using it as a theoretical construct to help inform and give insights as to what might be some of the scoping areas that a study could look at, that may actually help find another path forward. He said it does not make sense for the Working Group to incrementally go after cyber by sector. He feels they can bring the greatest leverage by taking a step back and identifying the aspects of a cyber study that might be most impactful and actionable. Mr. Wallace said the issue of not having resources is always the case, so they may think about a way to pool resources to accomplish the objective.

Mr. Wallace then described the matrix of entities on one side, and characteristics for what they do on the other, along with what is working and not working so they can look at the holistic where they might find the best opportunities to focus. He said they have to be about process with what they are doing. They will not be coming up with specific answers, it is a scope. Lastly, he said they are going to approach the study by gathering input from experts along the way. They have laid out, a schedule of about 10 meetings that would occur every other week. The first interview will be with Ms. Durkovich. The intent is to interview at least three more government entities and they will be doing that first due to the Administration change. Afterwards, they will reach out to the private sector, SCCs, ISACs, etc. In addition they have a list of people who they would also like to interview. He said they will provide framing questions ahead of the interview, so the interviewees are prepared ahead of time. This will allow them to get their answers on record and use the call to have a dialogue. He then turned the briefing over to Ms. McDonald.

Ms. McDonald thanked Mr. Wallace. She said as this Working Group has had discussions over the past few weeks, they have realized that this study will be evolving over the next 6-8 months. When it was first tasked, it seemed very straightforward that during the Administration transfer it would be a good time to step back and review recommendations that have been implemented, where the gaps are, and how best to move forward. They thought they could simply make a matrix, gather information from the outgoing Administration and hand it to the incoming Administration. However, they have discovered it's not that straight forward. She then thanked Ms. Wong for pulling together the information to-date, because having that data will be critical. She said each of the four questions in the tasking has 4-5 sub questions underneath it, such as how do they link what is happening on the national level to the state and local level, which is something Dr. Flynn discussed. Ms. McDonald's personal experience is at the state and local level and pointed out that in severe weather events, local governments are the first responders. She then said before Ms. Spaulding's briefing she did not consider voting and elections as part of critical infrastructure, but over time the definition changes. In response to Ms. Wong's presentation, she mentioned the difference between accepting the recommendation and executing the recommendation. She said that lag is something they have already discussed in the Working Group. Another topic brought up at the QBM is how the Working Group will take feedback from the implementing agencies and what they have learned, and incorporating that into the Working Group's analysis and recommendations for future studies. She said it will not be as cut and dry as "these are the recommendations and these are how we can improve it". From her year of experience on the NIAC, she feels it is an evolution of what they can do as a Council and provide a good service to the country going forward from one Administration to the next. She thinks they will be asking these questions and moving forward.

Ms. McDonald said they have an aggressive schedule. There will be many interviews and gathering of data over the next few months. They will be doing that analysis on two tracks, one focusing on cyber and the other on prior studies. One of the points that was captured today is the integration between cyber and physical infrastructure. While the paths seem to be separate, they are always knitted together. She said in December they will have an in-person Working Group meeting to see where they are and make an assessment of what needs to happen next. The goal is to publish the report in May 2017, which they hope will include ways to make the NIAC's process better, subject areas that should be addressed, and the roadmap of how to begin a cyber study. She said the study is aggressive, as well as exciting and that the Working Group believes it is critically important to take stock and hand this study from one Administration to the next. She said it is an honor to be on the Council and that they know it will move forward regardless of changes. She then opened it up to questions.

Dr. Benjamin said it was a great plan and asked what would happen if something bad happens between now and the new Administration and the NIAC needed to accelerate the study, in particular the cyber piece Mr. Wallace said if something bad happens, it is not likely to come to the NIAC. The nature of the NIAC is not to solve real time problems in the nation. He said they may be called on to do whatever can be helpful, but there is not likely to be an acceleration. General Edmonds said Ms. Durkovich had briefed them on operations that started with the Senate, though the names have not changed yet. Ms. Durkovich said the NCCIC and the NICC have integrated and they are now co-located to better integrate operations. She said there are multiple elements across the US government to include what goes on at the NSC in the event of a bad day that would bring everyone together to ensure it is dealt with appropriately. Mr. Hawkins said that has been a very good conversation and he is impressed with the depth and the speed that this is being done. He said it addresses two topics on different tracks. In terms of the question of what is the next subject for study, he would put it into three buckets. The first would include how the NIAC process is doing, what the NIAC should study next, and the roadmap to a cyber study. The second bucket would be what an external audience wants to know the most such as the new Administration. The third would look at if NIAC is structured the right way, such as if NIAC has the right people to do the work properly. He said this is not as outward facing, though a new Administration might be curious about NIAC's organization, but they probably have other things on their mind. He thinks the new Administration will want to see a roadmap to cyber and what issues NIAC is going to focus on. He said in terms of how NIAC functions and does its work process-wise, that may be on a different track. Ms. Lau asked Ms. Morrison if this is what the White House thought the NSC was tasking the NIAC to do because it has evolved. Ms. Morrison said she thinks it has changed, but the basic structure of what they are looking for is still in place. She said she likes that the NIAC has decided to study both cyber and the future focus. She said they appreciate that the NIAC has taken on a lot, and it will be a comprehensive study taking on key points in a very compressed time frame. She added that the NSC can support the Council to let them know. Ms. Lau then concluded the Working Group presentation section, and invited any further comment to be routed through Ms. Norris after the meeting.

VIII. OPEN DISCUSSION AND PUBLIC COMMENT — *Ginger Norris,* DFO, NIAC, DHS

Ms. Lau then turned the meeting over to Ms. Norris for public comment. Ms. Norris announced that at the conclusion of the public comment period, the Council will still accept written comments. Ms. Norris said as DFO, she will moderate the public comments and called forward Mr. Charles Job who signed up to make a public comment. Mr. Job is with the National Groundwater Association, which represents thousands of scientists, engineers, manufacturers, suppliers, installers and managers. He applauded the NIAC's study on water sector resilience. The association sees it as something they would like to see applied more broadly to include groundwater. He feels the study fits with the larger water system portion of the Water Sector. There are a lot of interdependencies. There are many small water systems. He said from his organization's perspective, it is important to recognize the ground water source container (aquifer) as part of the infrastructure assets of a community water system that also need focus and attention. There is a considerable amount of management and attention that that water needs. They recognize that ground water and water in general should be evenly distributed and equally accessible. Ground water has its own vulnerabilities such as drought and waste disposal. He said focusing on ground water aquifers as part of the infrastructure, the condition of water in that container from level, availability and quality standpoints is an important part of considering the infrastructure need of communities, states, and the whole nation. Ground water supplies about 42% of public water and private water supplies, and 43% of agriculture irrigation water. There are significant interdependencies, which were seen in California. He said that if the NIAC were to take up this topic again, he thinks they should focus on ground water as a significant portion of that, particularly small water systems and the communities that rely on groundwater but are not part of the water system that are affected by infrastructure investments. He feels that would be very useful. He said he would like to propose as a first step, an evaluation of climate scenarios focusing on long term water availability and use across hydrologic regions, aquifers, economic sectors and interdependency aspects to inform future total water infrastructure decision making for water resilience. Mr. Baylis thanked Mr. Job for his input. He said it was valuable and timely. The Working Group had a lot of dialogue on water resources including groundwater, upstream reservoirs and other critical infrastructure. They did narrow it down to water treatment and wastewater treatment with the caveat that they also recognize all those water resources to the environment and infrastructure in the long term. Dr. Scott said she thinks in upcoming recommendations, in terms of simulations, they can actionably build that element in the exercise, which would be a first step. Mr. Baylis said what they learned in the transportation study is that transportation and water are very broad and complicated to include everything in one report, but he supported including other aspects in the exercise. Mr. Hawkins supported what Mr. Job said. He said in San Antonio, Southern California, Las Vegas, etc. groundwater is an instrumental part of the future of those communities, not just for water, but also development. He said in New Jersey, development is limited first and foremost by groundwater. He said Mr. Job's point is very well taken. Mr. Job said much of his career has been in public finance in water system, so he appreciated Mr. Hawkins' work**.** Ms. Norris noted that written comments were also provided by Mr. Job that were distributed to the members. Those comments can be found at the end of the meeting minutes. Ms. Norris said there were no other registered public comments and she closed the public comment period, though invited people to continue to make written comments. Ms. Norris then turned the meeting over to Ms. Lau.

IX. Closing Remarks

Constance H. Lau, NIAC Chair

Caitlin Durkovich, Assistant Secretary for Infrastructure Protection, DHS

Stephanie Morrison, Director Critical Infrastructure Protection Policy, NSC

Ms. Lau said it was time for closing remarks and invited Ms. Morrison to begin. Ms. Morrison thanked Ms. Lau and Dr. Scott for a very productive and interesting meeting. She said the speakers were great and she thanked them for their helpful presentations during which she learned a lot. She also thanked Mr. Brian Scully from DHS, as well as Ms. Norris and their team for all the logistics that go into planning these meetings. She also thanked Ms. Durkovich for her dedication to making the nation's critical infrastructure more secure, noting that she would be missed. Ms. Durkovich noted that the NIAC has produced 28 studies and more than 265 recommendations over 12 years, which is having an impact. She thanked the Council. She also acknowledged Ms. Wong for getting the NIAC to this point and congratulated Ms. Norris on her role as DFO. She thanked the DHS IP team for putting this together. She looks forward to continuing to work with the NIAC in the last months of the Administration and feels their paths will continue to cross. Ms. Lau said this is a bittersweet meeting because it is the last public meeting of the Administration. She also thanked the DHS IP team including Ms. Durkovich, Mr. Scully, Ms. Norris, and Ms. Andrea Gagliardi of the Secretariat Team. She noted the challenges of having four meetings in two days culminating with the public Quarterly Business Meeting. She also thanked Mr. Wallace and Ms. McDonald for chairing the next study. She thanked all the Members that were able to join on the phone and in person, especially the new Members Mr. Hawkins and Senator Bingaman.

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

Ms. Lau adjourned the meeting, noting the next quarterly business meeting would be in 2017.

Written Public Comment Submission

National Ground Water Association (NGWA) Statement on Groundwater and the Subsurface Environment as Critical Infrastructure

Aquifers in the subsurface environment exist as natural capital infrastructure, storing, transmitting and treating groundwater. Groundwater is the country's largest freshwater source. Within the natural infrastructure, constructed infrastructure exists and is augmented as wells, pumps and pipes are added to draw on groundwater. Groundwater and the subsurface are critical infrastructure that must be maintained to provide goods and services for the US economy. Forty-two percent of public and household water supply and 43 percent of irrigation water for food production come from groundwater. Our national capability for coordinated collaboration to address groundwater source availability, quality and resilience is challenged in recent times in response to drought and groundwater level decline, floods, saltwater intrusion, and underground wastewater and residuals disposal.

Groundwater is principally managed by states and territories, has no national jurisdictional point for planning and coordination of the myriad of activities that agencies of the federal and state governments undertake and oversee to utilize, conserve and protect this vital resource for services across economic sectors. The exception, of course, is when agencies are convened to deal with crises and disasters, such as Superstorm Sandy which affected numerous groundwater supply systems. Surface water has many federal and state management agencies overseeing its interstate flow, quality and related infrastructure, coming under the principal federal jurisdiction of the US Army Corps of Engineers and the Environmental Protection Agency. An issue for the Nation is how the existing regulation of groundwater and the subsurface environment comes together in a well-orchestrated way to provide the large range of essential services on which the Nation relies on a continuing long-term basis. Excessive continuing drought in dry areas and rapid runoff from intense storms in humid areas only exacerbate a reduction in water storage in aquifers over extensive areas. As was seen in California, more and deeper groundwater is viewed as the replacement source for lack of surface water and shallow groundwater – deeper groundwater that is not rapidly renewable and when over-extraction occurs more pumping can cause land subsidence. More energy is required to pump from greater depths as water levels decline.

A productive future-looking coordinated federal-state approach has emerged for monitoring the Nation's principal aquifers as a logical infrastructure component of water source availability, the National Groundwater Monitoring Network, through the Federal Advisory Committee on Water Information. This effort is just beginning and is only focused on groundwater monitoring of near and long-term levels and quality. Fifteen states have contributed monitoring data and seven more will plan to provide data beginning in 2017. Other federal-state coordinating points are needed to consider and respond to climate effects on groundwater affecting or related to long-term water supply for drinking water and food production, saltwater intrusion, extended drought and water storage, energy and minerals production, water quality of aquifers in areas of extensive land-applied chemicals, and storm water management for replenishing groundwater sources. Evaluation of scenarios of long-term groundwater availability and use integrated across hydrologic regions, aquifers and economic sectors is needed to inform future total water infrastructure decisions for water sector resilience.

Groundwater and the Subsurface Environment are Critical Infrastructure

While out of sight and heavily relied on but not often considered, groundwater and the subsurface environment provide significant natural capital, including:
Supply and Production Infrastructure

- Over 15 million household wells rely on the natural storage and transmission of groundwater without an extensive pipe system.
- Likewise, over 173,000 public water wells rely for this same natural storage and transmission of groundwater to their well screen intakes and provide 37 percent of total public water supply.
- Stream base flow is maintained by 492 billion gallons/day of groundwater discharge through streambeds to supply larger public water systems using surface water, provide inland river navigation and support ecosystem services.
- The nation’s food supply relies on over 400,000 irrigation wells that depend on the storage and transmission of groundwater through aquifers without a vast pipe network – with 43 percent of agricultural irrigation and 26 percent of livestock and aquaculture water coming from groundwater – nearly 150 percent greater irrigation demand for groundwater since 1950.
- Thousands of ground-source heat pumps exchange heat with groundwater efficiently reducing dependence on extensive pipe networks for fuel to heat homes and buildings.

Storage Infrastructure

- Aquifers around the nation store groundwater for the 15 million households, 137,000 public water systems, and 121,000 irrigated farms without extensive collection and distribution pipes and vast surface storage areas.
- Hundreds of aquifer storage and recovery sites store and protect water supplies for future use by towns, cities and industries.

Waste Treatment and Disposal Infrastructure

- The subsurface provides disposal services for 19.5 million domestic septic systems and for shallow waste injection through up to 1 million wells without extensive collection pipes.
- Deep disposal of hazardous waste occurs in 272 wells and 167,000 wells are used for brine disposal by the oil and gas industry.
- 418 land disposal facilities for solid waste are subject to groundwater monitoring to ensure groundwater protection.

Protective Services Infrastructure

- Thousands of groundwater monitoring wells are in place across the country to ensure that groundwater is safe to drink, usable for crop irrigation and manufacturing processes and managed to provide sufficient quantity and quality of water for a large range of products and services, including ecosystem support; data from these monitoring points need to be compiled centrally to understand national groundwater status.

Even though groundwater and the subsurface environment are not visible, the essential products and services of this unseen natural infrastructure must be recognized and maintained to sustain the wellbeing of the nation – we all rely on it daily!

Sources

Margat, J., and J. van der Gun. 2013. Groundwater around the World, CRC Press/Balkema.
USGS. 2014. Estimated Water Use in the United States in 2010.USGS Circular 1405.
Vrba, J., and J. van der Gun. 2004. The World's Groundwater Resources, http://www.un-igrac.org/dynamics/modules/SFIL0100/view.php?fil_Id=126
Vrba, J., and J. van der Gun. 2004. The World's Groundwater Resources.
USGS. 2004. Estimated Water Use in the United States in 2000.USGS Circular 1268.
Siebert, S, Burke, J., Faures, J. M., Frenken, K., Hoogeveen, J., Döll, P., and Portmann, F. T . 2010. Groundwater use for irrigation. Hydrology and Earth Systems Science, 14, 1863–1880. www.hydrol-earth-syst-sci.net/14/1863/2010/doi:10.5194/hess-14-1863-2010.
USGS. 1986. National Water Summary 1985. Circular 2300; USGS. 2005. Communication, D.M. Wolock.
Job, C.A. 2010. Groundwater Economics. CRC Press.
US Department of Agriculture. 2013. 2013 Farm and Ranch Irrigation Survey - Census of Agriculture. https://www.agcensus.usda.gov/Publications/2012/Online_Resources/Farm_and_Ranch_Irrigation_Survey/fris13_1_007_007.pdf, Accessed May 4, 2016.

Submitted for the National Ground Water Association by
Charles Job, Regulatory Affairs Manager
National Ground Water Association
601 Dempsey Road
Westerville, Ohio 43081
(800) 551-7379