NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

QUARTERLY BUSINESS MEETING MINUTES
August 22, 2017
9:00 AM - 12:00 PM EDT
Eisenhower Executive Office Building
Washington DC, 20004

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

Ms. Ginger Norris, NIAC DFO, opened the quarterly business meeting (QBM) and welcomed all in attendance.

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

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

NIAC MEMBERS PRESENT IN PERSON:
Ms. Joan McDonald, Mr. Michael Wallace, Ms. Constance Lau, Dr. Beverly Scott, Ms. Jan Allman, Mr. Robert Carr, Ms. Margaret Grayson, Mr. George Hawkins, Mr. Georges Benjamin, Mr. William Terry Boston, and Mr. Carl Newman.

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
General Albert Edmonds, Ms. Diana Perreiah, Mr. James Reid, Mr. Keith Parker, Chief Rhoda Kerr, Mr. Ben Fowke, and Mr. Thomas Noonan.

MEMBERS ABSENT:
Mr. Rand Beers and Mr. James Murren.

SUBSTANTIVE POINTS OF CONTACT PRESENT IN ARLINGTON:
Mr. Nathaniel Millsap with Ms. Jan Allman
Mr. Scott Seu with Ms. Constance Lau

SUBSTANTIVE POINTS OF CONTACT OBSERVING VIA CONFERENCE CALL:
Mr. Frank Prager with Mr. Ben Fowke

OTHER DIGNITARIES PRESENT:
Rob Joyce, NSC; Mr. Robert Kolasky, DHS, NPPD; Arthur Ray, NSC; Devon Streit, Department of Energy (DOE); Grant Schneider, NSC; Kevin Reifsteck, NSC; Brian Peretti, Department of Treasury (DOT)

III.	**OPENING REMARKS AND INTRODUCTIONS**	*Constance H. Lau,* NIAC Chair
		Rob Joyce, Cybersecurity Coordinator, Executive Office of the President
		Robert Kolasky, Acting Deputy Under Secretary, National Protection and Programs Directorate (NPPD)

Ms. Constance Lau, NIAC Chair, welcomed everyone to the QBM. She welcomed two members who were attending in person for the first time, Mr. Carl Newman and Mr. Terry Boston. Ms. Lau said the goal of today's meeting is to deliberate on the Cyber Study, co-chaired by Mr. Mike Wallace and Mr. Bob Carr. She noted in all prior NIAC studies they have heard from critical infrastructure owners and operators how important the cyber issues are and that there has been a continuous, crying need for assistance. She stated this report provides recommendations on how the Federal government can assist owners and operators of critical infrastructure with cyber issues.

Dr. Beverly Scott, NIAC Vice Chair, thanked everyone for coming and for the honor of serving the country through the Council. She welcomed Mr. Newman and Mr. Boston. She stated she has served on the Council for five years and worked on tremendous studies, but in terms of urgency she believes this study to be the most meaningful.

Mr. Rob Joyce, the Cybersecurity Coordinator, thanked everyone for attending the meeting. He believes the tasks taken on by the NIAC are some of the most important work being done. This includes keeping critical infrastructure, especially Section IX entities, running in order to provide vital services. He added that from his position, he does not need to be convinced that there is an urgent need to reanalyze cyber policies and the authorities by which public and private sectors cooperate and collaborate. He added there is room for improvement and believes the Cyber Report includes thinking and expertise that is vital for the government. He noted having the understanding from those individuals that own and operate the vast majority of our critical infrastructure is irreplaceable. He values the opinions of the NIAC Members and said he looked forward to their discussion.

Mr. Bob Kolasky, Acting Deputy Under Secretary, thanked Ms. Lau and Dr. Scott for having him. He said since the Cyber Executive Order (EO), DHS and the NSC have been working hard to implement work coming out of the EO and the issues the NIAC is studying, such as those on cyber. He noted DHS has created a task force, to which Mr. Kolasky is an executive co-lead. They try to meet their deadlines and work with their partners in the interagency and obtain input from the critical infrastructure community to get the best reports forward and help the

administration make decisions and set the policy agenda. He said the cyber topic is very important to DHS and he is grateful for the Council's work and Mr. Wallace and Mr. Carr's leadership in the Cyber Study. Mr. Kolasky added that he knows after his many years working with the NIAC, this report is important and he looks forward to the deliberation. He said his team was a part of the body that identified the Section IX entities. He agrees with some of the fundamentals of the Cyber Study that despite progress being made, there are still gaps and it is time for the community and senior-level government to get Congress involved and the best people to see what areas of policy are not enough and need improvement. Mr. Kolasky also appreciated that while the NIAC is asking a lot from the Federal government, the burden is also being shared with industry in order to reach a common vision. He believes the report lays out a number of points and provides a blueprint to start discussion.

IV.	**APPROVAL OF MAY 2017 MINUTES**	*Constance H. Lau*, NIAC Chair

Ms. Lau asked for any edits to the May 2017 Minutes. Mr. Boston had an editorial change to page 11. He stated it should read, "65,000 electrical workers" rather than "6,500." With that change, Ms. Lau asked for a motion to approve the final draft of the May 2017 QBM minutes, as amended. All Council Members present unanimously approved the minutes.

V.	**FINAL REPORT OF CYBER WORKING GROUP**	*Mike Wallace* and *Robert Carr,* Working Group Co-Chairs

Mr. Wallace stated that he and Mr. Carr appreciated the opportunity to present their findings, because they believe what they have to say is important. He said the last few months were some of the most fast-paced efforts for a NIAC study that he had been involved with during his 10-year membership. He added none had been as intense and those individuals outside of the NIAC they engaged with have been equally as important in providing impactful input. He said there is urgency recognized by everyone at the highest levels in the Federal government and in the private sector, as Mr. Joyce and Mr. Kolasky indicated. He thanked all the Members of the Cyber Working Group for all of their participation and hard work; Ms. Jan Allman, Mr. Ben Fowke, Ms. Margaret Grayson, Ms. Connie Lau, Mr. Tom Noonan, Mr. Keith Parker, and Dr. Beverly Scott. He and Mr. Carr would briefly discuss the Council's tasking and their assessment. Then, they will be moving on to more specific discussion of the recommendations.

Mr. Carr said he had only been a Member of the NIAC for a year and half, but agreed with Mr. Wallace's assessment that it was an intense study.

Mr. Wallace and Mr. Carr went through the Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure slide deck, which outlines the final report publically available on the NIAC website. Their presentation covered 11 recommendations and discussed how the Working Group arrived at each recommendation and described what departments or agencies they believe are best suited to take action on each. The recommendations and action required are as follows:

1. Establish separate, secure communications networks specifically designated for the most critical cyber networks, including "dark fiber" networks for critical control system traffic and reserved spectrum for backup communications during emergencies.
   ➢ Action required by: DOE, DHS, Office of the Director of National Intelligence (ODNI), NSC, and the Strategic Infrastructure Coordinating Council (SICC)

2. Facilitate private-sector-led pilot of machine-to-machine information sharing technologies, led by the Electricity and Financial Services Sectors, to test public-private and company-to-company information sharing of cyber threats at network speed.
   ➢ Action required by: DOE, DHS, ODNI, NSC, and the SICC

3. Identify best-in-class scanning tools and assessment practices, and work with owners and operators of the most critical networks to scan and sanitize their systems on a voluntary basis.
   ➢ Action required by: NSC, DHS, and Congress

4. Strengthen the capabilities of today's cyber workforce by sponsoring a public-private expert exchange program.
   ➢ Action required by: NSC, DHS, and Congress

5. Establish a set of limited time, outcome-based market incentives that encourage owners and operators to upgrade cyber infrastructure, invest in state-of-the-art technologies, and meet industry standards or best practices.
   ➢ Action required by: DOE, DHS, ODNI, NSC, and the SICC

6. Streamline and significantly expedite the security clearance process for owners of the nation's most critical cyber assets, and expedite the siting, availability, and access of Sensitive Compartmented Information Facilities (SCIFs) to ensure cleared owners and operators can access secure facilities within one hour of a major threat or incident.
   ➢ Action required by: DHS, ODNI, NSC, Federal Bureau of Investigation (FBI), Office of Personnel Management, and all agencies that issue/sponsor clearances

7. Establish clear protocols to rapidly declassify cyber threat information and proactively share it with owners and operators of critical infrastructure, whose actions may provide the nation's front line of defense against major cyber-attacks.
   ➢ Action required by: NSC, DHS, ODNI, FBI, and the Intelligence Community

8. Pilot operational task force of experts in government and the Electricity, Finance, and Communications industries—led by the executives who can direct priorities and marshal resources—to take decisive action on the nation's top cyber needs with the speed and agility required by escalating cyber threats.
   ➢ Action required by: DOE, DHS, ODNI, NSC, the SICC, the Department of Defense (DOD), Treasury, and the Department of Justice (DOJ)

9. Use the national-level GridEx IV Exercise (November 2017) to test the detailed execution of Federal authorities and capabilities during a cyber incident, and identify and

assign agency-specific recommendations to coordinate and clarify the Federal government's response actions where they are unclear.
> ➤ Action required by: DOE, DHS, ODNI, NSC, and the SICC

10. Establish an optimum cybersecurity governance approach to direct and coordinate the cyber defense of the nation, aligning resources and marshaling expertise from across Federal agencies.
> ➤ Action required by: DHS, ODNI, NSC, DOJ, and DOD

11. Task the National Security Advisor to review the recommendations included in this report and within six months convene a meeting of senior government officials to address barriers to implementation and identify immediate next steps to move forward.
> ➤ Action required by: National Security Advisor

After the recommendations were outlined, Mr. Wallace described three suggested changes to the entities listed to take action on recommendations. The revision was to remove Congress form Recommendation Three and add Congress to Recommendation Five and Ten.

Mr. Wallace and Mr. Carr thanked everyone who took part in the process of the study. Ms. Lau thanked them for their leadership.

Mr. Boston suggested editorial changes to strengthen the report. He said mutual assistance contracts work well with linemen and electricians. Although, if a broad cyberattack occurs, he believes it will be difficult for companies, like PJM Interconnection LLC, to release its workforce to help another company, such as Pacific Gas and Electric Company, located across the country. Mr. Boston said at PJM, they had 3-4 thousand attempts per month at their firewalls to breach their system. He suggested on Recommendation Four, where it discusses cyber workforce, they add cross-training Federal DOE contractors on industry control systems to have a stronger response team, with appropriate clearances when under attack. Mr. Boston's second suggestion regarded Recommendation Seven. He suggested adding to Section A that industry needs to know when, how, and what to protect under the threat, not necessarily who or why. He said generally information is classified because of who the threat is from and that information is not required to mitigate the threat on the system. Mr. Boston's last editorial suggestion was to page 29, he believes there are more facilities than 3300 in the Electric Sector. Mr. Boston said he will send over all editorial changes to Ms. Norris.

Mr. Wallace thanked Mr. Boston for taking a close look at the report and for his editorial changes. He added that Mr. Boston's changes are not substantive and do not require a Council vote in order to be accepted.

Ms. Joan McDonald said she was impressed by the report and strongly supports the use of pilots, because they are a great way to test policy protocols and operations. She likes how each recommendation identifies the individual Federal agencies and departments that would be responsible, as well as the task force approach. She asked if all the recommendations would "flow up" through the National Security Advisor. She noted the timetable is aggressive and also

asked if it were known who the final point person would be.

Mr. Wallace said they respectfully named the National Security Advisor individually to take on a role, because as they said in their presentation- people get things done, not agencies. He noted as the Working Group came to the end of their report, they also wondered what they could recommend that would help place a marker in the future to ensure accountability. The Working Group wanted to avoid a lack of action taken, such that befell on numerous reports in the past. In this report, they also stated in 12 months if the NIAC is tasked that they be asked to perform a follow-up study. He stated the Working Group understands 100% implementation of the recommendations is unlikely, but do believe important progress on critical items need to be made.

Mr. Joyce thanked Mr. Wallace and Mr. Carr for their passionate leadership, as well as the full Working Group for putting together powerful recommendations. He believes they hit a key point when they said there was a lot of "echo chamber-like" resonance of things that need to be done. He said while there have been previous studies done inside and outside of government that mirror some of their recommendations, their report brings everything together in a tight, well-packaged and well-defined way forward. Mr. Joyce said throughout the recommendations the Strategic Infrastructure Coordinating Council (SICC) is highlighted. He asked if that entity already exists or if it needs to be built.

Mr. Wallace said the SICC as a concept in discussion and a basis for dialogue is "possibly several months in the making." He noted it is one side of an effort ready to go forward, but he made the point that CEOs engage if there is senior leadership from the government side that are also engaged, otherwise they do not have time. As he understands, the leadership of the Electricity Sector Coordinating Council (ESCC) is championing their report and discussions have taken place with the Financial Services Sector and Communications Sector, but he said the purpose to drive action forward has been lacking, yet is needed. Mr. Wallace noted the Working Group included the SICC from the point of view of recommended accountability to show that the NIAC is not only interested in making recommendations about what the President of the United States (POTUS) should do, but also all of the entities that work for him. He said they are "pointing the finger back at themselves" and saying if there is to be real executive public-private partnerships (P3), the private sector needs to come together in a more focused way. The concept of the SICC, which evolved from the 2015 NIAC report that discussed the recommended Strategic Infrastructure Executive Council (SIEC), led to that notion of private sector and Federal government leaders coming together.

Mr. Joyce asked how that related to the eighth recommendation, which describes the operational task force of experts led by a CEO-level body.

Mr. Wallace said it is to be determined by the leaders of the Federal government they identified in the report and the SICC. He said the first agenda stands to include some of the recommendations, but he added it will be "formation itself." Mr. Wallace noted that level group (which includes CEOs and senior leaders in government) sets priorities, performs strategic thinking, applies resources, and holds others accountable. If those leaders are meeting on a

quarterly basis, they need their Chief Operating Officers or Chief Information Security Officers to be executing a specific agenda, which requires a lower tier of people at the operational level to do work. Mr. Wallace explained there should be more full-time staff coming from private sector companies and government, creating a team to carry out the work of the operational executives.

Mr. Joyce said he did not understand the relationship of the SICC, which is called out as a responsible body, and the CEOs. He asked if they were the same, if they had a relationship, or if they were different.

Mr. Wallace clarified that they are one in the same. The SICC constitutes a source of senior executives. He added between the individuals who have been involved in the formation of that to date and the senior people in government, the senior people could be newly added or not have been involved to date. He said it is a facilitating approach to achieve the overall structure in place.

Mr. Joyce acknowledged the passion of the Electric community to join in at the CEO level. Although, he noted other sectors have not had the same desire. He mentioned sectors like the Telecommunications Sector, who he said are facing unique challenges in committing their CEOs time on a quarterly basis to make meetings at that level. He added, however, that they will keep pursuing that effort for the future.

Ms. Lau commented that she believes the NIAC's experience with the formation or the reconstitution with the ESCC was when the senior government side was willing to come to the table and it was that level of senior government involvement that attracted CEOs from private sector to join as well.

Mr. Wallace agreed that was the Working Group's observation as well. He said there is so much at stake for the Financial Services and Communications Sector executives that he believes it is extremely important for them to engage in the direction the NIAC is recommending. Mr. Carr agreed they must be involved in the first recommendation, because with a dark fiber system- the nation needs communications capabilities, should a disaster occur.

Mr. Joyce agreed and added he believes the entities themselves wish to be involved. He said the third recommendation identified the "best-in-class" tools. He cautioned the recommendation to remove Congress as a body recognized to help that effort. He said government entities have Federal ethics laws that do not allow the government to advise, recommend, or endorse industry efforts.

Mr. Carr spoke more on Recommendation Three. He said there is a "non-intuitive set of thoughts" and believes many in the room would agree that compliance is a primary driver of cyber hygiene. He added if something is done reluctantly, it is usually because there is a cost with no revenues to offset it. He estimated 30% of all network systems are compromised already, yet government and industry officials do not believe they have malware in their systems. Mr. Carr said when one understands they have ransomware in their system, suddenly self-

preservation becomes the driver. In order to make this voluntary, assessment tools need to be identified on an ongoing basis.

Mr. Joyce noted their second recommendation suggested a pilot of machine-to-machine information-sharing technologies. He said the Electric Sector has the Cybersecurity Risk Information Sharing Program (CRISP), which has recently proved tremendous value and able to take lead information and see the penetrations of intrusions in various areas, starting with leads and then looking at large volumes of data. Mr. Joyce asked if there was a conversation on how to increase the penetration of those data sources or whether regulation should be explored to mandate those. He also asked if they believe it should be voluntary.

Mr. Wallace answered that the Working Group did not go in the direction of a mandated approach. Through much of what they provided in their study, they encourage the opposite-create incentives (including market-based incentives), such as those provided for companies after 9/11. He said it can provide opportunity for companies not fully invested in machine-to-machine information-sharing. Additionally, he said mid-sized and smaller companies cannot be involved for a variety of reasons. He said the notion of advancing the pilot was there to create a "full airing" of the barriers to greater machine-to-machine adoption, what the experiences are, or what the marketplace competition is. Mr. Wallace clarified it was not their thought to principally need government regulation to mandate. He said their view was to begin with a helpful approach and if that is ignored, then return with more force.

Ms. Lau added that for mid-sized and small companies, the issue is not that they do not recognize there is a problem but rather there are other factors, such as cost. She believes it would be beneficial to be able to look across all organizations to ensure that CRISP and other machine-to-machine programs can be participated in by companies of all sizes.

Mr. Joyce commented that the NSC is very supportive of the concept of a national level GridEx that goes beyond the Electricity Sector. He noted POTUS received a brief on that and the concept of integrating the Financial Services and Communications Sectors. He said they are in the process of working with individuals that plan it and make it a more robust, real-world exercise. His last comment was on the recommendation of the National Security Advisor taking on the recommendations. He offered that the Homeland Security Advisor is more appropriate. Mr. Joyce said the Homeland Security Advisor directly reports to the President and has the cybersecurity portfolio, he also shepherded the EO responsible for this activity. He added that more problems could be created by crossing lines with people who do not directly engage in this expertise.

Mr. Wallace responded by saying he was fortunate to facilitate the executive tabletop for GridEx in 2013 and 2015. He has also been participating in the development of the scenario for 2017. He concluded it will be challenging, yet very insightful for those participating. He said he is glad to hear of the President's endorsement of broader participation in GridEx. Mr. Wallace responded to Mr. Joyce's second comment by saying the NIAC Members are not experts at knowing who in the Federal government should be in charge of what, but they specifically recognized DOD and ODNI in a number of areas because they see this as "whole of nation" and national security.

They made the recommendation from that perspective, but ultimately it is up to the President to determine how to respond to the recommendations. He added that is also how they came to conclusion of referencing NSA, because they are looking at the ability to bring the principals committee together with DOD and ODNI, in addition to the usual government agencies.

Mr. Joyce noted that he did not mean the National Security Advisor does not care passionately about cybersecurity, but the Homeland Security Advisor chairs those principals committees with DOD, ODNI, NSA, and CIA.

Mr. Kolasky spoke on the theme of governance. He was interested by the use of the phrase, "operation control," when discussing the tenth recommendation. He was interested in hearing more about that and noted within DHS, they are in the process of making the NPPD an operational component of DHS and working with Congress to give more authorities and streamline DHS' work on cybersecurity and critical infrastructure protection. Mr. Kolaksy asked what it would mean to have a governance structure above that, which has operational control of operations from different cabinet agencies.

Mr. Wallace said a question the Working Group asked, for which they received a consistently null answer was, "Who is responsible for the protection of the country in cyberspace?" He said presumably it is POTUS, but there is no accountable entity. He said the nation's private sector has a very strong capitalistic system. He said companies are not responsible for national security, but only responsible their shareholder or stakeholders interests. Conversely, the government is responsible for national security, but does not directly control the private sector entities needed to carry out its role. Mr. Wallace said the notion of tangible executive P3 is to recognize that if a disaster occurs, it can be easier to determine who is capable of making decisions to respond to allocate resources. He said it should be somewhat agnostic in extreme situations as to whether it should be private sector or government. He said they received similar feedback from numerous sources, both former government and industry, that there is a better approach which combines private and public sector. Mr. Wallace also mentioned in their report that they suggest looking at the way other countries are handling these same issues and have made recent changes to consolidate efforts. He did note that the Working Group intentionally did not lead with Recommendation Ten because they understand the challenge of vetting the alternatives.

Mr. Kolasky said his concern is it leads to a creation of a cyber agency, which he believes is an inefficient path. He is not sure if it would ultimately take the country to a better stance, but as an individual who has been with DHS for almost 15 years he understands DHS has aspects of homeland security, but so do other agencies. He said standing up another department creates a lot of agency inefficiency. Mr. Kolasky said as the Working Group talks about operational control, creating a new department seems to be the way they would achieve operational control.

Mr. Wallace said as they deliberated, Recommendations 1-7 and 9 all are exercised, with eight taking a facilitated approach to cause things to happen. He said many insights will come to the table about how the nation can be more efficient and effective, their job as NIAC Members is to identify the issue. The recommendation manifested from the echo chamber of this topic, because people are frustrated both in and outside of government. He said they made the recommendation

because it is something that needs to be done, but they do not have the foundation to say what to do.

Ms. Jan Allman said going through the GridEx recommendation, it can be unclear who is responsible for the response action. She said they will need to focus more on that area, which may also improve response.

Mr. Kolasky said there is a difference between not practicing the plan enough to know how it will work, rather than just not knowing.

Ms. Devon Streit said she was appreciative of the report. She thinks some of the progress they can make against the more difficult recommendations are nuanced. Ms. Streit spoke to Mr. Boston's comment about declassification and said she has received mixed responses from utilities whether it is important for them to know the classified information. She sees potential in that area. She also spoke to Mr. Joyce's comments regarding the government not being able to be more unambiguous, she believes the government is interested in researching test beds and other cautious ways to find out what works, but not if they are asked "why or who?" She said progress could be made through nuances and a mutual understanding of what is attempting to be done and the limitations the government faces. Ms. Streit asked if there was an echo chamber in the barriers they faced while working on the report and if they could identify the top three barriers.

Mr. Wallace said among the barriers that arose- legal issues, liability issues, and privacy issues were among the top. Mr. Carr added another area was the FS-ISAC has developed an effective way of sharing information. He said the barrier to advancing is the large amount of classified information and they do not have the machine-to-machine capabilities to exchange information quickly enough.

Ms. Streit said in a number of conversations she has had with Section IX companies, they have said they are collecting information at a significant rate. She asked if there were any conversations on the industry side of ways to share that information with the government.

Mr. Wallace said it runs into the same legal, liability, and privacy issues. He said CEOs must serve their stakeholder and shareholder's interests and not expose the company. He said while there are CEOs who wish to do more as patriots, the system does not facilitate doing that without taking risks.

Mr. Brian Peretti, from DOT, said there is a lot of process mentioned in the report moving forward. He said the examples identified in the discussion were helpful and he believes it would be beneficial to have a dialogue almost immediately. Additionally, he asked to be provided some clear examples of the barriers mentioned. He said those could begin to be tackled right away as everything else is worked through. Mr. Peretti said many of the recommendations are "big picture", but he believes there may be some "on the ground" items that could be tackled relatively quickly.

Mr. Wallace said the ESCC and FSCC have legal, liability, and privacy issues that they are dealing with at all times. He said he would defer to getting specific with an engaged dialogue with those groups, which DHS could facilitate. He said he could provide examples, but it would only be from his own ESCC perspective. Mr. Wallace believes it would be more beneficial coming directly from the coordinating councils.

Mr. Peretti said his concern is that is a "stovepipe." He said while he works with those councils regularly, the issues of a particular sector may have just not happened or recognized yet on the government side. He continued that if there is a specific problem that can be recognized, it would be helpful for DOT to help work through and solve that problem. He said the discovery process should not be what drives the solution if someone else has already discovered it. Cross-sector sharing is what achieves the dialogue. Mr. Peretti reiterated if there were any examples anyone from the NIAC could identify, DOT could help work through those.

Ms. Lau said that was one of the reasons for the formation of the SICC, because of the desire of the Electric Sector and Financial Services Sector to share across other sectors. Furthermore, the NIAC has discussed how it is important for sectors who are more advanced to help those other sectors that may not have the resources to move as quickly. Mr. Lau said the SICC may be a good source for Mr. Peretti.

Mr. Peretti said he knows it will take a while before that begins. Therefore, if there are examples they have already identified, DOT could begin to work on them immediately.

    VI.   **PUBLIC COMMENT**   *Ginger Norris,* DFO, NIAC, DHS

A written public comment was emailed to the NIAC inbox on August 23rd, 2017, by Daniel Gallington. His comment is as follows:

Response to the draft report on "Securing Cyber Assets - Addressing Urgent Cyber Threats to Critical Infrastructure", please consider the following comments:

1) A program of proactive cyber stress testing is the best way to identify and fix our cyber weaknesses, and we should be doing it for our critical infrastructure, both public and private.
2) Voluntary reporting is unreliable as there are inherent conflicts of interests for management to report, hence a reluctance to disclose. Therefore, the "voluntary reporting" concept in cyber related legislation and implementing regulations simply does not address the scope of the cyber risk.
3) The following articles pertain to this issue set and should be mentioned in the draft report:
    a) http://www.govexec.com/magazine/features/2011/08/the-challenge/34654/
    b) http://www.washingtontimes.com/news/2015/sep/21/daniel-gallington-the-chinese-hack-of-opm/

VII. COUNCIL DELIBERATION   *Constance H. Lau,* NIAC Chair
          AND ACTION

Dr. Scott said what makes this report so different is the urgency. She said most NIAC reports are not as action-oriented, but she stressed the point in that report that warned of a potential pre-9/11 moment in the nation's cybersecurity. She discussed barriers and mentioned a knowledge and information gap. She added some of that is due to the fragmentation in addition to the overwhelming amount of information to absorb. Dr. Scott said, "We have stayed on the voluntary and incentive side," but she believes there is a bully pulpit opportunity if private and public sector adjoin. She said the country is counting on them to do something very different.

Mr. George Hawkins said he was impressed by the report and the passion in which it was delivered. He noted the inherent risk between recommendation two and one. He said he constantly hears how everyone wants to be more integrated and communicate better, yet also wish to be isolated and separate. He said the more machine-to-machine technology is used, they create an avenue of risk while creating a connection point. Mr. Hawkins said they are trying to accomplish just that at DC Water- connect everything, but also be able to isolate it quickly at the same time. His second point was on the notion of identifying the "best" of anything and the difficulty of government attempting that. He said a possible outcome could be instead of a "best", there could be a minimum standard. Mr. Hawkins' third comment was that if the numbers of recommendations are meant to be priorities, he believes Recommendation Six and Seven should be flipped. He explained he recently obtained a security clearance and discussed his frustrations with the limitations of discussing classified information or how it can be utilized. He said the notion of declassifying information that needs to be disseminated should be the higher priority. Mr. Hawkins was fascinated with comments on Recommendations Eight and Ten. He was invited to attend the ESCC and is still astonished by the scale of participation and its effectiveness. Mr. Hawkins' final point was that he does think mandates should still be an option. He provided an example of the standards for water quality. He said DC Water does many voluntary and incentive-driven work, but at least half of what they do is required. He said he thinks there will be participation in Recommendations Eight and Ten if the prospect is out there, but he believes there may be aspects of cybersecurity that are so important they must be done by all companies. He said if there are areas of companies in industry that cannot afford standards or mandates, the next question is how to solve that rather than have those areas not be protected, because their customers deserve it as much as those served by larger entities. He reiterated how impressed and supportive he is of the report.

Mr. Wallace said the Working Group chose to not describe how to get to the right place in the report, because they wanted to begin with what must be done, followed by incentives. He said the goal is to maximize or optimize a set of incentives. If that does not work, the third stage would be mandates. He said they had conversations when working on the report that they would support regulation if it came to that stage. Mr. Wallace said they could invert recommendation six and seven.

Ms. Norris read a comment from General Albert Edmonds,

"In Recommendation One, DOD should be added to the Action Required By section, because they already have the mission to provide the White House and National Command Authority Communications, via Defense Information Systems Agency (DISA). The idea in Recommendation Ten was not to create a new agency, but to put someone in charge who would be responsible for pulling together government and industry players to defend or recover from a major cyber event. DHS Command Center or United States Northern Command in conjunction with DHS was the thought process."

Mr. Wallace said their thinking was with ODNI and NSC, which also includes access to DOD. He said they could still specifically mention them there, but wondered how his government colleagues felt about that.

Mr. Joyce said he thinks it relates to the Working Group's intent for separate, secure communications networks. He said if they meant something that would pull the OT of the electric and power companies off the standard internet and give it its own fibers, he believes that is in the recommended organizations identified. He said if they are talking about creating a national level emergency set of communications that the government will use to coordinate responses to national emergencies, then DOD should also be listed.

Mr. Wallace said their intent was the latter and he believes that was what General Edmonds was referring to. He suggested to Ms. Lau they amend the first recommendation to add DOD. Mr. Wallace commented on the second half of General Edmonds' comment and clarified that the Working Group did not want to solve the tenth recommendation with a finite answer.

Ms. Margaret Grayson said she had nothing significant to add, but commented on Recommendation Four. She said there is significant risk of not having enough people to have the appropriate training, education, or background for the needed cyber assets that will be coming forward. She said it is important for education to not only be introduced at the university level, but at technical schools as well.

Mr. Hawkins believes it should be "on the table" in Recommendation Eight for the enterprise to create standards of what must be done as an option, because that will drive people into the discussion.

Mr. Boston added on to Ms. McDonald's earlier comments on pilot programs. He added that the CRISP software was developed by the Pacific Northwest Laboratory and the classified analysis required is also run by the Pacific Northwest Laboratory. He suggested where they said, "sharing best practices" on Recommendation Three, he suggests adding the sharing of industry and government tools.

Ms. Lau said the suggested changes to the report were on slide 19, along with the amendment from General Edmonds to Recommendation One to add DOD. Mr. Boston also made an amendment to Recommendation 3; subparagraph B to read, "to showcase best-in-class tools across government and industry."

The Council voted upon and unanimously approved the Working Group's *Securing Cyber Assets* report, as amended.

    VIII. **NEW BUSINESS**   *Constance H. Lau, NIAC Chair*

No recommendations of new business.

    IX. **CLOSING REMARKS**   *Constance H. Lau,* NIAC Chair

                                                    Robert Kolasky, Acting Deputy Under Secretary, NPPD

Mr. Joyce thanked the Working Group for their time and effort. He said cybersecurity is an up and coming focus of the Trump Administration and of the nation as a whole. He thanked them for their effort in considering what needs to be done to make the nation's cybersecurity stronger and better.

Mr. Kolasky echoed Mr. Joyce's sentiments and said he has participated in many NIAC report deliberations and believes the discussion they just had was of the richest. He said it matches the hypothesis they have of the impact of the report. He added that DHS is leading parts of the task to implement the EO on Section IX. Their deliverable is due in about 70 days from the QBM and he said they will be considering this input. He thanked the Working Group for all their work and said it will be very useful.

Ms. Streit thanked the NIAC for offering the opportunity for her to attend the QBM. She said having spent many hours with her government colleagues, she assured the Council that although they may be sitting quietly, they share the NIAC's sense of urgency. Her last comment was that none of the great recommendations they have submitted will be possible without very strong industry support.

Mr. Peretti thanked the Council for inviting him to the QBM. He thinks the report is very interesting and they have a lot of opportunities to work together. He believes the Working Group's work has leveraged many of the discussions to be had moving forward. He said one challenge is how to fix the more difficult problems that have been raised by industry and have been constricting the private sector's ability to move forward and to secure their systems. Mr. Peretti said the more examples the NIAC can provide, the easier it will be to create real progress.

Ms. Lau said their discussion has been one of the richest and most robust. She is encouraged by the interchange they had, because their job is to make recommendations to the government, but in order to establish true P3s the private sector must also increase their efforts. She said some parts of the private sector already want to come to the table and provide faster support, but those sectors must also aid the other, less advanced sectors to create complete cross-sector participation. Ms. Lau added that they think private sector and government working together will most likely have all the capabilities, but there needs to be more organization in order to deliver for the nation.

Dr. Scott said the NIAC is a very serious partner for the government and wish to be as helpful as possible.

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

Ms. Lau adjourned the quarterly business meeting.