## NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

**BUSINESS MEETING AGENDA**
April 8, 2013
1:30 p.m. – 4:30 p.m. EDT
United States Access Board
1331 F Street NW, Washington, DC 20001

| | | |
|---|---|---|
| **I.** | **OPENING OF MEETING** | *Nancy J. Wong*, Designated Federal Officer (DFO), National Infrastructure Advisory Council (NIAC), Department of Homeland Security (DHS) |
| **II.** | **ROLL CALL OF MEMBERS** | *Nancy J. Wong*, DFO, NIAC, DHS |
| **III.** | **OPENING REMARKS AND INTRODUCTIONS** | *Constance H. Lau*, NIAC Chair<br><br>*Suzanne Spaulding*, Deputy Under Secretary for the National Protection and Programs Directorate, DHS<br><br>*Caitlin Durkovich*, Assistant Secretary for Infrastructure Protection, DHS<br><br>*Charles Donnell*, Special Assistant to the President for Resiliency, National Security Staff<br><br>*Dr. Ahsha Tribble*, Senior Director for Response, National Security Staff<br><br>*Nitin Natarajan*, Director, Critical Infrastructure Policy, National Security Staff |
| **IV.** | **NIAC PRESENTATION ON REGIONAL RESILIENCE WORKING GROUP** | *Constance H. Lau*, NIAC Working Group Chair<br><br>*Dr. Beverly Scott*, NIAC Working Group Co-Chair |
| **V.** | **PUBLIC COMMENT: DISCUSSION LIMITED TO MEETING AGENDA ITEMS AND PREVIOUS NIAC STUDIES** | *Nancy J. Wong*, DFO, NIAC, DHS |

| | | |
|---|---|---|
| **VI.** | **REGIONAL RESILIENCE WORKING GROUP DISCUSSION** | *Nancy J. Wong,* DFO, NIAC, DHS |
| **VII.** | **BRIEFING AND DISCUSSION ON EXECUTIVE ORDER 13636 AND PRESIDENITAL POLICY 21 BY THE DEPARTMENT OF HOMELAND SECURITY** | *Robert Kolasky,* Executive Director, Integrated Taskforce for the Implementation of EO 13636 and PPD-21, DHS |
| **VIII.** | **CLOSING REMARKS** | *Constance H. Lau,* NIAC Chair<br><br>*Suzanne Spaulding,* Deputy Under Secretary for the National Protection and Programs Directorate, DHS<br><br>*Caitlin Durkovich,* Assistant Secretary for Infrastructure Protection, DHS<br><br>*Charles Donnell,* Special Assistant to the President for Resiliency, National Security Staff<br><br>*Dr. Ahsha Tribble,* Senior Director for Response, National Security Staff<br><br>*Nitin Natarajan,* Director, Critical Infrastructure Policy, National Security Staff |

## MINUTES

**NIAC MEMBERS PRESENT IN WASHINGTON:**
Mr. Glenn Gerstell; Ms. Margaret Grayson; Mr. Michael Wallace

**NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:**
Mr. Albert Edmonds; Mr. David Kepler; Ms. Constance Lau; Mr. Thomas E. Noonan; Dr. Beverly Scott; Mr. James Reid

**MEMBERS ABSENT:**
Mr. Jack Baylis; Mr. David Bronczek; Mr. Gilbert Gallegos; Mr. Philip Heasley; Commissioner Raymond Kelly; Mr. Donald Knauss; Mr. James Nicholson; Mr. Gregory Peters; Mr. Bruce Rohde; Mr. Greg Wells; Mr. David Grain

**SUBSTANTIVE POINTS OF CONTACT ATTENDING VIA CONFERENCE CALL:**
Sgt. Tom Brennan (for Commissioner Raymond Kelly); Ms. Joan Gehrke (for Mr. James Nicholson); Mr. Joseph Long (for Mr. Gregory Peters); Katherine English (for Mr. Kepler)

**OTHER DIGNITARIES PRESENT:**
Ms. Caitlin Durkovich, Assistant Secretary, IP, DHS; Mr. Robert Kolasky, IP, DHS; Mr. Charles Donnell, NSS; Ms. Samara Moore, NSS; Mr. Nitin Natarajan, NSS; Ms. Suzanne Spaulding, Deputy Under Secretary, NPPD, DHS; and Ms. Nancy Wong, DFO, NIAC, DHS

## I, II. OPENING OF MEETING, ROLL CALL *Nancy J. Wong*, DFO, NIAC, DHS

Nancy Wong opened the meeting and called the roll. She then turned the meeting over to Constance Lau, NIAC Chair, and Dr. Beverly Scott, NIAC Vice Chair.

## III. OPENING REMARKS AND INTRODUCTIONS

*Constance H. Lau*, NIAC Chair

*Suzanne Spaulding*, Deputy Under Secretary for the National Protection and Programs Directorate, DHS

*Caitlin Durkovich*, Assistant Secretary for Infrastructure Protection, DHS

*Charles Donnell*, Special Assistant to the President for Resiliency, National Security Staff

*Dr. Ahsha Tribble*, Senior Director for Response, National Security Staff

*Nitin Natarajan*, Director, Critical Infrastructure Policy, National Security Staff

Ms. Lau welcomed all NIAC members and Federal Government representatives, and provided an overview of the meeting. Topics included a status report from the Regional Resiliency Working Group (RRWG), as well as a briefing and response from the Council to questions from the government on Executive Order 13636 (EO) and Presidential Policy Directive 21 (PPD-21). Ms. Lau then opened the floor for opening remarks from administration officials.

Mr. Donnell thanked all those present and gave introductory comments on the EO and PPD-21. Both policies were signed by the President on February 12, 2013 to build on the previous work the Department of Homeland Security (DHS) has accomplished over the past 10 years. Three key imperatives are driving the Federal approach: refining and clarifying functional relationships across the Federal Government, enabling effective information exchange and becoming better partners with the private sector, and implementing an integration and analysis function that can inform planning and operations decisions regarding critical infrastructure. PPD-21 will focus on security and resilience as key tenets of critical infrastructure protection and will address both cyber and physical threats. Public-private partnerships will be affirmed by these policies, which seek to ensure that owners and operators are engaged throughout the implementation process —

rather than just in the final stages. The EO will go hand in hand with PPD-21 to enhance cybersecurity.

The National Security Staff Cybersecurity and Resilience Directorates are working together to ensure implementation in a collaborative and simultaneous manner. The goal is to facilitate an environment that is efficient, innovative and economically justifiable, while also promoting safety, security, business, confidentiality, privacy, and civil liberties. These policies clear the way for more efficient sharing of cyber threat information with the private sector, and direct the establishment of a cybersecurity framework to identify and implement better security practices among the critical infrastructure sectors. DHS will be responsible for implementing the majority of these deliverables from the directives with the help of all levels of government and the private sector.

Mr. Donnell thanked Ms. Spaulding, Ms. Durkovich, and Mr. Kolasky for their work with the Integrated Task Force (ITF) and other efforts aiding implementation of the EO and PPD-21. The Administration is looking forward to working with critical infrastructure owners and operators, as well as with State, local, tribal, and territorial leaders, to build on past successes while charting a course for the future. He ended by noting that the security of the Nation is not dependent on the Federal government alone, but rather will require a "whole of Nation" approach that not only includes all levels of government and critical infrastructure, but also the general public.

Ms. Lau thanked Mr. Donnell for his comments, and noted that the Council appreciates the tremendous importance of the changing critical infrastructure security and resilience (CISR) mission. She pointed to cyber resiliency and protection as topics she believes will be key to the Nation's security.

Ms. Spaulding thanked Ms. Wong, Ms. Lau and Dr. Scott, Mr. Wallace, and all NIAC members. She emphasized that a conscious decision was made early in the drafting process for the EO and PPD-21 to implement these policies holistically. She added that prior lessons learned will be used as the National Infrastructure Protection Plan (NIPP) is updated in the coming months.

The ITF's work is informed by past NIAC reports, Ms. Spaulding said. The work the Council is doing on resilience is critically important, as the task force's work on resilience will be informed by the findings of the report. One particular challenge for the ITF will be measuring resilience, in accordance with the Government Performance and Results Act, which requires agencies to provide measurable outcomes from projects.

Ms. Spaulding noted the Council's work studying the aftermath of Superstorm Sandy. There are lessons to be learned in terms of resiliency; what can be done better; how information can be distributed quicker; and what can be done before, during, and after a storm to provide further

protection, resilience, and assistance to communities. She added that this effort also provides an opportunity to determine ways of building resilience to critical infrastructure assets, as well as considering creative new means for funding via the public-private partnership.

Innovators and engineers have changed society's architecture and infrastructure, so partners need to change their thinking, particularly in terms of creative financing for resiliency and aging infrastructure.

Ms. Durkovich began her comments by thanking Ms. Spaulding and all NIAC members. She commended Council members for their work, and noted that the value and influence of their contributions was evidenced by the number of Administration and DHS officials in attendance. She also thanked members for balancing their Council work with their full-time jobs, and expressed her interest in the resilience report.

Ms. Durkovich noted that the nation's infrastructure is aging and failing; some water systems were built 150 years ago, and some Federal transportation systems are more than 50 years old, including the interstate highway system. In many cases, ownership is complex, making long-term investment difficult. The government needs private sector help with investment and incentive programs to secure critical infrastructure for the next generation, while balancing those needs against an equally strong demand for short-term funding.

Collaboration under the EO and PPD-21 will be necessary to achieve deliverables and set new performance goals, Ms. Durkovich said. She encouraged leveraging and borrowing concepts and ideas as part of the holistic approach to integrating cyber and physical security and resilience.

Ms. Durkovich also suggested that a joint study between the NIAC and the National Security Telecommunication Advisory Committee (NSTAC) could be launched to focus on shared cyber problems.

Dr. Scott thanked Ms. Wong, Ms. Lau, NIAC members, and administration and DHS officials. She echoed Ms. Lau's gratification to DHS leadership for having situational awareness on all of their projects. She also thanked NIAC and working group members for continuing to pursue ways to improve resiliency by building on what exists and working smarter and more efficiently.

## IV. NIAC PRESENTATION ON REGIONAL RESILIENCE WORKING GROUP

*Constance H. Lau*, NIAC Working Group Chair

*Dr. Beverly Scott*, NIAC Working Group Co-Chair

Ms. Lau requested the Regional Resilience Working Group to deliver its briefing. Dr. Scott and Mr. Wallace began the Regional Resilience Working Group (RRWG) presentation. Dr. Scott noted that Mr. Wallace would have an additional brief on current work in the Electric and Nuclear sectors. That work has yielded more focused and regular executive-level engagement with the Government, and could be a model for enhanced information sharing in other sectors to support regional resilience.

Dr. Scott reiterated that the purpose of the study is to identify ways regions can become more resilient, and the steps the Federal Government can take to help regions accomplish resilience goals. She noted that the RRWG hopes to find best practices, process improvements, and define the Federal role over the course of the study.

Since the last quarterly business meeting, the Regional Resilience Working Group initiated the Philadelphia Case Study on Superstorm Sandy. The work plan was also revised to reflect the new schedule and to integrate the case study work plan. The RRWG began scheduling interviews with Federal agencies to understand what they learned from Superstorm Sandy and what role Federal Government can play in helping regions improve resilience. The working group also plans to interview national resilience leaders to understand how Federal policies match and can influence resilience behaviors of individuals, communities, companies, as well as State and local governments.

At the October 2012 Quarterly Business Meeting, the working group reported on their original plan to start a case study to examine the effects of infrastructure stresses in the Philadelphia Metropolitan Statistical Area (MSA) to gain insights and recommendations to pass on to other regions of the country. Shortly after that meeting, Superstorm Sandy hit the Mid-Atlantic, causing loss of life and billions in damage. The working group decided to study the storm's effects, in order to see how critical infrastructure can be strained in times of great need. The working group then formed a study group, composed of members representing all 16 critical sectors, as well as State and local officials of Pennsylvania, New York, and New Jersey, which will extract lessons learned from the storm to understand steps regions can take to improve resilience.

The study group was formed in late February. The study group collected personal experiences, conducted discussions, and did research and interviews. Sector-specific panel discussions are planned over the next few months.

Dr. Scott emphasized that initial observations are provisional and not final findings or conclusions. These observations include:

- The scale and scope of Sandy was much larger than many had previously seen, creating shortages of equipment and supplies not experienced in other storms.
- In New Jersey, preplanning and coordination focused on the Lifeline Sectors. Coordination during the storm was handled through a private sector desk in the State EOC, and pre-event conference calls were held with the private sector.
- As a disaster escalates, companies can spend a lot of time educating outside leaders on their decisions and actions. Companies should do as much outreach up front so that State and Federal partners understand the company's response rationale, operating procedures, and capabilities going into an event. Ongoing outreach is also needed between sectors, as officials may leave or be assigned different roles between events.
- The advanced warning of the storm enabled preplanning and prepositioning of assets. Had this type of destructive force been an unexpected terrorist attack or cyber event, the preparation would not have been as coordinated.
- Social media played a big role in Sandy, with both positive and negative implications. Rumors were more rampant and spread faster with social media, but the tools were also used as a source of information on outages, which aided operations.

The work plan for the regional resilience study consists of research, interviews, and case studies that will produce findings and recommendations over the next six months. Last fall, the working group examined Federal authorities for disaster response, processes and measures for regional resilience, as well as best practices from regional resilience groups from across the country. Results of these studies were reported at the October 2012 Quarterly Business Meeting.

The working group intends to continue research through May. Each piece will be incorporated into the regional resilience study, and then developed, integrated, and analyzed. The working group plans to provide a final report and set of recommendations for presentation at the October 2013 Quarterly Business Meeting.

Mr. Wallace then discussed executive-level engagement efforts in the Electricity and Nuclear sectors. Three previous NIAC recommendations on executive-level engagement were published in October 2008, October 2010, and January 2012. Several current NIAC members were involved in all or some of these studies; Mr. Wallace was involved in all three, and offered his observations.

The insights included in this presentation did not become obvious until the production of the January 2012 study, when working group members realized the recommendations from all three were similar. In all three studies, the top recommendation focused on executive-level engagement, though the recommendations were worded differently. The recurring

recommendations all suggested that greater engagement should exist within sectors, as well as between sectors and partners in government. They also stressed that without improved executive-level engagement, it will be difficult to implement other recommendations from the studies.

Mr. Wallace cited three past executive-level engagement efforts:

- Project Aurora, a 2006 engagement effort based around a control system vulnerability for nuclear plants that was discovered by the government. The information was highly classified, but one senior executive was made aware of the issue, and was subsequently able to translate the system vulnerability to other private sector partners. In 4 months, all U.S. nuclear plants were mitigated against this vulnerability, thanks to a timely declassification process.

- The Critical Infrastructure Key Resources (CIKR) Executive Industry Council, which was a product of the 2008 study on executive-level engagement. Formed under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework, the Council was meant to involve CEOs across multiple sectors because the initial recommendation focused on the need for policy-level discussions between the private sector and the Federal Government. Ultimately, the Council lost momentum because it lacked immediate benefits, and the complexity and speed of the effort was unsustainable. The Council was working at a high policy level across sectors, but the benefits were broad and long term rather than immediate. He stressed that a lot of good work was done, even to the point of funding resources for implementation. But when the 2008 financial crisis hit, members were overwhelmed by personal and professional commitments, to the detriment of the Council.

- Kaleidoscope, a U.S. Secret Service (USSS) program that provides physical and cyber protection for the President. As it was being developed, there were problems deploying the approach to the field, and the USSS engaged senior executives to gain insights. In roughly 12 months, the program was altered based on those insights to make it more effective. Benefits of the new approach were observable shortly thereafter. The approach was formalized and established as the standard operating procedure for the USSS when dealing with National Security Special Events that have a cybersecurity focus.

After synthesizing pertinent information concerning executive-level engagement from the three studies, Mr. Wallace and fellow members extracted three key elements of success that were reported out in the January 2012 study: trusted relationships, CEO engagement, and simple process. Trusted relationships should be both within sectors as well as between sectors and Federal partners. He noted that these foundational trust relationships were present in all successful efforts. CEO engagement is a tough issue; there are many demands on one's time, but determining why and when CEOs can and should get involved is an important issue. Once CEOs

do get involved things happen, Mr. Wallace said, emphasizing the example provided by the Kaleidoscope project. Finally, he explained the need for a simple process for executive level engagement. Complexity is the antithesis of success when busy people are trying to coordinate among themselves, he added.

Mr. Wallace added that in his experience, value proposition also plays a role in executive-level engagement. CEOs need to understand the benefits of engagement before they put time or resources into the process, as there are already too many activities competing for their time. As the value proposition increases, time and attention become greater as well.

The Electricity Sector provides a model for other sectors' efforts to establish executive-level engagement. The model builds off the success of the Kaleidoscope program, which successfully engaged five CEOs — including Ms. Lau — to help deploy the USSS model. This success has created a strong precedent for future engagement.

The sector began seeking interactions with the Federal Government on some additional opportunities reported in 2011, though success did not immediately follow. Mr. Wallace explained that they were not able to resonate with the public-private partnership at a senior level for about a year. In addition, the Fukushima Daiichi nuclear disaster sidetracked engagement efforts, though the incident was informative for many CEOs and government partners, whose nuclear clients were forced to re-evaluate resiliency after the disaster. Engagement efforts resumed following mitigation of the Fukushima disaster, and the event helped public and private partners realize that the threat environment was changing significantly. As a result, the value proposition became clearer to executives in the context of risk management. Electricity Sector CEOs had a meeting with the Secretaries of DHS and the Department of Energy (DOE) in July 2012. This was an introductory meeting, but started a process that, by January 2013, led to a framework that is being aggressively implemented.

Leaders in the electricity and nuclear sectors are working with the Edison Electric Institute (EEI) to initiate regular engagement with government leaders on resilience issues through two groups: the Joint Electric Executive Committee and the Senior Executive Working Group. The Joint Electric Executive Committee consists of 23 CEOs and the Deputy Secretaries of Energy and Homeland Security. The committee meets quarterly to examine priorities, policy, resources, and accountability issues. The Senior Executive Working Group consists of 16 senior executives (COO, CIO, and Senior VPs from a cross section of the industry) working with the Assistant Secretaries of Energy and Homeland Security. The working group meets bi-weekly to monthly to work on focused agendas and deliverables through subgroups. A progress report from a recent joint meeting of the two groups will be published at the end of May.

In addition, Mr. Wallace noted that four trade associations have come together to ensure the physical and cybersecurity of the electric grid as concerns grow in the current threat environment

and the value proposition for involvement increases. This is a rather uncommon and unprecedented feat, Mr. Wallace said, and the cooperation needs to continue in case future events overwhelm the private sector and prevent traditional means of cooperation.

After the presentation of the Working Group, Ms. Wong opened the meeting to comments on the presentation from the Working Group, and other topics addressed by the Council in the past. Subsequent to the public comment session, the Chair opened the floor to further discussion of the Working Group report.

Ms. Spaulding noted that the objectives will be helpful to the Federal Government. She was pleased to see an aggressive schedule, and commented that it pairs well with the aggressive timetable set by the National Security Staff. Ms. Spaulding added that CEO engagement efforts have been very meaningful in the past, and offer promise moving forward.

Mr. Donnell thanked Mr. Wallace for his partnership and continued hard work, noting the value of his efforts before, during, and after Superstorm Sandy. He voiced support for the utility of the electric sector model for other sectors, and noted his interest in continuing their working relationship.

Ms. Lau said the working group will be interviewing Federal officials who dealt with Superstorm Sandy. She added that NIAC members may still join the working group, in order to cross-pollinate successes and best practices from others and their sectors.

Ms. Wong requested Ms. Lau to conduct a Council vote for the proposed moving of the final report for the Regional Resilience Working Group from the July to the October QBM. Mr. Wallace motioned for this change with Mr. Kepler seconding the motion. No Council members opposed.

| | | |
|---|---|---|
| **VII.** | **BRIEFING AND DISCUSSION ON EXECUTIVE ORDER 13636 AND PRESIDENITAL POLICY 21 BY THE DEPARTMENT OF HOMELAND SECURITY** | *Robert Kolasky,* Executive Director, Integrated Taskforce for the Implementation of EO 13636 and PPD-21, DHS |

Ms. Lau then introduced Bob Kolasky, Director of the Integrated Task Force for the Implementation of the EO and PPD-21 (ITF).

Mr. Kolasky thanked Ms. Lau, National Security Staff, and NIAC members for the opportunity to speak about the EO and PPD-21. Mr. Kolasky noted that there is still plenty of work to be done. He also emphasized the appreciation of White House members for the work completed and the issues raised by NIAC members over the past few years, all of which have shaped policy.

Mr. Kolasky noted that the briefing would address some common themes and areas of discussion, including the public-private partnership, value proposition, and risk management, as well as critical infrastructure security and resilience (CISR). These terms — which have been used in previous NIAC reports — were purposefully chosen for use in the EO and PPD-21 as a means of building upon the advice NIAC members have offered to the President over the years. Mr. Kolasky stressed that this is part of a larger effort to converge actionable themes into an enduring framework for CISR that involves a whole-community approach.

Mr. Kolasky outlined his presentation, noting topics would include questions relevant to NIAC members and relating to the value proposition for businesses in improving security and resilience; the benefits of the public-private partnership model; the successes and challenges of the security and resilience mission; and a discussion of ideas under review.

He began by discussing the value proposition of teamwork and incentives for the private sector. Government can encourage the private sector to take higher levels of security and resilience to help mitigate gaps stemming from a lack of information or from general risk mismanagement. Previously enacted policies emphasize that CISR is best done in partnership between owners and operators and government. Mr. Kolasky added that the primary responsibility lies with owners and operators, but that the government has a role as a facilitator of information sharing, as well as in the promotion of best practices, scaling of standards and other mechanisms, and in incentivizing research and development to play a role in enhancing security and resilience.

Mr. Kolasky then discussed the driving forces behind the new policies. The policies were meant to look at where the Federal Government fit in the whole-community and whole-of-nation approaches, and how deeper integration and synergies could be created between the public and private sector. Mr. Kolasky also noted that the 21$^{st}$-century risk and threat environment is more challenging and uncertain than it was even a decade ago. Cyber threats pose some unique challenges; this threat underlines the need to share information and to collaborate on vulnerability mitigation measures in terms of risk management for cybersecurity.

EO 13636 and PPD-21 were signed on February 12, 2013. The documents represent a tremendous opportunity for the ITF to work with industry, State, and local government. Participants have noted that they want this to be an ongoing dialogue between the government and the private sector. This transition from infrastructure protection to infrastructure security and resilience is meant to instill confidence that critical services will be functioning on a consistent basis, especially when called upon during a crisis or post-crisis situation.

Mr. Kolasky continued his presentation by outlining the EO. The document has five themes: encouraging development of a technology-neutral cybersecurity framework; promoting and incentivizing the adoption of cybersecurity practices; increasing the volume, timeliness, and

quality of cyber threat information sharing; incorporating strong privacy and civil liberties protections; and exploring the use of existing regulation to promote cybersecurity.

Development and adoption of a technology-neutral cybersecurity framework is central to the EO, Mr. Kolasky said. The framework provides a baseline level of cybersecurity, which is derived from domestic and international standards and best practices. The hope is that owners and operators across the country, whether their assets are critical or non-critical infrastructure, will adopt the cybersecurity framework. The framework is not a remedy for all challenges, but it promotes cybersecurity risk management and good cybersecurity hygiene, Mr. Kolasky said.

On the subject of promoting and incentivizing the adoption of cybersecurity practices, Mr. Kolasky noted that one of the keys of the EO is promoting adoption of the cybersecurity framework. That comes with defining the cybersecurity framework, an effort that has been led by the National Institute for Standards and Technology (NIST) at the Department of Commerce. NIST released a public Request for Information (RFI), to which they are expecting a substantial number of responses and comments on the framework for critical infrastructure cybersecurity. The comments will be taken, analyzed, addressed, and incorporated into the framework over the next 6 to 8 months.

The ITF is also examining potential incentives the Government can use to encourage adoption of the voluntary framework. Mr. Kolasky said DHS expects that the cybersecurity framework will be adopted by many companies as a good business practice, and that there is a role the Government can fill to encourage broader adoption. The ITF will study what role that is.

The EO also requires a review of methods to increase the volume, timeliness, and quality of cyber threat information sharing. Threat information sharing at both the classified and unclassified level is imperative, so simply granting more security clearances to handle the information would be insufficient. Sharing information at the unclassified level, with open-source methods, is also of great value. Bringing together what works in both the government and private sector helps provide a holistic picture of the cybersecurity landscape.

There is a two-way cybersecurity information service challenge that the nation must work through. Relationships must be created based on trust so that information can be shared with confidence. In addition, there is a need for expanded processes for sharing on the classified level with partners who are attempting to mitigate active threats. The Enhanced Cybersecurity Services (ECS) program, which DHS runs, is an operational threat information sharing program that seeks to address this challenge. The EO addresses the need to expand this concept to all sectors of the critical infrastructure community. The ITF is working through communication service providers on this issue

Privacy, civil rights, and civil liberties are also addressed in the EO. As information sharing is enhanced to promote the use of cybersecurity and the cybersecurity framework, it should be done so with respect for the importance of individual privacy and civil liberties, and not using gathered information for unintended purposes. DHS and other Cabinet agencies are required to study the effects that any new cybersecurity programs will have on privacy and civil liberties, and conduct a follow-up report.

The EO also includes a request of those departments and agencies with regulatory authority to explore the use of existing regulation to promote cybersecurity. Mr. Kolasky emphasized that this part of the EO is not a call for new regulation. The ITF is also asking regulatory departments and agencies to look at existing regulations that may reduce the likelihood of an organization adopting the cybersecurity framework. Between the two pursuits, the ITF hopes this will provide a balanced regulatory approach, with additional regulations where needed, and reduced regulations where necessary.

Mr. Kolasky continued his presentation by discussing the three strategic imperatives associated with PPD-21: refining and clarifying functional relationships across the federal government, enabling effective information exchange and becoming better partners with the private sector, and implementing an integration and analysis function that can inform planning and operations decisions regarding critical infrastructure.

There is a need to use the processes within the Directive to develop a situational awareness capability stressing physical and cyber risks. The capability should be able to provide as much information as possible about the state of critical infrastructure to Federal decisionmakers, response decisionmakers, Emergency Operations Centers (EOCs) from around the country, State and local governments, and private sector organizations. But that capability should also have a related ability to integrate the analysis function. That function could analyze the downstream effects on other industries and other sectors of the economy, a need that was made apparent in the aftermath of Superstorm Sandy.

As studies on lifeline sectors often note, there is a complex web of infrastructure interdependencies. One malfunctioning critical infrastructure asset might cause disruptions in seemingly unrelated businesses or sectors. Because of this, part of the ITF's work is to determine ways to improve modeling capabilities that can be broadly used by critical infrastructure decisionmakers.

There also is a need to evaluate and develop the public-private partnership, Mr. Kolasky said. He noted that the EO offers an opportunity to exercise the partnership at the core of policy as a

means to deal with immediate threats. Simultaneously, PPD-21 affords the Government the opportunity to make long-term improvements to the CISR mission.

He continued his presentation by discussing the deliverables required as a result of the two policies, as well as the timeframe for completion.

Within 120 days, DHS is expected to publish instructions for unclassified threat information, in order to better improve the production and dissemination of unclassified threat information; report on cybersecurity incentives that will encourage adoption of the voluntary cybersecurity framework; and Publish procedures to expand the Enhanced Cybersecurity Services.

At the 150-day mark, DHS has two deliverables due: identification of cybersecurity critical infrastructure, and an evaluation of public-private partnership models.

The Cyber critical infrastructure identification requirement refers to the need to identify critical infrastructure for which a cybersecurity incident could result in catastrophic regional or national effects. Mr. Kolasky noted that this deliverable will require a review of the definition of critical infrastructure and criticality, as well as how those concepts relate to cybersecurity, and are changed by a threat to cyber infrastructure. As part of this effort, there will be an examination of the physical damage or service disruptions to businesses and organizations nationwide that could be caused by a cyber incident. He added that the assessment is more focused on criticality than risk, though it does identify infrastructure at high cybersecurity risk. Businesses identified in the assessment will be informed of the judgment, and they may go through a remediation process if they think the analysis was in error.

The CISR public-private partnership model is also being reviewed, in order to determine the successes and challenges of the partnership. Mr. Kolasky noted that there are many ways to engage the partnership model at present. While this prevents an overly rigid system from stifling engagement, it also has the effect of becoming confusing for owners and operators. The ITF is examining working models, including those outside the NIPP, as part of this effort.

Within 240 days, DHS is required to develop a situational awareness capability; update the National Infrastructure Protection Plan (NIPP); and publish the voluntary cybersecurity framework.

The situational awareness deliverable refers to physical and cyber capability for mitigation measures. The goal for the capability is to develop near-real-time awareness for CISR decisionmakers.

For the update to the National Infrastructure Protection Plan, the ITF will seek input from a broad range of sources, via Federal Register Notices, social media, and workshops, among others. The conversation will review the effective and ineffective parts of the plan, as well as governance structures, the core of the risk management framework, research and development, and other components of the document. The changes will be consolidated into themes that will be incorporated into a new NIPP, which in turn will lead to the development of new Sector-Specific Plans.

The voluntary cybersecurity framework standards and performance goals will be published by NIST. Mr. Kolasky noted that the performance goals are not focused on determining the number of participants in the framework, but rather are tied to the ability of a partner to respond to a cyber threat.

At the 1-year mark, the ITF will report on privacy and civil rights and civil liberties cybersecurity enhancement risks. Mr. Kolasky re-emphasized that any cybersecurity enhancements will need to be consistent with the need to respect individual privacy and civil liberties, and that it is important that information is not used for any unintended purposes.

Gen. Albert Edmonds complimented Mr. Kolasky for the quality of the presentation, and noted the timeliness of the release of the EO and PPD. He then asked if the ITF was considering giving advice about new infrastructure build-out. He noted new buildings, facilities, and power plants as potential examples of places where new cybersecurity protections could be included during construction. Gen. Edmonds also asked whether the Government would be providing training assistance that could help industries quickly identify whether a cyber incident is a system failure or a system attack.

Mr. Kolasky responded that the enhancement of cyber protection and resilience is a prime focus of the two documents, and that there are certain levers the government can use, particularly if they are funding the construction, to encourage better cybersecurity posture during construction. Areas of focus for the Federal Government include tying resilience and security requirements to construction requirements, and using the procurement process as a way to ensure that businesses are getting a base level of cybersecurity built into products purchased. These approaches will provide a market for enhanced security and resilience, as any firms wishing to enter the infrastructure services market will be meeting a standard level of security in their products.

To the second question, regarding training for correct identification of a cyber incident, Mr. Kolasky referred the question to Ms. Moore and Mr. Natarajan. But Mr. Kolasky acknowledged that improved identification of an incident was an area of concern for the Government.

Gen. Edmonds elaborated that as physical and cyber policies are integrated, it will be important to include a plan for speedy recovery of assets. He mentioned degradation and restoration grants as valuable methods for reducing recovery time, and added that communities can recover faster when there is an expectation of external support.

Mr. Natarajan noted that proper expectation setting is the best policy both before and after a crisis, as it allows the public to better prepare. He added that when communities are aware of the realistic restoration times following a major incident – typically between 2 and 4 days – it allows for a better, calmer response to the process.

In response to an earlier comment about the exponential changes to the threat environment, Mr. Wallace noted that much of the private sector is lagging in its response to those changes. A challenge of the implementation of the EO and PPD-21 is that those individuals or groups who are most likely to provide the comments are farther along in their responses to the new environment, as they are more aware of the changes that have taken place in recent years. He commented that it will be important not to tie the future of the security and resilience mission solely to comments based enhancing the mission as it currently is. A key part of the new environment will be executive engagement of the various highest levels across sectors, though that, too, presents a challenge; essentially, there will be a new model in place that may be difficult to visualize today because of its uniqueness.

Mr. Kolasky responded that the goal is to engage CEOs in ways that will influence their business practices, including conversations with government, insurance, legal issues, investments, and what their peers are doing.

Ms. Lau added that this process has to do with getting stakeholders engaged and soliciting input. She noted that getting such input may not always be easy, as not all CEOs have the situational awareness to provide the information offhand. A longer, back-and-forth process may be necessary, because once the CEO is engaged, they then have to talk with their experts within their organizations – particularly when the subject is cybersecurity, as many CEOs do not have a background in the subject. Following internal discussions, the CEOs return with issues that they — or their organizations — may have raised, and which may or may not be on point. Her final point she stressed was to strive not just for input, but for dialogue and exchange.

Mr. Kepler noted the importance of maintaining a focus on physical security and resilience while adopting the new focus on cyber issues, and in integrating the two in risk analysis, though he acknowledged that Mr. Kolasky's presentation suggested such an approach would be implemented. He added that the IT Sector and community are vital to establishing an effective

model, and it will be important to engage that sector to ensure the cybersecurity framework will actually work for all sectors.

Mr. Kolasky agreed with Mr. Kepler's comments about engagement with the IT Sector. He noted that the ITF is evaluating potential causes of malfunction in cyber control systems, regardless of whether the disruption was cause by attack. The ITF is examining lessons learned on identifying physical risks to critical infrastructure, and hopes to apply those lessons as a merged process for analyzing all hazards is developed, as part of an enterprise risk management strategy.

Mr. Kolasky continued his presentation by outlining the purpose of the public-private partnership. He stressed that the partnership model seeks to reduce risk to critical infrastructure for the aim of achieving critical infrastructure security and resilience. Mr. Kolasky summarized the purpose of the partnership by quoting Deputy Under Secretary Spaulding, who said the purpose of the public-private partnership is "joint problem-solving."

Mr. Wallace added his support for Mr. Kolasky's "Enterprise Risk Management Model," and noted that the private sector and CEO leadership has a distinct focus on carrying out their producer responsibility to shareholders for the assets they have under their control, and the risk management model reflects that approach.

Ms. Lau added that in regulated industries, the Enterprise Risk Management responsibility is an executive board-level concern; once that level is involved, the entire structure of an organization is engaged with the issue.

Mr. Kolasky reiterated that information sharing is a top priority, not only between owners and operators and governments, but also among key stakeholders within a company. It is hoped that the mechanisms included in the framework will help CEOs and Chief Information Security Officers (CISOs) better communicate about threats, security, and resilience.

Mr. Wallace emphasized the importance of a voluntary framework. He noted that there are implicit concerns when regulation is discussed — such as the adaptability and continued relevance of the regulations — and that a combination of a voluntary framework and incentives are more likely to get stakeholder buy-in.

Mr. Kolasky noted that the next portion of his presentation was largely covered in previous discussion. He then paused to ask whether there were any additional comments about those issues, which included expanding and continued commitment at the board level; how to ensure appropriate participation; current gaps; engagement at an executive level; and using goal-setting, to develop high-level shared goals and priorities.

Mr. Wallace commented that while there are 16 sectors, it is unlikely that private sector members of the NIAC are fully aware of the alignment and structure of all sectors. He suggested that it would be beneficial to have a high-level criterion that establishes what a successful public-private partnership engagement model is, in order to better gauge the relative successes of the sectors in assessing engagement efforts.

Mr. Kolasky asked whether the existing model is too reliant on each sector operating similarly in a one-size-fits-all model, or is suitably flexible.

Mr. Wallace responded that the key principles, objectives, and criteria would be the same wherever they are applied, whether to a company, a sector, or the entire critical infrastructure construct. But there also needs to be flexibility in the program; the present system has some flexibility built in, but there might be room for more, as well as better integration. Mr. Wallace also noted that the lifeline sectors, while often central to NIAC discussions, are dissimilar from many of the other sectors, and that the Federal Government should not try to view all sectors through the same lens.

Ms. Durkovich commented that in light of the interdependencies among the 16 sectors, each one is important. She added that cross-pollination — whether through information sharing or the leveraging of best practices — should be explored. She expressed interest in the Regional Resilience project, and what recommendations are made on improving awareness of dependencies and interdependencies.

Mr. Kepler noted that the NIAC has not discussed such issues before, but should consider studying in this report. He added that interconnectedness could be seen as a value chain — there are downstream effects, but also direct economic and safety issues — and developing an understanding of the links among those concerns is a critical issue.

Mr. Kolasky then outlined the incentives proposed by the ITF. He noted that there in the areas of critical infrastructure sectors that are regulated, there are regulations in some sectors that exist for safety purposes, as well as a few that are regulated explicitly for security purposes. Voluntary adoption and adherence inspires deeper engagement and makes varying incentive programs possible for continued promotion. The ITF has drafted 14 categories of incentives as part of the framework. Proposed incentives include:

- Expedited Security Clearance Process
- Grants
- Include Cybersecurity in Rate Base
- Information Sharing

- Insurance
- Liability Considerations
- New Regulation/Legislation
- Prioritized Technical Assistance
- Procurement Considerations
- Public Recognition
- Security Disclosure
- Streamline Information Security Regulations
- Subsidies
- Tax Incentives

Mr. Wallace observed that the proposals were similar to tax incentives that were tied to security improvements post-9/11, which had a time limit or were perceived to have a time limit, encouraging companies to move quickly. He emphasized that nothing gets individuals and businesses moving quicker than knowing there are economic incentives that have a sunset clause. Because of this, there is a tangible value in understanding the incentives and incorporating them into a risk management model before they expire.

Ms. Durkovich commented that she would have to leave the meeting because of a personal matter, and encouraged the Council to continue the EO and PPD-21 discussion. The Council elected to continue following Ms. Durkovich's closing remarks.

The Assistant Secretary thanked NIAC members, and emphasized the value the Federal Government takes from the Council's quarterly business meetings. She also highlighted the importance of being able to learn directly from CEOs who run much of the Nation's critical infrastructure, and thanked the NIAC members for taking time out of their schedules to work on the Council. Ms. Durkovich expressed her excitement for the upcoming findings of the Council. She also noted that the Nation, over the past 10 years, has done considerable work to improve security — but it is still important to step back, review gaps, highlight areas of improvement, and continue improving efficiency.

Ms. Lau thanked the Assistant Secretary for her participation, and asked whether there was a mechanism that would allow the NIAC to assist in the evaluation and implementation of the EO and PPD-21 in a more efficient and timely manner. Ms. Durkovich responded that she would be speaking with the Office of General Counsel and the DFO to identify an approach. Ms. Lau then thanked Ms. Durkovich again, and directed the Council back to the EO and PPD-21 conversation.

Ms. Margaret Grayson asked how the Council should prioritize or set up where the incentive categories might provide the most value for those particular infrastructures dependent on lifeline sectors — and don't have the resources, strength, or internal capabilities to bring themselves up to the level needed in the case of an actual emergency.

Ms. Lau connected this question to previous working group discussions and points made by Mr. Wallace earlier in the meeting. She noted that in the Electricity Sector studies, hearing a common refrain over the course of several discrete studies made clear some of the key themes.

Mr. Kolasky commented that the uniqueness of the governing structures for each Lifeline Sector is still being researched, and determining those structures is key to determining relevant incentives.

Ms. Grayson added how important it is to look at a combination of some of the sectors that have an element of regulatory requirement. She noted that even in the Lifeline Sectors, there are assets or companies that are considerably smaller and more vulnerable than the larger entities within the sector. Those smaller firms would benefit greatly from the support and mentoring of the larger entities, in order to improve the overall resilience landscape. Support for the smaller firms would come from both regulative and voluntary policies. She commented that the incentives that would allow that to happen across the broad sector, is a very complex matrix of questions and answers, and how to actually get that done is an issue.

Ms. Lau noted that she thought the list of incentives was good, and that the discussion on the prioritization of those incentives relates to the discussion on the different organizational structures of the sectors. She added that it might be worthwhile to focus on the key aspects of each lifeline sector to determine the value of an incentive to a sector. In the Electric Sector, the industry makes money by putting capital to work, and that capital has to be incentivized through inclusion in rate base — though that notion may not apply to other sectors, Ms. Lau said.

Mr. Kolasky thanked the Council for the feedback. He noted that challenges will include prioritizing incentives, distinguishing between certain industries and certain sectors, and establishing a cutoff for direct outlays of Federal funds.

Gen. Edmonds pointed out that industries that are state regulated — such as power, water, and telecommunications — are given leeway by the states when justified to raise rates as an incentive to improve service. He noted that in almost all cases, Lifeline Sectors have support from a state organization or the National Guard that can assist and ensure that the community and its economy can continue functioning. He added that in the Banking and Finance Sector, there are

internal regulations, so it will be important to understand how those rules are incentivized and integrated.

Dr. Scott re-emphasized that there will be differences among the sectors — whether structural or regulatory — about the value proposition, and those distinctions will be helpful as progress is made.

Mr. Gerstell also commented that he thought the list of incentives was highly useful, and that the conversation conveyed that some incentives resonate with some sectors more than others. He added that some high-value incentives will require greater effort on the part of the Federal Government — such as changing tax codes — which will have an effect on how quickly and feasibly they can be implemented. He urged the Council to look at the incentives that will yield the biggest payoff and can be achieved the most quickly, but also to consider the long-range, challenging incentives, such as taxes or structural changes.

Mr. Gerstell also noted the value in using an educational outreach program that would provide information about what could happen in the event of a cyber incident. Some industries are already aware of the dangers, but others that are less dependent on cyber infrastructure may not consider the issue, and there is a disparity in preparation by State and local governments. The process of becoming informed could then serve as an incentive itself for some of those sectors.

Mr. Kolasky thanked Mr. Gerstell for the feedback, and noted that while incentives are an important part of the process, the Government also believes that the utility and benefits of the framework itself, in guiding better cybersecurity practices, will also inspire wider adoption.

Ms. Lau then discussed, in relation to comments made by Gen. Edmonds, that while the EO and PPD-21 are intended to cover all critical infrastructure sectors, the lifeline sectors — being more important to public safety and the economy — have attracted more regulations over time because they have been very important to the economy. Because of this, the lifeline sectors may be able to more quickly adapt to regulatory changes, as those structures are built to handle regulation. She also reiterated the need to consider the value proposition, as overly burdensome regulations will have little to no value, and industries that are already heavily regulated are unlikely to need additional rules.

Mr. Kolasky thanked participants for the feedback and reiterated that the NIAC is a key part of the public-private partnership. Because of this, the Government wants to provide different levels of dialogue, and the feedback obtained during this quarterly business meeting will help with the evaluation of the public-private partnership.

## VIII. CLOSING REMARKS

*Constance H. Lau,* NIAC Chair

*Suzanne Spaulding,* Deputy Under Secretary for the National Protection and Programs Directorate, DHS

*Caitlin Durkovich*, Assistant Secretary for Infrastructure Protection, DHS

*Charles Donnell*, Special Assistant to the President for Resiliency, National Security Staff

*Dr. Ahsha Tribble,* Senior Director for Response, National Security Staff

*Nitin Natarajan,* Director, Critical Infrastructure Policy, National Security Staff

Mr. Natarajan thanked the NIAC for their continued hard work to secure and enhance the resilience of the nation's critical infrastructure. There are many layers of complexity to achieving this goal, but he is optimistic that the combination and integration of cyber and physical concerns will help create a greater value proposition for dealing with these problems. Bringing the cyber and physical communities together is essential in looking at cascading consequences and larger effects that are likely to increase time and resources allocated to enhancing resilience through the public-private partnership.

Mr. Natarajan then emphasized the continued importance of reforming information sharing practices. He added that distributing the right information to the right partners in a timely manner is important in efforts to reduce uncertainty by decisionmakers. Reforming this process will increase synergies between critical infrastructure owners and operators at all levels nationwide, and establish a solid platform for addressing international critical infrastructure concerns.

The implementation of the EO and PPD-21 is a huge undertaking, with hundreds of partners across the 16 critical sectors. Mr. Natarajan expressed his desire to create a joint value proposition among partners as the requirements for time and resources increase within sectors. The submission of ideas, perspectives, and expertise from all sectors and partners will be crucial to this process. Consistent dialogue is the only way to successfully implement the two policy documents and streamline operations.

Ms. Moore echoed Mr. Natarajan's comments, and thanked the NIAC for the opportunity to leverage their recommendations and bodies of work in the development of the EO and PPD-21.

She noted that as important as it is to get everything right in the planning phase, implementation is just as important in producing the intended outcomes.

Ms. Lau and Dr. Scott thanked all participants and expressed their confidence in the Regional Resilience Study and the implementation of the EO and PPD-21. Ms. Lau then adjourned the meeting.

## VIII. ADJOURNMENT

*Constance H. Lau,* NIAC Chair

Ms. Lau thanked all in attendance and adjourned the meeting.

I hereby certify the foregoing minutes accurately represent the discussion and events that transpired at the meeting held on the date first noted above.

By: Constance H. Lau Date: July 17, 2013
Constance H. Lau, Chair, NIAC

# National Infrastructure Advisory Council (NIAC)

## Regional Resilience Working Group

April 8, 2013– Report #3

**Constance H. Lau**
*President and Chief Executive Officer,*
*Hawaiian Electric Industries, Inc.*
Co-Chair

**Dr. Beverly Scott**
*General Manager*
*Massachusetts Bay Transportation Authority*
Co-Chair

# Agenda for Regional Resilience Study Update

- Study Purpose and Objectives
- Status Update
- Philadelphia Case Study on Superstorm Sandy
- Work Plan and Schedule
- Executive-Level Engagement in the Electricity Sector Case Study
- Next Steps

# Regional Resilience Study

**Purpose:** Identify ways regions can become more resilient and the steps the Federal Government can take to help regions accomplish resilience goals.

**Objectives**

1. **Best Practices**: Identify the characteristics that make a region resilient and the steps that can be taken to improve resilience within a region.
2. **Process Improvements**: Determine how public and private critical infrastructure partners can work together to improve regional resilience.
3. **Federal Role**: Recommend how Federal Government capabilities and resources can help accomplish resilience goals and address any gaps that can help regions become more resilient.

# Status Update

- Philadelphia Case Study on Superstorm Sandy initiated
- Working Group Work Plan revised
- Working Group Federal interviews scheduled

# Philadelphia Case Study Refocused

- NIAC Philadelphia Case Study had planned to examine infrastructure failures that could extend beyond the Philadelphia metro area and which could provide insights and recommendations applicable to other regions across the country
- Superstorm Sandy created an unfortunate opportunity to examine how a major disaster stresses lifeline infrastructures
- The Philadelphia Case Study was refocused to examine the impact of Superstorm Sandy on the lifeline sectors and its implications for regional resilience

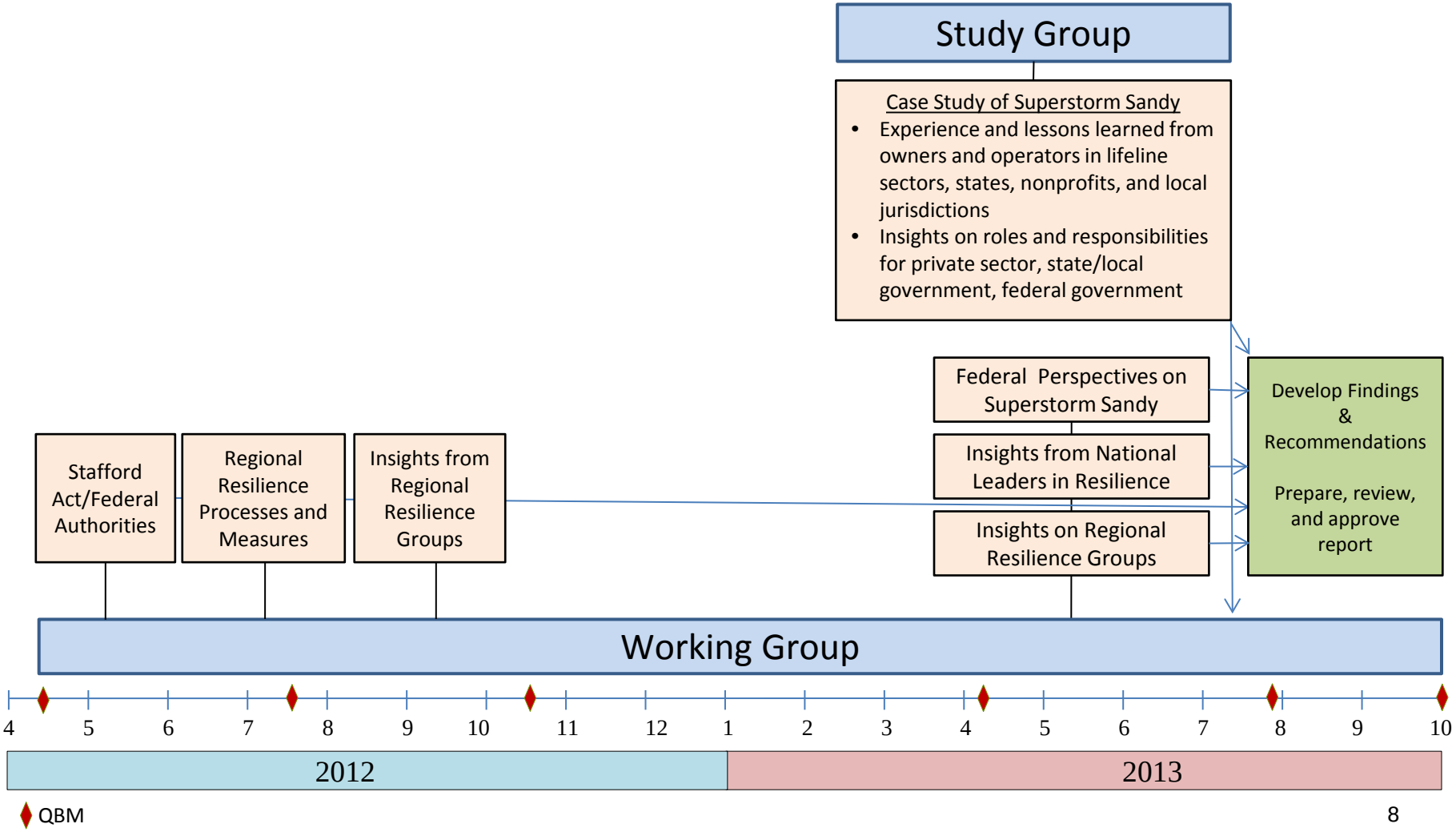
# Study Group Members

| Company | Sector |
|---|---|
| Hawaiian Electric Company | Electricity |
| Exelon Corp | Electricity |
| PECO | Electricity |
| Metrolink<br>Southern California Regional Rail Authority | Transportation/Rail |
| Airports Council International | Transportation/Aviation and Maritime |
| Owner-Operator Independent Drivers Association | Transportation/Highway Motor Carrier |
| Phillips 66 Company | Oil and Natural Gas |
| Frontier Communications | Telecom |
| MTN Government Services | Telecom |
| New Jersey Office of Homeland Security and Preparedness | State Government |
| City of Philadelphia | Local Government/Emergency Operations |
| City of Philadelphia | Local Government/Water |

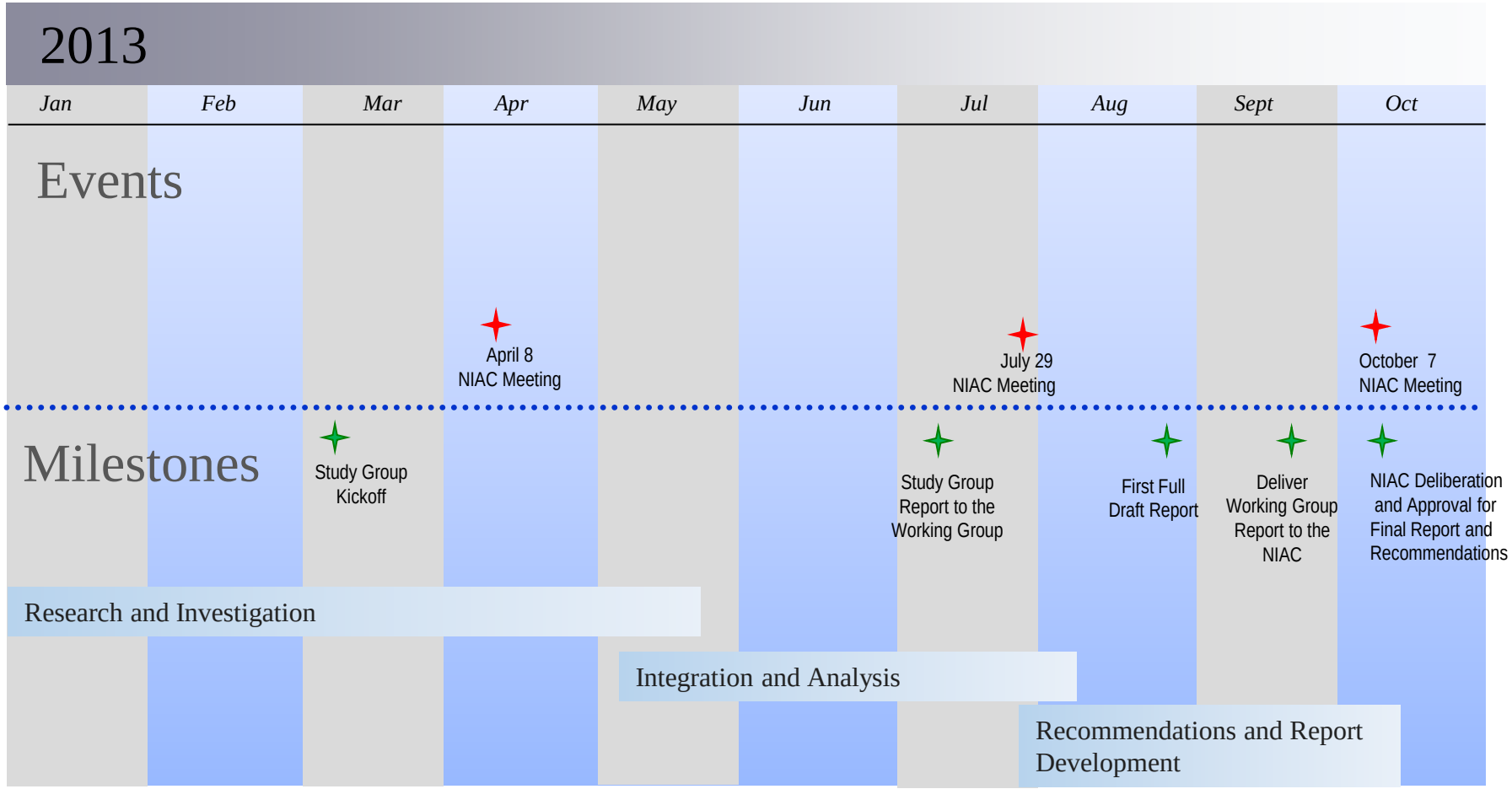
# Initial Insights on the Hurricane Sandy Experience

- The scale and scope of Sandy was much larger than many had previously seen, creating shortages of equipment and supplies not experienced in other storms.
- In NJ, preplanning and coordination focused on the lifeline sectors. Coordination during the storm was handled through a private sector desk in the state EOC and pre-event conference calls were held with the private sector.
- As a disaster escalates, companies can spend a lot of time educating outside leaders on their decisions and actions. Companies should do as much outreach up front so that state/federal partners understand the company's response rationale, operating procedures, and capabilities going into an event. Perpetual outreach is also needed between disasters as people move into new roles.
- The advanced warning of Sandy's arrival enabled preplanning and prepositioning of assets. Had this type of destructive force been an unexpected terrorist attack or cyber event, the preparation would not have been as good.
- Social media played a big role in Sandy with both positive and negative implications. Rumors were more rampant and spread faster; but it also became a source of information on outages that can aid operations.

# Work Plan for Regional Resilience Study



# Revised Schedule



# Case Study: Executive-Level Engagement in the Electricity and Nuclear Sectors

- Previous NIAC Recommendations on Executive-Level Engagement
- Past Success and Failure in Achieving Executive-Level Engagement
- Key Elements of Success
- Electricity Sector Success – A Model?

# Previous NIAC Recommendations on Executive-Level Engagement

- Intelligence Information Sharing, January 2012
  - "The White House should additionally employ current or new partnership mechanisms for senior executives in the private sector to engage their government counterparts to facilitate a truly national approach that leverages public-private resources for large-scale, persistent threats."
- A Framework for Establishing Critical Infrastructure Resilience Goals, October 2010
  - "The White House should initiate an executive-level dialogue with electricity and nuclear sector CEOs on the respective roles and responsibilities of the private and public sectors in addressing high-impact infrastructure risks and potential threats, using an established private sector forum for high-level, trusted discussions between industry executives and government leaders."
- Critical Infrastructure Partnership Strategic Assessment, October 2008
  - "The private sector should initiate a strategic dialogue between industry CEOs and the White House soon after the inauguration to reinforce their commitment to partnership principles, followed by similar dialogues with the Congressional leadership and state governors."

# Past Success and Failure in Achieving Executive-Level Engagement

- Project Aurora – a control system vulnerability discovered in 2006 required executive-level information sharing
  - Classified but mitigated across Nuclear Sector in 4 months
- CIKR Executive Industry Council
  - Formed after 2008 Study
  - Failed due to loss of momentum/timing
- Kaleidoscope – a U.S. Secret Service effort
  - Formalized a protocol developed from incremental successes
  - The "elements for success" become clear

# Key Elements of Success

- Trusted relationships
- CEO engagement
- Simple process

# Electricity Sector Success – A Model?

- Builds off of Kaleidoscope success
- Inclusive of all trade groups, with clear leadership
- Key structure: Leaders in the Electricity and Nuclear Sectors worked with Edison Electric Institute to initiate regular engagement with government leaders on resilience issues through two groups:
  - **Joint Electric Executive Committee** of 23 CEOs and S-1/S-2 leaders now meeting quarterly; examining priority, policy, resources, and accountability
  - **Senior Executive Working Group** of 16 senior executives now meeting bi-weekly/monthly with Assistant Secretaries, using focused agendas and deliverables

# Appendix

# Working Group Members

| WG Member | Sector Experience |
|---|---|
| **Constance H. Lau**, *President and Chief Executive Officer, Hawaiian Electric Industries, Inc. (HEI)* Co-Chair | Electricity, Financial Services |
| **Beverly Scott**, *General Manager, Massachusetts Bay Transportation Authority* Co-Chair | Transportation |
| **Jack Baylis**, *Executive Director and Senior Vice President for The Shaw Group* | Water |
| **Glenn S. Gerstell**, *Managing Partner, Milbank, Tweed, Hadley, & McCloy LLP* | Water, Telecommunications |
| **David J. Grain**, *Founder and Managing Partner, Grain Management* | Telecommunications |
| **Margaret E. Grayson**, *President, Grayson Associates* | IT, Defense Industrial Base |
| **James A. Reid**, *President, Eastern Division, CB Richard Ellis* | Commercial Facilities |
| **Michael J. Wallace**, *Former Vice Chairman and COO, Constellation Energy* | Electricity, Nuclear |

This page left blank intentionally

# Implementing the Administration's Critical Infrastructure and Cybersecurity Policy

Cybersecurity Executive Order and Critical Infrastructure Security & Resilience Presidential Policy Directive Integrated Task Force

*Discussion with the National Infrastructure Advisory Council*

April 8, 2013

Homeland Security

# The Need to Enhance Security and Resilience

- America's national security and economic prosperity are dependent upon the operation of critical infrastructure that are increasingly at risk to the effects of cyber attacks
- The vast majority of U.S. critical infrastructure is owned and operated by private companies
- A strong partnership between government and industry is indispensible to reducing the risk to these vital systems
- We are building critical infrastructure resiliency by establishing and leveraging these partnerships

# Taking Action

- In February 2013, the President issued two new policies:
  1) Executive Order 13636: Improving Critical Infrastructure Cybersecurity
  2) Presidential Policy Directive – 21: Critical Infrastructure Security and Resilience
- Together, they create an opportunity to work together to effect a comprehensive national approach to security and risk management
- Implementation efforts will drive action toward ***system* and *network*** security and resiliency

# Integrated Cyber-Physical Security

- ***Executive Order 13636: Improving Critical Infrastructure Cybersecurity*** directs the Executive Branch to:
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security

- ***Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*** replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

# Major Deliverables

| Within… | …do the following: |
|---|---|
| 120 days | ▪ Publish instructions to produce and disseminate unclassified threat information |
| | ▪ Report on incentives for cybersecurity |
| | ▪ Expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors |
| 150 days | ▪ Identify critical infrastructure for which a cybersecurity incident will result in catastrophic regional or national effects |
| | ▪ Evaluate and enhance public-private partnership models |

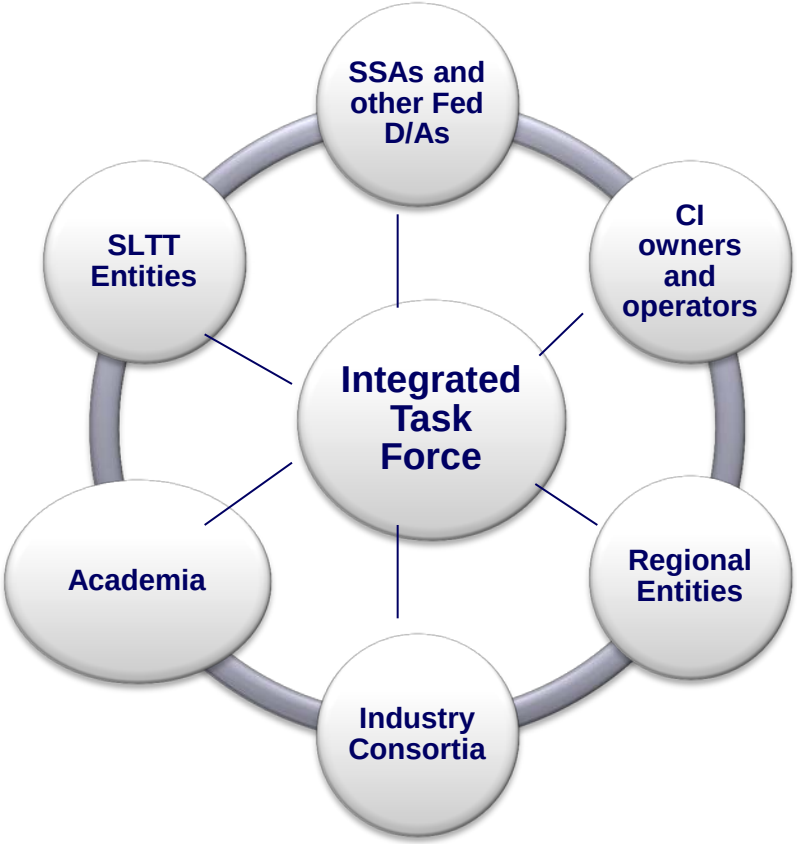
# Major Deliverables (continued)

| Within… | …do the following: |
|---|---|
| 240 days | ▪ Develop a situational awareness capability for critical infrastructure<br>▪ Update the National Infrastructure Protection Plan |
| | ▪ Publish voluntary Cybersecurity Framework standards |
| 365 days | ▪ Report on privacy and civil rights and civil liberties risks associated with cybersecurity enhancements |
| Beyond 365 Days | ▪ Implement a voluntary critical infrastructure cybersecurity program |

***Other deliverables are required from both documents***

Homeland Security

# Stakeholder Engagement Model




Guiding Principles

- Involve those responsible for critical infrastructure security and resilience.
- Reflect stakeholder views in program design and policy implementation.
- Use existing bodies and channels when possible, supplemented as needed to ensure a diversity of relevant viewpoints.

# Purpose of the Critical Infrastructure Partnership

- The purpose of the public-private partnership model is to manage risks to critical infrastructure for the aim of achieving critical infrastructure security and resilience.

This is achieved via:

| | | | |
|---|---|---|---|
| Shared risk mitigation | Information sharing | Research and development | Capability building |
| Policy coordination | Public-private financing models | Risk transfer | |

# Questions for Discussion – Existing Public-Private Partnership

- Do we have the right purpose?
- How do we get expanded and continued commitment at the corporate level, in the full range of security and resilience issues?
- Through that commitment, how do we ensure right person/people are participating?
  - Where do gaps currently exist?
- How can we engage the Executive Level in goal setting, and to drive toward a specific set of high-level shared goals and priorities?
- What are incentives for participating in the partnership, and what must the value proposition look like from an industry perspective?

# Incentive for Promoting Voluntary Adoption: Examples

- The 8 sources reviewed proposed the following broad categories of remunerative and coercive incentives (1-7):

1. Expedited Security Clearance Process: a procedure to expedite the provision of security clearances to appropriate personnel employed by CI owners/operators under the framework.
2. Grants: direct federal funding for investment in cybersecurity products and services for framework owners and operators; alternatively, tie existing grants to adoption of cybersecurity framework.
3. Include Cybersecurity in Rate Base: rate-based recovery of cybersecurity investments in the rate base for services provided by framework owners and operators.
4. Information Sharing: a procedure for ensuring that framework owners and operators are informed of relevant real-time cyber threat information.
5. Insurance: promoting cybersecurity insurance through related incentives and/or federal reinsurance programs to help underwrite the development of cybersecurity insurance programs.
6. Liability Considerations: reduced liability in exchange for improved cybersecurity or increased liability for the consequences of poor security.
7. New Regulation/Legislation: for example, a Cyber SAFETY Act.

# Incentive Category Examples

- The 8 sources reviewed proposed the following broad categories of remunerative and coercive incentives (8-14):

8. Prioritized Technical Assistance: ensure framework owners/operators receive prioritized cybersecurity technical assistance (e.g. ICS-CERT).
9. Procurement Considerations: preferential consideration in the procurement process for framework owners and operators and/or requiring framework adoption by federal goods/services providers.
10. Public Recognition: create an award for companies that adopt the framework and/or best practices.
11. Security Disclosure: requiring public notification of disclosures to encourage owners and operators to take care to avoid breaches.
12. Streamline Information Security Regulations: create unified compliance model for similar requirements and eliminate overlaps among existing laws (e.g. Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley).
13. Subsidies: direct purchase of cybersecurity products and services for framework owners/operators.
14. Tax Incentives: tax credits and/or deductions for framework owners and operators.

# Questions for Discussion – Incentives for Participation

- Are there suggestions for additional incentive categories beyond the list of 14 incentives proposed that the ITF should consider in its analysis. Is anything missing?
- Can participants enumerate incentive sub-types not already clearly included in the 14 broad incentive categories (i.e., do specific subtypes come to mind)?
- Are specific types/subtypes more likely to increase the adoption of the voluntary framework? Why/why not? Are there examples in other arenas that stand out?
- Is there particularly relevant research and/or experience on the effectiveness of the incentive categories from non-cyber contexts in the literature the ITF should consider?

Homeland Security