NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

BUSINESS MEETING AGENDA

November 21, 2013
1:30 PM – 4:30 PM EST
United States Patent and Trademark Office, 2800 South Randolph Street, Room 3C71,
Arlington, VA 22206

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 INTRODUCTION**	*Constance H. Lau,* NIAC Chair *Caitlin Durkovich,* Assistant Secretary for Infrastructure Protection, DHS *William F. Flynn,* Deputy Assistant Secretary for Infrastructure Protection, DHS *Dr. Ahsha Tribble,* Acting Deputy Homeland Security Advisor, National Security Staff *Nitin Natarajan,* Director, Critical Infrastructure Protection and Resilience, National Security Staff *Samara Moore,* Director for Cyber Security and Critical Infrastructure, National Security Staff
IV.	**APPROVAL OF MEETING MINUTES**	*Constance H. Lau,* NIAC Chair
V.	**UPDATE ON IMPLEMENTATION OF NIAC'S INTELLIGENCE INFORMATION SHARING REPORT RECOMMENDATIONS**	*Kshemendra Paul,* Program Manager, Information Sharing Environment
VI.	**REGIONAL RESILIENCY REPORT WORKING GROUP PRESENTATION**	*Constance H. Lau,* NIAC Chair, Working Group Co-Chair *Dr. Beverly Scott,* NIAC Working Group Co-Chair

VII. PUBLIC COMMENT: TOPICS LIMITED TO REGIONAL RESILIENCE REPORT	*Nancy J. Wong,* DFO, NIAC, DHS
VIII. REGIONAL RESILIENCY REPORT DISCUSSION AND DELIBERATION	*Constance H. Lau,* NIAC Chair
IX. EO 13636 AND PPD 21 IMPLEMENTATION: FEDERAL GOVERNMENT STATUS REPORT ON EO-PPD IMPLEMENTATION INTEGRATED TASK FORCE	*Robert Kolasky,* Director, Integrated Taskforce for the Implementation of EO 13636 and PPD 21, DHS
X. EO 13636 AND PPD 21 IMPLEMENTATION: NIAC WORKING GROUP REPORT PRESENTATION	*David Kepler,* NIAC Working Group Co-Chair *Philip Heasley,* NIAC Working Group Co-Chair
XI. PUBLIC COMMENT: TOPICS LIMITED TO EO 13636 AND PPD 21 IMPLEMENTATION REPORT	*Nancy J. Wong,* DFO, NIAC, DHS
XII. EO 13636 AND PPD 21 IMPLEMENTATION: REPORT DISCUSSION AND DELIBERATION	*Constance H. Lau,* NIAC Chair
XIII. DISCUSSION AND STATUS OF TRANSPORTATION RESILIENCY STUDY WORKING GROUP	*Nancy J. Wong,* DFO, NIAC, DHS
XIV. CLOSING REMARKS	*Constance H. Lau,* NIAC Chair *Caitlin Durkovich,* Assistant Secretary for Infrastructure Protection, DHS *William F. Flynn,* Deputy Assistant Secretary for Infrastructure Protection, DHS *Dr. Ahsha Tribble,* Acting Deputy Homeland Security Advisor, National Security Staff

	Nitin Natarajan, Director, Critical Infrastructure Protection and Resilience, National Security Staff
	Samara Moore, Director for Cyber Security and Critical Infrastructure, National Security Staff
XV. ADJOURNMENT	*Constance H. Lau,* NIAC Chair

MINUTES

NIAC MEMBERS PRESENT IN WASHINGTON:
Mr. Albert Edmonds; Mr. Glenn Gerstell; Ms. Margaret Grayson; Mr. David Kepler; Ms. Constance Lau; Dr. Beverly Scott; Mr. Michael Wallace

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Mr. James Nicholson

MEMBERS ABSENT:
Mr. Jack Baylis; Mr. David Bronczek; Mr. Gilbert Gallegos; Mr. Philip Heasley; Commissioner Raymond Kelly; Mr. Donald Knauss; Mr. Thomas E. Noonan; Mr. Gregory Peters; Mr. James Reid; Mr. Bruce Rohde Mr. Greg Wells

SUBSTANTIVE POINTS OF CONTACT PRESENT IN WASHINGTON:
Mr. Rick Houck (for Ms. Constance H. Lau); Ms. Katherine English (for Mr. David Kepler); Ms. Joan Gehrke (for Mr. Nicholson)

SUBSTANTIVE POINTS OF CONTACT ATTENDING VIA CONFERENCE CALL:
Ms. Sarah Watson (for Commissioner Raymond Kelly)

OTHER DIGNITARIES PRESENT:
Mr. Raymond Alexander, NSS; Ms. Caitlin Durkovich, DHS-IP; Mr. William Flynn, DHS-IP; Ms. Samara Moore, NSS; Mr. Nitin Natarajan, NSS; Mr. Kshemendra Paul, ISE; Dr. Ahsha Tribble, NSS; 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

Caitlin Durkovich, Assistant Secretary for Infrastructure Protection, DHS

William F. Flynn, Deputy Assistant Secretary for Infrastructure Protection, DHS

Dr. Ahsha Tribble, Acting Deputy Homeland Security Advisor, National Security Staff

Nitin Natarajan, Director, Critical Infrastructure Protection and Resilience, National Security Staff

Samara Moore, Director for Cyber Security and Critical Infrastructure, National Security Staff

Ms. Lau welcomed all NIAC members and Federal Government representatives, and provided an overview of the meeting. She noted that the Regional Resilience Working Group and the EO-PPD Working Group would be presenting their final reports, and the Council would provide an update on the scoping of the Transportation Sector study that the NIAC has been tasked with producing. She then asked Dr. Scott to offer opening comments.

Dr. Scott noted her appreciation for the opportunity to work on matters of national importance with the intelligent and skilled members of the Council. She added that the NIAC has completed considerable work during the past year, and complimented Ms. Lau's leadership during that time.

Ms. Lau then asked Dr. Tribble and other representatives from the National Security Staff present to provide opening remarks.

Dr. Tribble thanked Ms. Lau and Dr. Scott, and commented that the NIAC's reports have been of great value to the Administration. She noted that the Council's recommendations are helpful as the Federal Government works to enhance critical infrastructure security and resilience (CISR), regardless of the complexity of those recommendations.

Dr. Tribble noted that the resilience portion of the CISR mission has required dedicated and focused effort to implement, and that the NIAC's recommendations are therefore vital to furthering that cause. With a substantial portion of the Nation's critical infrastructure aging and deteriorating, the strengthening and hardening of assets will need to be a collective effort of all levels of government, as well as the private sector. She also praised the Council for its decision to emphasize the importance of the lifeline sectors – Energy, Water, Telecommunications, and Transportation, as it furthered the goals laid out in Presidential Policy Directive 21 (PPD-21).

Dr. Tribble thanked the Council for its hard work; she noted that the Government listens closely to the NIAC, and looks forward to continued engagement.

Mr. Natarajan thanked the Council for its hard work, particularly with regard to the short-term tasking on the implementation of Executive Order 13636 (EO 13636) and PPD-21. He commented that the NIAC's perspective affords it the ability to make unique recommendations the Federal Government does not otherwise receive. He also noted that there is considerable work still to be done to enhance security and resilience, and that the Council's recommendations will aid that effort.

On the subject of Regional Resilience, Mr. Natarajan commented that the issue can be almost unresolvable when considered from a top-down perspective. He noted that there have been advances on the issue via public-private partnerships at sub-Federal levels, but that the challenge has been translating those successes to a wider area.

Mr. Natarajan commented that a key challenge in the upcoming year will be better linking cyber and physical security and resilience concerns. He noted that while the cyber and physical spheres are interdependent – and that the security and resilience of each is reliant on the other – they have typically been treated as discrete entities. Reducing the vulnerability of assets and regions will be reliant on overcoming this issue.

Ms. Moore offered her gratitude to the Council for its work and the time members dedicated to completing the reports, and added that the findings and recommendations offered therein have been and will continue to be useful to the Federal Government. She then noted that the challenge will be ensuring that the outcomes of the long-term efforts to enhance the CISR mission are aligning with the goals of those efforts as laid out by the NIAC.

Ms. Moore noted her eagerness to hearing the Council's presentations.

Ms. Lau then asked Ms. Durkovich if she had any opening remarks.

Ms. Durkovich thanked Ms. Lau and Dr. Scott for their leadership, and the Council members for their effort. She noted that she was grateful for the opportunity to participate in the NIAC discussions. Ms. Durkovich re-emphasized Dr. Tribble's comments on the value of the Regional

Resilience report. She also noted that Superstorm Sandy provided a real-life test of a region's ability to withstand a catastrophic event, and praised the Council for leveraging those effects in its report.

She then noted the importance of several NIAC findings and recommendations from the regional resilience report. In particular, she highlighted public-private partnerships, maintaining the continuity of lifeline sector services, and the downstream effects of lifeline sector failures as key challenges, as those issues are the hardest to anticipate.

Ms. Durkovich thanked members for providing such valuable insight and recommendations, particularly with regard to the implementation of EO 13636 and PPD-21. She noted that the Council's recommendations on encouraging adoption of the cyber security framework and enhancing information sharing have already served as valuable guides throughout the implementation process. The Council's contributions are well-regarded and respected, and they will help shape the priorities of DHS, IP, and the public-private partnership model. With regard to public-private partnerships, Ms. Durkovich noted that she always emphasizes three NIAC principles – trust, simplicity, and executive-level engagement – when discussing how best to establish a better working relationship between government and private sector owners and operators.

Mr. Flynn was then recognized to make remarks.

Mr. Flynn began by thanking Ms. Lau, Dr. Scott, and the members of the Council. He commented that, as had been noted in earlier remarks, the Regional Resilience report – and its recommendations on public-private partnerships and the importance of the lifeline sectors – and the report on the implementation of EO 13636 and PPD-21 are of great value to the Federal Government.

He then added that, as Mr. Paul planned to address, there has been significant progress in the efforts to improve information sharing, and those improvements are a direct result of NIAC recommendations.

IV. APPROVAL OF MEETING MINUTES — *Constance H. Lau,* NIAC Chair

Ms. Lau called for a motion on the approval of the interim approved meeting minutes from the July 29 Quarterly Business Meeting, as well as the August 14 and September 17 public meetings. She asked members for any changes or comments; hearing none, the minutes were voted on and approved.

V. UPDATE ON IMPLEMENTATION OF NIAC'S INTELLIGENCE INFORMATION SHARING REPORT RECOMMENDATIONS — *Kshemendra Paul,* Program Manager, Information Sharing Environment

Mr. Paul thanked the Council for allowing him to make his presentation during the meeting. He then commended members for their work in producing the 2011 Intelligence Information Sharing report, and highlighted a statement in that report's executive summary:

> "[T]here have been marked improvements in the sharing of intelligence information within the Federal Intelligence Community, and between the Federal Government and regions, States, and municipalities. However, this level of improvement has not been matched in the sharing of intelligence information between the Federal Government and private sector owners and operators of critical infrastructure."

He noted that the ISE's efforts have been a targeted response to that notion.

Mr. Paul provided an overview of the Information Sharing Environment (ISE), which is within the Office of the Director of National Intelligence (ODNI). The mission of the ISE is to empower front-line owners and operators and investigators with the necessary information to protect critical infrastructure. This is achieved through three primary mission objectives: advance responsible information sharing to further counterterrorism and homeland security missions; improve nationwide decisionmaking by transforming information ownership to stewardship; and promote partnerships across all levels of government, with the private sector, and internationally.

He then discussed the efforts to incorporate the NIAC's recommendations on accelerating private sector integration into the ISE. In 2012, a joint collaboration among DHS, the ISE, and ODNI was formed to develop a targeted response to the Intelligence Information Sharing report. The agencies sought to accelerate integration of the private sector owners and operators into the broader information sharing environment. Mr. Paul noted that the efforts were based around a three-phase approach, which included outreach and fact-finding, developing findings and recommendations, and implementation of recommendations.

The agencies had three primary goals in framing its recommendations: developing actionable, effective improvements; leveraging partner efforts to enhance the CISR mission; and ensuring alignment with the NIAC report.

A central priority was to target activity areas that would deliver tangible, valuable improvements. Mr. Paul noted that the agencies sought to find improvements that could be made to individual activities. While this method might not provide a comprehensive addressing of the recommendations offered, it does begin the process of enhancing security and resilience, by at least making partial improvements to information sharing integration efforts.

Mr. Paul also noted that the agencies sought to leverage planned and ongoing efforts by ISE partners to implement national policy directives to enhance the CISR mission. These included recent reports, such as EO13636 and PPD-21, and the ongoing update to the National Infrastructure Protection Plan (NIPP).

The agencies also noted the importance of alignment with key recommendations from the NIAC's Intelligence Information Sharing report. In particular, the joint agency effort sought to advance four main recommendations in that report: increasing the capacity of fusion centers in sharing information; enhancing doctrine to recognize the private sector as a customer and recipient of information; increasing the use and sharing of best practices across Federal agencies; and building sector-specific analytic capacity.

Mr. Paul commented that the nationwide network of fusion centers, over the past three years, has matured; what was once dozens of individual centers has become more of an organized system. He added that while many fusion centers still focus primarily on prevention, which is primarily law enforcement focused, some centers are now integrating the private sector into their information sharing efforts. Mr. Paul added that the joint committee is working on the subject with the National Fusion Center Association, which has a private sector community.

The joint committee of agencies also sought to develop relevant policy in regards to the enhancing of doctrine to recognize the private sector as a customer and recipient of information. Mr. Paul commented that this topic has been an active source of discussion and effort, and was referenced in PPD-21 as an objective to refine and clarify functional relationships across the Federal Government to advance national unity of effort.

Mr. Paul also discussed the joint committee's work to accelerate the sharing and use of best practices among Federal agencies. He noted that this effort focused on DHS, the Federal Bureau of Investigation (FBI), and other Federal agencies, and sought to bring together and share the best practices of all agencies. This plan was aligned with the PPD-21 objective mandating the enabling of efficient information exchange by identifying baseline data and systems requirements.

Mr. Paul then addressed the objective to build sector-specific analytic capacity. He commented that this objective included the goals of increasing analysts' capacity related to sectors, and improve their understanding and ability to provide timely threat information to owners and operators; identifying and promoting tools to enhance risk management; and expanding existing capabilities to increase the relevance and timely distribution of products at the lowest possible classification level.

Mr. Paul also discussed the National Strategy for Information Sharing and Safeguarding (NSISS), an Administration policy document that guides agencies on sharing the information with the partners in a timely manner. The NSISS is a key touchstone that is being used to assist in the development of the information sharing environment, and has three key principles: information as a national asset; information sharing and safeguarding requires shared risk management; and information informs decisionmaking. Mr. Paul noted that there are 16 priority objectives for the NSISS:

- Governance
- Agreements
- Data Tagging
- Federal Identity, Credential, and Access Management (FICAM)
- Safeguarding
- Interoperability Baseline Capabilities
- Training
- Discovery & Access
- Private Sector Sharing
- Data Aggregation Reference Architecture
- Shared Services
- Standards-based Acquisition
- Foreign Partners
- AWN & Request For Information Process
- NSI
- Fusion Centers

In relation to the goal of building on a national information sharing environment, Mr. Paul noted that the concept of statewide and regional information sharing environments have been gaining support. In New Jersey, the State has been leveraging the national standards for ISEs into a statewide information sharing system that links the 476 law enforcement agencies in the State. At present, the system is primarily focused on law enforcement, though the ultimate goal is to provide a broader mission that includes emergency management and public safety. In addition, the New Jersey ISE is innovating in the sharing of information, by working with industry to use an interoperable system architecture that will allow the linking of systems. Mr. Paul noted that

this approach will help to reduce costs and increase effectiveness. He added that similar efforts are in place or in development in other parts of the country, such as a regional ISE for New England.

Mr. Wallace commented that the speed of the ISE's work to enhance information sharing has been impressive, and that it would be helpful to learn more about the metrics being used to gauge the improvement of bi-directional information sharing between the Federal Government and the private sector. He added that the private sector has a wealth of information that has not been fully accessed, and asked Mr. Paul to discuss the ISE's progress on that part of the effort.

Mr. Paul responded that the approach has been to work closely with mission partners. He also highlighted the effort during Superstorm Sandy to provide information on operational gas stations as an area in which the State-level public-private partnership had been particularly effective, and had generated good response from the public, demonstrating the maturation of those relationships. He noted that the ISE sees its role as encouraging that kind of dynamic.

Ms. Lau then asked whether there are ways to make fusion centers more effective, and if the Council should further examine that issue.

Mr. Flynn commented that there has been a concerted effort to speed the security clearance process for the private sector, but noted that there is a significant amount of work to leverage the technology to streamline the process. He also noted that IP is working – as a result of another NIAC recommendation – to help fusion centers develop their own analytic capabilities. DHS is working to help develop fusion center working products that can be easily shared widely with the private sector. He added that the New Jersey fusion center had recently produced such a document following a recent active shooter incident in mall; that product was distributed to malls and retailers shortly after the incident.

General Edmonds commented that part of the process should include the creation of an inventory of all the relevant parties that might need to know that information, in order to inform others of an incident or issue occurring within an industry. He noted that in his experience, industry is most interested in getting the information the government has, as was the case in the active shooter incident Mr. Flynn had referenced. He added that the work of the joint committee is headed in an appropriate direction, though he added that it might be wise to do more to highlight that work.

Mr. Paul noted that as part of the maturation process of fusion centers, they are constantly re-assessing their methods and procedures for information sharing, both in a receiving and processing context. That process will support bi-directional information sharing in an efficient, effective way. He added that there should be an expectation of a process improvement, and that process has worked with State and local governments in prior efforts.

Mr. Natarajan noted that there are many organizations that exist to share information. These include industry-established organizations, such as Information Sharing and Analysis Centers (ISACs), which assist in the sharing of information among businesses and firms, in addition to serving as a clearinghouse for Federal information. He added that it is likely that there will always be multiple mechanisms for information sharing, as no one format is going to work for every sector, firm, and region. Fusion centers have shown considerable progress since the creation of the concept. But he added that the model is still maturing, and there is a need to develop a process that lessens the burden on the recipient of the information to synthesize and act upon intelligence. Metrics can assist in determining whether there is adequate information sharing nationwide – and whether that information is being shared in a suitably timely manner. Mr. Natarajan also noted that the metrics would inform the decisionmaking process more effectively.

Ms. Lau commented that there are many organizations working on the efforts to improve information sharing, and asked how those efforts can be best coordinated to address the need for efficient, effective sharing, as well as how private sector owners and operators can assist in the streamlining of mechanisms.

Mr. Natarajan responded that as part of the mandates of PPD-21, Federal Government recognizes this is an issue, and agencies have been meeting and discussing means of streamlining operation as a result. But he noted that the process will take time, and that the Federal Government hopes to be able to display improvements within the next year.

VI.	**REGIONAL RESILIENCY REPORT WORKING GROUP PRESENTATION**	*Constance H. Lau*, NIAC Chair, Working Group Co-Chair *Dr. Beverly Scott*, NIAC Working Group Co-Chair

Ms. Lau commented that the members of the NIAC Regional Resilience Working Group appreciated the opportunity to present their findings and recommendations.

She noted the report's title – *Strengthening Regional Resilience Through National, Regional, and Sector Partnerships* – was a theme that surfaced throughout the report development process. Partnerships are vital to the protection of national security, and the Federal Government has an important role in the establishment of those relationships. Both of these concepts were particularly clear in reference to the work done by the Federal Government and private sector representatives of the Electricity Sector, which Ms. Lau highlighted as an example by which other lifeline sectors can develop their own strong Federal-level partnerships. The application of such relationships throughout the lifeline sectors – rather than just in the Electricity Sector – would, in addition to strengthening those sectors, also enhance regional resilience by providing greater stability for those services upon which other sectors are reliant.

Mr. Lau then noted that some of the report's findings and recommendations are more specific, such as the establishment of national credentialing waivers, and permitting related to weigh stations. She commented that the Council has frequently heard —and recommended — that remedies for these types of issues could substantially ease response and recovery efforts, though resolutions for those issues have not been forthcoming. The NIAC therefore chose to re-emphasize some of those challenges, in order to encourage further work on the topics.

With regard to the Working Group's presentation on the report, Ms. Lau noted that she and Dr. Scott would present the bulk of the recommendations related to regional resilience, followed by a presentation from Mr. Gerstell on the report's social media recommendations, and an update from Mr. Wallace on the Electricity Sector executive-level engagement efforts. She also thanked Mr. Gerstell and Mr. Wallace for participating in both the Regional Resilience Working Group and the EO-PPD Working Group.

The purpose of the study was to identify methods for enhancing regional resilience, as well as the steps Federal Government can take to assist in the achievement of those goals. The Council's focus was on three primary subjects: best practices, process improvement, and the Federal role in the process. The Working Group gathered its data from more than 370 documents; 37 interviews with State and local government representatives, national leaders, infrastructure owners and operators, and Federal agencies; insights from the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC); and Webinars and conferences with regional government and critical infrastructure representatives. Ms. Lau noted that the Chair of the SLTTGCC, Mike McAllister, Deputy Secretary of Veterans Affairs and Homeland Security for the Commonwealth of Virginia, was in attendance for the meeting, and thanked him for the SLTTGCC's Regional Report series, which examines the CISR efforts in place at the State and local level. She also thanked Rick Houck, Vice President, Hawaiian Electric, for his work leading the Regional Resilience Study Group, which collected information on the effects of Superstorm Sandy on the CISR practices of governments and businesses in the mid-Atlantic region.

Dr. Scott then provided background on the regional resilience environment as it is presently constituted. She noted that there are three primary notions that underpin the subject of regional resilience: The current risk environment is dynamic and increasingly complex, in part because of interdependencies among communities and sectors, planning and decisionmaking models need to include the collective expertise, commitment, and resources of key security partners; and there is a need for flexible, agile systems, in order to allow for rapid response to disasters. She then thanked the support staff for their work in helping the Council work through the volumes of information dedicated to the study of resilient regions.

Dr. Scott continued by discussing the characteristics of a resilient region. She noted that national resilience is a product of resilient regions, and while top-down policy and leadership are

important, the challenge of strengthening and hardening critical infrastructure assets is largely one that exists at the ground level. Resilience requires a whole-of-community approach, and must include the following basic elements:

- Strategic intent and unity of effort
- Elevated priority of lifeline functions
- Exercised coordination and information sharing
- Intelligent infrastructure and innovation
- Partnerships and executive engagement
- Healthy and active community resources
- A clear value proposition
- Resilience measurement and risk management

Dr. Scott then noted the importance of tailoring regional resilience efforts to the characteristics and needs of each region. She commented that there can be no one-size-fits-all model for regional resilience, as each of the 10 Federal Regions has unique characteristics that must be recognized in the process of enhancing resilience. As examples, she noted that a key sector in the New York City metropolitan area — Banking and Finance — does not have the same resonance in other cities, such as Houston or New Orleans. Conversely, the Energy — Oil and Natural Gas Sector is a major economic driver in those cities, but not in New York.

Ms. Lau then briefly discussed the six key findings included in the report.

In discussing the first finding — lifeline sectors are top priorities for achieving regional resilience and their growing complexity creates hidden risks — Ms. Lau commented that the lifeline sectors provide critical operations for the other sectors, and the failure of a lifeline sector service can create life-threatening conditions. In addition, she noted the increasing number and range of interdependencies associated with these sectors, which need to be understood in order to better protect the services.

Ms. Lau noted Dr. Scott's earlier comments in relation to the second finding — Regional resilience efforts are most successful when tailored to the characteristics and needs of each region. She noted that as a result of the unique needs of a region, an effort to establish a one-size-fits-all policy toward regional resilience will, in effect, create a policy that actually serves none of the regions effectively.

Ms. Lau noted that the third finding — senior-level executive engagement creates strong public-private partnership, which is the most effective strategy for achieving long-term resilience within regions — has been highlighted in previous NIAC studies, but is important to re-emphasize. She added that strong public-private partnerships and relationships with and among senior executives

and senior-level officials in the Federal Government are essential to achieving meaningful gains in the CISR mission.

The fourth finding is that social media has emerged as a powerful but underutilized tool for communicating and collecting data during emergencies. Ms. Lau commented that social media — such as Facebook and Twitter — proved invaluable as a means of gathering and distributing information during Superstorm Sandy and the Boston Marathon Bombing, which had been highlighted by the Study Group, as well as in response to recent tornados in Central Illinois. As a result, better use of these emerging technologies is needed.

The fifth finding notes that complex rules, regulations, and processes hinder rapid recovery of lifeline infrastructures. Ms. Lau explained that, as with some of the findings, this observation had been noted in previous NIAC reports. Response efforts in the aftermath of Superstorm Sandy underlined this finding, as there were persistent challenges associated with rules, regulations, and processes.

The sixth finding states that without a strong value proposition, owners and operators are unable to invest in new and innovative infrastructure that can mitigate long-term structural risks within regions.

Ms. Lau then discussed the Working Group's recommendations on regional resilience.

She commented that the Working Group viewed the report as a special opportunity to help the Federal Government address some of the challenges facing infrastructure. She noted that the Nation is investing roughly $1 billion per day in new and upgraded infrastructure, and suggested that this outlay may not necessarily be addressing resilience concerns.

The Working Group's first recommendation is that the Federal Government should form partnerships with senior executives from the lifeline sectors. The recommendation also included three sub-recommendations: The President should direct the heads of appropriate Sector-Specific Agencies (SSAs) to convene a meeting with CEOs from each lifeline sector to develop partnerships to address high-priority risks; the process used for the engagement of the Electricity and Nuclear sectors should be documented, in order to provide best practices and lessons learned for other lifeline sectors; and the NIAC should be tasked with identifying the highest priority cross-sector risks affecting national security and resilience, and recommend subsequent executive-level cross-sector action.

The Working Group's second recommendation is that the Federal Government should identify regional, public-private, cross-sector partnerships led by senior executives. Sub-recommendations include that the Secretary of DHS should work with governors, mayors, local governments, and senior lifeline sector executives to develop sustainable cross-sector partnerships within selected regions; and that the Secretary initiates a pilot program with State

and local governments to conduct regional joint exercises, develop maps of critical interdependencies, and extract lessons learned.

The Working Group's third recommendation is that the President should designate the Energy, Communications, Water, and Transportation sectors as lifeline sectors. Ms. Lau noted that this recommendation was directly tied to the Working Group's first finding, which highlights the importance of the lifeline sectors. Sub-recommendations include that DHS should examine how action is currently coordinated and support is provided to lifeline sectors during event response; that Federal, State, and local emergency operations plans are modified to allow for co-location of lifeline sector representatives in emergency operations centers during major disasters; and a requirement from the President that Federal agencies explicitly consider the unique qualities of a region when establishing security and resilience rules and guidance — as well as expressly stating how implementation has been made customizable for each region, if necessary.

Ms. Lau then asked Mr. Gerstell to discuss the Working Group's fourth recommendation — social media should be integrated into the public alert and warning systems, and that social media training and information sharing capabilities are developed. Mr. Gerstell commented that the recommendation is a departure for the Council, as the subject has not been previously addressed. In referencing the Working Group's fourth finding, Mr. Gerstell noted that social media is an important two-way communication tool — but one that can have negative or positive effects, depending on the user. Sub-recommendations include that FEMA and the Federal Communications Commission (FCC) should examine how emerging social media capabilities could be used to support emergency notification and response; social media platforms should be integrated into FEMA's Integrated Public Alert and Warning System (IPAWS); recipients of FEMA non-disaster preparedness funding should designate personnel through IPAWS for the issuing of targeted emergency alerts; and a conference or Webinar series should be developed regarding innovative social media use and best practices in State and local emergency management. Mr. Gerstell added that there is a considerable amount that could be done with social media, and suggested that the issue remain under consideration beyond the recommendation in the report.

Ms. Lau thanked Mr. Gerstell, and discussed recommendation five: launch a cross-agency team to develop solutions to site access, waiver, and permit barriers during disaster response. She noted that many studies have referenced this issue, though the process of remedying it seems to be more complicated to address. As a result, the Working Group elected to make more specific recommendations on the subject, Sub-recommendations include that IP and FEMA work with SLTT governments to develop a common process or system of credentialing for lifeline sector personnel, in order to grant access to disaster areas; DHS should work with SLTT governments and owner/operators to catalogue commonly sought waivers during disaster recovery efforts, and develop a streamlined process for obtaining those permits; and that DHS work with lifeline

sector regulators to identify actions that could assist in the expediting of waivers, as well as in removing impediments to fleet movement.

Ms. Lau then discussed the Working Group's sixth recommendation: create the value proposition for investment in resilient lifeline infrastructures and adoption of innovative technologies. She noted that this subject was one in which the Working Group believed an opportunity could be missed to address the issue of aging infrastructure, as there is a chance to build resilience and innovative technologies into new or updated infrastructure. While the new technologies and building-in of resilience tend to be expensive, they are less expensive when incorporated into replacement infrastructure on an ongoing basis. Sub-recommendations include a Department of Energy-developed pilot analysis of the value proposition for investment in grid modernization, followed by collaborative work between lifeline sectors and their SSAs to establish the value proposition for investment in critical sectors; an examination by the National Oceanic and Atmospheric Administration (NOAA) on weather and climate forecasting models, in order to have as accurate as possible severe weather prediction capabilities; and development of Applied Centers of Excellence for Infrastructure Resilience, to provide an operating environment to test and validate technologies and processes that build resilience into new infrastructure projects.

Mr. Wallace then provided an update on the executive-level engagement efforts under way in the Electricity Sector. He noted that the Working Group included the update because the work to date has been substantive, and is demonstrating the value of such forms of public-private engagement. Prior to the engagement efforts, the sector had what Mr. Wallace deemed a minimal level of engagement, at least in terms of response or recovery. But in the time since then, the sector and the Federal Government are collaborating in a much more substantial way, and the partnership has already begun maturing.

Five primary concepts have served as principles of successful public-private partnerships: executive engagement; trusted relationships; simple processes; value proposition; and having a trusted executive facilitator. Mr. Wallace noted that Ms. Durkovich had noted some of these principles in her opening comments; he commented that those three principles were drawn from the Council's 2010 resilience study and its 2008 strategic assessment study, as they were the recommendations that were most valuable for creating substantive partnership. Mr. Wallace suggested that those in attendance consider the five principles and how they can be implemented in future partnerships.

Mr. Wallace then addressed the concept of executive-level engagement, and why it is necessary to involve CEOs in the partnership development and deployment process. He commented that among a CEO's duties, there are four key responsibilities — all of which are vital to developing movement on a partnership or an initiative: set strategy and direction; establish priorities and importance of the subject throughout management; providing and allocating resources; and exercising accountability. While some partnerships have been successfully established without

top-level leadership on the private sector side, Mr. Wallace suggested that such relationships are not only harder to sustain, but also tend to be personality-dependent, rather than process-dependent. The engagement of executives, on the other hand, tends to lead to more sustainable partnerships, as the executives have a fiduciary responsibility to shareholder and stakeholders to run the business successfully.

The catalyst for the Electricity Sector's executive-level engagement came from the NIAC's 2010 report on regional resilience for Electricity and Nuclear sector assets. A group of CEOs, inspired by the report, contacted the White House to request senior-level engagement, followed by a formal request for engagement in relation to the first recommendation in the 2010 report. From there, the executive-level engagement effort proceeded rapidly. The speed of the process provided a lesson to be learned both for the Government and CEOs; there is a value proposition associated with a specific, tangible engagement with the Federal Government, Mr. Wallace said.

Building trusted relationships is also vital to the process of enhancing executive-level engagement, Mr. Wallace said.

In the Electric Sector, that process has moved on an accelerated timetable. In July 2012, a meeting of CEOs with the Secretaries of DHS and DOE serving as co-chairs offered the opportunity to discuss common goals. Mr. Wallace noted that while the meeting itself was not intended to produce substantive outcomes, the act of meeting further inspired CEOs and senior government officials to begin working on methods to improve the risk profile of the grid. A subsequent meeting in September 2012 also helped to provide tangible resilience benefits, as those discussions helped to improve the trust and collaboration during Superstorm Sandy response efforts barely one month later. Mr. Wallace noted that the Joint Electric Executive Committee — which included 28 CEOs from the Electric Sector and was established in 2013 — engaged COOs and CIOs, and led to the creation of a working group focused on tactical deliverables. He thanked Ms. Durkovich and Patricia Hoffman, Assistant Secretary for DOE, for their commitment to engaging with the committee in its meetings.

Executive facilitators are also important to the building of trusted relationships. Mr. Wallace noted that this figure should be someone with industry experience who has high-level clearance — in order to work with the government — but is also able to work with CEOs to provide more connection with the Government. In the case of the Electric Sector, the executive facilitator gathered input from industry on tools and technologies, information sharing, and event response capabilities and plans, and was able to provide that information to the Federal Government to establish the dialogue that helped to bring together the partnership. Since then, the Joint Electric Executive Committee has become the Sector Coordinating Committee (SCC) for the Electricity Subsector.

Mr. Wallace then commented on the importance of using a clear and tangible process, as there have been several large items added to the Joint Electric Executive Committee's agenda as a result of these changes. He added that only those items with tangible value added are moving forward, such as the Joint Electric Executive Committee's recent work on the "Poison Apple" cyber security tabletop exercise.

In November 2013, the Electricity Sector partnership performed an extensive exercise known as GridEx II. More than 200 venues and 1,800 participants tested the electricity grid's resilience against cyber and physical attacks, in order to determine how the grid would respond to a series of disruptive scenarios. That was followed by a 5-hour tabletop exercise, in which the grid was tested for the effects of an intentional catastrophic cyber failure, in order to provide a sense of the extreme effects possible in such an event. Mr. Wallace noted that the Committee is currently developing recommendations and action items from the GridEx II exercise.

Mr. Wallace expressed his confidence that industry and the Federal Government will continue to work together on the partnership, and the challenges faced by both the public and private sectors in relation to the resilience of the Electricity Sector. He noted that while the Electricity Sector's advances and methods may not exactly correlate to those most effective for other lifeline sectors, he recommended that the overall concepts that served the sector – executive engagement, trusted relationships, simple processes, value proposition, and having a trusted executive facilitator – should be a focus of any efforts to establish executive-level partnerships.

Members were then afforded time to offer comments and ask questions.

Ms. Grayson commented that in considering the outcomes and recommendations, the Council has continued to build upon its work in previous reports. She noted that in looking forward, there are subjects – such as the social media recommendation – that the Council should continue to focus on in the future.

VII. PUBLIC COMMENT: TOPICS LIMITED TO REGIONAL RESILIENCE REPORT — *Nancy J. Wong,* DFO, NIAC, DHS

No public comments were registered.

VIII. REGIONAL RESILIENCY REPORT DISCUSSION AND DELIBERATION — *Constance H. Lau,* NIAC Chair

Mr. Kolasky praised the report, and commented that the Government used previous NIAC concepts in the development of EO 13636 and PPD-21 — though he noted that the language used is not identical. He then asked for clarification on what constitutes a cross-sector risk.

Ms. Lau responded that in considering the lifeline sectors, the Working Group felt there might be considerable value in convening the sectors to address some of the critical interdependencies that affect all lifeline sectors, but not necessarily within a sector. Mr. Wallace noted the example of moving fuel into a disaster area, which requires the coordination of both the Energy and Transportation sectors. He added that another important cross-sector interdependency is the contrast in vulnerabilities, which he noted is less about one sector relying on another, and more about the diminished capacity to multiple sectors because of threats or vulnerabilities.

Gen. Edmonds commented that the report seemed to be on target, and noted the Emergency Telephone System was funded by the Federal Government as a priority for improving response and preparedness efforts, and suggested that a similar effort and investment be put in place for the lifeline sectors.

Dr. Scott, in reference to Mr. Kolasky's comments, added that in addressing cross-sector threats, the key will be to find the common intersection point of each of the lifeline sectors. She noted that this will help inform the Federal Government on the most valuable and appropriate areas for resource allocation.

Mr. Flynn asked Mr. Wallace for his opinion on how executive-level engagement might be achieved in other sectors. He noted that the Electricity Sector's efforts had begun with a letter from CEOs to the President, and asked how the Federal Government can engage with other sector CEOs who have not made similar efforts.

Mr. Wallace responded that the Federal Government should focus on the financial benefits for CEOs to become engaged in the partnership. The concept of enhancing the protection of assets provides a value proposition that is more likely to generate sustained participation than impressing the national security aspects of engagement. He re-emphasized the value of having a third-party facilitator who has the trust of both executives and senior-level Federal officials, and noted that a simple process is essential.

Dr. Tribble commented that some CEOs are skeptical of Government overtures to collaboration. In addition, she noted that the Electricity Sector may be unique. A similar effort undertaken with the Fuel Sector has not generated the same maturing partnership; generally, those executive-level owners and operators have been more concerned with overseas issues than domestic concerns. Because of these observed challenges, she asked that there be flexibility in the implementation of the recommendation, as the successes of the Electricity Sector may not apply in all cases. Dr. Tribble also noted some challenges specific to other lifeline sectors. In the Water Sector, owners and operators are typically at the local or municipal level. And in the Transportation Sector, sub-sectors and systems can be run federally, at the State and local level, privately, or a mix of one or more collaborative arrangements.

Ms. Lau responded that the Working Group had used the term CEOs primarily as a means to direct focus toward engaging those with leadership and decisionmaking responsibilities for a critical infrastructure asset. She noted that further clarification of that point in the report might be worthwhile.

Mr. Kepler observed that the case study of the Electricity Sector was meant to be an example of the beneficial effects of the Council's previous recommendations on engagement.

Gen. Edmonds reiterated that industry is unlikely to invest in efforts that are solely for national security, as it is generally held that the Federal Government is responsible for those issues.

Dr. Tribble noted her appreciation and agreement with Recommendation 1.1 and 2.1, and emphasized that she wanted to ensure that the appropriate agencies and organizations are engaged.

Mr. Kepler expressed concern that while the idea of encouraging specific investment is a good one, and should be considered, it may need to be considered further.

Gen. Edmonds noted that it is important to begin considering how to go about funding those efforts, Ms. Lau agreed, and said that the concept ties in to the recommendation on the value proposition than can be created.

A question was then raised as to whether the Council considered cyber security as part of the resilience discussion.

Ms. Lau responded while cyber security was not specifically mentioned, it is central to the discussion. Cyber and physical infrastructure are closely tied, so the Working Group treated the inclusion of both aspects as assumed.

Mr. Natarajan noted his appreciation for including the recommendations and findings regarding the vulnerabilities and challenges of social media. He noted that there are considerable challenges surrounding the accuracy of information, and thanked the council for addressing the potential for misinformation as it considered the subject.

Dr. Tribble noted that the Council's comments on social media will be challenging for the Federal Government. She added that she appreciated the suggestion that the Council could take on further study of the subject. She thanked the NIAC for bringing the issue forward, as she noted that privacy and data collection have proven to be substantial challenges so far.

Ms. Lau responded that the Working Group tried to make specific and actionable recommendations on social media in order to assist the Government in gaining value from social media via IPAWS.

Mr. Gerstell then commented that Recommendation 6.2 might need to be re-worded. At present, the recommendation's wording may imply that the Council is unaware that NOAA is already developing on extreme weather and climate forecasting models. Instead, he suggested that the recommendation advocate that NOAA and the Administration develop an understanding of how those models can be more effective and better communicate danger. He also suggested that the report title be changed to *Strengthening Regional Resilience*. Mr. Gerstell noted that the inclusion of "partnerships" in the current title -- *Strengthening Regional Resilience Through National, Regional, and Sector Partnerships* – is somewhat misleading, as four of the six recommendations are not related to partnerships.

NIAC members then voted in favor of approving the report, subject to the suggested changes.

IX.	**EO 13636 AND PPD 21 IMPLEMENTATION: FEDERAL GOVERNMENT STATUS REPORT ON EO-PPD IMPLEMENTATION INTEGRATED TASK FORCE**	*Robert Kolasky,* Director, Integrated Taskforce for the Implementation of EO 13636 and PPD 21, DHS

Mr. Kolasky began by thanking the Council for its work on the Regional Resilience study. He noted that the work aligns well with the ongoing revisions to the National Infrastructure Protection Plan (NIPP), which the Government plans to publish by the end of 2013.

A majority of the deliverables required by EO 13636 and PPD-21 have been completed. Mr. Kolasky noted that there is still considerable work on the cyber security framework and the voluntary program to be completed, but that a final framework will be released in February.

A key focus in 2014 for the ITF will be encouraging organizations to adopt the voluntary framework by demonstrating the value of participation. The ITF will highlight the cyber risk reduction that can be achieved via the framework, as well as the flexible, repeatable, performance-based, and cost-effective nature of the framework.

X.	**EO 13636 AND PPD 21 IMPLEMENTATION: NIAC WORKING GROUP REPORT PRESENTATION**	*David Kepler,* NIAC Working Group Co-Chair *Philip Heasley,* NIAC Working Group Co-Chair

Ms. Lau thanked Mr. Kolasky for the update, and then asked Mr. Kepler to discuss the Council report on the implementation of EO-13636 and PPD-21. Ms. Lau also thanked the Administration for the opportunity to provide advice in an ongoing context such as this one, and noted her appreciation for the attention paid to the NIAC's input on the two documents.

Mr. Kepler began by complimenting members of the EO-PPD Working Group for their work on the report. He noted that the report was created in a different way than many NIAC reports;

rather than being given an area of study and then structuring a report around that concept, this study involved reviewing the two documents and responding to questions based on the implementation of those policies, as well as positing framework questions to provide context for the Federal Government on the subject.

Mr. Kepler then briefly discussed the Working Group's findings. He noted that members based their findings and conclusions around the notion of the critical purpose of the system — securing the Nation from cyber threats — as well as how that purpose can be achieved, how to measure those advances, and how to incentivize sector collaboration. The Working Group also reviewed several potential incentives that might encourage participation, and determined those incentives to be an effective framework, good-faith protection of shared information, streamlining of regulations, and outcome-based metrics.

On the subject of metrics, Mr. Kepler noted that some systems already in use may provide useful templates. In particular, he highlighted the Department of Labor Occupational Safety and Health Administration (OHSA) Voluntary Partnership Program and the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 as programs that could guide the development of the cyber security framework.

Mr. Kepler then discussed the Working Group's findings regarding how to improve information sharing as part of the EO13636 and PPD-21 implementation process.

The creation of a Safe Harbor for information sharing would encourage greater participation, Mr. Kepler said. A Safe Harbor would provide private sector owners and operators who are acting in good faith a means to share information with the Government, without fear of that information later being used in a regulatory or punitive context.

In addition, more companies would be inclined to take part in the program if the information being shared is specific, actionable, and delivered in a timely manner. Mr. Kepler noted that the mechanisms currently in place for information sharing should also be reviewed, in order to determine if any of the systems are redundant, and therefore unnecessary.

The Working Group also highlighted the over-classification of information as a barrier to better sharing. Mr. Kepler noted that cyber and physical security are different in this sense; while a threat to a physical asset is localized to the threat site — and can therefore be addressed with limited sharing of information with onsite personnel — a cyber threat can have an effect on any part of the asset, and therefore may need more personnel monitoring the system and mitigating issues.

Mr. Kepler then discussed the Working Group's findings in relation to the cyber security framework. He commented that the framework had been well structured, and that its draft forms had shown promise as discussed by the Working Group.

The Working Group noted the importance of metrics and milestones to the success of the framework, and Mr. Kepler commented that the recommendations relating to those concepts were developed as a means to help provide focus. He noted the importance of first focusing on the lifeline sectors, by engaging the IT Sector in the recognition that enhanced security of products and services are necessary. Mr. Kepler added that there are standards for many IT products that could be incorporated into this concept.

The Working Group also pointed out that the process of extracting the most value from the framework will be reliant on an ongoing effort to improve and enhance the program. Mr. Kepler noted that there is a need for more specific information with regard to where the framework will be housed, and who will be responsible for the upkeep and advancement of the system. He added that the Working Group suggested that the framework would be housed and maintained outside of the Federal Government, and noted that a university might be the ideal location.

Mr. Kepler also discussed the Working Group's findings in relation to the revision of the NIPP. He commented that many of the observations offered by the Working Group in previous public meetings have already been incorporated, but re-emphasized the value of a risk management framework, and an outcome-based and process-driven approach.

Mr. Kepler then noted that many of the Working Group's recommendations had been discussed during the three public meetings held between July and September, but that he would discuss the report's recommendations on the engagement of small- and mid-sized owners and operators. He commented that it is important to include a focus on these firms, as they are part of the supply chain for larger owners and operators — meaning a security failure at those levels could have downstream consequences for larger firms. The Working Group recommended that the Government should fund programs at universities that could assist these small- and mid-sized operators in understanding and leveraging the framework. Mr. Kepler noted that small businesses do not have the necessary resources to adequately staff information security departments. As a result, such university-based programs could greatly aid in the enhanced cyber security of smaller owners and operators. In addition, the Government could use the power of procurement as a means of encouraging IT providers and suppliers to create programs that have security as primary design criteria.

XI. PUBLIC COMMENT: TOPICS LIMITED TO EO 13636 AND PPD 21 IMPLEMENTATION REPORT — *Nancy J. Wong,* DFO, NIAC, DHS

No public comments were registered.

XII. EO 13636 AND PPD 21 IMPLEMENTATION: REPORT DISCUSSION AND DELIBERATION — *Constance H. Lau,* NIAC Chair

Mr. Kepler recommended that that the Working Group make minor administrative revisions to the report, as members had limited time to finalize it prior to the meeting.

Mr. Kolasky commented that Finding 13, regarding centralized ownership of the cyber security framework, should be moved, as its inclusion in the section on the NIPP revision could produce confusion. The Working Group agreed to incorporate that finding into Recommendation 6, which addresses how an independent housing of the framework can assist small- and mid-sized businesses in enhancing their ability to face cyber threats.

NIAC members then voted to approve the report, pending administrative changes.

XIII. DISCUSSION AND STATUS OF TRANSPORTATION RESILIENCY STUDY WORKING GROUP

Nancy J. Wong, DFO, NIAC, DHS

Dr. Scott provided a brief update on the work to date on recruiting members and scoping for the Transportation Sector resilience study. Mr. Gerstell and Mr. Baylis will be serving as co-chairs on the study; Dr. Scott encouraged members of the Council to contact the NIAC Secretariat if they wish to participate in the Working Group. In addition, she noted that because of the complexity of the sector — with its mix of modes and forms of public, private, and hybrid ownership — the study will require considerable focus. It will be important to incorporate all aspects of resilience related to national priorities and cyber security, and to address executive-level engagement in the sector.

XIV. CLOSING REMARKS

Constance H. Lau, NIAC Chair

Caitlin Durkovich, Assistant Secretary for Infrastructure Protection, DHS

William F. Flynn, Deputy Assistant Secretary for Infrastructure Protection, DHS

Dr. Ahsha Tribble, Acting Deputy Homeland Security Advisor, National Security Staff

Nitin Natarajan, Director, Critical Infrastructure Protection and Resilience, National Security Staff

Samara Moore, Director for Cyber Security and Critical Infrastructure, National Security Staff

Ms. Durkovich reiterated her thanks to the Council. She noted that members have considerable responsibilities in their daily work lives, and that the Federal Government values their willingness to dedicate time to the NIAC. Members' feedback and recommendations — both on the Regional Resilience report and the EO-PPD Implementation report — have been greatly appreciated, and are given serious consideration. She added that the Government will continue to update the NIAC on the progress of implementing previous and current recommendations, as appropriate.

Mr. Flynn also thanked the members for their hard work, and commented that a review of EO 13636 and PPD-21 demonstrates the attention and interest the Government has paid to previous NIAC reports, as many Council recommendations have been implemented in those documents.

Dr. Tribble noted her appreciation for the time commitment displayed by Council members. She commented that the Administration will work to incorporate and implement the recommendations as quickly as possible into policy. She also acknowledged that while there are many impediments to implementation of any policy, there is considerable interest in doing so — despite what the speed of implementation might suggest.

Mr. Natarajan thanked the members, and commented on the volume of work needed to produce both reports over the past year. He noted that in attending all six of the Council's meetings, he has seen the scale of production needed, and that he was appreciative for those efforts. In addition, he emphasized that NIAC reports are frequently referenced in other meetings and public forums, including academia, demonstrating the inherent value of the Council's work.

Ms. Moore also offered her thanks for the meaningful insight offered by the NIAC. She added that the release of the reports is well-timed, as the Administration is actively engaged in both areas of study.

XV. ADJOURNMENT — *Constance H. Lau,* NIAC Chair

Ms. Lau thanked members, Federal Government representatives, and attendees for their attendance and participation, 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: 2-15-14
Constance H. Lau, Chair, NIAC

Improving Public-Private Information Sharing in Support of Critical Infrastructure

Kshemendra Paul, Program Manager
Information Sharing Environment

November 21, 2013

VISION

National security through responsible information sharing

MISSION

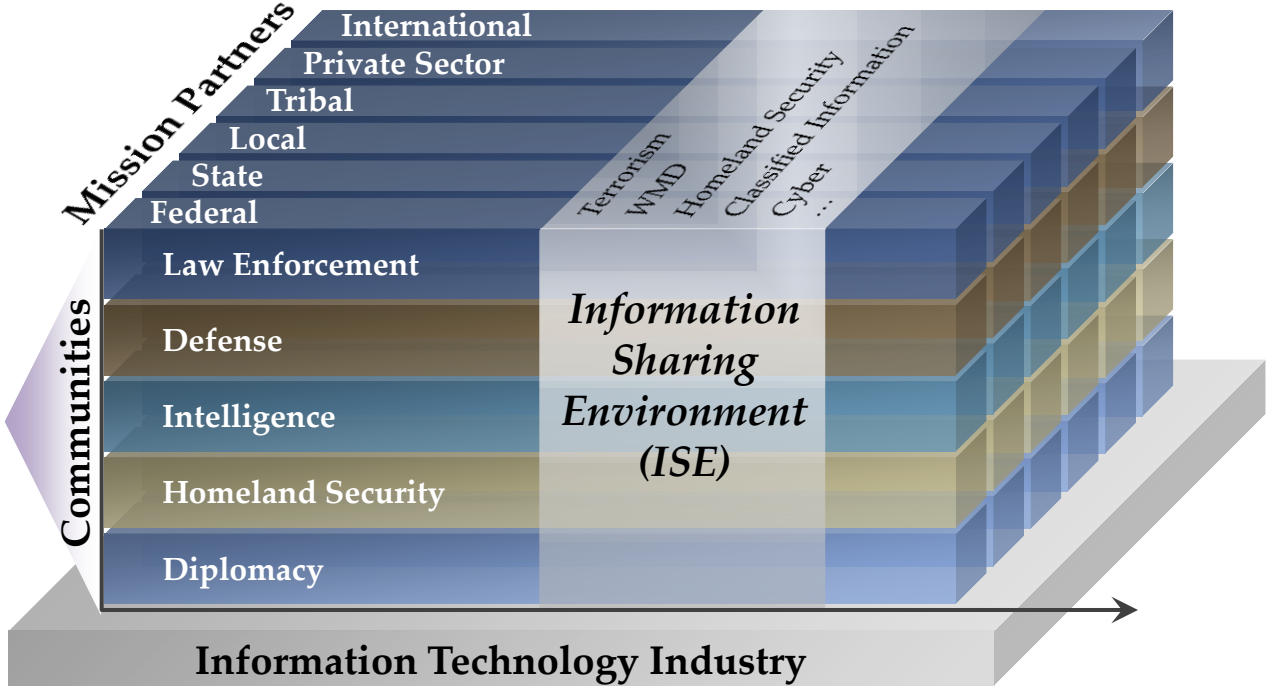
Advance responsible information sharing to further counterterrorism and homeland security missions

Improve nationwide decision making by transforming information ownership to stewardship

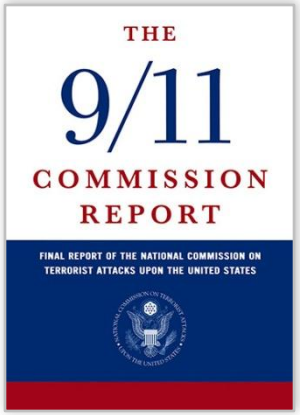
Promote partnerships across federal, state, local, and tribal governments, the private sector, and internationally

SCOPE OF THE ISE

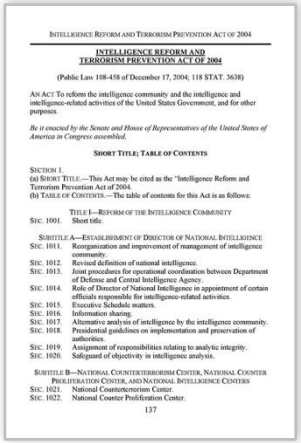
Frontline
- Investigators
- Analysts
- Operators



ISE FOUNDATION



IRTPA
Intelligence Reform and Terrorism Protection Act of 2004


INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

(Public Law 108-458 of December 17, 2004; 118 STAT. 3638)

AN ACT To reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE; TABLE OF CONTENTS

SECTION 1.
(a) SHORT TITLE.—This Act may be cited as the "Intelligence Reform and Terrorism Prevention Act of 2004.
(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

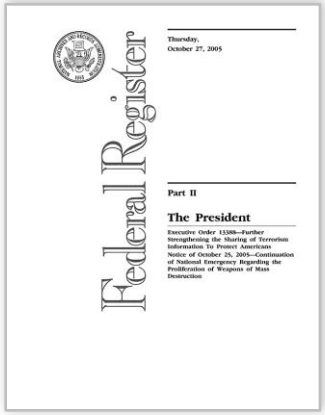
TITLE I—REFORM OF THE INTELLIGENCE COMMUNITY
SEC. 1001. Short title.

SUBTITLE A—ESTABLISHMENT OF DIRECTOR OF NATIONAL INTELLIGENCE
SEC. 1011. Reorganization and improvement of management of intelligence community.
SEC. 1012. Revised definition of national intelligence.
SEC. 1013. Joint procedures for operational coordination between Department of Defense and Central Intelligence Agency.
SEC. 1014. Role of Director of National Intelligence in appointment of certain officials responsible for intelligence-related activities.
SEC. 1015. Executive Schedule matters.
SEC. 1016. Information sharing.
SEC. 1017. Alternative analysis of intelligence by the intelligence community.
SEC. 1018. Presidential guidelines on implementation and preservation of authorities.
SEC. 1019. Assignment of responsibilities relating to analytic integrity.
SEC. 1020. Safeguard of objectivity in intelligence analysis.

SUBTITLE B—NATIONAL COUNTERTERRORISM CENTER, NATIONAL COUNTER PROLIFERATION CENTER, AND NATIONAL INTELLIGENCE CENTERS
SEC. 1021. National Counterterrorism Center.
SEC. 1022. National Counter Proliferation Center.

137

Executive Order 13388


Federal Register

Thursday,
October 27, 2005

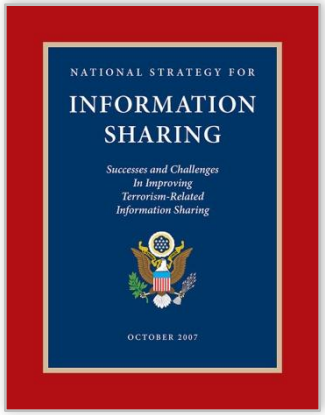
Part II

The President

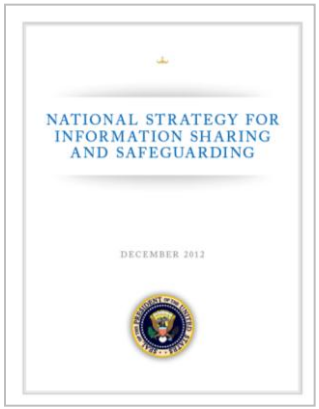
Executive Order 13388—Further Strengthening the Sharing of Terrorism Information To Protect Americans

Notice of October 25, 2005—Continuation of National Emergency Regarding the Proliferation of Weapons of Mass Destruction

2007 National Strategy



2012 National Strategy



Markle Task Force

Presidential Guidelines


Guideline 2 – Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector

I. Introduction

In the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Congress directed the establishment of an Information Sharing Environment (ISE) to improve and facilitate the sharing of terrorism information. On December 16, 2005, and in furtherance of his efforts to implement the enactment, the President issued a Memorandum for the Heads of Executive Departments and Agencies, which establishes guidelines and directs particular actions to effect the creation and operation of the ISE.

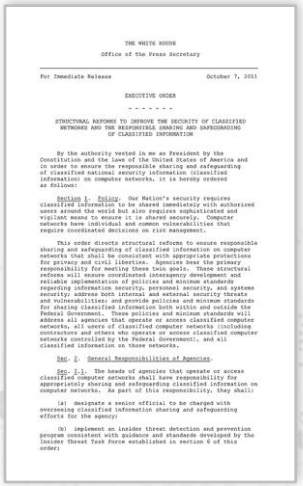
Guideline 2 of the President's Memorandum directed the development of "a Common Framework for the Sharing of Information Between and Among Executive departments and Agencies and State, local, and tribal Governments, Law Enforcement Agencies, and the Private Sector." Specifically, Guideline 2 directed the Attorney General and the Secretary of Homeland Security, in consultation with the Secretaries of State, Defense, and Health and Human Services and the Director of National Intelligence, to

(i) perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing with State, local, and tribal governments, law enforcement agencies, and the private sector; and

(ii) submit to the President for approval, through the [Assistant to the President for Homeland Security and Counterterrorism] APHS-CT and the [Assistant to the President for National Security Affairs] APNSA, a recommended framework to govern the roles and responsibilities of executive departments and agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and among such departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities.

In response to the President's directive, the Department of Justice (DOJ) and Department of Homeland Security (DHS), with assistance from the Office of the Program Manager for the Information Sharing Environment (PM-ISE), have proposed such a framework for information sharing. This document delineates that framework by outlining the principles that guided the construction of the framework, explaining the framework's

Executive Order 13587


THE WHITE HOUSE
Office of the Press Secretary

For Immediate Release October 7, 2011

EXECUTIVE ORDER

STRUCTURAL REFORMS TO IMPROVE THE SECURITY OF CLASSIFIED NETWORKS AND THE RESPONSIBLE SHARING AND SAFEGUARDING OF CLASSIFIED INFORMATION

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Section 1. Policy. Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Sec. 2. General Responsibilities of Agencies.

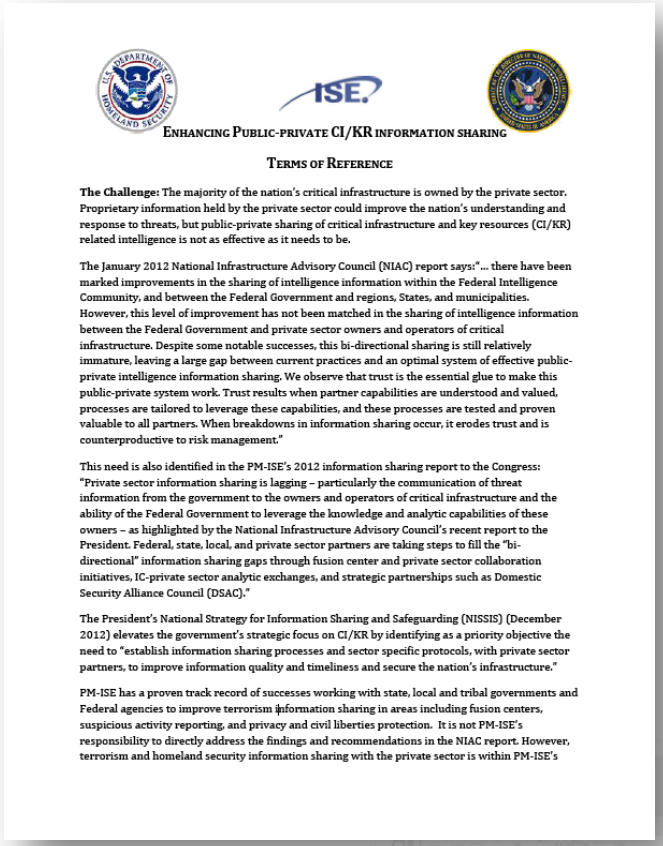
Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

Accelerating Private Sector Integration into the ISE

Terms of Reference



ENHANCING PUBLIC-PRIVATE CI/KR INFORMATION SHARING

TERMS OF REFERENCE

The Challenge: The majority of the nation's critical infrastructure is owned by the private sector. Proprietary information held by the private sector could improve the nation's understanding and response to threats, but public-private sharing of critical infrastructure and key resources (CI/KR) related intelligence is not as effective as it needs to be.

The January 2012 National Infrastructure Advisory Council (NIAC) report says:"... there have been marked improvements in the sharing of intelligence information within the Federal Intelligence Community, and between the Federal Government and regions, States, and municipalities. However, this level of improvement has not been matched in the sharing of intelligence information between the Federal Government and private sector owners and operators of critical infrastructure. Despite some notable successes, this bi-directional sharing is still relatively immature, leaving a large gap between current practices and an optimal system of effective public-private intelligence information sharing. We observe that trust is the essential glue to make this public-private system work. Trust results when partner capabilities are understood and valued, processes are tailored to leverage these capabilities, and these processes are tested and proven valuable to all partners. When breakdowns in information sharing occur, it erodes trust and is counterproductive to risk management."

This need is also identified in the PM-ISE's 2012 information sharing report to the Congress: "Private sector information sharing is lagging – particularly the communication of threat information from the government to the owners and operators of critical infrastructure and the ability of the Federal Government to leverage the knowledge and analytic capabilities of these owners – as highlighted by the National Infrastructure Advisory Council's recent report to the President. Federal, state, local, and private sector partners are taking steps to fill the "bi-directional" information sharing gaps through fusion center and private sector collaboration initiatives, IC-private sector analytic exchanges, and strategic partnerships such as Domestic Security Alliance Council (DSAC)."

The President's National Strategy for Information Sharing and Safeguarding (NISSIS) (December 2012) elevates the government's strategic focus on CI/KR by identifying as a priority objective the need to "establish information sharing processes and sector specific protocols, with private sector partners, to improve information quality and timeliness and secure the nation's infrastructure."

PM-ISE has a proven track record of successes working with state, local and tribal governments and Federal agencies to improve terrorism information sharing in areas including fusion centers, suspicious activity reporting, and privacy and civil liberties protection. It is not PM-ISE's responsibility to directly address the findings and recommendations in the NIAC report. However, terrorism and homeland security information sharing with the private sector is within PM-ISE's

- DHS, PM-ISE, and ODNI joint collaboration
- Targeted response to the January 2012 NIAC Report Findings
  - "Despite some notable successes, bi-directional sharing is still relatively immature, leaving a large gap between current practices and an optimal system of effective public-private intelligence information sharing."
- Accelerate private sector integration (with a focus on Critical Infrastructure owners and operators) *into the broader Information Sharing Environment*
- Phased Approach
  - P1: Outreach and Fact-Finding
  - P2: Develop Findings and Recommendations
  - P3: Implement Recommendations

Goals in Framing Our Recommendations

- Target activity areas that would deliver impactful improvements.
- Leverage planned and on-going efforts by ISE partners to implement National Policy directives to enhance Critical Infrastructure security and resilience.
  - PPD-21
  - Executive Order 13636
  - 2013 Update to the National Infrastructure Protection Plan
- Ensure alignment with key recommendations from the January 2012 NIAC Report.
  - Increasing Fusion Center capacity to share information
  - Enhancing doctrine to recognize the Private Sector as a customer and recipient of threat information
  - Increasing the use and sharing of best practices across federal partners
  - Building sector-specific analytic capacity

Joint Initiative Recommendation Objectives

Leveraging Fusion Center Capabilities	Alignment to NIAC Recommendations	Alignment to E.O. 13636 & PPD-21 Objectives
• Improve how fusion centers individually and collectively can better support Critical Infrastructure Owners and Operators by leveraging existing programs, including field-based programs sponsored by DHS and the FBI • Increase Critical Infrastructure Owners and Operators access to relevant Fusion Center Products •Increase private sector awareness of, and connectivity to, their local Fusion Centers • Provide training and awareness of emerging threats to Critical Infrastructure Owners and Operators	**NIAC Recommendation 7:** Enhance fusion center capabilities as one mechanism for sharing. **NIAC Recommendation 5:** Build accepted practices for timely information delivery. **NIAC Recommendation 3:** Improve information content by leveraging partner capabilities.	**PPD 21 and EO 13636:** Promote increased information sharing to strengthen security and resilience. **PPD 21:** Enhance security and resilience against emerging threat streams. **E.O. 13636:** Establish a consultative process w/ (SLTT, SSAs, SCCs, P/S, etc.) to coordinate improvements to cybersecurity of Critical Infrastructure

Joint Initiative Recommendation Objectives

	Alignment to NIAC Recommendations	Alignment to E.O. 13636 & PPD-21 Objectives
Developing Relevant Policy		
•Support decision options and doctrine that establish the Private Sector as a customer and recipient of threat information	**NIAC Recommendation 2:** Improve the implementation of existing authorities; ODNI should aim to reduce ambiguity and simplify engagement points and processes in the rules and relationships for information sharing.	**PPD 21:** Refine and clarify functional relationships across the Federal Government to advance national unity of effort.
Accelerating the Sharing and Use of Best Practices		
•Identify information Sharing Best Practices across Sectors and with Sector Specific Agencies	**NIAC Recommendation 5:** Build accepted practices for timely information delivery.	**PPD 21:** Enable efficient information exchange by identifying baseline data and systems requirements.

Joint Initiative Recommendation Objectives

	Alignment to NIAC Recommendations	Alignment to E.O. 13636 & PPD-21 Objectives
Building Analytic Capacity		
•Increase analysts' capacity related to critical sectors and improve their overall understanding and ability to provide Critical Infrastructure Owners and Operators with relevant and timely threat information. •Identify and promote tools in use across the government that enhance risk management of infrastructure assets. •Expand existing capabilities to increase the relevance and timely distribution of analytical products to state, local, and Critical Infrastructure Owners and Operators at the lowest possible classification level.	**NIAC Recommendation 3:** Improve Information content by leveraging partner capabilities. **NIAC Recommendation 4:** Improve the value of information products to industry risk-management practices. **NIAC Recommendation 5:** Build accepted practices for timely information delivery.	**PPD-21:** Develop a Situational Awareness Capability for Critical Infrastructure. **E.O 13636:** Increase the volume, timeliness and quality of cyber threat information shared with P/S entities. **PPD 21:** Support the integration and analysis function and develop a Situational Awareness Capability for Critical Infrastructure.

NATIONAL STRATEGY FOR INFORMATION SHARING AND SAFEGUARDING

Principles:

- Information as a national asset
- Information sharing & safeguarding requires shared risk management
- Information informs decision making

NSISS Priority Objectives

1. Governance
2. Agreements
3. Data Tagging
4. FICAM
5. Safeguarding
6. Interoperability Baseline Capabilities
7. Training
8. Discovery & Access
9. ***Private Sector Sharing***
10. Data Aggregation Reference Architecture
11. Shared Services
12. Standards-based Acquisition
13. Foreign Partners
14. AWN & RFI Process
15. NSI
16. Fusion Centers

Other PM-ISE Initiatives Relevant to NIAC Priorities

State-Wide, Regional, & Domain-Specific ISEs

NEXT STEPS

- Resolve way-forward on NSISS Priority Objective 9
- Examine feedback from this forum on accelerating private sector integration into the Information Sharing Environment

To Learn More

BUILDING BLOCKS

How do you promote responsible information sharing? What do you need to build information sharing across all levels of government, the private sector, internationally, or within your organization? It's a challenge, and we've learned a lot working toward that goal.

Those important lessons we've learned - coupled with best practices from our partners - are incorporated into the following "Building Blocks." Each of the icons below represents one of the fundamental components needed for responsible information sharing. Learn more about us.

HOW CAN I USE BUILDING BLOCKS?
READ AND SHARE CONTENT AND SUCCESS STORIES.

Search Building Blocks

SEARCH

Glossary | FAQ | Contact Building Blocks

GOVERNANCE

BUDGET & PERFORMANCE

ACQUISITION

STANDARDS & INTEROPERABILITY

COMMUNICATIONS & PARTNERSHIPS

VISIT ISE.GOV

@shareandprotect

@info-sharing-environment

Responsible Information Sharing to Enhance National Security

National Infrastructure Advisory Council (NIAC)

Regional Resilience Working Group Report and Recommendations

November 21, 2013 – Final Report (#5)

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

- Study Overview
- General Observations
- Findings
- Recommendations
- Questions & Deliberations
- Executive Engagement in the Electricity Sector

Study Overview

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

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.

Information and Data Sources

- Council member experiences
- Results from the Superstorm Sandy Case Study
- 370 documents (reports, studies, videos, news articles, testimonies, and policy directives)
- 37 interviews with state and local government representatives, national leaders, infrastructure owners and operators, and Federal agencies
- Insights from the State, Local, Tribal, and Territorial Government Coordinating Council
- Webinars and conferences with regional government and critical infrastructure representatives

General Observations

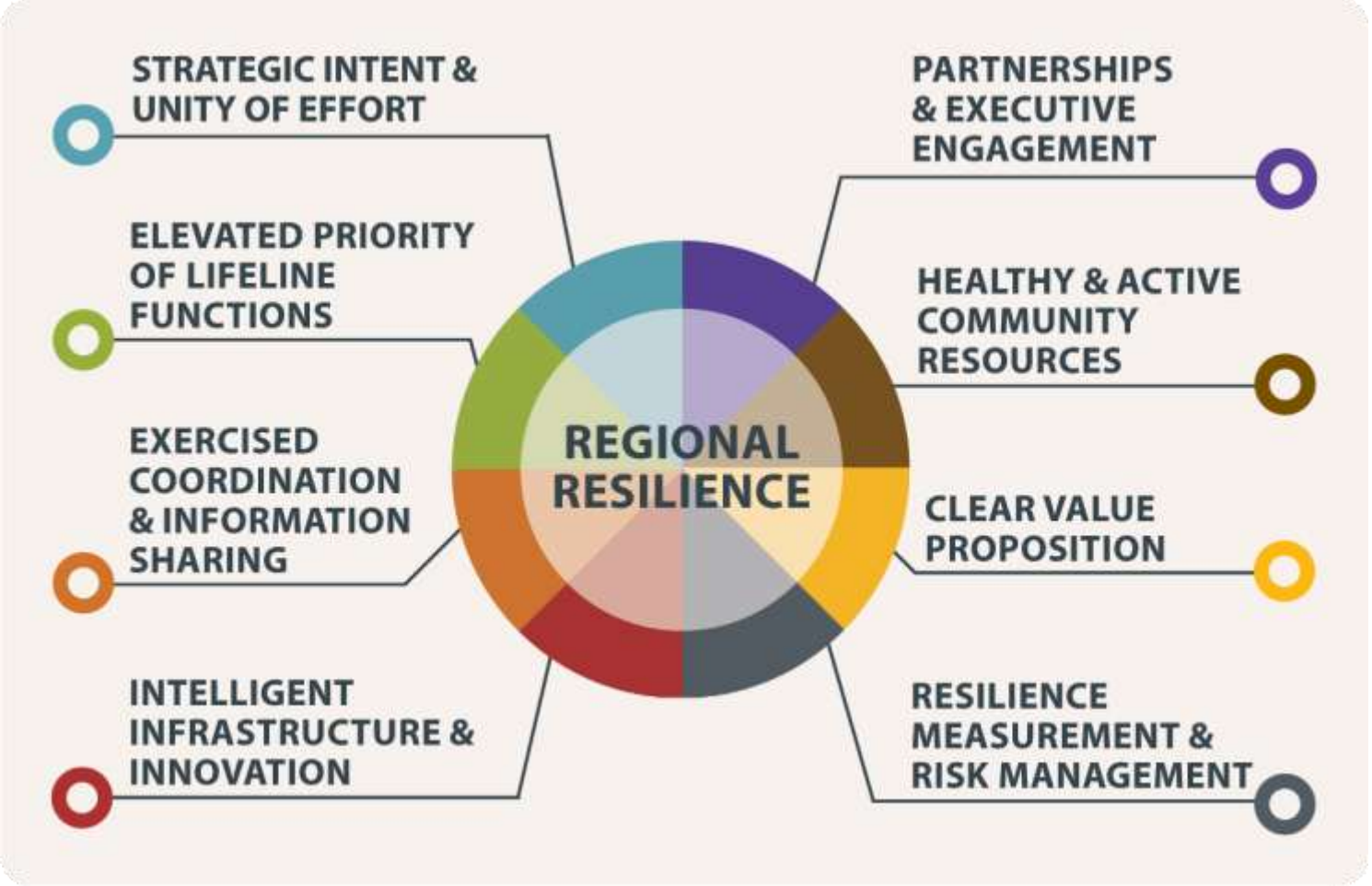
Today's Realities

1. We live in a **dynamic risk environment of increasing complexity** and interdependence of related communities, regions, and lifeline infrastructures that must be reflected in our national strategies.
2. The model for planning and decision-making must include the **collective expertise, commitment, and resources of key security partners**, including owners and operators; Federal, state, and local government; non-profits; and communities.
3. Despite our best efforts, disasters will continue to occur, requiring more **flexible and agile systems** to rapidly respond to and recover from events.

Principles of Regional Resilience

1. Resilience requires a **whole-of-nation approach** that integrates top-down policy and leadership with bottom-up community capability to withstand and survive disasters.
2. Regional resilience strategies must be tailored to the **distinct needs of each region** and designed to manage complex regional risks that span multiple jurisdictions and sectors.
3. Creating strong public-private partnerships and relationships with **senior executive involvement** is the most effective and enduring strategy for achieving sustainable resilience.

Characteristics of Resilient Regions



Findings

Six Key Findings

1. **Lifeline sectors are top priorities for achieving regional resilience** and their growing complexity creates hidden risks.
2. Regional resilience efforts are most successful when **tailored to the characteristics and needs of each region**.
3. **Senior executive engagement creates strong public-private partnership**, which is the most effective strategy for achieving long-term resilience within regions.
4. **Social media has emerged as a powerful but underutilized tool** for communicating and collecting data during emergencies.
5. **Complex rules, regulations, and processes hinder rapid recovery** of lifeline infrastructures.
6. **Without a strong value proposition, owners and operators are unable to invest** in new and innovative infrastructure that can mitigate long-term structural risks within regions.

Recommendations

Recommendation 1. Form partnerships with senior executives from the lifeline sectors.

1.1 Within six months, the President should direct the heads of appropriate Sector-Specific Agencies to **convene a meeting with CEOs from each lifeline sector to explore the formation of a partnership** to address high-priority risks to the sector's infrastructure.

1.2 The Department of Energy, in collaboration with the Department of Homeland Security (DHS), should **work with the electricity and nuclear sectors to document the process used for CEO engagement** in the electricity sector to discern lessons learned that can guide senior executive partnerships in other lifeline sectors.

1.3 The President should task the NIAC **to identify the highest priority cross-sector risks affecting national security and resilience** and produce a written report to the President within 18 months recommending executive-level, cross-sector action.

Recommendation 2: Identify or develop regional, public-private, cross-sector partnerships, led by senior executives.

2.1 The Secretary of Homeland Security should work directly with governors, mayors, local government, and senior executives from the lifeline sectors to **facilitate the development of sustainable cross-sector partnerships within selected regions**, with the objective of improving the region's resilience to very large-scale events that could impact national security, resilience, and economic stability.

2.2 The Secretary of Homeland Security should **initiate a pilot program with state and local governments in select regions to conduct regional joint exercises**, develop risk maps of critical sector interdependencies, and extract lessons learned on regional needs and gaps for government and sector partners.

Recommendation 3. The President should designate energy, communications, water, and transportation as lifeline sectors.

3.1 DHS should **examine how the Federal Government, state governments, and regional entities currently coordinate action** and provide support to the lifeline sectors in event response.

3.2 The Federal Emergency Management Agency (FEMA) National Response Coordination Center, Federal agencies, and state and local governments should modify their processes and plans for emergency operations to **include the co-location of representatives of lifeline sectors in their emergency operation centers during major disasters**.

3.3 The President should **require that Federal agencies: a) explicitly consider and address the differences among regions when promulgating security and resilience rules, programs, or guidance**; and b) expressly state how they have customized implementation to each region if there is not generic applicability.

Recommendation 4. Integrate social media into public alert and warning systems and develop social media training and information sharing capabilities.

4.1 FEMA and the FCC should **convene a task force to examine how new and emerging social media apps, platforms, and capabilities can be used** to support emergency notification and response.

4.2 FEMA, the FCC, and social media providers should **integrate social media platforms into FEMA's Integrated Public Alert and Warning System (IPAWS)**.

4.3 FEMA non-disaster preparedness funding to SLTT emergency management agencies should **require recipients to designate personnel through the IPAWS system to issue targeted emergency alerts**.

4.4 FEMA and DHS S&T should work through the SLTTGCC to **develop a conference or webinar series on innovative social media use and best practices in state and local emergency management** including examining social media successes in recent large-scale disasters.

Recommendation 5: Launch a cross-agency team to develop solutions to site access, waiver, and permit barriers during disaster response.

5.1 DHS's Office of Infrastructure Protection (IP) and FEMA should collaborate with SLTT governments and owners and operators to **develop a commonly applied process or system to credential lifeline sector owners and operators** and grant them access to disaster areas.

5.2 DHS should work with SLTT governments and owners and operators to **catalog the waivers and permits commonly required during various disaster scenarios and develop a streamlined process for rapidly issuing those permits** and waivers at the Federal, state, and local level.

5.3 DHS should work with lifeline sector regulators **to identify actions that will expedite waivers and remove impediments to fleet movement**, including driver-hour limitations, road and weight restriction, port access restrictions, and toll crossing processes.

Recommendation 6. Create the value proposition for investment in resilient lifeline infrastructures and adoption of innovative technologies.

6.1 Within one year, the Department of Energy should **complete a pilot analysis of the value proposition for investment in grid modernization** and recommend any approaches that encourage long-term investment to modernize lifeline infrastructures. **All lifeline sector SSAs should then work with their sector partners to establish the value proposition for investment in critical sectors**.

6.2 The President should direct the National Oceanic and Atmospheric Administration (NOAA) and appropriate Federal agencies to **examine existing weather and climate forecasting models to ensure they provide the best available prediction of severe weather events** to enable private, state, and local partners to make informed investment decisions that manage risk.

6.3 DHS should work through Federal research organizations, academic institutions, and the national laboratories to develop Applied Centers of Excellence for Infrastructure Resilience **to provide an operating environment to test and validate innovative technologies and processes that build resilience into new large-scale infrastructure projects**.

Questions/Deliberation

Executive Engagement in the Electricity Sector

Principles of Successful Public-Private Partnerships

1. Executive engagement
2. Trusted relationships
3. Simple process
4. Value proposition
5. Trusted executive facilitator

Why Executive-Level Engagement?

- CEOs have the authority to:
  1. Set strategy and direction
  2. Establish priorities and importance of the topic down the management line
  3. Provide resources (people, money, time)
  4. Exercise accountability through follow-up
- CEOs have a "fiduciary duty" to their stockholders to manage the "risks" that could impact the success of the business.

Electricity Sector Executive Engagement: Catalyst

- NIAC report of 2010 energized CEOs
- CEO wrote to POTUS to request engagement
- Principles of successful public-private partnerships become mantra:
  1. Executive engagement
  2. Trusted relationships
  3. Simple process
  4. Value proposition
  5. Trusted facilitator/executive champion
- Building a successful track record of executive engagement
  - Kaleidoscope

Building Trusted Relationships

- July 2012: CEOs met with Secretaries of DOE and DHS to explore partnership.
- Sept 2012: Gov't provides first-ever cleared briefing for 70+ industry CEOs on threat environment.
- Oct 2012: Critical CEO coordination in Superstorm Sandy
- Jan 2013: Key industry CEOs meet with Secretaries of DHS and DOE and White House staff
- 28 CEOs form Joint Electric Executive Committee; engaged COOs and CIOs to form Executive Working Group focused on tactical deliverables
- Executive facilitator (w/ high level clearance) gathered executive-level industry input to federal entities on tools and technologies, information sharing, and event response capabilities and plans – facilitated partnership dialogue

Clear and Tangible Progress

- May 2013: Second meeting of CEOs, White House, and DOE/DHS Deputy Secretaries
  - Transitioned to Electricity Sub-sector Coordinating Committee led by a 9-member steering committee
  - Several Executive Working Groups of COOs and CIOs met over coming months with Assistant Secretaries
- "Poison Apple" cyber security tabletop exercise involved CEO participation

Results: Actions to Reduce Risk

- Sept. 2013: Third significant meeting of CEOs, White House, DOE/DHS Deputy Secretaries with hard commitments set
- Based on trusted relationships with cleared industry executives, CEOs reduce risk by deploying hardware and software.

Results: GridEx II

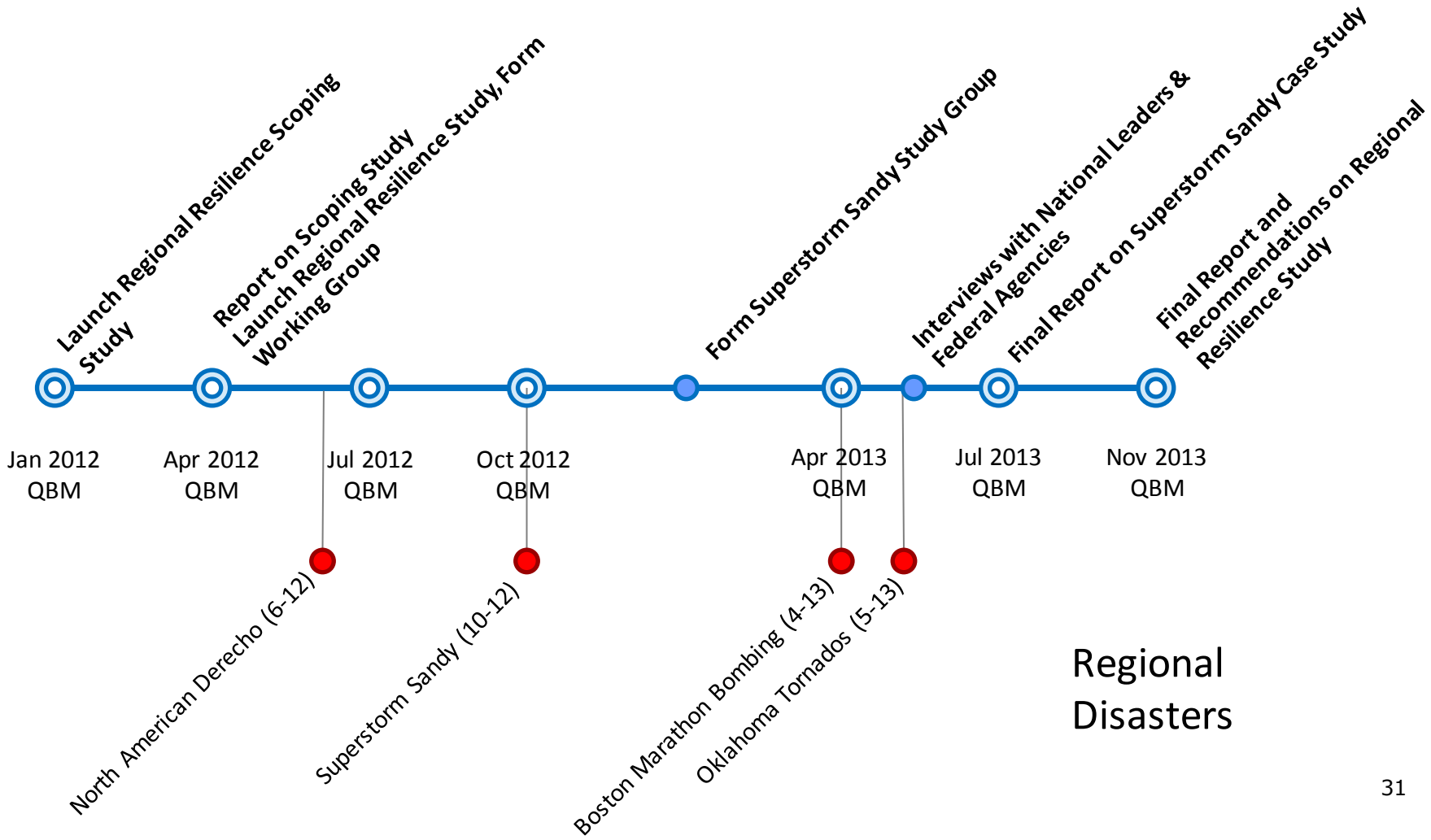
- Nov. 13-14, 2013: 200 venues with more than 1,800 participants exercised cyber and physical attacks to the grid
- 31 key "executive players" from industry and government, including CEOs and the Deputy Secretaries of DOE and DHS, White House, NorthCom, and others as the grid was subjected to a "catastrophic cyber failure."

Key Outcomes of Electricity Executive Engagement

- Understanding of vulnerabilities that builds shared public-private value proposition
  - Industry is not responsible for national security, but has a fiduciary responsibility to protect assets and business for shareholders.
- Improved industry understanding of the reality of the threat environment.
- *Actual* risk reduction through:
  - Development and exercising of response plans to identify gaps that will reduce vulnerability when addressed.

Supporting Material

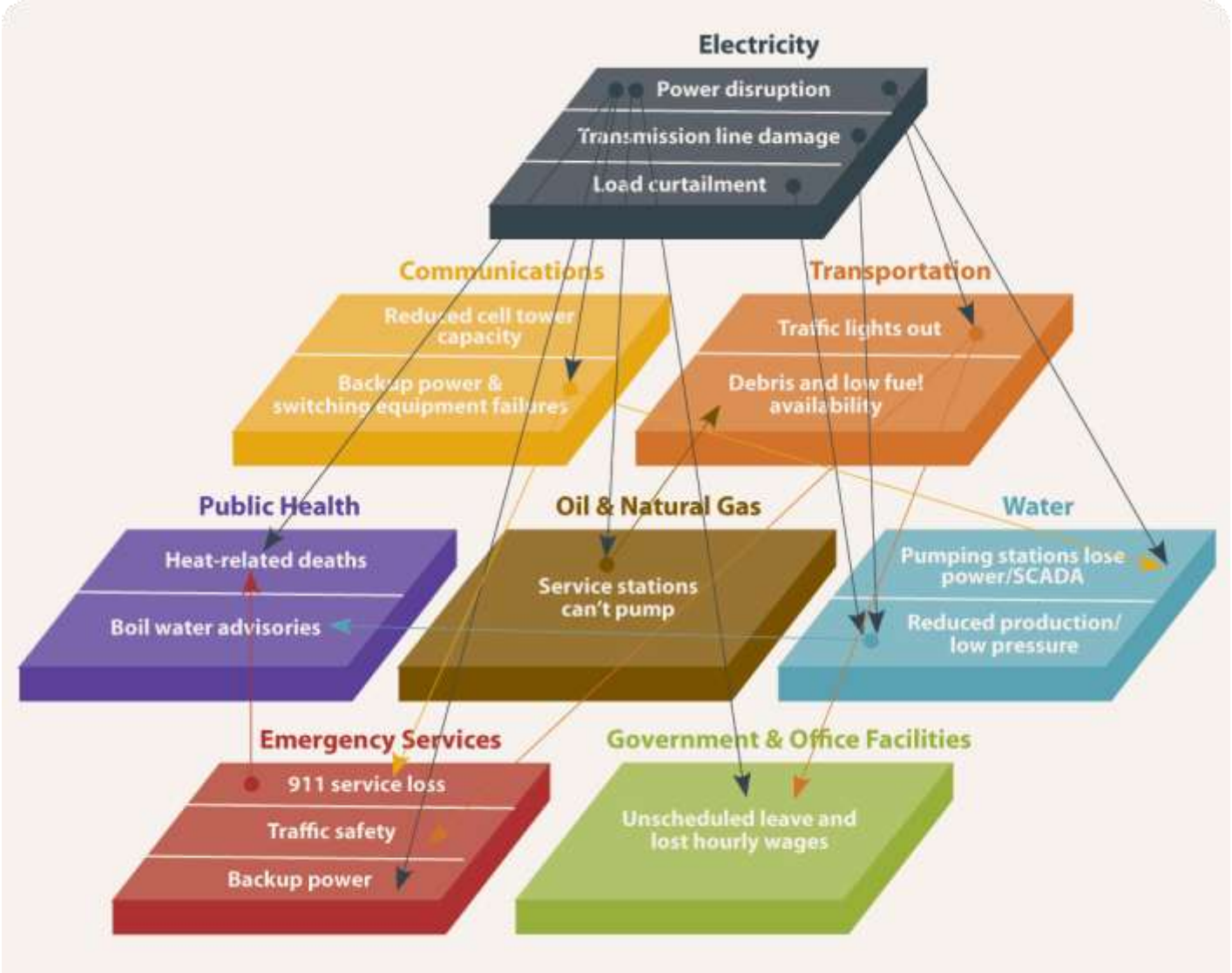
Study Process and Timeline



Defining Features of a Lifeline Sector

- **Provides essential products and services** that underpin the continued operation of nearly every business sector, community, and government agency.
- Typically delivers products and services that are ubiquitous in normal circumstances but **can create life-threatening conditions if they are unavailable** for long or even short periods of time.
- **Encompasses complex physical and cyber networks that are highly interconnected** within their sector, between sectors, and within and between adjacent regions.
- Its disruption or destruction **can cause failures that cascade across dependent infrastructures and regions**, producing a multiplier effect of impacts.
- Distinct from "life support" sectors such as Emergency Services

Cascading Impacts of June 2012 North American Derecho



Finding 1. Lifeline sectors are top priorities for achieving regional resilience and their growing complexity creates hidden risks

- **Maintaining the continuity of services of the energy, water, transportation, and communications** sectors is paramount to regional resilience.
- **Increasing interdependence creates hidden regional risks** that are not widely understood by businesses, governments, and communities.
- **Joint regional exercises that engage public and private partners at all levels** are highly effective in exposing gaps, identifying interdependencies, and improving response capabilities.

Finding 2. Regional resilience efforts are most successful when they are tailored to the characteristics and needs of each region.

- **All regions are different, requiring a tailored approach** to resilience that reconciles the types and density of a region's infrastructure with regional-based risk assessments.
- A community's capacity to withstand a disaster is improved when regional emergency managers **engage non-profit and community groups as critical partners** in disaster preparation, response, and recovery.

Finding 3. Senior executive engagement creates strong public-private partnership—the best strategy for achieving long-term resilience in regions.

- **Public-private partnerships based on senior executive-level engagement are the most robust** because they enable partners to set strategic direction, establish priorities, provide resources, and exercise accountability.
- **Strong public-private partnerships across all levels** of industry and government are a defining characteristic of resilient regions.

Finding 4. Social media has emerged as a powerful but underutilized tool for communicating and collecting data during emergencies.

- **Social media can improve situational awareness, inform public decision-making**, mitigate rumors, and enable emergency managers to collect a new stream of real-time information.
- **Government and businesses** are just learning how to effectively use these tools and **have not fully capitalized on their potential** in disaster response and recovery.

Finding 5. Rapid recovery of lifeline infrastructures is hindered by complex rules, regulations, and processes.

- Incident response personnel in critical sectors encounter **persistent problems gaining rapid access to disaster areas to repair damaged assets**.
- **Complex laws and regulations at the Federal, state, and local level** prevent the most effective and logical disaster response and impede interstate fleet movement of mutual aid repair crews in the lifeline sectors.

Finding 6. Without a strong value proposition, owners and operators are unable to invest in new and innovative infrastructure that can mitigate risks.

- **Investment in resilient infrastructure is difficult** without public support and the ability to recoup costs.
- **Regions can mitigate long-term risks by building resilience into new or upgraded structures**, and using novel infrastructure designs that are inherently resilient.

Implementing Executive Order 13636 and Presidential Policy Directive 21

Status Update Briefing For
National Infrastructure Advisory Council

November 21, 2013

Robert Kolasky, Director
EO-PPD Integrated Task Force

Homeland Security

Announcement of the EO and PPD

President Obama announced new policies on cybersecurity and critical infrastructure security and resilience in February, 2013:

Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

Presidential Policy Directive - 21:
Critical Infrastructure Security and Resilience

- Together, create an opportunity to effect a comprehensive national approach to cyber and physical security and resilience
- Implementation efforts designed to drive action toward ***system*** **and** ***network*** security and resiliency

EO-PPD Deliverables

120 days – **June 12, 2013**

- Publish instructions: unclassified threat information
- Report on cybersecurity incentives
- Publish procedures: expand the Enhanced Cybersecurity Services

150 Days - **July 12, 2013**

- Identify cyber-dependent critical infrastructure
- Evaluate public-private partnership models
- Expedite security clearances for private sector

240 Days – **November 8, 2013**

- Develop a situational awareness capability
- Publish a successor to the National Infrastructure Protection Plan
- Publish draft voluntary Cybersecurity Framework

365 days – **February 12, 2014**

- Report on privacy and civil rights and civil liberties cybersecurity enhancement risks
- Stand up voluntary program based on finalized Cybersecurity Framework

Beyond 365 - **TBD**

- Critical Infrastructure Security and Resilience R&D Plan

NIPP 2013: *PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE* DEVELOPMENT

Guiding Principles

Through partnerships, infrastructure is made more secure and resilient

Build on the successful work to date and leverage existing knowledge and structures wherever possible

Describe the conditions that necessitate an updated approach to critical infrastructure security and resilience

Lay out the broad principles and policies that underpin this approach in the public and private sectors

Describe the national program that will implement these principles and policies to achieve shared outcomes

Goals of National Effort

- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation, as well as effective responses to both save lives and ensure the rapid recovery of essential services;
- Efficiently share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
- Promote learning and adaptation during and after exercises and incidents.

NIPP 2013 *Partnering for Critical Infrastructure Security and Resilience*

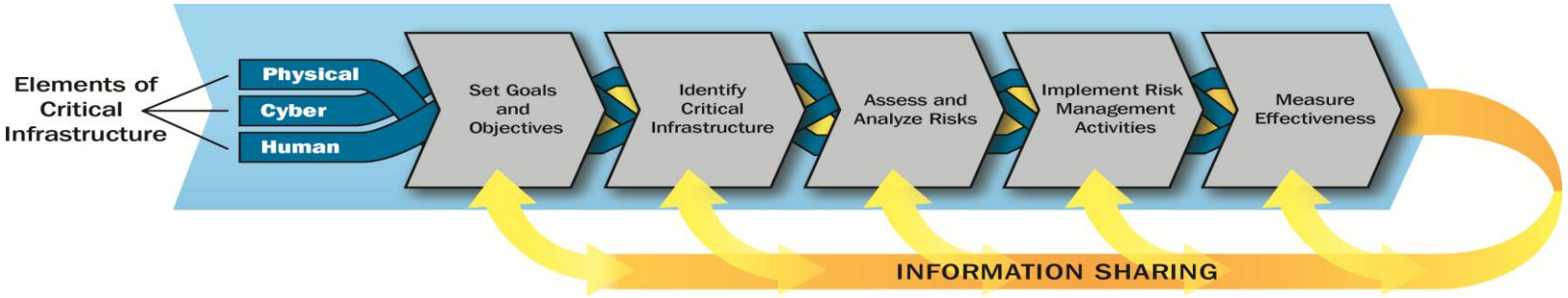
Contents

- Vision, Mission, Goals
- Critical Infrastructure Environment
  - Risk
  - Policy
  - Operational
  - Partnerships
- Core Tenets
- Collaborating to Manage Risk
- Call to Action
  - Build upon Partnership Efforts
  - Innovate in Managing Risk
  - Focus on Outcomes
- Acronyms, Glossary & Appendices

Homeland Security

Evolution from 2009 NIPP

- Recognize the change in the strategic environment
  - Risk landscape
  - Infrastructure operations
  - Policy changes
- More strategic and flexible document
- Focus on actions and implementation
- Retains a focus on risk management as the foundation of national CI security and resilience; makes enhancements to framework
- More closely integrates *information-sharing* as an essential element of the risk management framework



Changes and Evolution cont.

- Elevates security and resilience
- Aligns critical infrastructure risk management efforts with the National Preparedness System
- Focuses on national priorities jointly determined by public and private sectors
- Integrates cyber and physical security and resilience
- Continues progress to support execution of at both the national and community levels
- Affirms the value of international collaboration
- Incorporates practical lessons learned
- Is mindful of the perspectives of different partners
- Includes a detailed Call to Action

THE CYBERSECURITY FRAMEWORK

Cybersecurity Framework Requirements

- Incorporate voluntary consensus standards and industry best practice
- Possess the following characteristics:
  - Cross sector
  - Flexible
  - Repeatable
  - Performance-based
  - Cost effective
- Be cognizant of need for business confidentiality and individual privacy and civil liberties
- Be developed with awareness of the threat and vulnerability landscape to the Nation's cyber systems

Cybersecurity Framework Overview

- Developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk
- Supports the improvement of cybersecurity for the Nation's Critical Infrastructure using industry-known standards and best practices
- Provides a common language and mechanism for organizations to:
  1. Describe current cybersecurity posture;
  2. Describe their target state for cybersecurity;
  3. Identify and prioritize opportunities for improvement within the context of risk management;
  4. Assess progress toward the target state;
  5. Foster communications among internal and external stakeholders.
- Composed of three parts: the **Framework Core**, the **Framework Implementation Tiers**, and **Framework Profiles**

Framework Implementation Overview

An adopting organization would use the elements of the **Framework Core** as part of its risk management approach leveraging two additional Framework concepts:

Framework Implementation Tiers

- Demonstrate the implementation of the Framework functions and categories, and indicate how cybersecurity risk is managed.
- These Tiers range from Partial (Tier 0) to Adaptive (Tier 3), with each Tier building on the previous Tier.

Framework Profiles

- Conveys how an organization manages cybersecurity risk in each of the Framework functions and categories by identifying the subcategories that are implemented or planned for implementation.
- Profiles also can be used to identify the appropriate goals for an organization or for a critical infrastructure sector and to assess progress against meeting those goals.

Promoting Framework Implementation

- National Performance Goals
  - Promote consideration of cybersecurity investment as a strategic decision
  - Developed in collaboration with critical infrastructure partners
- Establish a Voluntary Program
  - Leverage existing cybersecurity initiatives
  - Provide a touch point for organizations interested in Framework adoption
- Incentives
  - EO-PPD conducted study and analysis
  - Administration is consideration options
  - Proposals would help to minimize the costs of, or maximize the benefits associated with, Framework adoption

Performance Goals

National Goals

1. Critical systems and functions are identified and prioritized and cyber risk is understood as part of a risk management plan.
2. Risk-informed actions are taken to protect critical systems and functions.
3. Adverse cyber activities are detected and situational awareness of threats is maintained.
4. Resources are coordinated and applied to triage and respond to cyber events and incidents in order to minimize impacts to critical systems and functions.
5. Following a cyber incident, impacted critical systems and functions are reconstituted based on prior planning and informed by situational awareness.
6. Security and resilience are continually improved based on lessons learned consistent with risk management planning.

Cybersecurity Incentives

Eight Recommended Areas for Further Analysis:

1. Cybersecurity Insurance
2. Grants
3. Process Preference
4. Liability Limitation
5. Streamline Regulations
6. Public Recognition
7. Rate Recovery for Price Regulated Industries
8. Cybersecurity Research

"While these reports do not yet represent a final Administration policy, they do offer an initial examination of how the critical infrastructure community could be incentivized to adopt the Cybersecurity Framework as envisioned in the Executive Order. We will be making more information on these efforts available as the Framework and Program are completed."

Michael Daniel,
Special Assistant to the President and Cybersecurity Coordinator
White House Blog
August 6, 2013

Homeland Security

Voluntary Program

DHS will establish a *"Voluntary Program"* to:

- Provide critical infrastructure owners and operators with a centralized resource to access guidance on Framework adoption;
- Identify DHS and government-wide assistance around other cybersecurity risk management activities;
- Share best practices with sector and cross-sector partners.

Specifically the program will:

- Serve as a link and customer relationship manager between stakeholders and government programs to implement the Cybersecurity Framework, and provide cybersecurity resources;
- Identify and advocate for mechanisms that promote Cybersecurity Framework adoption;
- Promote understanding of the impact of the Framework via risk management.

Homeland Security

National Infrastructure Advisory Council (NIAC)

Executive Order-Presidential Policy Directive Working Group (EO-PPD WG)

November 21, 2013

David E. Kepler
Executive Vice President/ Chief Sustainability Officer, Chief Information Officer
The Dow Chemical Company
Co-Chair

Philip Heasley
President and CEO
ACI Worldwide
Co-Chair

Agenda

- Study Overview
- General Observations
- Findings
- Recommendations
- Next Steps

Study Overview

Working Group Members

WG Member	Sector Experience
David Kepler, *Chief Sustainability Officer, Chief Information Officer, The Dow Chemical Co.* (Co-Chair)	Chemical
Philip Heasley, *President and CEO, ACI Worldwide* (Co-Chair)	Financial Services
Constance H. Lau, *President and Chief Executive Officer, Hawaiian Electric Industries, Inc. (HEI)*	Electricity, Financial Services
Glenn S. Gerstell, *Managing Partner, Milbank, Tweed, Hadley, & McCloy LLP*	Water, Telecommunications
Michael J. Wallace, *Senior Advisor and Director, Nuclear Energy Program, Center for Strategic and International Studies, Former Vice Chairman and COO, Constellation Energy*	Electricity, Nuclear

Background

Background

Incentives for Adopting the Cybersecurity Framework

- Successful implementation of the voluntary cybersecurity framework is reliant on widespread buy-in from private sector owners and operators, and incentives are a key component of generating interest and participation.
- The Administration offered several potential incentives that could assist in encouraging adoption of the voluntary cybersecurity framework.
  - The NIAC was asked to review these options, determine the relative value and the likelihood of adoption of each incentive, and to suggest any additional incentives that would encourage greater participation.

Background, continued

Information Sharing

- The NIAC was asked to consider information sharing, and the successes and challenges of the current public-private information sharing environment.
- Issues under consideration included obstacles to effective information sharing; incentives to encourage increased sharing; effective mechanisms; the differences between physical and cyber information sharing; principles to encourage voluntary participation; the core principles for cyber information sharing; and the appropriate metrics for the sharing of cyber threat information.

Background, continued

Cybersecurity Framework

- In reviewing elements of the proposed cybersecurity framework, the NIAC was asked to determine the aspects of the framework most likely to benefit private sector owners and operators.
- Issues under consideration included the elements that would facilitate widest adoption by owners and operators; efficient and effective processes to facilitate adoption; how to best measure participation in and the value of the framework; obstacles preventing adoption, particularly for non-Fortune 500 companies; which audiences to target; and any issues that require the alignment of Federal agencies with other levels of government.

Background, continued

NIPP revision

- As part of PPD-21, DHS is revising and updating the National Infrastructure Protection Plan.
- The NIAC was asked to review drafts of the revised documents, and offer comments on concepts including how the Federal Government can provide a clear, concise, flexible, and adaptable plan; what should be included to make the plan valuable to owners and operators; how to include a focus on critical functions and services, while maintaining appropriate and relevant risk-based momentum; and determining the forms of support that will allow the wider owner-operator community to benefit from the plan.

Findings

Key Findings – Cybersecurity Framework Adoption

1. The key factor to encourage adoption by the private sector of the Cybersecurity Framework is **creating confidence that it is effective in securing the nation from cybersecurity threats.**
2. The incentives most likely to encourage confidence and participation of critical infrastructure owners and operators are **an effective framework, good-faith protection of shared information, streamlining of regulations, and outcome-based metrics.**
3. Focus on Purpose - **Implementation will be better served by focusing on the Critical Purpose and related outcomes**, such as goals and metrics, that allow the private sector to continue to implement effective cybersecurity systems, while expanding the public-private partnership.

Key Findings – Information Sharing

4. **Creation of a Safe Harbor - with limited antitrust protection —ensures information is used for intended purposes only, and offers protection from liability** when acting in good faith will encourage participation in the Information Sharing program.
5. Information - **The opportunity to receive timely, actionable information is the most significant incentive** in encouraging companies to participate in the information sharing program.
6. Classification of Information - **Over-classification of information is a significant barrier to effective information sharing programs.**

Key Findings – Information Sharing, continued

7. Intended Use - The private sector is concerned that **the sharing of some forms of information could lead to governmental inquiries and regulation beyond the original purpose** for which the information was offered.
8. Information for Critical Purpose - As stated in the National Infrastructure Protection Plan, **information sharing is a means to an end, not an end itself.**

Key Findings – Cybersecurity Framework

9. **Metrics and milestones that measure outcomes will be key to the success of the cybersecurity framework**.
10. Evergreen Process - **An ongoing effort will be required in order to gain the most value from the cybersecurity framework**.

Key Findings – NIPP Revision

11. Collaboration - **The emphasis on promoting collaboration between governments and the private sector in development of the NIPP is particularly likely to increase the plan's chances of success**.
12. Risk Prioritization - **A risk management methodology is the right approach for determining the capabilities needed** to enhance infrastructure security and resilience.
13. Centralized Ownership - **Housing of the Security Framework within an educational institution can help further develop the framework** and promote the benefits of private sector adoption.

Recommendations

Recommendations – Cybersecurity Framework Adoption

1. Limit liability on damages resulting from cybersecurity events.
   - Liability limits are an effective incentive to drive adoption of the cybersecurity framework by industry.
   - However, the Council cautions against the creation of an environment where insurance underwriters are dictating security policies.
   - Transferring risk to insurance companies does little to bolster security.

Recommendations – Cybersecurity Framework Adoption

2. Use the Government's procurement power to encourage information technology suppliers to develop cybersecurity framework-compliant hardware and software.
   - Government procurement practices have numerous indirect benefits for the larger critical infrastructure community.
   - It incentivizes suppliers to enhance the security of their products and services, which are often the same products and services used throughout the critical infrastructure security and resilience (CISR) community.
   - Improvements to those systems and reducing the risk associated with hardware and software gaps also allow owners and operators to redirect their attention to other critical security concerns.

Recommendations – Cybersecurity Framework Adoption

3. The Government should ensure the availability of qualified, vetted security professionals.
   - New areas of compliance require additional professionals to ensure compliance, and qualified personnel can be challenging to find.
   - Federal assistance with background checks and leveraging of existing programs could establish a greater reserve of qualified professionals.

Recommendations – Cybersecurity Framework Adoption

4. Grants, if used, should be focused on capacity building.
   - Direct Federal funding for investment should encourage adoption of the framework, through training, implementation, and more robust IT products, especially for small- to medium-sized operators.
   - Any contingencies placed on grants must be outcome-based and clearly articulated.
   - Penalties for low success should not exceed the value of the grant.

Recommendations – Cybersecurity Framework Adoption

5. "Metrics for Measuring of Efficacy of Critical Infrastructure Centric Cybersecurity Information Sharing Efforts," by Fleming/Goldstein 2012, should be leveraged in creating outcome metrics that can be used to measure the success of the EO and PPD implementation, including metrics such as indicators shared, attacks prevented, attackers caught, and risk mitigated.
6. The cybersecurity framework should be housed at a university, with base funding coming from critical infrastructure companies.

Recommendations – Engagement of small- and mid-sized owner/operators

7. The Federal Government should put forward additional effort to assist small- to mid-sized owners and operators in meeting the critical purpose outlined in EO 13636, in order to ensure reliable functioning of the Nation's critical infrastructure in the face of cyber threats, including:
   - Government-funded programs at universities to develop training to understand and best leverage the cybersecurity framework.
   - Government encouragement of IT providers and suppliers to create products that have security as a primary design criteria.

Recommendations – Engagement of small- and mid-sized owner/operators

- Government-developed training to assist small- and medium-sized owners and operators who lack resources or expertise.
- Centralized ownership of the Security Framework within an educational institution to further develop the framework and promote the benefits of private sector adoption.
  - Successful examples of this type of development within the education sector can be found within Carnegie Mellon's Software Engineering Institute - Community Emergency Response Team (CERT) program.

Recommendations – Information Sharing

8. The Federal Government should adopt a policy that specifically addresses concerns that information sharing could lead to governmental inquiries and regulation beyond the original purpose for which the information was offered.

Recommendations – NIPP Revision

- Security should be designed to be built in to systems, rather than layered on top of systems.
- The Government should leverage its purchasing power to incentivize enhanced security and resilience in core cybersecurity systems and programs (Information Technology, Industrial Automation, and Telecommunications sectors).
- The Framework should include standards that address the risk management of Industrial Automation systems, which have unique control characteristics apart from general cybersecurity. Industrial Automation may warrant its own sector category.

Recommendations – NIPP Revision, continued

- The Government should develop policies and apply resources to pursue and discourage global cyber criminals from attacking critical infrastructure facilities.
- The revised NIPP should include a summary specifically written for executives, in order to improve the understanding of the CISR mission.
- The Government should convene a public-private advisory panel under CIPAC to ensure that the needs of the private sector are addressed in the implementation of the revised NIPP.

Questions?