National Infrastructure Advisory Council

Critical Infrastructure Security and Resilience National Research and Development Plan

Final Report and Recommendations

November 14, 2014

David Grain
Working Group Chair
Founder and Managing Partner
Grain Management, LLC

About the National Infrastructure Advisory Council

The National Infrastructure Advisory Council (NIAC) advises the President of the United States through the Secretary of Homeland Security on issues related to the security and resilience of the Nation's critical infrastructure sectors and their functional systems, physical assets, and cyber networks for the 16 critical infrastructure sectors. These critical infrastructure sectors span the U.S. economy and include the chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems sectors. The National Infrastructure Advisory Council also advises the lead Federal agencies that have critical infrastructure responsibilities. Specifically, the Council has been charged with making recommendations to:

- Enhance the partnership between the public and private sectors in securing and enhancing the security and resilience of critical infrastructure and their functional systems, physical assets and cyber networks, and providing reports on this issue to the President through the Secretary of Homeland Security, as appropriate;
- Propose and develop ways to encourage private industry to perform periodic risk assessments and implement risk reduction programs;
- Monitor the development and operations of critical infrastructure sector coordinating councils and their information sharing mechanisms and provide recommendations to the President through the Secretary of Homeland Security on how these organizations can best foster improved cooperation among the sectors, the Department of Homeland Security (DHS), and other Federal Government entities;
- Report to the President through the Secretary of Homeland Security who shall ensure appropriate coordination with the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for Economic Policy, and the Assistant to the President for National Security Affairs; and,
- Advise sector specific agencies with critical infrastructure responsibilities, to include issues pertaining to sector and government coordinating councils and their information sharing mechanisms.

Table of Contents

Executive Summary

Critical infrastructure protection/security and resilience has been a national mission for more than a decade. While intensive study of both theoretical and real-life events has led to improvements in many aspects of the mission, some lessons – such as those on interdependencies and dependencies, and coordinating activities across sector operations – have been repeatedly re-learned.

Increasing complexity is at the center of two major challenges: reliable operations and the mitigation of threat vectors. Rapid changes in technology and its use, operational dependencies on other sectors, and uncertainties in the world's natural and political environment have geometrically increased the complexity of operations. In addition, there is a sense of urgency and concern for the growing fragility of lifeline systems in the face of growing number of catastrophic natural events, and growing human-originated cyber and physical threats targeting them. The expanding range of threats adds to the complexity of making informed decisions that meaningfully reduce risk within an environment where resources are subject to multiple demands and priorities.

In February, 2013, President Obama issued Presidential Policy Directive 21 (PPD-21). The Directive required the Federal Government to develop a national plan to address critical infrastructure security and resilience research and development. This plan would identify priorities, as well as provide research and development requirements and guide investments. On September 5, 2014, the National Infrastructure Advisory Council was tasked by the National Security Council on behalf of the President to provide perspectives and recommendations on the development of this national research and development plan.

Findings

As findings, the Council identified six national strategic drivers that represent cross-sector challenges, critical needs and threats. In turn, the Council identified two categories of nationally significant required capabilities across the sectors to effectively address the strategic drivers. Full descriptions of these findings are provided in Chapter 2.

National Strategic Driver Findings

Finding 1: Overcoming Obstacles to Action: Policy, Regulatory and Structural Barriers

Current regulatory frameworks and national policy are often not harmonized, and do not encourage resilience against the broader geographic impact of catastrophes nor the growing operational complexity and dependencies of the critical infrastructures.

Finding 2: Dependency on and interconnectedness through cyber systems

Operations-critical systems in every sector are increasingly connected to networks, which is further expanding the range and forms of vulnerability that threaten sustainability of critical infrastructure operations.

Finding 3: Aging infrastructure and the effects of catastrophic natural disasters

Most of the lifeline sectors are in need of substantial efforts to address the concerns of aging infrastructure. The fragility of vital infrastructure carries substantial consequences when such systems are stressed by major natural disasters, which are forecasted to become both more frequent and more severe.

Finding 4: Evolving terrorist and other man-made physical threats

The terrorist threat remains a primary strategic driver, and it has evolved over the past few years. Where malicious threats were once contained primarily to a single terrorist organization, today's man-made threat landscape has become much more diffuse, and much less easy to predict.

Finding 5: Growing complexity and consequences of cross-sector dependencies, subject to a growing range of threats

Every critical infrastructure sector relies on one or more of the lifeline sectors to maintain functionality. But that reliance upon those sectors is also true of each of the lifeline sectors themselves. As a result, consequences can cascade across the country rather than being confined within a region.

Finding 6: Workforce changes, evolution and requirements

With increasing numbers of the most experienced members of the critical infrastructure operations workforce approaching or reaching retirement age, there will soon be a shortage of qualified personnel with an understanding of key specialty operations – and therefore a need for comprehensive effective workforce development strategies. The nation is already experiencing a shortage in a workforce that has the cyber security skills integrated with operations expertise necessary to secure and assure resilience of cyber dependent critical infrastructure operations, a shortage which continues to expand.

Required Cross-Sector Capabilities of National Significance

As findings, the Council identified two categories of required national critical infrastructure capabilities to advance critical infrastructure and security and resilience:

- Eliminating or reducing obstacles to action and to facilitate decisions to make investments;
- Improving the effectiveness and cost-efficiency of implementation and operations of security and resilience programs.

The required capabilities in order of priority are:

Finding 7: Approaches to overcome obstacles to actions

7.1. *Enabling and aligned regulations and policy*

A common theme from the information collected by the Council was the need for enabling policies, structures and regulations that will support action, both to execute programs and to make investment decisions.

7.2. *Appropriate market incentives for mission-critical investments*

While there have been countless lessons learned and after-action reports created following disruptive events and natural disasters, a substantial number of those lessons have not been acted upon. A key part of motivating action must be based around capabilities that incent action by owners and operators, either by mitigating either expenses or liabilities for implementation, and that make long-term investments in resilience an effective use of resources.

7.3. *Reduced barriers to cross sector and public-private collaboration*

Interdependencies, dependencies, and interconnectedness have become a core element of operations in a world driven by cost efficiencies, just-in-time service, and automation dependent customer service. Current research appears to show that the barrier of "stove-piping" must be overcome.

Finding 8: Required significant cross-sector capabilities to support security and resilience programs implementation and their operations

8.1. *Strengthened cybersecurity capabilities*

- Real-time identification and authentication of people, software and systems –
- Increased efficiency and real-time security analysis and data collection
- Integration of cyber security risks with other business risks for decision makers –
- Better understanding of human behavior and motivation
- Control system and sensor device security

8.2. *Understanding and management of cross sector dependencies and cascading effects*

The ways in which the operations of one system affect another have been an ongoing area of study. Owners and operators require a much better understanding and ability to plan with assurance that investments are rationalized and effective. Without this understanding, both the owners and operators and the public accept the risks.

8.3. *Built-in resilience in design and operations*

- Reduction in implementation costs
- Reduction of day-to-day disruptions to public and business operations
- Accelerated implementation

8.4. *Efficient and cost-effective workforce development*

- Cyber-savvy workforce as well as cyber experts
- Lifeline sector operations expertise

8.5. *Effective and actionable contingency and preparedness planning*

Even the most secure and resilient systems can fail, as no approach to preventing man-made threats is foolproof, and natural disasters will continue to occur.

Priority Research and Development Recommendations

To support the implementation of these capabilities, the Council recommends four **priority areas of research and development**. Each is described in greater detail in Chapter 2.

Recommendation 1: Address role and impact of regulation, public policy, and consolidation within sectors on resilience and innovation

1.1. Research and analyze the labyrinth of regulations and policies across all levels of government that impedes and dis-incent investments in security and resilience.
1.2. Identify essential elements of enabling policies and regulations that would encourage and facilitate owner and operator investment and gain public acceptance of such investments.
1.3. Determine the role of policies, regulation and consolidation within industries and its impact on resilience, security, innovation and resilience.

Recommendation 2: Identify and apply best practices

2.1. Identify and establish the elements for business and public justification for investments from lessons learned.
2.2. Develop an effective model of shared industry funding.
2.3. Determine design standards and best practices for the replacement, upgrading, and maintenance of critical infrastructure systems.
2.4. Identify innovative, cost efficient and accelerated approaches to develop a skilled workforce.
2.5. Determine factors and approaches to accelerate recovery following a disaster.
2.6. Establish resilience metrics.

Recommendation 3: Advance management of cyber risks

3.1. Develop real-time cybersecurity risk analysis and management tools.
3.2. Establish new architectures to "bake in" self-healing and self-protected cyber systems.
3.3. Develop automated security analysis and data collection tools and methods.
3.4. Understand cross-sector connections that could cause cascading effects.
3.5. Measure the effectiveness of security.

Recommendation 4: Develop and integrate modeling and simulation tools

4.1. Scale risk assessment and management decision support tools for local communities and individual institutions.
4.2. Develop, scale and integrate interdependency and consequence modeling, and simulations to support operational decisions to predict and prevent cascading failures.
4.3. Continue research and development for managing "big data".

The Council makes the following three part recommendations for **the timeline for action** for research and development. Each is described in greater detail in Chapter 3.

Recommendation 5: Timeline Recommendation

5.1. *Within 18 to 24 months, the Federal Government should develop and implement programs and initiatives addressing issues that have been substantially researched, and constitute simple, demonstrable gains that can be made quickly.*

5.2. *Within 5 years, complete comprehensive research on incentives, motivation and structures to facilitate action. The Council also recommends focusing on the identification and sharing of best practices within the next 5 years, as an efficient means of making available proven and illustrative methodologies and practices.*

5.3. *Beyond 2020, continue to invest in research as required in all areas, but to focus on development of integrated scalable tools, methodologies and practices.*

Public-Private Partnership Recommendations

The Council recommends two areas for **improvement in public-private partnerships to support research and development initiatives**. Each recommendation is described in greater detail in Chapter 4.

Recommendation 6: Greater leveraging of academic institutions, as neutral forums, to seat public-private partnerships to research and develop solutions identified in this report.

Recommendation 7: Identify meaningful metrics for effective public-private partnerships to justify their establishment and sustainability.

Next Step Recommendations

For a research and development agenda, which tends to be long term, the Council believes that effective results oriented first steps can be motivators for sustained interest and support by the community of stakeholders. Consequently, it makes the following recommendations for **next steps** to enhance the possibility of success of the national plan:

Recommendation 8: Upon the issuance of the National Plan, the President should immediately convene key representatives from the critical infrastructure sectors, subject matter experts from academic and research institutions, and all levels of government to identify key success elements for sustainable implementation of the plan.

Recommendation 9: Upon issuance of the National Plan, the Secretary of Homeland Security should convene a forum of research institutions, key critical infrastructure sector representatives and key agencies at Federal, State and local governments to develop a path forward to identify and document disincentives and potential enabling policies/regulations. The Council also recommends the sharing of such information across the sectors, and all levels of government.

Conclusion

This report underscores important realities that need to be addressed to advance critical infrastructure security and resilience:

- The world in which the critical infrastructures operate has become more operationally complex, with dependencies that are often not recognized.
- Structures, practices, policies, and regulations historically effective in achieving certain outcomes may now be unintended obstacles to efficiently enhancing resilience and security at the pace needed by the Nation.
- New models of behaviors and interactions may be required that may often put current practitioners and leaders in both government and private industry out of their "comfort zone" which impede action and cause acceptance of greater risks.
- Effective action requires much greater collaboration and coordination among sectors, and not just with government.

Research and development often is seen as technologically oriented. However, addressing these realities must address issues beyond technological tools and methods in the nation's research, analysis, and development agenda. Technological and analytic tools to make a systemic difference must also be utilized, in order to motivate and create consensus across critical infrastructure sectors, public and private sectors, and across disciplines. Tools alone, however, can only take the mission so far to incent action. In order to advance the national program of security and resilience to its next level of maturity, research and development needs to expand to the human and organizational dimensions of motivations, incentives, and approaches to efficient and effective systematic learning, application, and collaboration.

1. Introduction

Background

Increasing complexity is at the center of two major challenges to critical infrastructure industries. Technological advances have greatly expanded operations capabilities, but have also led to increasingly interconnected and interdependent structures for the delivery of essential services. In addition, the threat landscape for critical infrastructure assets is continually evolving and expanding: natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure are all sources of great concern for all levels of government and providers of critical infrastructure products and services.

To address these challenges, the President issued Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) and Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636) on February 12, 2013. Both documents provided guidance and direction on how government and the critical infrastructure owners and operators can work to ensure the continued operation and rapid recovery of essential services in the event of a disruptive event. PPD-21 required the Federal Government to develop a national plan to address critical infrastructure security and resilience research and development. The plan will identify priorities, as well as provide research and development requirements and guide investments. The plan, which will be reissued every 4 years and with interim updates as needed, will identify key national research and development priorities, support enhanced collaboration across the public and private sectors, and consider cross-sector vulnerabilities and interdependencies. Once completed, the plan will complement both the 2013 National Infrastructure Protection Plan (NIPP) and the National Cyber Security Framework by supporting critical infrastructure security and resilience efforts to prepare for, respond to, and mitigate threats to physical and cyber assets.

On September 5, 2014, the National Infrastructure Advisory Council (the Council) received a tasking to provide recommendations on the development of this national research and development plan. The Council was asked to consider cross-sector research and development priorities of national significance, a discussion on the rationale for prioritization, strategic drivers for future requirements, and recommendations for public-private partnerships to facilitate national priority investments. In addition, the Administration asked the Council to frame its efforts around the following two questions:

- What does industry view as the most significant cross-sector research and development priorities? How might this view change looking to 2020 and beyond?
- PPD-21 calls for the capability "to be secure and to withstand and rapidly recover from all hazards." What factors should be considered in prioritizing national research and development activities?

This report consolidates and presents the Council's perspectives, final findings, and recommendations within an integrated framework directed toward pragmatic actions and results.

Council's Perspective on Deliverables

Based on the limited time allotted for completion of its report, the Council believed that it should focus on strategic, directional recommendations, rather than on specific programs. Promoting and implementing critical infrastructure protection/security and resilience has progressed for almost a decade, and in that time, improvements have been made in understanding challenges and learning lessons in response to disruptive events and enhanced communication among mission partners. However, based on common theme in input provided by several research institutions, some lessons seem to continue to be learned and re-learned, particularly in the areas of interdependencies/dependencies and coordination of activities across sector operations. Rapid changes in technology and its use, as well as uncertainties in the world's natural and political environment, have geometrically increased complexity of operations. Seemingly intractable issues have been identified as a result. In order to advance the national program of security and resilience to its next level of maturity, the Council believes that research and development needs to be expanded beyond the technological tools, methods and practices, to the human and organizational dimensions of motivations, incentives, and approaches to efficient and effective systematic learning and collaboration.

Report Development Approach

To address this tasking, the Council established the Critical Infrastructure Security and Resilience Research and Development National Plan Working Group to collect perspectives, develop recommendations, and to draft a report for consideration by the entire Council.

The Working Group collected perspectives from members of the Council, with emphasis on the lifeline sectors (Electricity, Water, Transportation, and Communications) and Financial Services. In addition, the Council collected perspectives from several research institutions and academia, as well as individuals with broader policy and programmatic backgrounds. Several members reached out into their own sectors to collect information to deepen the offerings of their own knowledge base.

Data collected from the members and subject matter representatives were then consolidated into common themes, which working group members used in their deliberations to develop draft recommendations and this report for the full Council to consider, deliberate, and adopt. A consolidated summary of the data collected is attached in Appendix B.

2. Findings

The Council identified six primary strategic drivers for research and development requirements. Five represent threats, vulnerabilities, and consequences that need to be managed by the Nation's critical infrastructure to assure their security and resilience to support our communities. The sixth, however, identifies major obstacles to action identified through lessons learned and relearned over the past few years of experience with managing the risks and consequences from catastrophic disruptions.

National Strategic Drivers Findings

Finding 1: Overcoming Obstacles to Action: Policy, Regulatory and Structural Barriers

Current regulatory frameworks and national policy have not kept pace with the changing landscape of critical infrastructure security and resilience. They are often not harmonized, and do not encourage resilience against the broader geographic impact of catastrophes, nor the growing operational complexity and dependencies of the critical infrastructures. Policies and regulations can act as disincentives to investments and collaboration across sectors and between public and private sectors. There is often little to no value proposition for investment, either from a political or a commercial perspective. Consequently, appropriate regulations and policies could also act as an enabler.

> "We aren't just treading water, we are moving in the wrong direction."
>
> **Dr. Stephen Flynn**
> Founding Director, Center for Resilience Studies, Northeastern University

Historical policies that show a lack of consideration for the effects of industry restructuring, such as consolidation – and the subsequent stifling effects on research and development that results – is diminishing the ability to innovate and adapt to the evolving challenges facing the Nation. As an example, in the Communications Sector, the Nation as a whole is reliant on resolutions to a number of major issues. These include the impending need to share the limited space available on the Radio Frequency (RF) Spectrum for wireless communications; the establishment of an interoperable communications system for use in emergency response efforts; and public education and outreach regarding preparation, resilience, and response to emergencies. But with only the largest companies able to capitalize on available research and development funding, the entrepreneurial innovation of smaller companies has been limited.

There has been a longstanding interest, on the parts of the Federal Government and private sectors, to establish effective frameworks for information sharing – both within and across sectors, and among and between public and private partners. But, to date, the desire to successfully establish systems and approaches for doing so has been impeded by regulations regarding how data can be shared, and with whom in some sectors.

Finding 2: Dependency On and Interconnectedness through Cyber Systems

Mission-critical systems in every sector are increasingly connected to networks, which is further expanding the range and forms of vulnerability that threaten critical infrastructure operations. In addition, the proliferation of e-commerce and data collection for both commercial and government purposes has led to an exponential growth in the amount of sensitive or critical data being stored and requiring protection. While recent technological advances – such as mobile and cloud computing – have helped to overcome some of the stove piping of operations that has long complicated operations processes, they have also exposed additional vulnerabilities in each sector, by blurring the previously well-defined borders of perimeter security models. This interconnectedness increases the complexity of operations, making it more difficult to detect, assess, respond to, and recover from a disruption.

Complicating this expanded risk landscape is the evidence that threats against critical cyber systems are becoming more common – and that these threats are becoming more sophisticated. In the Energy Sector, the Electricity Grid and natural gas pipelines have seen a spike in threats that attempt to disrupt transmission of power or fuel. The Financial Services Sector has long been a target of cyber criminals, but where intrusion attempts were once focused solely on financial gain and intellectual property theft, there is an emerging strain of organized attacks seeking to disrupt critical infrastructure operations.

Finding 3: Aging Infrastructure and the Effects of Catastrophic Natural Disasters

To date, there has been little will or commitment to the restoration and replacement of critical infrastructure assets that are at – or past – the end of their useful lifespans. Because the few incentives available are not sufficient to encourage action, high costs and the lack of a value proposition have meant that aging, brittle, or failing critical infrastructure assets are vulnerable to disruption by a range of threats.

Most of the lifeline sectors are in need of substantial efforts to address the concerns of aging infrastructure. In the Transportation Sector, there has been a concerted effort in recent years to keep facilities and infrastructure in a state of good repair. But there is an urgent need for a

national vision and commitment to repairing and replacing aging and failing Transportation Sector assets – particularly those systems that are owned and operated by the public sector – and a willingness to view the mitigation of these issues through a lens of enhanced resilience, and to ensure that resources are allocated with resilience in mind. It is expected that those assets will be further strained, as an additional 66 million people are expected to use passenger transit in the next 25 years. In the Water Sector, many systems are in need of repair, and key pieces of distribution networks are well past their useful lifespans, and need to be replaced. In the Energy Sector, efforts have begun to pool resources and establish mutual aid. But because those programs are still in their infancy, a major disruption to the Electricity Grid would also prove disruptive to those programs. In the Communications Sector, incomplete broadband penetration – particularly in rural areas – is limiting the capabilities of business and government, and an interoperable first responder communication system has yet to be achieved, hindering the ability of response agencies to coordinate with one another.

The fragility of vital infrastructure carries substantial consequences when such systems are stressed by major natural disasters. The after-effects of Hurricane Sandy continue to loom large in the critical infrastructure landscape, with the storm leaving billions of dollars in damage in its wake and causing substantial damage to Energy, Communications, and Transportation sector systems. Climate and weather patterns are causing an increasing number of severe weather and other natural disasters, which further taxes aging infrastructure.

Finding 4: Evolving Terrorist and Other Man-made Physical Threats

The terrorist threat remains a primary strategic driver, and it has evolved over the past few years. Where malicious threats were once contained primarily to a single terrorist organization, today's man-made threat landscape is much more diffuse, and much less easy to predict. For years following the September 11, 2001 attacks, al-Qaeda was the primary source of credible threats against the Nation and critical infrastructure. But in recent years, terrorist organizations have splintered into several smaller and less closely affiliated groups. Furthermore, these smaller groups have capitalized on the growing availability of the Internet, and are using social media to reach and inspire lone-wolf attacks by followers worldwide.

The types of threats coming from individuals have also become more sophisticated. Recent active shooter events have demonstrated a growing frequency of attacks in which there are two phases: a primary attack, in which members of the public are targeted, followed by a secondary attack on emergency responders attempting to assist the injured and restore order to the scene. In addition, there is an ongoing concern of individuals infiltrating critical infrastructure facilities as employees, and using their access to launch an attack from within.

Finding 5: Growing complexity and consequences of cross-sector dependencies, subject to a growing range of threats

Every critical infrastructure sector relies on one or more of the lifeline sectors (Water, Energy, Communications, and Transportation) to maintain functionality. But that reliance upon those sectors is also true of each of the lifeline sectors themselves. For example, the Energy and Communications sectors have a foundational role in the operations of other sectors' systems. But both Energy and Communications services are also reliant on each other to maintain that baseline functionality – in the case of the Energy Sector, Industrial Control System and vulnerability management is dependent on reliable network service; for the Communications Sector, electricity underpins the ability for those and other network capabilities. In addition, the Energy Sector is reliant upon both the Water and Transportation sectors, for cooling and the transit of precursor materials, respectively.

Lessons learned from the most recent catastrophic disasters reflect how complex such dependencies are to identify, respond to, and recover from. Just-in-time operations and outsourcing of non-core activities capture cost efficiencies and enhance customer service. However, these dependencies increase the complexity of coordination, response, and recovery from an event. As a result, consequences can cascade across the country rather than being confined within a region.

With the ever growing use of the Internet, the cyber threat has become a primary and national security threat. Threats – whether man-made or from natural disasters and accidents – to both the cyber and physical dimensions of critical infrastructure continue to grow in number, as well as in consequence. Cyber systems can be disrupted from physical events and physical operations can be disrupted from cyber events. The variety of physical threats is increasing, with a growing number of catastrophic weather events, industrial accidents, and individuals with greater sophistication in their means and approaches to disrupt. This complexity requires multiple disciplines to work together efficiently and effectively across regions and across sectors. However, observations from researchers and practitioners have identified a cultural and operational "divide" between sectors, between levels of government, and among disciplines, such as physical and cyber security practitioners – which must be bridged in order to encourage cross-sector coordination and innovation.

Finding 6: Workforce Changes, Evolution and Requirements

The Nation's workforce is approaching a generational turnover, which presents both challenges and opportunities. With increasing numbers of the most experienced members of the workforce approaching or reaching retirement age, there will soon be a shortage of qualified personnel with an understanding of key specialty operations – and therefore a need for comprehensive

workforce development strategies. But this changeover will also present significant opportunities, as personnel with greater understanding and familiarity with new technologies may be able to produce new means of leveraging these capabilities.

In addition, the Nation's population is on the move. Demographic trends have shown increasing numbers of Americans are moving from northern parts of the country to southern areas and from suburban and rural areas to urban communities. It is forecasted that 87 percent of the population will be residing in urban areas by year 2050. This migration of the Nation's population has ramifications on the requirements on critical infrastructure operations, particularly the lifeline sectors.

The increasing number of retirements and need for comprehensive effective workforce development strategies also provide us with an opportunity to leverage federal infrastructure investment to create and sustain the greatest economic impact (jobs creation), stimulate local educational and business engagement, connect veterans, and provide opportunities for people living in disadvantaged communities.

Criteria for Nationally Significant Capabilities- Defining National Significance

In order to identify research to support capability priorities of national significance, the Council adopted a definition of "national significance" articulated by former Homeland Security Deputy Secretary Jane Holl Lute. Deputy Secretary Lute described events or issues as having national significance when they require coordination or support by the Federal Government beyond regional boundaries and resources beyond the ability of local or State governments to provide.

She also noted that although homeland security is regarded as part of national security, the execution and authorities that govern that execution are different. National security has traditionally been seen as the responsibility of the Federal Government which manages this mission in a highly centralized, top-down manner. In contrast, because execution of the homeland security mission requires the involvement and effort of all jurisdictional levels of government, private sector, and the public, the authority and execution

> "When you think about the National Security community, it is strategic centralized and top-down driven. In contrast, Homeland Security is de-centralized and issue driven. Washington is not a national command authority, it's a federal partner."
>
> **Jane Holl Lute**
> Former Department of Homeland Security Deputy Secretary

requires a highly decentralized, bottom-up approach. Consequently, homeland security, of which critical infrastructure security and resilience is a component, contains challenges for coordination, planning, and problem solving that is generally not well understood by the public.

Characteristics and indicators of nationally significant capabilities include:

- Commonality across sectors and regions
- Addressable interdependencies and cascading effects across the country
- Support needed from the Federal Government to coordinate decisions and actions
- Focus on lifeline and Financial Services sectors
- The need to remove obstacles to action across the sectors and multiple jurisdictions

Nationally significant critical infrastructure does have a major intersection and impact on national security for the Nation. This impact has been recognized by the Federal government and Congress in establishing critical infrastructure security and resilience as a national mission to provide it with a sense of urgency and priority.

Required Cross-Sector Capabilities of National Significance

The Council identified two nationally significant priorities for research and development that emerged from the data it collected for this report (see Appendix B). These two categories appeared as common themes through the sector data and data collected from other sources:

- Eliminating or reducing obstacles to action and to facilitate decisions to make investments; and
- Improving the effectiveness and efficiency of implementation and operations of security and resilience programs.

These two categories are composed of sub-elements and which the Council identified as required cross sector capability findings.

Finding 7: Approaches to overcome obstacles to actions

7.1. Enable and align regulations and policy

A common theme in the information collected by the Council was the need for enabling policies, structures, and regulations that will support action, both to execute programs and to make investment decisions. In many areas, current regulations and policy need further review or realignment with enhancing critical infrastructure security and resilience in the world in which critical infrastructure now has to operate. Many regulations and policies were developed under historically very different circumstances. Advances in technology and its

applications, and growth in the scope of threats and consequences have changed the operating environment for the core infrastructures over the last decade. Some of these regulations now have unintended consequences. For example, some overall mission goals – such as enhanced information sharing and more effective partnerships – are hindered by the conflict between policies advocating for greater collaboration and regulations that were put in place to prevent collusion in competitive markets, such as antitrust regulations on the Oil and Natural Gas sub-Sector that have hindered the distribution and transportation of fuel following major weather events. In other cases, outdated regulatory approaches – such as those allowing for the accumulation and consolidation of media and communications companies – are limiting the capabilities of the private sector to develop innovative solutions to mission-wide challenges.

7.2. Appropriate market incentives for mission-critical investments

While there have been countless lessons learned and after-action reports created following disruptive events and natural disasters, a substantial number of those lessons continue to be relearned in subsequent incidents (See Appendix B). Perhaps more troubling was the realization that some of those lessons had been reported several times previously, and that mitigation strategies had not been put in place. Owners and operators have obligations to shareholders and to the public in their local communities, particularly for publicly owned and operated critical infrastructure, to keep costs low. They do not see themselves as responsible for national security investments to harden and enhance resilience to prepare for low-probability, high-impact events that do not carry much return on investment. As such, a business case for the required level of capital expenditure is difficult to make. A key part of that motivation must be based around capabilities that incent action by owners and operators, by mitigating expenses and liabilities for implementation, and that make long-term investments in resilience an effective use of resources. The type of incenting capabilities can range from lowering insurance premiums to reducing liabilities for good faith efforts at implementation of security and resilience in compliance with established standards or best practices.

7.3. Reduced Barriers to Cross-Sector and Public-Private Collaboration

In a complex environment, partnerships and coordination across sectors and between government and the owners and operators of critical infrastructure are core elements to advancing security and resilience beyond its current state. Interdependencies, dependencies, and interconnectedness have become core elements of operations in a world driven by cost efficiencies, just-in-time service, and automation-dependent customer service.

But in order to maximize the efficacy of these partnerships at all levels, current research appears to show a barrier that must be overcome: The isolation of information and decision-

making that is relevant to multiple entities, but which is handled by each of those entities individually. Sometimes referred to as stove piping, this isolation can occur among the sectors (and even at times within a sector), within the different levels of government, and between public and private sectors. The complexity of the sectors and of different levels of government – whether in structure, culture, politics, regulatory approaches, operations, or even vocabulary – complicates efforts to establish repeatable, effective, sustainable, and institutionalized, coordinated preparedness and response.

Finding 8: Required cross-sector capabilities to support security and resilience programs implementation and their operations

8.1. Strengthened cybersecurity capabilities

With the growing understanding of the ways in which the disruption or manipulation of networks and systems can undermine essential services and undermine confidence in the nation's critical systems, certain critical capabilities are required to manage the risks inherent in operational reliance on cyber systems:

- **Real-Time identification and authentication of people, software, and systems** – Increasing business and operations are being conducted online, which requires the accurate and real-time verification of users, without relying upon personal secrets. The goal should be to develop a core transaction protocol layer that is integrated with transaction systems and processes, and which would be nearly impossible to tamper with.[1]
- **Increased efficiency and real-time security analysis and data collection** – Because of the increase in sophisticated attempts to disrupt cyber assets, owners and operators as well as government institutions will need to be able to more rapidly detect and understand threats, vulnerabilities, and consequences through more efficient analysis and data collection to effect that analysis.[2]
- **Integration of cyber security risks with other business risks for decision-makers** – While PPD-21 established that the Federal Government views the security and resilience of physical and cyber assets as inextricably linked, there is a need for better understanding on the implications emerging from integrating these risks and on how to address and mitigate these challenges.[3]

[1] See Appendix C, Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security Research and Development Committee, *Research Agenda for the Banking and Finance Sector*
[2] There is another form of footnote (e.g. Ibid---which says the same as above---please research and use the proper footnoting format for all these references in this section.
[3] See Appendix C.

- **Better understanding of human behavior and motivation** – One of the larger challenges associated with cyber intrusion is that the behavior of people – whether intentional or unintentional – can render effective security moot.[4]
- **Control system and sensor device security** – With industrial control systems increasingly connected to other parts of business and government networks, and GPS systems vulnerable to spoofing and disruption, vulnerability mitigation processes will be needed to ensure the security and resilience of these systems.[5]

8.2. Understanding and management of cross-sector dependencies and cascading effects

The ways in which the operations of one system affect another have been an ongoing area of study. Although progress has been made, challenges remain. There is a lack of understanding regarding the effects of several key changes taking place, such as the impact of climate change and severe weather on interdependent systems; the increasing complexity of essential services and critical assets; and a population that is increasingly based in and around the areas immediately around cities. Owners and operators require a much better understanding and ability to plan with assurance that investments are rationalized and effective, and programs providing this information will need to be established. Without this understanding, both the owners and operators and the public accept the risks.

8.3. Built-in resilience in design and operations

Building resilience into design and operational practices mitigate consequences for a community as well as institutions, and prove more cost-effective over time. Specific capabilities needed include:

- **Reduction in implementation costs –** The estimated costs of required replacement and upgrades to critical infrastructure have been estimated at levels beyond what is deemed doable by many. As a result, cost efficiency is a critical incentive in order to overcome this challenge, and encourage acceptance of the need to invest.
- **Reduction of day-to-day disruptions to public and business operations** – The process of rebuilding and replacing infrastructure often interrupts or diminishes service creating unwillingness to invest and to take action in a timely manner.
- **Accelerated implementation** – Faster installation, much like the reduction of day-to-day disruptions, provides the incentive for reducing the time that a business has to operate sub-optimally or adversely impacting its relationships with the public, while upgrading or replacing infrastructure.

8.4. Efficient and cost-effective workforce development

[4] See Appendix C.
[5] See Appendix C.

With generational turnover and exponential technological growth, innovative means for training and educational programs will be needed to ensure the workforce is available to build and sustain the effective and efficient operations of critical infrastructures, particularly in the lifeline sectors.

- **Cyber-savvy workforce as well as cyber experts** – Rapidly changing technology requires a workforce capable of maximizing the capabilities of new systems, as well as a pool of candidates capable of protecting and maintaining those systems. As a result, there will be a need to develop a workforce capable of understanding cyber issues, as well as education programs capable of producing the expertise needed to mitigate threats and vulnerabilities in networks and cyber assets.
- **Lifeline sector operations** – As a generation with decades of experience retires, there will be a lack of understanding of key operations and maintenance of critical lifeline sector operations. To prevent that loss of valuable expertise, appropriate training will be needed for the next generation of employees and specialists.

8.5. Effective and actionable contingency and preparedness planning

Even the most secure and resilient systems can fail, as no approach to preventing man-made threats are foolproof, and natural disasters will continue to occur. With this in mind, it is essential to have effective, actionable plans to ensure governments, businesses, and the public are ready for potential disruptions. In addition, there is great value in well-designed, informative exercises that can test the efficacy of contingencies and preparedness plans; more sophisticated and challenging scenario-based training will be vital in validating and revising these plans.

3. Research and Development Recommendations

Research and Development Priorities

Remembering that national resilience and homeland security are collectively implemented by one community or institution at a time, it is essential that tools, methodologies, and practices be practical, scalable, and efficient. There is also a need for their integration to make them more useful and efficient in holistic planning within the normal management practices of owner and operator organizations. What does not get protected or secured represents a trade-off for what has to be executed during response and recovery. In risk informed decision-making, information on trade-offs is an essential element for investment decisions.

Of highest priority, from lessons learned and relearned, it is essential to identify the necessary conditions that will motivate owners and operators, and all levels of government to take the necessary actions to invest, plan, and implement. Research must focus on obstacle identification, innovative analysis and capture of insights to develop creative approaches for issue resolution, while development needs to focus on tools, methodologies and practices, including rules of engagement that are efficient as well as effective and adaptable to the wide diversity of operations, within the critical infrastructures. The Council has identified four primary research and development categories of recommendations for national priority investment. These recommendations on research and development priorities are listed in the order of their priority to the Council. The Council identified these priorities based on its identification of the common sector-specific priorities from the sector specific data collected and general cross-sector subject matter expert data input. This data is summarized and documented in Appendix B.

Recommendation 1: Address role and impact of regulation, public policy, and consolidation within sectors on resilience and innovation.

1.1. ***Research and analyze the labyrinth of regulations and policies across all levels of government that impede and dis-incent investments in security and resilience.***

Research and analysis is needed across the entire range of supporting activities, including hardening, consequence mitigation, response and recovery, and cross-sector collaboration/coordination.

Research should focus on systematically identifying and inventorying the policies and regulations that conflict and have unintended consequences, and identifying efficient policy approaches for resolution. Research also should be focused on achieving two other objectives: Improving investment decisions by identifying mechanisms, structures, and processes to resolve stove-piping between and among sectors, jurisdictions, and regions; establishing methods for encouraging collaboration and coordination among all stakeholders.

1.2. ***Identify essential elements of enabling policies and regulations that would encourage and facilitate owner and operator investment and gain public acceptance of such investments, particularly for many of the lifeline sectors, for which rates and return on investment are determined through State and Federal commissions.***

1.3. ***Determine the role of policies, regulation, and consolidation within industries and its impact on resilience, security, innovation, and resilience.***

Small, entrepreneurial companies are recognized as engines of vital, innovative solutions to challenges associated with critical infrastructure security and resilience. Anecdotal evidence indicates that much of the innovation in cyber security is coming from small start-ups. There is a need for vigilant review of industry consolidation, as well as incentives to promote the inclusion of small businesses in the research and development process to incorporate entrepreneurship and innovative approaches to development.

The Council recognizes the critical role of Congress to facilitate or enact any changes to policy, legal framework, or regulations that may be identified out of the research in these areas. Consequently, to make real progress in removing these obstacles, the executive branch may have to propose legislative changes to Congress.

Recommendation 2: Identify and Apply Best Practices

2.1. ***Identify and establish the elements for business and public justification for investments from lessons learned.***

With limited resources, owners and operators must take care in making smart, informed decisions for expenditures. Research can establish which forms of incentives will carry the greatest value and will be most likely to be adopted. These include developing an increased understanding and articulation of the operational risks owners and operators face; reviewing best practices for how sectors organize themselves and with other sectors on industry-wide decision-making; and best practices to coordinate design requirements and processes for infrastructure investment.

2.2. ***Develop an effective model of shared industry funding.***

Coordinated and pooled investment in research and development can help to harmonize the demands of the critical infrastructure security and resilience with the requirements placed upon owners and operators with regard to business practices. The Electric Power Research Institute (EPRI), a non-profit scientific research organization, serves in this capacity for the Electric Sector, and provides an example of how such efforts can be coordinated. The Financial Services Sector, through its Sector Coordinating Council (FSSCC), has provided a best practice (see Appendix C) publication of a public agenda for research and development requirements for its sector. The agenda provides a clear operational context for its requirements, thereby focusing research much more meaningfully on its specific and unique requirements. The sector continually improves its agenda over time thereby continuing to solicit greater interest and support from the technology and other research communities.

2.3. ***Determine design standards and best practices for the replacement, upgrading, and maintenance of critical infrastructure systems.***

Our Nation invests $1 billion a day in new and upgraded infrastructure. Consequently, we have a special window of opportunity to ensure that infrastructure is built and rebuilt with the best design principles where it will make the most difference for resilience and survivability within and across sectors. Study of this issue should seek to resolve how best to incorporate security and resilience into the creation of a component piece, as well as how to encourage and incentivize the adoption of newer, more resilient technology by owners and operators. At the same time, research must identify the best practices for reducing the costs of replacement, upgrades and maintenance of critical infrastructure to make them affordable in the eyes of the shareholders and the public, as well as to minimize disruptions to the public and service while performing such activities. An example of potential best practices in this regard is seen in the Minneapolis 1-35 bridge replacement after its collapse in 2007.

2.4. ***Identify innovative, cost-efficient, and accelerated approaches to "People Readiness" in developing a skilled workforce.***

Innovative approaches to efficient and effective training will be needed. The shortage of a cyber-savvy workforce and cyber security experts has long been recognized as a national issue.

2.5. ***Determine factors and approaches to accelerate recovery following a disaster.***

Research should be done to identify the best practices and lessons learned from several recent storms (Hurricanes Ike and Irene, and Superstorm Sandy) on the subject of rebounding from disruptive events. Research should also be directed toward determining how to appropriately direct limited essential services in order to allow communities, consumers, and institutions to

continue functioning with partial or sub-optimal infrastructure function. In addition, social media should be integrated into public alert and warning systems, as well as information sharing capabilities.

2.6. ***Establish resilience metrics.***

The Council has made recommendations to develop security or resilience metrics in several of its previous reports. Return on investment may not always take a financial form, particularly for security and resilience investments. In its 2013 report to the President on *Implementation of EO 13636 and PPD-21*, the Council noted that developing metrics clarify and firm up desired outcomes. They can act as an incentive for investment by re-affirming concrete, meaningful progress towards accomplishing those desired results. Consequently, metrics is an essential element in investment decision-making.

Resilience is a risk reduction approach for infrastructure operations, particularly in assuring continuity of business and fulfills an owner and operator's obligation to their customers and their shareholders if they are to remain in business. Consequently, resilience metrics are also an essential element for communicating with key stakeholders of the business in order to make sustainable investments. Metrics tie investments to desired results as deemed appropriate for the risk posture of a community or an institution.

The Council also noted in its 2013 report that some good work had already been done on metrics, specifically on information sharing metrics. Consequently, the Council believes that research and development of resilience metrics can leverage on existing work that has already been done in order to accelerate delivery of the identification and deployment of useful standard metrics to support resilience investments.

Recommendation 3: Advance management of cyber risks

3.1. ***Develop real-time cybersecurity risk analysis and management tools.***

With increasing interconnectivity of physical and cyber assets, research should focus on developing cybersecurity and resilience products capable of offering real-time threat mitigation.

3.2. ***Establish new architectures to "bake in" self-healing and self-protected cyber systems.***

Smart systems capable of autonomously responding to and rebounding from disruptive events will provide vital assistance in defending against cybercrime, as they will allow security operations teams to better process intrusion and attack attempts in real time.

3.3. ***Develop automated security analysis and data collection tools and methods.***

Current detection tools will not be capable of keeping up with the complexity of emerging threat vectors. There is a need for additional automation of security health checks and monitoring during an incident and collect data on the attack signature, which can be used to further enhance security posture following the attack.

3.4. ***Understand cross-sector connections that could cause cascading effects.***

All critical infrastructures are dependent on services provided by other sectors, with networks and systems often creating the link between one or more industries. A comprehensive awareness and understanding of the ways a failure of cyber infrastructure can disrupt services in other sectors is essential to greater security and resilience.

3.5. ***Measure the effectiveness of security.***

As with resilience metrics, there must be clear direction on how to improve cybersecurity practices, and then to affirm progress and effectiveness in order to ensure security enhancements are achieving the desired effect. Affirming that practices will lead to concrete results is an incentive in itself. First, it will assure management that the investment was worthwhile; and secondly, it can reassure the institution's shareholders and customers of reduction of their risks in owning or using the institution's business.

Recommendation 4: Develop and integrate modeling and simulation tools

4.1. ***Scale risk assessment and, management decision support tools for local communities and individual institutions.***

While there are many methods to analyze the vulnerabilities or a region or a facility, there is not, at present, a means of synthesizing all of that data into a single integrated assessment. A standardized risk assessment process which addresses the entire range of risk mitigation activities could be used to populate both a risk assessment tool and a management decision support tool, both of which would assist communities and institutions in making smart investment decisions.

4.2. ***Develop, scale and integrate interdependency and consequence modeling, and simulations to support operational decisions to predict and prevent cascading failures.***

Research and development should be performed to develop a comprehensive and functional simulated environment that can be used to analyze the effects of infrastructure failure in the wake of a disaster. This environment will allow users to see how clear and present threat scenarios would affect infrastructure, and how the disruption of those essential services

would affect other vital services. Such a tool would be utilized by communities and institutions and government at all levels for planning, coordination, and focused investments to act on lessons learned and improve preparedness.

4.3. ***Continue research and development for managing "big data".***

"Big Data" management capabilities will continue to need research and efficient management approaches developed to ensure the protection and appropriate sharing of information, as well as to develop the most effective models and simulations of disruption. Research is needed to map the links, nodes, and intersections of infrastructures across networks. High-performance computing – which is in place at many organizations – may be of use in these efforts, but has not been leveraged in that manner to date based on the anecdotal information that the Council has received.

Recommendation 5: Timeline Recommendations

The Council sees all of these priorities as challenging and requiring short- and long-term investments. However, from our perspective, the availability of tools is not meaningful if there is insufficient motivation to use them or apply the results that they produce. The use of tools and methodologies often require short term investments. The implementation of longer term programmatic investments, however, requires a different degree and extent of managerial and often public commitment, particularly for publicly owned and operated critical infrastructure.

At the same time, the Council has a sense of urgency. The nation's critical infrastructure is more fragile and vulnerable than many are willing to acknowledge, with recent catastrophic disasters and continuing reports of cyber security intrusions demonstrating the costly consequences of inaction on the lives of millions of Americans, and in their sense of confidence in our institutions.

Consequently, the Council recommends:

5.1. ***Within 18 to 24 months, the Federal Government should develop and implement programs and initiatives addressing issues that have been substantially researched, and constitute simple, demonstrable gains that can be made quickly.***

These could include concepts such as the development of a social media toolkit that can assist governments in sharing information about public alerts, warnings, and response efforts, as well as the use of apprenticeship and technical training curricula to ensure a skilled critical infrastructure workforce.

5.2. ***Within 5 years, complete comprehensive research on incentives, motivation, and structures to facilitate action. The Council also recommends focusing on the***

identification and sharing of best practices within the next 5 years, as an efficient means of making available proven and illustrative methodologies and practices.

This research would particularly address the first three primary areas of research and development that the Council has recommended.

5.3. ***Beyond 2020, continue to invest in research as required in all areas, but to focus on development of integrated and scalable tools, methodologies and practices***

The Council recommends this timeline for this area as most useful and productive as owners-operators and governments become more encouraged to invest in resilience.

4. Role of Public Private Partnership

The Need for Joint Investments

The Council found that joint investment in research and development will be essential to enhancing the security and resilience of nationally significant critical infrastructure. Shareholders and the public generally see CISR-related research and development as being difficult to justify. Critical infrastructure organizations are naturally focused on capturing maximal return for capital expenses in a short period of time given the economic uncertainty in world markets. Shareholder equity and public perspective of affordability plays an important role in investments. Major expenses focused on reducing potential damage to business operations in the event of a substantially disruptive – but improbable – event typically do not meet the desired return on investment, either for shareholders or generally for the public who influence rate cases and bond offerings. Matters of national security are under the jurisdiction, and therefore the responsibility, of the Federal Government. Consequently, critical infrastructure owners and operators do not see that they have responsibility for national security investments.

In many of the sectors, particularly the publicly owned and operated sectors, funding for infrastructure improvements are very constrained to the point of crisis. Infrastructure failures or disruptions due to aging infrastructure reflect this constraint as maintenance and replacement of infrastructure that has reached the end of its useful life continues to be deferred. Consequently, funding for protection and particularly resilience initiatives need to be a shared effort.

At the same time, infrastructure and other relevant investments are being made by both public and private sectors. The government, for example, has spent billions of dollars developing capabilities that could be applied in critical infrastructure sectors to secure and enhance their resiliency. Critical infrastructure sectors are spending a billion dollars a day on infrastructure investments. The opportunities are there for these investments to be leveraged if public and private sectors can identify their mutual interests.

By taking a collaborative approach to investment, the Government can provide public and private owner and operator institutions both with the means and the justification for approving a substantial investment in protecting and strengthening the resilience of their critical infrastructure.

Characteristics for Effective Public-Private Partnerships

The use of public-private partnerships to meet the research and development challenges for critical infrastructure security and resilience emerged as a common theme from the perspective

of the Council's members and subject matter experts from whom it collected information.
Critical infrastructure security and resilience is a shared mission; neither government nor owners and operators can do it alone. Partnership is a mechanism which begins to break down stovepipes, share costs, and reduce the financial burden as an incentive to invest, and to build trusted relationships to facilitate needed planning and operational coordination.
Many lessons have been learned over the past decade on key elements for effective and sustainable public-private partnerships. Creating and fostering effective partnerships between governments of all jurisdictions and private sector owners and operators is reliant on clarity and strong, trusted relationships, which can be built by focusing on the following elements:

- **Appropriate policies and regulatory frameworks** – In order for partnerships to flourish, governments and agencies need to establish a policy and regulatory environment in which collaboration with owners and operators can take root and grow.
- **Establishment of clear objectives and goals with deliverables and milestones** – Unambiguous and actionable targets are essential in encouraging collaboration between owners and operators and governments of all levels.
- **Transparency of intent among partners in setting objectives** – Because trust is a key part of an effective collaborative relationship, government agencies, as well as owners and operators, must clearly describe what is to be gained from a partnership – and that involvement will not expose private sector partners' business practices or sensitive information.
- **Strong lines of communication across the partners** – Regular, process-based communication ensures that all members of the partnership are engaged and aware of relevant information related to critical infrastructure security and resilience investment efforts and their results. Because of the complexity of the goals, it is important that all parties involved in the critical infrastructure security and resilience mission are engaged as part of the partnership. This should include the various levels of government and private sector owners and operators already being engaged, as well as non-profit organizations – which offer collaborative capabilities on issues of preparation, response, and recovery – and employee organizations – which can serve to provide the perspectives and needs of the critical infrastructure workforce.
- **Strong, proactive management** – Clear leadership and direction guide partnership efforts and encourage continued and engaged participation in initiatives and commons goals.
- **Value proposition** – It must be clear to prospective participants what they can hope to gain by collaborating with government on initiatives, and how those efforts can aid, protect, and strengthen their day-to-day operations and overall ability to respond to incidents. The value proposition represents both an incentive and a justification for their shareholders and the public they serve, particularly the publicly owned critical infrastructures.

Public-Private Partnership Recommendations

Many successful and sustainable public-private partnerships have emerged over the past decade at the national and regional levels to implement and execute the critical infrastructure security and resilience mission. Best practices have been developed from those successes, and have been captured and shared among practitioners at all levels of government and owner-operator institutions. The 2014 Quadrennial Homeland Security Review has identified public-private partnerships as one of its five homeland security strategic priorities for the next four years. For research and development public-private partnerships, which are intended to focus on finding solutions to challenging and complex longer term issues involving many different and at times, conflictual perspectives, the Council makes the following recommendations:

Recommendation 6: Greater leveraging of academic institutions to seat public-private partnerships to research and develop solutions identified in this report.

Colleges and universities hold great potential for addressing the challenges of partnerships that include both private sector and governments at all levels. Historically, academic channels cut across borders and all institutional levels of governance in order to bring together expertise as required across boundaries of jurisdictions, disciplines and governance. They are generally seen as neutral, objective, and independent. Many of the solutions for advancing critical infrastructure security and resilience in a complex environment will require "out-of-the box" thinking that is natural in an academic setting.

Recommendation 7: Identify meaningful metrics for effective public-private partnerships to justify their establishment and sustainability.

Although the Council has seen many case studies of successful public-private partnerships, it has not seen any measures of success associated with them. Partnerships, as with other activities require commitments in resources and time. Under the adage that "what gets measured gets done," metrics, including benchmarks, involving deliverables, outcomes and results can be incentives.

5. Next Step Recommendations

The Council has historically been pragmatic and action-oriented in its recommendations. For a research and development agenda, which tends to be long term, the Council believes that effective results-oriented first steps can be motivators for sustained interest and support by the community of stakeholders over the years. Consequently, the Council recommends the following:

Recommendation 8: Upon the issuance of the National Plan, the President should immediately convene key representatives from the critical infrastructure sectors, subject matter experts from academic and research institutions, and all levels of government to identify key success elements for sustainable implementation of the plan.

Recommendation 9: Upon issuance of the National Plan, the Secretary of Homeland Security should convene a forum of research institutions, key critical infrastructure sector representatives, and key agencies at Federal, State, and local governments to develop a path forward to identify and document disincentives and potential enabling policies/regulations. The Council also recommends the sharing of such information across the sectors, and all levels of government.

Research and analysis of existing policy and regulatory disincentives and obstacles represent an effective first step and an incentive in itself for engagement and sustaining it by the critical infrastructure sectors. Sharing information on results will raise awareness and develop support to systematically and pragmatically address them in a coordinated way.

6. Appendices

Appendix A – Acknowledgements

Critical Infrastructure Security and Resilience Research and Development Working Group Members

David J. Grain (Chair)
Founder and Managing Partner, Grain Management
Sarasota, FL

Constance H. Lau
President and Chief Executive Officer, Hawaiian Electric Industries, Inc. (HEI)
Honolulu, HI

Dr. Beverly Scott
General Manager, Massachusetts Bay Transportation Authority (MBTA)
Boston, Massachusetts

Margaret E. Grayson
President, MTN Government
President, Grayson Associates
Leesburg, VA

James Murren
Chairman and CEO, MGM Resorts International
Las Vegas, NV

Member Respondents to Data Call

Margaret Grayson, President, MTN Government Services, Leesburg, VA
Michael Wallace, Senior Advisor, Center for Strategic and International Studies (CSIS), Director, Nuclear Energy Program, Washington DC
David Kepler, Chief Sustainability Officer, Chief Information Officer, Business Services and Executive Vice President, The Dow Chemical Company, Midland, MI
General Albert Edmonds (RET), Chairman and Chief Executive Officer, Edmonds Enterprise Services, Chief Executive Officer, Logistics Applications, Inc., Alexandria, VA
David Grain, Founder and Managing Partner, Grain Management, Sarasota, FL
Jack Baylis, President and Chief Executive Officer, The Baylis Group, LLC, Los Angeles, CA
Constance Lau, President and Chief Executive Officer, Hawaiian Electric Industries, Inc. (HEI), Honolulu, HI
Philip Heasley, President and Chief Executive Officer, ACI Worldwide, Naples, FL

Dr. Beverly Scott, General Manager, Massachusetts Bay Transportation Authority (MBTA), MassDOT Rail & Transit Administration, Boston, MA
Thomas Noonan, General Manager, Cisco Energy Services, Atlanta, GA

The Council would like to acknowledge the individuals and organizations who, on a very short timeline, took the time out of their very busy schedules to contribute their knowledge and perspectives to inform the Council's members work on this report. The Council extends to them its appreciation.

Interviewees

David Brannegan, Director of the Infrastructure Assurance Center, Argonne National Labs, Argonne, IL
Dr. Catherine, Baase, Global Director of Health Services**,** Dow Chemical, Saginaw, MI
Barry Kroeger, Executive Advisor to the CEO, ACI World Wide, Chantilly, VA
Michael Dinning, Director of Transportation Logistics and Security, Volpe, Cambridge, MA
Ronald Fisher, DHS Program Manager, Idaho National Labs. Idaho Falls, ID
Morgan O'Brien, Director, GTT, Washington, DC
Dr. Stephen Flynn, Director of the Center for Resilience Studies**,** North Eastern University, Boston, MA
Jane Holl Lute, President and CEO of the Council on Cybersecurity, Arlington, VA

Other Contributors

Electric Power Research Institute
Electricity Sector Coordinating Council
Financial Services Sector Coordinating Council

Department of Homeland Security Resources

Nancy J. Wong, Designated Federal Officer, Department of Homeland Security
Corey Thompson, NIAC Secretariat Support, VetFed Resources Inc.
Alastair Harley, NIAC Secretariat Support, VetFed Resources Inc.
Andrea Gagliardi, NIAC Secretariat Support, VetFed Resources Inc.
Kim Yager, VetFed Resources Inc.

Appendix B - Summary of Relevant Data Collected

In order to inform its deliberations and deliver its perspectives to the President as requested, the National Infrastructure Advisory Council collected information from some current research practitioners and other subject matter experts, in addition to its own members' perspectives and the data those members collected from within their own sectors. A consolidated summary of relevant data collected from these efforts follow. A list of the individuals providing this additional information is provided in Appendix A.

General Cross-Sector Themes and Perspectives

Obstacles to Action: Lessons Learned and Disincentives

Economic growth is tied to robustness of infrastructure. Several roadmaps for research and development have been issued since the President's Commission for Critical Infrastructure Protection issued its report in 1997. However, there has been very limited implementation of any of them, due to politics and lack of resources. One cannot apply layers of security that are not efficient. No one organization or sector is really set up to tackle the growing number and variety of threats such as pandemic, cyber, climate change, etc.

Because of droughts and other ongoing challenges like earthquakes, the nation may encounter some additional shocks to our infrastructure systems, predictable in general but not yet foreseeable in scope and impact. Unprecedented extreme weather in the last few years has been seen, and it is forecasted to continue. Although there is not a political force calling for more brittle and fragile infrastructure, in general, there is little acknowledgment of how unprepared the nation is to handle catastrophic foreseeable risk. Generally, people have a bias to discount risks. Most are comfortable with stationary assumptions about risk even though those assumptions are growing obsolete. A lack of resources to respond to risk creates a political liability for elected officials to recognize such issues. There is a need to be able to articulate a clear value proposition for the owners and operators and the public. The skills set that seems to be developing and refining is transferring risk to someone else rather than taking it on effectively.

Instead of being a lessons learned report, a study soon to be issued on Hurricane Sandy by researchers at North Eastern University became a report on lessons re-re-re learned. After action reports that look at the "big picture" dependencies and cascading effects seem to be missing. The current focus on after-action studies is usually very specific to what the sponsor is looking for. It is normally the role of the Federal government to sponsor the broader view.

A lesson is being learned by the insurance industry as catastrophic disasters grow in number and severity. Insurers are starting to realize they have significant exposure to risk that they may not make up in their premiums. A real challenge identified in the study on Hurricane Sandy was the belief that the federal government and insurance would protect them. There were such great losses with Sandy because some major measures did not take place ahead of time because there was no incentive. There is a need to recalibrate. One researcher noted "We are not just treading water; we are moving in the wrong direction."

Organizations have their own risk framework for low probability high impact events. If there is minimal return, then institutions will not take action. Regulatory environments can have unintended consequences for security and resilience, particularly when they restrict the ability to share information and communication. Some energy companies were chastised for not working closer during Hurricane Sandy, but there are anti-trust regulations that prevent them from doing that. Some utilities have gone back to using older equipment because it was easier than to comply with cyber standards. If cyber security is going to move forward in sectors where consequences are not immediate and direct to their customers, it has to have another value proposition.

Cross Sector Dependencies and Interdependencies

A lot of effort has been put into dependency and interdependency analysis. Only anecdotal information exists as to its importance for research. There has been very little useful information that qualifies or quantifies the impact of these connections. Private industry sees this issue through the lens of supply chains. This lack of definition and knowledge speak to a need for a higher level of quantification to prioritize criticality. There needs to be integrated emergency awareness, emergency planning, and continuity planning to understand fully the impacts of the dependencies. There is a need to show the immediate impact after an event and how quickly something can be reconstituted and what the priority of that is. Now one research institution is trying to take static data and automate them in a geographic information system (GIS) viewer so it can show a loss of a service based on a dependency and how quickly operations can come back online. Business continuity operation and strategic priorities of the assets owners for restoration and recovery is the backbone of such an analysis. Data has to be ingested into the overall analysis. The approach to dependencies is multi-disciplinary. It is difficult and long term. There needs to be an incorporation of a variety of different nontraditional data sets and inputs to really do analysis effectively.

Cyber Security Challenges

The nexus between cyber and physical represents a huge set of dependencies and interdependencies. However, there has not been significant progresses made, or even a definition

of what it means. There is a deficiency in areas of expertise to effectively communicate and understand each other in many sectors. The gap needs to be bridged. The analytic efforts appear to be moving back into their own (physical and cyber) worlds and not coming together to provide a truly integrated effort. Risks continue to be assessed and evaluated in their own stove-pipes. The cyber security world has good threat analysis capabilities, but limited on information on cascading impacts of dependencies. The national laboratories are trying to leverage physical expertise and apply it to the cyber realm to try to close the "divide" between the cyber and physical realms of security.

The danger in the inability to communicate and collaborate is that false conclusions may be made. Many physical operations and security experts think there is not a big cyber connection to their work and that cyber is not a threat. One observer noted that cyber experts trying to teach cyber analysis to non-cyber audiences get technical very quickly. The audience naturally tunes out. Consequently, many do not see a significant connection. There has been more success in exercises. Cyber experts are able to demonstrate consequences, without briefing, so people can digest and understand. There is a need to restart and reenergize the conversations about the cyber-physical nexus. There are a limited number of people who understand both.

Many cyber experts in intelligence in all levels of government appear comfortable in discussing threat, but not in the vulnerability and consequences areas. The physical experts want to talk about vulnerabilities and major consequences. The majority of the briefings today are focused on threat streams, how quickly those cyber threat streams can be mitigated and what technical solutions can be put in place. These discussions are only working on the first third of the risk equation for cyber security. Consequently, these discussions omit one of the most important aspects of a risk analysis to the critical infrastructure: what impact does this cyber threat have on continuity of critical infrastructure operations and how are consequences to those infrastructure operations to be mitigated? There is currently an analytic capability supporting DHS which focuses on physical incidents that have a national level of significance. There appears to be two different frameworks being used to analyze and address physical and cyber threats. Consequently, there is an opportunity to address this gap for cyber security.

The deep penetration of the Internet is creating an unmediated force for action. People need it and they want more. People are more active and empowered than any other time in our history. No government on the planet truly understands what's going on. The Internet allows people to know a lot about each other, but they know each other as consumers not as citizens. The power in cyberspace is the power to connect, not the power to protect. The law is not keeping up. There are very few tools to manage the explosion of the web. Existing vulnerabilities is the greatest worry. We have the capability to stop most attacks, but it is not being done.

National Security is considered strategic, centralized and top down driven. Homeland Security issues are de-centralized at the community, and bottom up driven. For homeland security,

Washington is not a national command authority, it's a federal partner. Homeland security sees a flattening and widening of consequences as opposed to a narrowing and deepening on the national security side. Nationally significant is defined as issues extending across regions and requiring coordination or resources beyond what one region can obtain or resource alone.

Our society has an enormous reliance on a free and open Internet. The communications infrastructure allows data flow. Storage, transmissions and computational power of data all play a part. Yet, there's nothing that one can safely and securely guarantee. There are key questions that need to be asked. Are you who you say you are and should we have to worry about you? Who is running your networks? What will the role of government be? Should we give this all to the government to handle?

Three things need to be done well and quickly during an event:

- The need to know what is happening—getting information quickly
- The need to mobilize to get resources out quickly.
- The requirement to continue these processes at high levels for as long as it takes to resolve

Having an informed population means a stable population. One thing people should keep in mind is that often there are two attacks, one to attack the population and a second to attack first responders.

Private sector must be willing to accept its role and responsibility for cyber security. As a result of the scope, growth and consequences of cyber-attacks, CEOs are getting fired. Institutions need to implement the basic steps for critical security controls. However, there is another strategic perspective that is emerging. We do not ask people to determine what they need in a car to keep them safe. Driving a car is a dangerous activity. Consequently, we say that cars should come with seatbelts and rear view mirrors. That is how cyber security needs to be approached in the future.

Best Practices

Investment decisions are bureaucratically driven. People have to be able to justify spending. The incentives which matter are the ones the market will reward. Market driven tools are needed. The question to study is what might these be? The critical infrastructure sectors are diverse. Some sectors are heavily regulated and others are not. Some sectors are incented through cost recovery for capital investments while others are funded through publicly approved bonds. Recent research has identified four core areas required for building resilience and framing of strategic risk:

- Understanding of the value of investment for operations and for the public
- Incentives to motivate investment and action
- Governance or coordination structures within and across sectors
- Structural engineering design processes, best practices and accepted standards

Social science research is needed to help understand why people are making certain types of decisions. It can assist to identify how desired outcomes as opposed to undesired outcomes are achieved through decisions made. When real events occur, capturing information soon after these events can provide this data. Such data can inform simulations and structural design development, as well as identify motivations and incentives to alter them to achieve the desired outcomes. There are capabilities in the national laboratories which do scientific analysis of personality traits, capability traits and capabilities preventing people from communicating and collaborating effectively.

We cannot measure resilience when we still do not yet know how to recognize it. There are different opinions in the engineering world. A consensus needs to be forged. There is a need for coordination of regional, interdependent infrastructure across the lifeline sectors to be able to plan ahead for response to multiple hazards. In reality, people tend to focus on the most recent hazard.

Methodologies and Tools

The good news is investment is being made in infrastructure[6] and the nation has opportunities to do it right. There is a need to understand vulnerabilities to a whole series of scenarios that are clear and present. One of the real challenges of risk is that the more "crystal ball" one gets, the more money has to be spent. This becomes a disincentive, particularly with limited budgets. There is capacity to do a range of scenarios that are functionally real through modeling with some of the new tools being developed. Much of the data on critical infrastructure right now is in the hands of the national laboratories. There are security concerns of giving too much information out. Bringing in academia, students and researchers will strengthen the nation's ability to solve problems. Academia and the research national laboratories have collected a lot of data, but under the price of silence, which creates an obstacle to innovative thinking through joint efforts.

There needs to be an overarching focus on engineering resilience by design. Research is needed to review vulnerabilities and merge them together in a cross-sector way to identify cascading effects. It translates to new capabilities for speediness of recovery.

[6] National Infrastructure Advisory Council. *Strengthening Regional Resilience*. Appendix E

A core element of what research and development has to accomplish is how to manage cascades and how to confine those cascades. There has been a major proliferation of tools in the last ten years that solve individual problems or provide pieces to a larger risk picture, but not an integrated one. The national laboratories in particular have a unique opportunity to merge expertise and tool sets into a much more comprehensive suite of capabilities that will cross different data streams and sectors to perform dependency analysis and to really produce actionable outputs for the stakeholders.

The national laboratories in the last few years have had to focus on near and real time outputs as required by their Federal customers. There is a certain level of discomfort because of the uncertainty inherent in the subsequent resulting analysis. The national laboratories try to be honest in articulating uncertainty levels. The issue is how to take the national laboratories' models that have been traditionally used for strategic purposes, to focus those on a really short fused, higher uncertainty level, real time analytic output.

Teams of multiple disciplines need to be created in order to perform effective research and analysis. The issues of critical infrastructure security and resilience are complex. These teams, including social scientists, economists, lawyers, public policy analysts, engineers, sector specific operations experts and cyber security professionals need to merge their expertise and knowledge to assist in identifying, analyzing, and testing issues and solutions in a controlled environment. They need to integrate different tools, capabilities and resources to ensure that a construct and adaptation of existing of infrastructure can be created in a most effective manner moving forward. Having the right multidisciplinary teams to work problems together is necessary. We have to have diverse teams working on these problems, social scientists, economics, lawyers, public policy, risk management, decision analysts in addition to computer scientists and engineers.

Data availability: There are challenges with the next level of analysis due to the level and currency of data available. Everyone wants more data and updated more often. The national laboratories have had some very successful small scale assessment of individual clusters of assets because they are able to get very specific. In order to conduct real time interdependency analysis, a different set of data is needed that will transcend the physical or electronic characteristics of an asset element of the system, but into the management practices and environment within which the element resides. It requires the use of significant time and energy to walk through facilities to get the data for comprehensive dependency analysis. There is a need to identify the analytic construct and set of questions that feed real time analysis for any incident.

It is a huge challenge to effectively collect data at a useful but viable scale. There are exciting things going on in regional resilience activities in integrating very detailed climate modeling and predictive analytics for future impacts of climate-driven events. Those are feeding a lot of really

interesting planning scenarios for state and local communities. There is a lot of progress, but a lot of opportunity remains to integrate multidisciplinary climate adaptation models and new thinking in terms of resilient design capabilities. A lot of investment and strategic thinking is needed in these areas. There are pockets of best practices that can be replicated across the nation.

There is an alternate view that collecting data for tools and models may be better by identifying and collecting key data. This observation noted that interdependency analysis and tools are still in their infancy. There seems to be more of a need for real time dashboard during an incident. However the data required accomplishing such real time reporting is difficult to acquire because of the unpredictability of what information may be required for the circumstance. It was also noted that there is a need to develop planning and analytic tools that integrate protection, migration, response and recovery to determine a complete picture of risk. There are already a lot of vulnerability tools.

Such risk assessments may be one way to help drive investment decisions. There are a lot of organizations with high performance computing but that has not tapped into for analyzing infrastructure issues. High performance computing is needed for critical infrastructure dependency analysis. There are thousands of nodes and links.

Public Private Partnerships

Creating and sustaining private-public partnerships across sectors means dealing with significant issues of how each sector is regulated. Each sector brings its own challenges. One of the lessons learned from Hurricane Sandy was how public and private sectors were blind to how each operated. In addition, solutions that may have made sense at one time may no longer make sense now. Building and siting codes are not evolving with changing risk. For example, locating generators in the basement with the advent greater flooding risk no longer makes sense, but a local building code may require that siting for safety reasons that existed historically.

Academia is a source for seating these partnerships. Academics can work across jurisdictions where it can be a problem for government.

Work Force Development

As people move from north to south to warmer climates, cities have rapidly decreasing populations, which puts unanticipated stresses on the infrastructure systems they are leaving, and on the systems they are moving to. There is also a shift from rural to urban. This is an opportunity to explore a higher level of dependencies, by asking: How can urban centers become a central hub for the ingestion for a lot of different capabilities?

It was noted that there is a need to develop skills and create the next generation of engineers and IT specialists. There are embedded systems everywhere. There will be 50 billion devices connected to the internet by the end of the decade.

Common Sector Priorities

Data was collected from a data call to the members on their perspectives for what they considered a priority in each of their own sectors. Some members individually reached out to their own sectors to collect and submit additional information as part of their response. The data collected was organized by the following topics: Strategic drivers for future sector research and development investments; required capabilities and research and development for those capabilities to meet the challenges of the strategic drivers; the role of public private partnerships for research and development. Common priorities and themes emerged from an analysis of the data from across the sector specific input from the members and their data sources. The common themes are summarized in the following.

Cyber Risks – An Expanding Threat Surface

Cyber threats and cybercrime were highlighted as areas of particular concern in majority of the responses by the members. Mission-critical systems are increasingly connected to cyber systems, which is further expanding the range and forms of vulnerability that threaten critical infrastructure assets. A common observation by respondents was that while recent technological advances – such as mobile and cloud computing – have helped to overcome some of the silo-ing of operations that has long complicated operations processes, they have also created additional vulnerabilities in each sector, by blurring the previously well-defined borders of perimeter security models.

Responses also noted that with the proliferation of e-commerce and intelligence data collection, there has been exponential growth in the amount of data in existence, and it will be vital to dedicate research and development toward ensuring secure storage of that information.

With regard to the Energy and Information Technology sectors, it was noted that the Electricity Grid and natural gas pipelines are vulnerable to physical and cyber threats, and that those threats are increasing in source, frequency, and sophistication. To combat these issues, there will need to be better cross-sector communication and coordination; a consistently reliable interconnected system of vulnerability management; threat detection and mitigation; and scalable, efficient response capabilities. Research and development will be needed on incident sharing and analysis; research in cloud and information technology security; advanced cryptography for data

protection; enhanced cyber detection and analysis tools; and machine-to-machine deployment of mitigation measures.

For the Financial Services Sector, recent years have seen the emergence of more sophisticated and coordinated threats. Previously, intrusion attempts were the province of individuals seeking financial gain or the theft of intellectual property. But more recently, there has been a rise in organized attacks focused on the disruption of Financial Services operations and the disruption of other critical infrastructure sector operations which rely on financial services systems. To reduce these vulnerabilities, there will be a need for research and development on more secure payment systems and mobile banking.

Cross-Sector Dependencies – Mutual Reliance among the Lifeline Sectors

As has been noted in previous Council studies, the operability of each of the designated lifeline sectors – Water, Energy, Communications, and Transportation – is essential to the overall functionality of all critical infrastructures. But responses to the data call also highlighted that each of the lifeline sectors are symbiotically reliant on one another for their own continued operation.

A key aspect of any efforts to address these issues will be enhanced, effective, and timely cross-sector coordination, as well as coordination with Federal, State and local governments. Energy and Communications service are essential to the operations of other sectors' operations. But both Energy and Communications services are also reliant on each other to maintain their baseline functionality – in the case of the Energy Sector, Industrial Control System and vulnerability management is dependent on reliable network service; for the Communications Sector, electricity underpins the ability for those and other network capabilities. In addition, the Energy Sector is reliant upon both the Water and Transportation sectors, for cooling and the transit of precursor materials, respectively.

Responses also noted that the Financial Services Sector – while not designated as a lifeline sector – also plays a key role underpinning the efforts of the four lifelines.

Responses also noted the cross-sector need for several future capabilities necessary to protect, strengthen, and restore service for the sectors, including: targeted expansion of electricity backup systems; the development of modular, universally adaptable equipment; a consistently reliable interconnected system of vulnerability management; and research and development on SCADA/industrial control system vulnerabilities.

Regulations and Policy – Addressing the Current Environment

Multiple respondents observed that current regulatory frameworks and national policy have not kept pace with the changing landscape of critical infrastructure security and resilience.

There has been a longstanding interest, on the parts of the Federal Government and private sectors, to establish effective frameworks for information sharing – both within and across sectors, and among and between public and private partners. But, to date, the desire to successfully establish systems and approaches for doing so has been impeded by regulations regarding how data can be shared, and with whom.

It was also noted that the ongoing consolidation of telecommunications and media companies is having a detrimental effect on the ability for the Communications Sector to adapt to and innovate in response to the evolving challenges facing the industry, such as the impending need to share the limited space available on the Radio Frequency (RF) Spectrum for wireless communications; the establishment of an interoperable communications system for use in emergency response efforts; and public education and outreach efforts. Because this has limited the capability of smaller, entrepreneurial companies to contribute to the resolution of these issues, there may be a need for more vigilant review and management of industry consolidation, as well as incentives promoting the inclusion of small businesses in the research and development process.

Aging Infrastructure – In Need for a Coordinated Approach

A common concern for both government and the private sector is the effect that aging infrastructure have on the overall resilience of sectors. Respondents from multiple sectors highlighted the challenges that owners and operators face in attempting to repair and replace systems and assets that are at – or past – the end of their useful lifespans, and carry substantial capital requirements to address. As a result, respondents indicated that there will be a need for public-private partnership to assist with the mitigation of this challenge.

For the Transportation Sector infrastructure, there is an urgent need for a national vision and commitment to repairing and replacing aging and failing assets. Transportation infrastructure affects the ability of nearly all other sectors to execute their missions, and as such plays a key role in the Nation's economic prosperity. But to date, there has been a lack of will, or a lack of consensus, on how to address the short- and long-term work that the sector needs to remain functional. In addition, it is expected that the Nation's transportation assets will be further strained over the coming quarter-century, as a 20 percent increase in passenger transit – an additional 66 million people – is expected in that time period.

In the Water Sector, responses noted that many systems are in need of repair, and key pieces of distribution networks are well past their useful lifespans, and need to be replaced. But because of the costs associated with replacing miles of old pipes, repairs and replacements have been deferred by many municipalities.

In the Energy Sector, responses noted that efforts have begun to pool resources and establish mutual aid. But because those programs are still in their infancy, a major disruption to the Electricity Grid would also prove disruptive to those programs.

Public Awareness – A Need for Better Understanding and Preparation

Another issue raised by multiple respondents was that the public is, generally speaking, not aware of the vulnerability of critical infrastructure. Because of this, there is considerable concern the public would not only be unprepared for a systemic failure in one or more sectors, but would also be unlikely to trust in those systems even after restoration, contributing to a general sense of chaos and instability.

To address these issues, respondents noted that there will be a need to commit research and development to establishing better community resilience – such as in the post-Superstorm Sandy community-based focus on neighborhood self-support – expanding community communications; raising understanding of national, regional, and local event resilience plans; and on the expansion of city/county emergency drills.

The Energy (specifically the Electric Sector) Communications and Transportation sectors were all highlighted as major, nationally significant dependencies key to the continuity of operations of critical infrastructure assets, with electricity and communications capabilities each mentioned by multiple respondents from multiple sectors. Multiple responses emphasized the importance of better coordination and communication across sectors, as well as cross-sector collaboration on the detection, mitigation, and remediation of vulnerabilities and threats; operating in a resilient manner; and coordinating and testing communication and response capabilities in threat scenarios. In addition, as part of those sectors' Nationally Significant Priorities, there will be a need for research and development on cyber vulnerabilities related to the security and resilience of assets.

With regard to the Electric Sector, multiple respondents highlighted the destabilizing effect that an attack aimed at, and succeeding in, a long-term disruption to the Electricity Grid could have, as a large share of essential systems – including water, power, supplies and personal communications -- are tied to the grid. Adding to this challenge is that since national security is the province of the Federal Government, rather than individual corporations, the case in favor of expending the resources and effort required on the part of Electric Sector entities to achieve resilience in the grid without Federal support is a difficult one to make.

In addition, a key driver for many of the priorities provided by members was financial concerns. For the Communications Sector, better computing capability in more compact machines allows for greater throughput and bandwidth, and wider broadband access would provide greater

opportunity and capabilities for small businesses and individuals nationwide. For the Chemical Sector, though enhanced Transportation Sector assets would enhance efficiency and provide greater resilience against cross-sector dependencies and cascading vulnerabilities, the research and development requirements of the recommended priorities would be unlikely to meet the threshold for investment by either sector.

Relevant Programmatic Perspectives by Key Sectors

Perspectives specific to various sectors provided by individual members through a call for information to the Council at large were provided. This summary incorporates additional sector specific perspectives received through interviews and other sources.

Financial Services

Perspectives provided for this sector included strategic issues having an impact on the sustainability of business operations primarily focused on cyber security:

- Cyber-attacks and advanced persistent threats
- Dependency on electric power & telecommunications
- Increasing use of mobile communications
- Cyber Risk and Global Instability

Future capabilities needed to address these issues include:

- More secure payment systems
- More secure mobile banking
- Investment in technology and contingency planning

More improved information security for payments and mobile banking services are needed without increasing costs dramatically and threatening business profitability.

These capabilities and the research and development to support them are nationally significant for this sector. Research and development can be conducted internally within the industry, primarily in partnership with universities.

A common yet non-competitive threat would drive a need for joint investments across industry or with the government. The need for capitalization at a national level, protection of assets across the industry, global effectiveness, and competitiveness are the characteristics and the principle framework for such joint partnerships.

One observation noted that there is little manual back up now for electronic based processes. There is a perspective that financial services have become overly dependent on technology, but there may be little choice given the speed and efficiencies required on a global basis for financial transactions. If operations fail to function for a period of time due to cyber disruptions, it would be thought of as a fundamental failure of the system, more so than for a physical disruption. If the public was not able to access their accounts for ten days, it would be a huge issue because confidence would be lost in the financial system itself. The financial services system is based on trust.

Companies are afraid to talk about these topics because of their fear of being seen as collaborating on pricing. If there is a way to give companies a safe way to exchange points of views on these system wide issues, that would be a great benefit to the whole financial system. A number of leading universities could provide the means to convene discussions on these topics.

The Sector through its Sector Coordinating Council produces a periodic report on Research and Development priorities for the financial services sector. (See Appendix C for link to a copy of the document.)

Chemical

Secure and sustainable business operations in the chemical industry, both short and long term, require collaboration within the sector and with it's extended a value/supply chain, such as Transportation and Energy. The sector includes large and small companies and their communities that seek to continuously improve their ability to operate in a move volatile external environment. Consequently, the sector also needs to address the issues of small companies and their ability to keep up with required security and resilience capabilities.

Future needed capabilities include the development of next generation transportation equipment, specifically rail, truck, passenger cars and ships. Possible research and development opportunities to address these proposed capabilities include next generation rail cars, cargo tracking, congestion management of key bottle necks in country, and simple models of effective cyber security protection for small critical infrastructure operators. All of these research and development opportunities require cross-sector and government engagement.

The Chemical Sector's major dependencies on other sectors include transportation (ports, rail, and truck), energy, communications and waterways. For research and development, the sector benefits from continued improvement in areas such as emergency response to supplement local capability, and congestion management. All of these capabilities are nationally significant; economic impact and national safety being the drivers for this consideration.

Many of these capabilities, such as rail car design, positive train control, traffic control systems, and emergency response systems, may be so difficult to develop. They will need to be addressed

through joint efforts with government and other sectors. The following factors should be considered in prioritizing investments in research and development: Inter-sector dependency, cascading vulnerability, and short term economic factors.

Current regulatory bodies in some of these industry segments are not structured to accept research outside of their normal regulatory process. Characteristics that might enable joint partnerships across industry or with the government include a targeted national objective and a balanced oversight of how research will be prioritized based on technology costs/impact.

Water

Strategic issues with an impact on the sustainability of business operations in the water industry for both the short and long term include:

- Vulnerability, to the dependency of home/work distribution and collection of sewage following an event --- e.g. if power goes out, people get out candles, but if the tap is dry and/or the toilets don't flush, people, especially in a large urban area would be more likely to panic.
- The general public has grown to expect clean water and sewage collection. With little recent historical problems coupled with systems, which are largely hidden and out of sight, there is a general lack of knowledge of the vulnerability of water supply and wastewater collection systems. A good way to remedy this is to start with education on the systems and their independent resiliencies. Additionally, recent history, such as the event of Hurricane Sandy, demonstrated how well the local agencies were able to keep pump stations running and sewage flowing.
- Following 9/11, there were communications with many water supply agencies focused on the potential poisoning of our water supply systems. Many agencies beefed up security. Generally, it would take tanker trucks of poison to contaminate a large reservoir of supply. The smaller, coordinated, targeted events at multiple locations could disrupt water supply or sewerage treatment and disposal. This could create immediate distrust of traditionally well run systems, with short and long term resiliency ramifications.
- Other than operators in the Sector, little is known about the multitude of various agencies, even multiple agencies in one county or region that provide wholesale, retail water and collect untreated, potential toxic water, and wastewater.

Future capabilities needed to address risks to this sector include educating existing agency sub-departments that already focus on community communications on national, regional, and local Event Resiliency Plans. Additionally, many large urban areas, which hold "city" or "county" emergency drills for events should include water and wastewater agencies in those drills. Energy

and Communications are obvious sectors that impact, for example, large water pumping stations; most agencies also have backup generators specific to each system.

Research and development for this sector needs to include requirements to incorporate resilience and security into the status of their infrastructure and their respective Capital Improvement Plans (which are generally required by law). Many of the systems, especially underground, have old infrastructure and due to reasons including financial constraints, repair/replacement has been deferred.

Of the capabilities required by this sector, some may be so difficult to develop that joint efforts with the government and/or other sectors may be required to address them. Joint efforts could include EPA, Communications, and Energy Sectors on sharing "Big Data" and new technologies, especially in the areas of usage and detection. It was noted that current security efforts are somewhat misguided in their focus. Since the September 11, 2001 attacks, the approach has been predicated on protecting water against poisoning, though it was noted that the quantities of contaminants needed to achieve that goal would be prohibitively difficult to obtain and deploy. But while that form of threat would be unfeasible and unlikely to succeed, a series of coordinated and targeted events and multiple locations could effectively disrupt water supply and sewage treatment.

Prioritization for this sector's research and development needs to focus on the latest technologies, engineering design and "big data" sharing. It will likely require multiple agency involvement, such as coordinating with some of their National Professional Groups headquartered in Washington DC (e.g. National Clean Water Agencies (NACWA), etc.). Factored into the priorities that should be areas which are most subjected to Man-made or Natural Events.

Public – Private Partnerships are used in this sector, to some degree for engineering and construction Project-by-Project level support and, to a more limiting degree, operations. Most operations and major decision making are done at the local government level (Department Level General Manager reporting to a Mayor, etc.).

Communications

The Communications sector requires increased efficiency to be profitable in a commoditized market. Continued investment in infrastructure improvement is essential for long-term sustainability of operations. Sophisticated new requirements in telecommunications are driving an evolution toward development of new technologies offering greater throughput, usage versatility and lower cost. To meet this demand, providers need to diversify or convert their service portfolios to include the new technologies and package offerings into niche solutions,

enabling enough margins to be built in to ensure operations and long-term company sustainability. The challenge is identifying niche solution requirements, creating products and services to meet them, and successfully competing to secure the new business. The business model is complex with much inherent vulnerability for the service provider.

A concern is the rapidity of technological changes that constantly make this year's model obsolete. In the long term, the concern is the ability to fund research and development when smaller, low profile, high throughput, ruggedized satellite communications, and wired and wireless delivery systems innovations are called for by the federal government to support the work protecting and ensuring the resiliency of our nation.

Management of consolidation within the telecommunications and media industries, the assurance of competition and a role for smaller, entrepreneurial ventures remains a challenge. The massive sweep of large mergers and acquisitions has put too much control into too few hands. Diversity in itself can provide a measure of resilience and security. The risk of a monotone voice in today's media and communications is greater than ever, particularly if Internet regulation increases beyond reasonable measures; a move which could stifle innovation. In addition, the availability of data and data security are essential.

Future needed capabilities include:

- Artificial intelligence and virtual systems --- new capabilities do not have to make current investments obsolete.
- The capability for efficient network resource sharing, including spectrum and spectral efficiency. The ability to share the finite resource of radio frequency spectrum has yet to be developed, but is essential to allow the highest and best uses of information access in the coming decades. Delivery systems compatible with the new data payloads.
- Secure storage and analysis of the data to correlate the various sources of structure and unstructured data into usable information for mitigation of threats.
- Development of predictive analytical tools to search all forms of data in an environment that will allow human analysis of aggregated data to identify threats and mitigate risks to the infrastructure.
- Large data analysis
- Predictable metrics
- Smart systems that are self-healing and self-protected from cyber-crimes and extensive cyber-attacks,
- Unbiased research to fairly characterize the regulatory needs of our nation relative to the telecommunications and media industries.

The promotion of entrepreneurial ventures and innovation in the telecommunications and media space can greatly improve the research and development of these capabilities. For this to occur, more vigilant management of conditions around consolidation will be necessary along with incentives for small business inclusion in the space.

The communications sector has major dependencies on other sectors that include energy and logistics.

Since 9/11, it has been clear that emergency communications and information distribution are key needs across state, local and federal levels. While there have been steps taken to organize such investments, very little progress has actually been made in achieving nationwide interoperable emergency communications. FIRSTNET is a joint project to support this capability. It is in its initial stages.

Emergency Services Dependency on Sector: A fundamental premise is that first responders and those who are responsible for critical infrastructure, specifically public utilities, need to be supported by the best technology available. It needs to be more secure and more reliable. It needs to not be subject to easy compromise by hackers.

To deliver these capabilities inherent in this requirement, there needs to be a complete integration with the commercial sector. The commercial sector drives innovation. A public-private partnership in this area must develop a structure that completely integrates government requirements into the private sector. There are successful examples outside of the country. There has to be an agreement reached that share risks. In sharing risk there has to be an agreement of a shared upside for the private sector.

There is an element of the commercial world that is always fishing for, adopting and expanding new technology. Government does not operate that way. So, to support such a capability, there needs to be a combination of government supervision and control, nationwide standards, compatibility etc. so they can communicate seamlessly when something happens. The devices and protocols need to be integrated. It's more than money, there needs to be a long term Private/Public Partnership that is funded and operates in a way that the talent running the system that supports first responders is equal to the talent running technology. Research and development that identifies the characteristics of successful partnering and the attempts to tailor that to this situation would be effective use of public dollars. There needs to be some kind of consensus on what is needed for success and to avoid failure. The most important element is risk sharing. Government's instinct is to take no risk. It's a very political environment to get public-private partnerships to work.

Research on creative financing for infrastructure investments is needed. Competition spurs innovation. There is not much in fundamental technologies. Anyone who thinks that they know what will happen in technology in a few years is wrong because innovation turnover is so rapid.

Electricity

The vulnerability of the grid and the gas supplies to power plants to both physical and cyber-attack, growing in number and sophistication, in a changing geo-political landscape, impacts the sustainability of operations. The potential for serious disruptions will grow for years to come. In the context of the electric power system, strategic risk issues include a number of high-impact, low frequency (HILF) events that could result in significant impact not only to the electric sector but the entire U.S. economy. Resiliency is the ability to harden the system against – and quickly recover from – HILF events that can severely damage generation, transmission, and distribution systems, as well as interdependent systems such as natural gas pipelines and other fuel transport, and telecommunications. HILF events, that create strategic risk issues, include the following:

- Coordinated cyber or physical attacks
- Coordinated physical and cyber attacks
- Advanced persistent threats
- Electromagnetic pulse (EMP), high altitude EMP (HEMP), and intentional EM interference (IEMI) attacks
- Disruption of voice and data services
- Severe weather or natural events
- Pandemic
- Supply Chain Disruption or Compromise
- Catastrophic Human Error
- Insider sabotage
- The remaining unknowns regarding cyber threats, vulnerabilities and associated interdependencies

Other strategic risk issues include the availability of transportation for electricity replacement components, workforce and fuel during catastrophic disasters; and the impact of variable distributed generation assets on the stability of the grid.

Future capabilities needed to address these issues include greater cross-sector communications and coordination, tested against threat scenarios. There may be a tendency for other sectors to seek more emergency electricity backups, and in some applications, but not all, this may be appropriate.

Recent extreme weather events – including U.S. hurricanes, and the Tohoku earthquake and tsunami in Japan (often called the Fukushima disaster) – have demonstrated the need for resiliency. However, extreme weather has occurred as long as the power system has existed. Other trends and events in the last decade – with profound pace and scope – have increased the risk associated with HILF events and their potential impact on society, and hence, further shaped the need for enhanced resiliency. For the 2020 and beyond view, the vulnerability to cyber security attack is probably the most severe risk facing the electric sector as both individual criminals and rogue states increase their capabilities to disrupt the power system and other interdependent systems.

To address these issues, capabilities needed by the sector include:

- Enhanced data sensing, collection and analysis of grid interruptions
- Secure information sharing capabilities
- Improved sharing and coordination between federal agencies, owners and operators, and states.
- Smarter grids, smarter self-securing and healing control systems, integrated grids, and energy delivery system devices
- Enhanced cyber security tools, methodologies and approaches
- Enhanced transportation coordination capabilities, particularly under catastrophic disaster circumstances
- Robust capability sharing programs among utilities
- Better protection, transportation of natural gas supplies
- More flexible, adaptable regulatory and market models
- Improvement in storage technologies
- Advancements in grid integration
- Better predictive capabilities on the availability of intermittent renewable resources like solar and wind power
- Predictive threat modeling
- Damage assessment modeling
- Machine to machine information sharing of threat indicators and automated integration with existing controls
- Capabilities that enable security solutions to continue operation during a cyber-attack
- Self-configuring energy delivery system network architectures

Enhanced resiliency of the power system is based on three elements: damage prevention, system recovery, and survivability (see Figure 1). The development of capabilities, such as tools, methodologies and information, must be structured across three related elements which

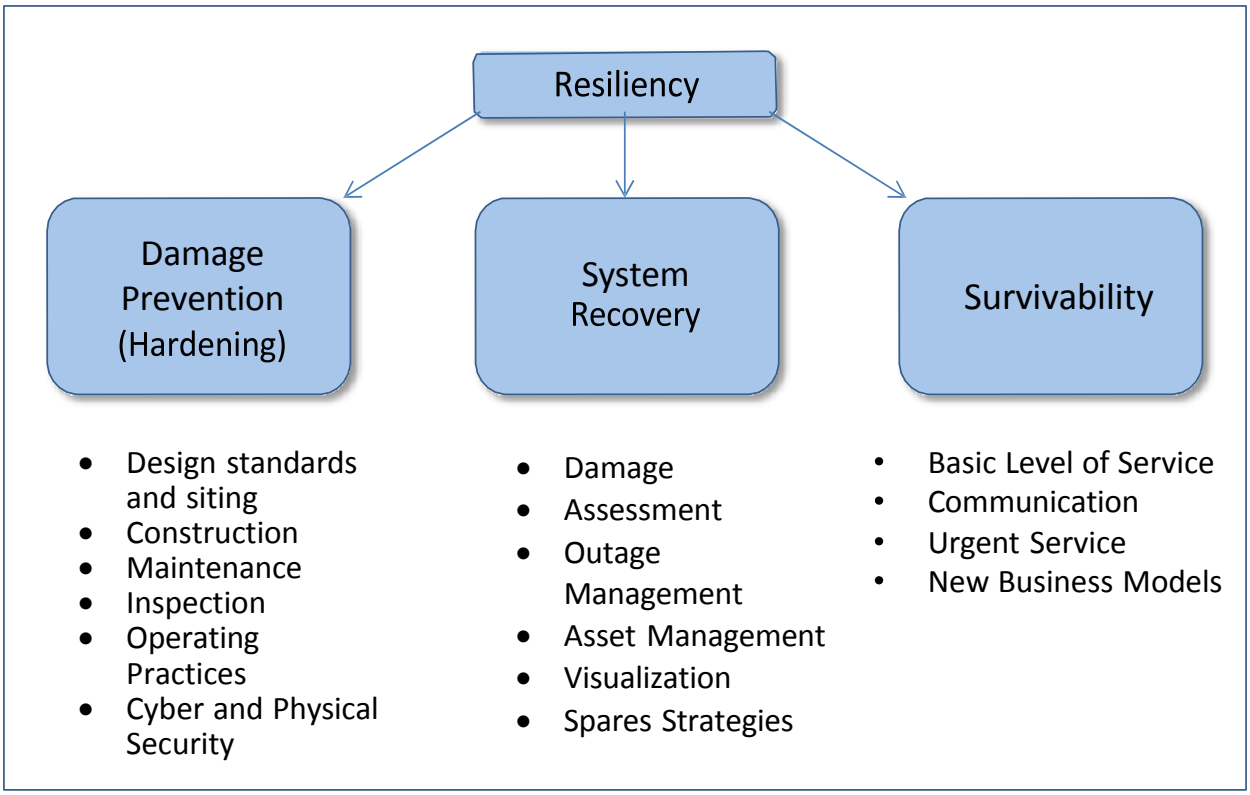
together contribute to the overall resiliency of the electric power system.

Damage prevention: Refers to the application of engineering designs and advanced technologies that harden the power system to limit damage. The foundation for resiliency involves hardening the system to prevent damage through changes in design standards, siting, construction, maintenance, and inspection and operating practices. An energy company's approach to these changes can be adapted to its specific system and work environment. Research and development that could enhance the adoption of these changes include:

- Developing and deploying cyber security detection measures and isolation/restoration response capabilities
- New materials and coatings to enhance the physical security of power plants, transmission systems, and substations against attack
- Materials and design research to reduce the cost of selective undergrounding of T&D facilities
- Research to better design and reinforce overhead lines
- Pre-emptive operating practices upon the approach of a threat
- New ways for utilities to approach the design of systems and workforce training

System recovery: Refers to the use of tools and techniques to quickly restore service as soon as practicable.

Survivability: Refers to the use of innovative technologies to aid consumers, communities, and institutions in continuing some level of normal function without complete access to their normal power sources. This involves the ability to maintain some basic level of electricity service to customers, communities, and institutions when they do not have complete access to their normal power sources. Key to survivability is the effective facilitation of enhanced communications with customers. Research and development should focus on the use of distributed generation options such as plug---in electric vehicles (PEVs), fuel cells, photovoltaics, and high-efficiency generating sets to enable urgent service to cell phones, traffic lights, hospitals and prisons.



[7]

Figure 1
Resiliency Consists of Damage Prevention, System Recovery, and Survivability

Improving the power system's resiliency requires advancement in all three aspects. The most cost-effective approach combines all three.

Of these capabilities, some may be so difficult to develop that joint efforts with the government and/or other sectors may be required to address them. For key equipment like transformers, there is already some effort by the Department of Energy to develop new types of modular equipment that can be universally adapted. However, the "spares" needs are so capital intensive that some type of financial assistance will be needed.

Because of the interdependencies between the multiple infrastructure systems; including electricity, natural gas, water and telecommunications systems; research coordination on cyber and physical security is critical. Prevention, isolation and recovery technologies and methodologies could be applicable across all the interdependent infrastructures and minimizing the risk/impacts to one system benefits all the systems as well.

[7] Provided by the Electric Power Research Institute

Coordination in the development of advanced outage management systems may also be beneficial to all the interdependent infrastructures. This is especially needed in the increased operational interdependency between the electricity grid and the natural gas grid as an increasing percentage of new generation is natural---gas based.
Storage technologies also provide an opportunity for a joint effort as they are far from commercial feasibility but could transform the industry and significantly improve the resilience of the nation's electric grid because of the opportunities to reduce fuel consumption and integrate more renewable energy sources.

Communications and Natural Gas are key needs for the electricity sector, with Transportation potentially key also. It is clear that electricity is central for critical infrastructure resilience. In particular, the key life line sectors of finance, communications, and water.

Greater cross-sector communications and coordination, tested against threat scenarios is needed to manage the risks of these dependencies on the sustainability / resilience of business or sector wide operations. All of the essential services systems in the United States are highly dependent on reliability of the electricity system. Therefore, the resiliency of the electricity system is nationally significant. Any loss in availability of electricity not only impacts the financial aspects of nearly all business, but also the well-being of the public. Social order can be challenged when electricity is lost for an extended time.

Cyber security tools and technologies have high priority since such threats and vulnerabilities are increasing and morphing at light speed making it difficult for industry to address without assistance.

Another high priority should be the development of enhanced capabilities to prevent and recover from cyber and/or extensive physical security events.
Advanced damage assessment modeling through various technologies such as radar, Light Detection and Radar (LiDAR), satellite, etc. would be helpful. This priority is due to the extensive level of attacks currently occurring to the electricity grid and sector, even though these attacks generally have be mitigated successfully to date.

Capabilities to prevent against electro-magnetic pulse (EMP) or similar attacks are also important due to the potentially broad nature of the impact to the electricity grid, even though such events may be very low in possibility of potential occurrence. This also requires active interaction with agencies of the federal government.

The top three research and development priorities for the electricity sector, by agreement are:

1. Machine to machine information sharing of threat indicators and automated integration with existing controls

2. Capabilities that enable vendors and asset owners/operators to assess and mitigate cyber supply chain risk
3. Innovative solutions to speed up restoration and recovery of damaged transmission and distribution equipment

In discussions with other sectors, the first two priorities are shared by other critical infrastructure sectors.

On public-private partnerships, within privately owned and operated companies, it is not consistent with "fiduciary responsibility to shareholder interests" for companies to plan and provide for events which are "an act of war and the responsibility of the government to preclude". Companies are not responsible for "national security".

Some "pooling" of assets and resources is in place, and a program of "mutual aid" is in place. The electric sector pools its research dollars through the Electric Power Research Institute (EPRI) and leveraged with other research funding. A severe and potentially continuing attack to the grid would deplete and freeze investments as each company worries about its own near term needs.

Only a severe attack would encourage joint investments across industry or with the government. The inability of individual businesses or an individual sector to address a vulnerability or increase resiliency without the cooperation/collaboration of government or another sector could also drive joint investments.

The characteristics / principles framework for such joint partnerships might include:

- Shared value proposition
- Engagement of the right levels of individuals and including senior-level executives
- Trusted relationships
- Efficient organizational structure which optimizes the contribution of participants

The success of joint research and development partnerships also require the characteristics of:

- Establishment of clear objectives and goals
- Transparency of intent among partners in setting objectives
- Strong lines of communications across the partners
- Strong, pro-active management of the programs

Transportation

The following strategic issues were identified in the data gathered on the sustainability of business operations in the transportation industry for both short and long term:

- Urgent national infrastructure crisis (impacting all of the critical infrastructure sectors, including transportation) – not broadly understood nor appreciated by the general public – lack of will/consensus to address – maintenance and expansion are necessary to accommodate an additional 20% growth (66 million people) in the next 25 years
- Performance of our transportation system is not reliable or resilient (all modes) – yet they are key to US economic prosperity, competitiveness and overall quality of life
- Lack of a national transportation vision, plan and/or funding/investment strategy (ies) tied to outcomes and performance measures
- Continued lack of multi-modal and cross sector planning for resilience and recovery at all levels
- Inadequate attention to the significant demographic shifts, impacts of seriously aging infrastructure, the impacts of climate change on transportation infrastructure, modernization and security needs for IT infrastructure/information systems coupled with the continued explosion of new technologies (and associated vulnerability to security threats and risks – including cyber vulnerability), critical workforce challenges and shortages at all levels, particularly in specialty operations, maintenance, engineering and technical areas– current and future workforce
- Outdated institutional and regulatory frameworks (i.e., governance structures, need for greater coordination within and across jurisdictions, coordination within and across functions and modes/sectors, public-private-nonprofit partnerships, barriers to incorporating innovation from the private and non-profit sectors, performance management)
- Focus on transportation sector's critical role in ensuring access to opportunity/impact on social societal outcomes – i.e., equity, affordability, livability

Future capabilities needed to address these issues include:

- Urgent, bold and sustained public information, education and advocacy re: the criticality of transportation (infrastructure) investment
- Increased US investment in top notch Research and Development -- major effort needed to define appropriate performance measures, develop consistent, valid indicators, and support data collection – quality research and analysis is key to national leaders having the information to make good decisions
- As technologies become increasingly automated and complex, the task of integrating the human with technology deployment is essential
- Significantly increased US investment in "people-readiness" across the transportation sector – at all levels – a coordinated national focus is needed involving the Departments of Labor, Education and Transportation

- Resolution of the national policy debate re: our national transportation vision; consensus on prioritization; who pays – in what proportion -- and how is critically needed
- Concerted funding is required not only in Research and Development – but also in technology transfer and deployment/pilot programs – with incentives for private/non-profit sector participation and innovation

Some examples to illustrate potential requirements include:

- Planning for adaptation, accompanied by an analysis of alternative strategies, to guide policy decisions about protecting/located vulnerable transportation assets of regional and national significance
- New vehicle technologies – navigation and entertainment systems, autonomous vehicles, and increasing driver distraction challenges
- Lessons learned and best practices re: developing and sustaining a safety culture
- Deeper understanding of the effects of changing energy supply, geographic shifts in oil and gas supply, changing American preferences for urban lifestyles etc. -- in relationship to congestion mitigation, reduced energy consumption and emissions reduction
- Use of information technologies, social media, transportation demand management strategies – flex schedules, telecommuting etc. as a strategy to cost effectively reduce travel and provide more efficient travel options
- Reducing the number and severity of commercial motor vehicle crashes and related fatalities and injuries – enhance the safety and efficiency of CMV operations by implementing safety innovations (identify, develop, test and deploy) innovative roadside and on-board technology solutions and practices
- Minimizing risks associated with the transportation of hazardous materials
- Finding ways to increase the number of people and goods able to travel on different road types
- Investment in the development, testing and deployment of low emissions and no emissions vehicles to promote clean energy and improve air quality

The ability to effectively move people and goods has major implications across all sectors. Transportation accounts for two-thirds of US petroleum consumption and drives the demand for oil imports – national consensus will need to be achieved on best ways to sustain benefits of transportation while reducing emissions.

Capabilities needed to manage the risks of these dependencies on the sustainability / resilience of business or sector wide operations in order of priority, include:

- Adequate and predictable transportation funding/investment – including research and development
- Comprehensive workforce development strategies – "people readiness" to support quality national transportation system
- Consensus on national transportation outcomes (multi-modal) and cross sector performance measures

The current sources of federal transportation funding (e.g., the major funding source for surface transportation is motor fuel and other highway use taxes that support the Highway Trust Fund) are eroding. There is a critical need to identify alternative viable and sustainable options to sustain the transportation industry, and ultimately major changes in transportation spending, revenues, or both will be needed to bring the two into balance.

The research and development process would require a multi-pronged approach that may include a nationwide workforce development strategy committee led by the Research & Innovative Technology Administration (RITA), or another credible transportation research center. This effort would require an ongoing collaboration between the key national transportation and professional organizations that will develop inputs and outcomes for improved workforce development (e.g., expanded training partnerships between transportation entities and educational institutions).

Research and development must first confirm that existing transportation performance measures are currently aligned with the goals and objectives they were originally paired with. Then, research and development would direct a comprehensive analysis that must be performed on the existing processes in order to identify inherent and necessary correlations between sectors. These measures will serve several purposes, and may be used to recognize and assess problems; evaluate and compare alternative improvement strategies; and develop quality and control measures, and conduct monitoring to evaluate effectiveness.

Of these capabilities, consensus on national transportation outcomes, cross sector performance measures and adequate and predictable transportation funding/investment are most nationally significant although consensus and comprehensive workforce development strategies will require joint efforts with government or other sectors.

Funding and comprehensive workforce strategy directly impact transportation sustainability in all facets; a consensus outcome is a vital requirement to gauge the sector's resilience to threats and vulnerabilities both individually and collectively. Consensus and funding are issues that impact all the modes; a comprehensive workforce has an equal impact and is important, but its magnitude may vary depending on the mode, sector, or state.

From a research perspective, the biggest issue right now in transportation is cyber security. The areas that need the most research are control systems. Aviation is good in this area, but most other modes are lacking. This will be more critical with more automation in private vehicles. Unmanned aircraft systems will surpass manned by 2035. The transportation sector is dependent on the Global Positioning System (GPS), which has vulnerabilities and risks. GPS is very susceptible to jamming and spoofing. Navigation is a big issue. The timing signal is another one

Research will be needed to examine the impacts of automatic systems. If there is any failure we have to make sure it happened in a safe manner.

There is limited understanding of what the long term impact of climate change and severe weather will be on transportation. Sea level rise and other occurrences need to be studied in terms of transportation infrastructure and operations nationally. A lack of real understanding on the dependence of transportation on energy and communications is a major issue. There has not been very much work done in what the true risks is if transportation infrastructure loses energy or communications for a period of time. Contingency planning for dependencies on other sectors has been limited.

There needs to be research on how to replace transportation infrastructure cost effectively, without disrupting daily operations. The replacement of the Minneapolis Bridge is an example of how structures can be built with an expedited approach, at the same time minimally impacting the daily flow of the public. Infrastructure risk is not just losing and replacing the structure, but consequence to operations. All the sectors need designs that can be implemented quickly, but also processes. In Minnesota they had expedited procurements and environmental policies that allowed them to acquire and build that bridge quickly. It had one of the best intelligent transportation systems. There's a whole network of sensors in the roadway to monitor the highway system to keep track of conditions and demands. The sensors are based on networking and communications that need to be secure.

There is a real and growing lack of expertise in transportation in both cyber and operations. It's not just in security, but the interrelations between them. All types of risks to be managed will need availability of expertise: safety, reliability and security. A workforce development strategy/framework to support the framework for cybersecurity should be developed. Another need is modeling and simulations so recovery can be prioritized from any kind of hazard. In New York City in Hurricane Sandy the port was out of commission and they did not have a good plan to divert the cargo.

Results of any interdependency work in terms of transportation have been limited to non-existent. The American Association of Railroads did a study on how long different industry sectors could operate if rail lines went down. There does not appear to be comprehensive work

done otherwise. It's a big gap. In terms of national significance, some industries dependent on transportation systems can go for two weeks; others start having lapses in less time. As infrastructure gets rebuilt, it needs to be made smarter. Increasing the fluidity of cargo flow to make things more efficient is a top priority. Understanding is needed on how resilient the supply chain is.

Research on effective partnerships is needed. The sector needs a systems view, but the cultures and operations are so different. Each mode has a pretty good relationship with their stakeholders but they don't talk to each other very often. They need to integrate resilience into structural planning and cross-modal interdependencies. Partnerships would support coordination and a cross sector view.

Requirements to Address Pandemic-Dependency on Health Care

Availability of workforce is essential to sustainability of critical infrastructure operations. The approach to risk assessment, preparedness, response and contingency planning, although requiring tailoring for specific operational norms, are common across the critical infrastructure sectors. The current Ebola situation illustrates the need to have a more effective way to find people who are infected. Critical infrastructure service providers need a certain amount of people in order to maintain operations. It must identify that critical group of people. This could mean that an institution must plan to have exercises using hypothetical situations as a means to identify gaps and develop plans.

Biological hazards happen every day. There is experience dealing with them in a contained way. A pandemic can occur on such a huge scale that it can overwhelm the system.

When people are so fearful that they refuse to come to work it becomes a big problem. Managing humans as well as technology is important. If there are ways to be confident and protected, the fear factor can be handled better. If certain capabilities and procedures are drilled and practiced, fear can be minimized. No research and development appears to be required for how sectors outside of the healthcare sector to address the issue of pandemics.

Appendix C - Reference Papers Utilized

Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security – Research and Development Committee 'Research Agenda for the Banking and Finance Sector' (Update)

Overview

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) supports research and development (research and development) initiatives to enhance the Sector's resilience and integrity and to protect both the physical and electronic infrastructure of the Banking and Finance Sector, and its customers.

The FSSCC established the Research and Development Committee ("research and development Committee") in 2004 as a standing committee to:

1. Identify needs and priorities for research relevant to significantly improving the security and resilience of the Financial Services Sector.

2. Engage the research community (including academic institutions and government agencies) to help them better understand the needs and environmental constraints of the Financial Services community.

3. To identify and help to transition promising research to operational deployment.

4. To coordinate all these activities on behalf of the Banking and Finance Sector.1

This research agenda is the research and development Committee's vehicle to communicate the research needs of the Financial Services Sector to the research community. It is envisioned as a "living" document to be updated periodically to reflect changes in the financial services operational environment; the changing threat; and advances in technology.

This document is the third one of the same title. It represents ongoing efforts of the financial industry to ensure that research and development priorities support the objectives of national infrastructure protection plans. This update reflects changes in the FSSCC Threat Matrix, as well as changes in both technology and operational environments. Similar to its predecessors, it incorporates valuable input from the Government, Academic and Industry research community. It describes the Sector's environments, threat, and research needs, and provides guidance in the evaluation and validation of promising research and development. FSSCC support for research and development entails provision of domain expertise to support researchers who profess to be addressing the sector's present and future needs for critical infrastructure protection. Where research and development is deemed by the FSSCC to align with this agenda, the FSSCC may be

expected to take an active role in the transfer of such research and development to operational use.

Deloitte – 'Measuring Facebook's economic impact in Europe'

https://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/TMT/uk-tmt-media-facebook-europe-economic-impact.pdf

Cisco – 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018'

http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

Executive Summary

The Mobile Network in 2013

***Global mobile data traffic grew 81 percent in 2013**. Global mobile data traffic reached 1.5 exabytes per month at the end of 2013, up from 820 petabytes per month at the end of 2012.*

***Last year's mobile data traffic was nearly 18 times the size of the entire global Internet in 2000.** One exabyte of traffic traversed the global Internet in 2000, and in 2013 mobile networks carried nearly 18 exabytes of traffic.*

***Mobile video traffic exceeded 50 percent for the first time in 2012.** Mobile video traffic was 53 percent of traffic by the end of 2013.*

***Over half a billion (526 million) mobile devices and connections were added in 2013.** Global mobile devices and connections in 2013 grew to 7 billion, up from 6.5 billion in 2012. Smartphones accounted for 77 percent of that growth, with 406 million net additions in 2013.*

Globally, smart devices represented 21 percent of the total mobile devices and connections in 2013, they accounted for 88 percent of the mobile data traffic. In 2013, on an average, a smart device generated 29times more traffic than a non-smart device.

***Mobile network connection speeds more than doubled in 2013.** Globally, the average mobile network downstream speed in2013 was 1,387 kilobits per second (Kbps), up from 526 Kbps in 2012.*

In 2013, a fourth-generation (4G) connection generated 14.5 times more traffic on average than a non-4Gconnection. *Although 4G connections represent only 2.9 percent of mobile connections today, they already account for 30 percent of mobile data traffic.*

The top 1 percent of mobile data subscribers generated 10 percent of mobile data traffic, down from 52percent at the beginning of 2010. *According to a mobile data usage study conducted by Cisco, mobile data traffic has evened out over the last year and is now lower than the 1:20 ratio that has been true of fixed networks for several years.*

Average smartphone usage grew 50 percent in 2013. *The average amount of traffic per smartphone in 2013 was529MBper month, up from 353 MB per month in 2012.*

Smartphones represented only 27 percent of total global handsets in use in 2013, but represented 95percent of total global handset traffic*. In 2013, the typical smartphone generated 48 times more mobile data traffic (529 MB per month) than the typical basic-feature cell phone (which generated only 11 MB per month of mobile data traffic).*

Globally, there were nearly 22 million wearable devices (a sub-segment of M2M category) in 2013 generating 1.7 petabytes of monthly traffic.

Globally, 45 percent of total mobile data traffic was offloaded onto the fixed network through Wi-Fi or femtocell in 2013. *In 2013, 1.2 exabytes of mobile data traffic were offloaded onto the fixed network each month. Without offload, mobile data traffic would have grown 98 percent rather than 81 percent in 2013.*

Per-user iOS mobile devices (smartphones and tablets) data usage marginally surpassed that of Android mobile devices data usage*. By the end of 2013, average iOS consumption exceeded average Android consumption in North America and Western Europe.*

In 2013, 18 percent of mobile devices were potentially IPv6-capable*. This estimate is based on network connection speed and OS capability.*

In 2013, the number of mobile-connected tablets increased 2.2-fold to 92 million, and each tablet generated 2.6 times more traffic than the average smartphone. *In 2013, mobile data traffic per tablet was 1,374 MB per month, compared to 529MB per month per smartphone.*

There were 149 million laptops on the mobile network in 2013, and each laptop generated 4.6 times more traffic than the average smartphone. *Mobile data traffic per laptop was 2.45 GB per month in 2013, up17percent from 2.1 GB per month in 2012.*

Average no smartphone usage increased 39 percent to 10.8 MB per month in 2013, compared to 7.8 MB per month in 2012. *Basic handsets still make up the vast majority of handsets on the network (73 percent).*

The Mobile Network Through 2018

Mobile data traffic will reach the following milestones within the next five years.

- *Monthly global mobile data traffic will surpass 15 exabytes by 2018.*
- *The number of mobile-connected devices will exceed the world's population by 2014.*
- *The average mobile connection speed will surpass 2 Mbps by 2016.*
- *Due to increased usage on smartphones, smartphones will reach 66 percent of mobile data traffic by 2018.*
- *Monthly mobile tablet traffic will surpass 2.5 exabyte per month by 2018.*
- *Tablets will exceed 15 percent of global mobile data traffic by 2016.*
- *4G traffic will be more than half of the total mobile traffic by 2018.*
- *There will be more traffic offloaded from cellular networks (on to Wi-Fi) than remain on cellular networks by2018.*

Global mobile data traffic will increase nearly 11-fold between 2013 and 2018. *Mobile data traffic will grow at a compound annual growth rate (CAGR) of 61 percent from 2013 to 2018, reaching 15.9 exabytes per month by2018.*

By the end of 2014, the number of mobile-connected devices will exceed the number of people on earth, and by 2018 there will be nearly 1.4 mobile devices per capita. *There will be over 10 billion mobile-connected devices by 2018, including machine-to-machine (M2M) modules—exceeding the world's population at that time (7.6billion).*

Mobile network connection speeds will increase two-fold by 2018. *The average mobile network connection speed (1,387 Kbps in 2013) will exceed 2.5 megabits per second (Mbps) by 2018.*

By 2018, 4G will be 15 percent of connections, but 51 percent of total traffic. *By 2018, a 4G connection will generate 6 times more traffic on average than a non-4G connection.*

By 2018, over half of all devices connected to the mobile network will be "smart" devices. *Globally, 54percent of mobile devices will be smart devices by 2018, up from 21 percent in 2013. The vast majority of mobile data traffic (96 percent) will originate from these smart devices by 2018, up from 88 percent in 2013.*

By 2018, 48 percent of all global mobile devices could potentially be capable of connecting to an IPv6 mobile network*. Over 4.9 billion devices will be IPv6-capable by 2018.*

Over two-thirds of the world's mobile data traffic will be video by 2018. *Mobile video will increase 14-fold between 2013 and 2018, accounting for 69 percent of total mobile data traffic by the end of the forecast period.*

By 2018, mobile-connected tablets will generate nearly double the traffic generated by the entire global mobile network in 2013. *The amount of mobile data traffic generated by tablets by 2018 (2.9 exabytes per month) will be 1.9 times higher than the total amount of global mobile data traffic in 2013 (1.5 exabytes per month).*

The average smartphone will generate 2.7 GB of traffic per month by 2018, a 5-fold increase over the 2013 average of 529 MB per month. *By 2018, aggregate smartphone traffic will be 11 times greater than it is today, with aCAGR of 63 percent.*

By 2018, more than half of all traffic from mobile-connected devices (almost 17 exabytes) will be offloaded to the fixed network by means of Wi-Fi devices and femtocells each month. *Without Wi-Fi and femtocell offload, total mobile data traffic would grow at a CAGR of 65 percent between 2013 and 2018 (12-fold growth), instead of the projected CAGR of 61 percent (11-fold growth).*

The Middle East and Africa will have the strongest mobile data traffic growth of any region at 70 percent CAGR*. This region will be followed by Central & Eastern Europe at 68 percent and Asia Pacific at 67 percent.*