NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

CRITICAL INFRASTRUCTURE RESILIENCE
FINAL REPORT AND RECOMMENDATIONS

SEPTEMBER 8, 2009

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

NIAC Working Group Members

Wes Bush, (Co-Chair) President and COO, Northrop Grumman
Margaret Grayson, (Co-Chair) Principal, Essential2Management
Alfred R. Berkeley III, Chairman and CEO, Pipeline Trading, LLC.
John Thompson, Chairman and CEO, Symantec Corporation

Study Group Members
Jerry Buckwalter, (Study Group Chair) Northrop Grumman
Pat Andrew, Andrew Associates
Cherrie Black, State of New Jersey
Scott Borg, U.S. Cyber Consequences Unit
Terry Boss, Interstate Natural Gas Association of America
Kathryn Condello, Qwest
Tom Davies, National Fuel
Clay Detlefsen, International Dairy Foods Association
Martin Fertal, Northrop Grumman
Bill Fisher, PVS Chemicals
Mike Hickey, Verizon
Tiffany Jones, Symantec Corporation
Robert Lentz, Northrop Grumman
Ron Luman, Johns Hopkins University Applied Physics Laboratory
Brooke Beebe, Dow Chemical
Bill Muston, Oncor Electric Delivery
Frances Paulson, FedEx Express
Audrey Plonk, Intel Corporation
Robert Prieto, Fluor Corporation
Vance Taylor, Association of Metropolitan Water Agencies
Susan Vismor, Bank of New York Mellon
Evan Wolff, Hunton and Williams LLP
Brian Willis, Intel Corporation

Staff
Jack Eisenhauer, Energetics Incorporated
Alicia Jones, Energetics Incorporated
Sabrina Malkani, SRA International
Jennifer Rinaldi, Energetics Incorporated
Mike Schelble, SRA International
Matt Sickbert, SRA International

ABOUT THE NIAC

Through the Secretary of the Department of Homeland Security (DHS), the National Infrastructure Advisory Council (NIAC) provides the President with advice on the security of the 18 Critical Infrastructure and Key Resource (CIKR) sectors and their information systems. These CIKR sectors span the U.S. economy and include the Banking and Finance, Transportation, Water, Energy, and Emergency Services Sectors, among others. The NIAC also advises the lead Federal agencies that have critical infrastructure responsibilities and industry sector coordinating mechanisms. Specifically, the Council has been charged with:

- Enhancing cooperation between the public and private sectors in protecting information systems supporting critical infrastructures in key economic sectors and providing reports on the issue to the President, as appropriate;
- Enhancing cooperation between the public and private sectors in protecting critical infrastructure assets in other key economic sectors and providing reports on these issues to the President, as appropriate; and
- Proposing and developing ways to encourage private industry to perform periodic risk assessments of critical information and telecommunications systems.

CURRENT NIAC MEMBERSHIP

Chair - Mr. Erle A. Nye, Chairman Emeritus, TXU Corp.
Vice Chair - Mr. Alfred R. Berkeley III, Chairman and CEO, Pipeline Financial Group, LLC *(Vice Chairman (retired) NASDAQ)*
Mr. Edmund G. Archuleta, President and CEO, El Paso Water Utilities
Mr. David J. Bronczek, President and CEO, FedEx Express
Mr. Wesley Bush, President and COO, Northrop Grumman
Lt. Gen. Albert J. Edmonds (ret.), Chairman, Edmonds Enterprise Services, Inc.
Chief Gilbert L. Gallegos (ret.), Chief of Police, City of Albuquerque, New Mexico
Ms. Margaret E. Grayson, Principal, Essential2Management
Mr. Philip G. Heasley, President and CEO, ACI Worldwide
Mr. D.M. Houston, Executive Vice President, ExxonMobil Refining and Supply Company
Mr. David Kepler, Executive Vice President, Chief Sustainability Officer, Chief Information Officer, Corporate Director of Shared Services, Dow Chemical
Commissioner Raymond W. Kelly, Police Commissioner, New York Police Department
Ms. Martha H. Marsh, President and CEO, Stanford Hospital and Clinics
Mr. James B. Nicholson, President and CEO, PVS Chemical, Inc.
Mr. Thomas E. Noonan, Former General Manager, IBM Internet Security Systems
Hon. Tim Pawlenty, Governor, State of Minnesota
Mr. Gregory A. Peters, CEO, News Distribution Network, Inc.
Mr. James A. Reid, President, CB Richard Ellis
Mr. Bruce Rohde, Chairman and CEO Emeritus, ConAgra Foods, Inc.
Dr. Linwood H. Rose, President, James Madison University
Mr. Matthew K. Rose Chairman, President and CEO, Burlington Northern Santa Fe
Mr. John W. Thompson Chairman and CEO, Symantec Corporation
Mr. Michael J. Wallace, Vice Chairman, Constellation Energy Nuclear Group; Chairman, UniStar Nuclear Energy
Mr. Greg Wells, Senior Vice President-Operations, Southwest Airlines
Mr. John M. Williams, Jr., President, Salt River Project
Ms. Martha B. Wyrsch President, Vestas Americas / Vestas Wind Systems, NA

STUDY OVERVIEW

The Critical Infrastructure Resilience Study originated from a recommendation by the preceding NIAC *Critical Infrastructure Partnership Strategic Assessment Study* (2008). The NIAC Partnership Study emphasized the importance of critical infrastructure resilience as necessary for government and business to create a comprehensive risk-management strategy. That report identified the significance that private-sector partners placed on resilience in managing risks, to ensure a robust, reliable, and rapidly recoverable infrastructure.

Resilience has become an important dimension of the critical infrastructure protection mission, and a key element of the value proposition for partnership with the government because it recognizes both the need for security and the reliability of business operations. To address the gap between private-sector business practice and protection-focused government policies, the Critical Infrastructure Partnership Study called for renewed focus on resilience efforts. It issued a specific recommendation that the NIAC conduct a study to "*examine what steps government and industry should take to best integrate resilience and protection into a comprehensive risk-management strategy.*"

Objective

The NIAC initiated the Critical Infrastructure Resilience Study to recommend how government and industry can integrate resilience and protection into a comprehensive risk-management strategy. To achieve this, the NIAC sought to identify and address key questions about the role of resilience in the public-private partnership for infrastructure protection.

Scope

This Study focuses on critical infrastructure resilience, as opposed to community resilience. It also examines how resilience is currently practiced by critical infrastructure businesses and where challenges lie in achieving both enterprise- and sector-level resilience. This Study also examines current government policies and programs for resilience in critical infrastructure and key resource (CIKR) sectors. It focuses on identifying measures to achieve sector- and national-level resilience, cross-sector and supply chain related issues as they relate to resilience, and measures implemented by individual enterprises.

Approach

The Study was conducted in three phases. The initial phase focused on developing a working definition of resilience and gathering perspectives from the different sectors on the advantages and challenges faced in achieving sector resilience. The second phase focused on gathering data through secondary research as well as interviews and panel discussions and identifying current efforts in government and business that promote or support critical infrastructure resilience. The third phase of the Study focused on developing potential recommendations that promote resilience through actions by government and private sector CIKR owners and operators.

For the study, the NIAC convened a diverse study group of executives and subject matter experts (SMEs) with extensive experience across the critical infrastructure sectors. The study group conducted weekly teleconferences, structured interviews with SMEs, and held in-person workshops. The study group developed a comprehensive data collection plan that included the following sources:

- Perspectives of executives and SMEs from business and government obtained through more than 30 interviews
- 90 minute panel interviews with groups of executives from critical infrastructure sectors
- Interviews with senior executives representing diverse critical infrastructure sectors
- Over 100 documents related to resilience practices and efforts in both the government and private sector

From these data sources and the collective knowledge of the group, the Working Group developed a set of key findings that shaped the policy recommendations contained in this report.

EXECUTIVE SUMMARY

Business and society operate in an increasingly complex world marked by interconnection and interdependence across global networks. This complexity requires that owners and operators of critical infrastructures manage their operational risks in an all-hazards environment across the full spectrum of prevention, protection, response, recovery, and reconstitution activities. Most leaders have come to understand that protection of critical infrastructures is an important component of managing infrastructure risk, but other elements must also be considered, including resiliency. The expanding risk landscape demands a continual reevaluation of the roles of governments and businesses in ensuring the delivery of basic infrastructure services. These factors have increased the focus on resilience as an important strategy to help mitigate the multitude of risks facing owners and operators of critical infrastructures in the United States.

Last year, the Council examined the role of the public-private partnership in achieving critical infrastructure protection. That study noted that resilience has become an important dimension of the critical infrastructure protection mission and a key element of the value proposition for partnership with the government because it recognizes both the need for security and the reality of business operations. Because of the importance of resilience in infrastructure security, the Council launched this study to better define resilience in the context of critical infrastructures, clarify appropriate public- and private-sector roles, and examine what steps government and industry should take to best integrate resilience and protection into a comprehensive risk-management strategy.

Infrastructure resilience is about "delivering the goods" regardless of disruptive events that may occur. Although each critical infrastructure sector operates differently, a common definition of infrastructure resilience is needed for public policies and governance to be effective. Toward this end, the Council has developed the following definition based on discussions with executives and security experts across many sectors.

> ***Infrastructure resilience*** *is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.*

The NIAC recognizes that protection and resilience are not opposing concepts; they represent complementary and necessary elements of a comprehensive risk management strategy. The strong foundation developed for infrastructure protection continues to be an essential and vital part of risk management in all critical infrastructure sectors. What is needed now is a strengthening of resilience policies and strategies to build on the successes of the infrastructure protection efforts.

Infrastructure resilience is closely aligned with the way modern businesses manage strategic, operational, and financial risks and the way governments absorb societal shocks from disasters. For companies, the need to be resilient is driven by competitive market forces because customers and shareholders expect products and services to be delivered despite disruptive events. In certain sectors, especially those that operate in highly dynamic threat environments and manage extensive global value chains, leading companies have incorporated risk management into their corporate culture and many consider it a competitive differentiator. This sophisticated risk management includes protection, which is a critical component of risk management in asset-based sectors.

Yet market forces alone are insufficient to ensure that sectors are resilient. Not all enterprises are driven to focus on managing operational and strategic risks and the resilience of individual companies does not guarantee the resilience of the entire sector. Small- and medium-size companies, for example, may lack sophisticated continuity of operations plans and may not have the resources to continually monitor the risk landscape. In addition, the resilience of publicly-owned infrastructures, such as many roads and dams, is not governed by market forces. At the federal level, the government is responsible for providing for public security, health, and safety. Maintaining delivery of critical infrastructure services is a significant component of that mission and ensuring the resilience of critical infrastructures in the face of all types of hazards should be evaluated, even when there is no business case for CIKR owner and operator investment and action.

Lessons Learned Since 9/11

Protection of key facilities and assets from terrorist attacks was a logical and immediate priority after the September 11 attacks. With the good progress made in securing the nation's most vulnerable assets, attention is on managing all-hazards risks by fostering resilience strategies and practices. Sectors such as telecommunications, in which the critical assets are networked systems rather than distinct physical assets, companies find resilience to be well aligned with their strategies for managing risks. For other sectors, such as nuclear and chemical, protection of critical assets is essential to ensure continuity of operations and prevent significant loss of life. Cybersecurity has changed the thinking of many companies that once believed they are unlikely targets for attack or that they could adequately protect themselves from most attacks. Cybersecurity also represents an opportunity to blend together concepts and practices of protection and resilience. It is little wonder that business and government alike have increased their focus on resilience.

In practice, infrastructure security is a shared responsibility. The NIAC believes that aligning the interests, motivation, and distinct capabilities of owners, operators, and government through the public-private sector partnership is central to improving infrastructure resilience. For many companies interviewed, Hurricane Katrina was a turning point in learning how to work with the federal government to better anticipate risks, respond more effectively, and share information before, during, and after a disaster. Many of the owners and operators we spoke with noted the tremendous progress made since Katrina by the DHS Office of Infrastructure Protection in helping to bring critical infrastructure services back up by providing better information to owners and operators

and removing impediments. By serving as an enabler, DHS allows companies to do what they do best: get operations back in service.

Understanding the value proposition for infrastructure resilience at the enterprise, sector, and national level is essential in defining stakeholder roles and crafting strategies, programs, and practices that will reduce risks to critical infrastructures. The challenge facing government is to maintain its role in protecting critical infrastructures, while determining how best to encourage market forces to improve the resilience of companies, provide appropriate incentives and tools to help entire sectors become resilient, and step in when market forces alone cannot produce the level of infrastructure security needed to protect citizens, communities, and essential economic systems.

Findings

The Council has developed the following high-level findings based on the comprehensive interviews and documents reviews we conducted.

- **Because definitions of resilience vary, a common definition will help guide policy development.** Strong federal policies and programs must be based on a common definition of infrastructure resilience. Without this, resources may be allocated ineffectively and programs may not be properly aligned with security goals.

- **The current policy framework for infrastructure security is fundamentally sound but could be improved to better reflect principles of resilience.** Homeland Security Presidential Directive 7 and the National Infrastructure Protection Plan heavily emphasize infrastructure protection while including some resilience concepts. Strengthening the policy framework to fully incorporate resilience principles would better guide the development and execution of federal activities.

- **The Public-Private Sector Partnership Framework provides an excellent collaborative mechanism for improving infrastructure resilience.** Although initially developed for the purpose of improving infrastructure protection, the public-private partnership has proven to be an effective tool for collaboration planning, coordination, and communication. Strong support was received for using this partnership to cultivate infrastructure resilience programs and efforts.

- **The business case for infrastructure resilience is well suited for a federal government role as an enabler and facilitator for owners and operators.** Owners and operators are motivated by market forces to maintain operations despite disruptions. The federal government can help the private sector strengthen resilience by removing barriers, improving risk transparency, and facilitating learning.

- **Current market mechanisms may be inadequate to achieve the level of resilience needed to ensure public health, safety, and security.** Even with a strong business case, there are low-probability, high-consequence events for which investments in resilience by private companies cannot be justified. In these cases, stronger

government involvement is warranted to ensure adequate functioning of critical infrastructures during disasters.

Recommendations

After careful consideration of the aforementioned findings, the Council recommends the following actions to strengthen critical infrastructure resilience:

- **Fortify government policy framework.** The government should use a White House level authority to adopt a common definition for resilience and disseminate a high level, top-down strategy for the development and funding of resilience efforts.

- **Improve government coordination.** Increased coordination among all levels of government and CIKR owners and operators is critical to mitigating the potentially detrimental effects of competing regulations and standards across regions, states, and local entities. The White House should coordinate and adjudicate conflict among regulatory agencies and actions in each sector to support the established resilience goals.

- **Clarify roles and responsibilities of critical infrastructure partners.** Review current incident management documents including the National Response Framework and National Incident Management System and identify opportunities to expand training and outreach activities to the CIKR owners and operators. Such activities provide Federal, state and local entities a better understanding of the components of resiliency during an event and allow for increased information sharing.

- **Strengthen and leverage public-private partnership.** Make full use of existing public-partnerships to provide a set of common, agreed upon sector specific goals, with clear input from both CIKR owners and operators and government on feasibility and objectives.

- **Encourage resilience using appropriate market incentives.** The Council advocates the use of market-based incentives to provide a non-regulatory means to stimulate resilience efforts within private CIKR entities.

- **Implement government enabling activities & programs in concert with critical infrastructure owners and operators.** Exercises involving fact-based scenarios are critical to identifying cross-sector interdependencies. Exercises allow CIKR owners and operators to execute their continuity of operations plans and make adjustments where unforeseen gaps occur. Plans for such activities must include evaluation of critical infrastructure resilience after an event as well as a means for distributing lessons learned to an audience wider than exercise participants.

TOWARD A MORE RESILIENT NATION

In the aftermath of September 11, both private industry and government made the immediate protection of critical infrastructures and key resources (CIKR) a natural priority. Eight years later, protection based strategies continue to be emphasized by government, however, not all CIKR sectors are best served by this strategy. Instead, a number of critical infrastructures (i.e. telecom, electric power distribution, etc.) may lend themselves to a resilience-based approach that focuses on the timely and efficient restoration of services in the event of a disruption. CIKR owners and operators are embracing integrated risk-management strategies that consider a variety of operational risks in an all-hazards environment across the full spectrum of prevention, protection, response, recovery, and reconstitution activities. In the current operational risk environment—where increasingly interconnected systems are vulnerable to threats brought on by sector interdependence, terrorism, pandemic potential, energy volatility, and climate, all with the potential to trigger interrelated, cascading disturbances—it is important to consider resilience as a component of critical infrastructure protection strategy.

Resilience is not a specific, easily definable term. A myriad of definitions can be found in a wide range of literature, addressing all manner of public and private concerns. Some blur the lines between what is meant by critical infrastructure resilience, straying into the realm of infrastructure protection or community resilience. Though infrastructure *protection* and infrastructure *resilience* represent complementary elements of a comprehensive risk management strategy, the two concepts are distinct. **Infrastructure protection** is the ability to prevent or reduce the effect of an adverse event. **Infrastructure resilience** is the ability to reduce the magnitude, impact, or duration of a disruption. Resilience is the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

- **Absorptive capacity** is the ability of the system to endure a disruption without significant deviation from normal operating performance. For example, fire-proofing foam increases the capacity of a building system to absorb the shock of a fire.
- **Adaptive capacity** is the ability of the system to adapt to a shock to normal operating conditions. For example, the extra transformers that the U.S. electric power companies keep on store and share increases the ability of the grid to adapt quickly to regional power losses.
- **Recoverability** is the ability of the system to recover quickly—and at low cost—from potentially disruptive events.

For the purpose of this study, critical infrastructure resilience is characterized by three key features:

- **Robustness:** the ability to maintain critical operations and functions in the face of crisis. This can be reflected in physical building and infrastructure design (office buildings, power generation and distribution structures, bridges, dams, levees), or in system redundancy and substitution (transportation, power grid, communications networks).

- **Resourcefulness:** the ability to skillfully prepare for, respond to and manage a crisis or disruption as it unfolds. This includes identifying courses of action, business continuity planning, training, supply chain management, prioritizing actions to control and mitigate damage, and effectively communicating decisions.

- **Rapid recovery**: the ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption. Components include carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right place.

CIKR owners and operators routinely address enterprise operational risks in the regular course of business. To varying degrees, resilience within their own organizations is dictated by the need for redundancy or reliability, motivated by market forces or even government regulation. As companies and sectors better understand how to manage their own operational risks, they are paying more attention to identifying and addressing cross-sector risks.

CIKR owners and operators not only provide services, they also are users of other critical infrastructure services. A company that assesses its interdependencies with the services of another sector is able to make more informed decisions about how to prepare internally for possible disruptions (e.g., installing back up power systems) and how to work with companies in the other sector to provide needed services through other means. Once established, effective redundant systems may also serve as a level of protection, a deterrent against crimes, such as terrorism. Malicious actors cannot achieve their goals (terror) against a resilient system.

The complexity of today's interconnected infrastructures, particularly communications, energy, information technology, and financial services, may make it difficult for other sectors to determine exactly how susceptible their businesses are to various types of service disruptions or cross-sector events. In the absence of direct measurement, assumptions may be made (e.g., the power is out but the water will still be running) that could prove a hindrance to contingency plans in the event of an actual disturbance. Leading companies and sectors view cross-sector interoperability as the new frontier in infrastructure resilience. Thus, in the interest of minimizing unforeseen circumstances, greater emphasis must be placed on understanding real-time interdependencies and the expectations and limitations of interconnected sectors.

Government must work with the private sector to identify areas where market forces may not support achievement of resilience goals and then develop a commonly agreed upon approach to address these gaps. If government were able to articulate objectives around achieving resilience goals, critical infrastructure owners and operators would be even better equipped to assess their own ability to meet those stated objectives.

Government cannot establish goals in a vacuum. In *Building Resilience*, the Conference Board of Canada advised that as security threats continue to evolve, so too must our response, with private sector organizations playing an increasingly important role. Infrastructure owners and operators have practical knowledge of their own operations, risks, and potential mitigations that is superior to that of government policy makers. Regulations often "stovepipe" risks and impede a company's ability to be truly resilient. As a result, government needs a better understanding of private sector risks.

CIKR sectors are diverse by their nature. Therefore, resilience policy cannot be applied equally to all sectors but rather understood and analyzed on a sector-by-sector basis, taking into consideration the complexity of existing regulatory and voluntary protection programs, the fundamental nature of the sector and the cost and benefit of potential resilience programs. Given its historic and successful experience in working with CIKR owners and operators on infrastructure protection, the Department of Homeland Security should collaborate with each Sector Specific Agency to define resilience, establish policy, goals, or standards. Transparency and measurement of performance is key to developing and continuously altering resilience goals and efforts as needed. Without this collaboration, enacted policies may fall short of intended results.

Once sector definitions of resilience have been developed, practical application of the concepts must be emphasized from the highest levels of governmental authority downward, moving toward development of a common set of agreed-upon, sector specific resilience goals. Leadership at the White House level is necessary commitment. The current policy framework must be adjusted to recognize resilience as a key component of critical infrastructure protection and strengthened to support CIKR owners and operators efforts to make their enterprises and wider sectors more resilient. Such an effort includes expansion of the Department of Homeland Security’s critical infrastructure protection programs and planning activities to allow funding for programmatic and grant funding of resilience efforts.

Acting as a neutral party, Government can facilitate conversations between and among sectors and companies that can better their infrastructure resilience and provide each stakeholder with an enhanced perspective on potential risks.

Using the existing Sector Partnership Framework to enhance dialogue between CIKR owners and operators and government will also improve resilience efforts. The

partnership should consist of a group of equals with clearly defined roles and responsibilities, who work together effectively and efficiently. Collaboration among CIKR owners and operators and government draws upon the knowledge of each entity, which is essential to developing feasible resilience policy tailored to sector-specific services or actions. This framework presents a real opportunity to develop and apply resilience mechanisms in a complimentary nature to protection activities.

Promoting resilience by leveraging existing mechanisms and creating new ones is central to government's ability to coordinate with CIKR sectors to develop a resilience strategy that will effectively respond to national incidents. Government incentives to maintain, improve, and prepare CIKR for rapid recovery when faced with potential incidents will provide greater protection of public health and safety during such an incident.

It is vital for government to work with CIKR owners and operators to establish resilience goals, facilitate contingency planning, foster relationships, ease information sharing and garner best practices, all toward the ultimate goal: a more resilient nation.

FINDINGS AND RECOMMENDATIONS

The NIAC identified six categories comprised of individual recommendations for strengthening CIKR resilience. First, the government should use a White House level authority to adopt a common definition for resilience and disseminate a high level, top-down strategy for the development and funding of resilience activities. Second, increased coordination among all levels of government and CIKR owners and operators is critical to the effectiveness and coordination of similar regulations and standards across regions, states, and local entities that can promote efficient and timely responses to incidents. Third, providing clear expectations of all involved entities during an incident is vital to an efficient response. Without prior planning, incident management quickly becomes chaotic, impeding CIKR owners and operators ability to restore services to the affected infrastructure in a timely manner. The fourth area identified for potential improvement to CIKR resilience is through the use of existing public-partnerships to provide a common, agreed upon set of sector specific goals, with clear input on feasibility and objectives. The fifth recommendation advocates the use of market-based incentives to provide a non-regulatory means to stimulate resilience efforts within private CIKR entities. The final focus area is the importance of exercises that allow CIKR owners and operators to execute their continuity of operations plans and make adjustments where unforeseen gaps have occurred. Building upon the strong efforts and activities in the CIKR community, exercises involving fact-based scenarios are critical to identifying cross-sector interdependencies. Plans for such activities should include evaluation of critical infrastructure resilience after an event as well as a means for distributing lessons learned to an audience wider than exercise participants.

1. Fortify Government Policy Framework to Strengthen Critical Infrastructure Resilience

Resilience policy cannot be developed without a common definition for resilience itself. As stated previously, three features define critical infrastructure resilience:

- **Robustness:** the ability to maintain critical operations and functions in the face of crisis.
- **Resourcefulness:** the ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds.
- **Rapid recovery**: the ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption.

This definition, adopted by the NIAC for the purpose of this study, has been tested for compatibility among the sectors and has been found to be adaptable and applicable to each. This definition should be central to all the U.S. Government activity, similar to the approach that Congress and the Administration took in defining the term critical infrastructure (Reference USA PATRIOT Act).

> ***Recommendation:*** The President should adopt the NIAC definition for resilience for development of resilience policy.

A common definition for resilience is only the first step towards strengthening the resilience of critical infrastructures. Application of the concept must be focused toward developing a set of common, agreed-upon sector specific goals. From the very beginning, this process should be highly interactive and based on private sector involvement, utilizing the existing Critical Infrastructure Partnership Advisory Council (CIPAC) mechanisms and reaching out to additional private sector actors. Public CIKR owners and operators must similarly be engaged. With established sector specific high level resilience goals CIKR owners and operators will be able work with government to identify where the market or current governmental funding approaches will not support their achievement and begin a dialog with government on policy initiatives that can address these gaps.

> ***Recommendation:*** Government should establish a collaborative dialog with CIKR owners and operators in each sector to develop a commonly agreed-upon set of outcomes-focused goals for each sector.

Leadership on resilience requires White House level authority. DHS lacks sufficient leverage to coordinate among the involved federal agencies to support development of resilience policy or goals. Based on the statutory guidance under Section 201 of the Homeland Security Act of 2002, the Office of Infrastructure Protection (OIP) should lead and coordinate the government's activities related to CIKR resiliency activities. OIP leadership is also necessary as it will allow for a natural integration of resiliency concepts into the existing protection programs.

> ***Recommendation:*** The President should continue his leadership on resilience by directing establishment of authority within the White House to support development of appropriate sector level resilience goals and subsequent policy and coordinate relevant federal, state and local agencies.

The current government policy framework should be updated to provide necessary support to CIKR operators in strengthening resilience. Government has substantial influence over infrastructure development and management but no integrated policy framework for prioritization and optimization. Although the NIPP's all-hazards approach references resilience strategies and approaches, there also needs to be a greater focus on

managing operational risk from a resiliency perspective. In the future, there should be a national strategy, incorporated in the NIPP, which identifies mechanisms to support resiliency practices and approach to managing operational risks.

In order to accomplish this goal, the White House should consider either revising HSPD-7 to include specific resiliency policy goals or creating additional Presidential Directives that establishes national resiliency policy goals. However, these directives should not impact the current partnership framework established under HSPD-7 and the NIPP, which is important to building infrastructure resilience. As HSPD-7 has proven to be valuable in creating infrastructure protection mechanisms, there will need to be analogous and congruous resiliency mechanisms.

> ***Recommendation:*** The President should issue an HSPD-level authority to develop a national policy on resilience in a manner similar to and consistent with HSPD-7 policy for *protection,* but ensure the authorities under this guidance and public private infrastructure protection partnership is retained.

Under this new authority, government should create a national framework for coordinated planning, assessment, prioritization and performance measurement of the nation's infrastructure systems that recognizes legacy infrastructure, new and emerging interdependencies, and the multiple ownership and financing structures that exist. Using the guidance laid out in this new HSPD authority, DHS should integrate resilience goals into a new national plan for infrastructure security. This plan can leverage resources and work accomplished to date under the NIPP development process.

DHS must recognize that resilience and protection are both critical components of risk management. During the stand up of DHS, there was an initial emphasis on protection of CIKR. That should now be balanced with policies and programs that encourage resilience to improve infrastructure risk management, when applicable.

Resilience is a key aspect to critical infrastructure risk management and needs to be incorporated more thoroughly into current policy and program approaches. "As a key element of the national economy, private-sector resilience and continuity of operations planning, as well as recovery and restoration from an actual incident, represent essential homeland security activities (National Response Framework, 19)." DHS is the protection agency for CIKR, and resilience needs to accompany that as a part of an overall risk management profile.

> ***Recommendation:*** DHS should expand the criteria for allocation of resources, such as grant funding programs, to support resilience-focused approaches to risk management. DHS needs to coordinate the grant program across all of the sectors, and also examine the net effect of the outcomes from the resulting resilience practices from all the connected industries and sectors. DHS and other relevant

federal agencies should recognize and support resilience as a strategy in risk management so that grant funding and other programs can take into consideration resilience and protection issues.

2. Improve Government Coordination to Enhance Critical Infrastructure Resilience

Most critical infrastructure sectors are regulated by multiple government agencies towards achievement of different goals, which can include employee health and safety, environment protection, public health and safety, and even reliability services. New resilience policy, objectives, and goals will compete with these regulations for priority and in some cases may directly conflict. These different regulatory goals are valid, but for resilience policy to be effective, it must have an appropriate priority.

> ***Recommendation:*** The White House should leverage its authority and leadership on resilience to coordinate and adjudicate conflict among regulatory agencies and actions in each sector to support the established resilience goals.

A strong CIKR resilience strategy will require leadership and coordination that can bring together all of these different groups to establish priorities, adjudicate conflict and achieve resilience goals.

3. Clarify Roles and Responsibilities of Critical Infrastructure Partners

Coordination among varying levels of government and CIKR sectors is essential to the efficient restoration of operations during a disruption. CIKR sectors need clear direction of who is in charge during a disaster situation and a plan for how to best mitigate the circumstances. An incident management system provides a clear structure of how recovery efforts will be addressed, and who is addressing them. Government's ability to articulate objectives and goals surrounding resilience will also enable CIKR owners and operators to assess their ability to meet those objectives, and partner with government to be well-equipped to restore services.

Furthermore, it is critical that the dialogue between government and CIKR sectors continues during times with no disruptions in order to develop metrics to assess resilience in each sector. These metrics should reflect the national-level goals for resilience and provide data to CIKR owners and operators to achieve them. In order to continue the ongoing process of developing resilience-based business practices, government and the CIKR sectors have a responsibility to maintain or consider additional funding for the maintenance and sustainability of critical infrastructure.

CIKR sectors would benefit from better incident management information and a clear understanding of roles and responsibilities during recovery efforts. During the course of an interview with the Transportation Sector, the NIAC learned that aviation professionals had conducted a senior officials exercise of a manned portable air defense system, looking at response in the event of a threat of an aircraft being targeted by ground to air missiles. As reported to the NIAC, what became clear in the exercise is that "nobody knew who would be in charge. DHS assumed it would be them, but FAA and DOT also claimed responsibilities. Some participants even said it would be the White House's responsibility." This example illustrates how critical the understanding of roles and responsibilities are to resiliency. Communications between all involved entities, including how best to prepare for a foreseen incident, is vital to efficient execution of recovery efforts.

> ***Recommendation:*** Review current incident management documents including the National Response Framework and National Incident Management System and identify opportunities to expand training and outreach activities to the CIKR owners and operators. Such activities provide Federal, state and local entities a better understanding of the components of resiliency during an event and allow for increased information sharing.

If government can articulate objectives around achieving resilience goals, the CIKR owners and operators will be better equipped to assess their own ability to meet those stated objectives. DHS should establish national and sector goals for resiliency as a part of the CIPAC and NIPP planning process. Gaps should be identified where CIKR resilience objectives and market mechanisms or public sector infrastructure funding programs do provide adequate resilience. Once established, these goals and accompanying scenarios should be used as a component of the DHS National Level Exercise (NLE) program and associated training and exercise programs.

> ***Recommendation:*** Utilizing the CIPAC framework, all involved government agencies should collaborate with the CIKR owners and operators to incorporate their insight and establish a common understanding on national federal resilience goals. Upon establishment of goals, government must work with both public and private sector CIKR owners and operators to identify areas where the market will not support achievement of federal and regional resilience goals and then develop a commonly agreed upon approach to address these gaps.

All critical infrastructure events happen at a local level. Alignment on resilience goals is critical for the states and local governments. Federal efforts to support resilience must be informed of and support regional goals to achieve success at the local level. Roles and responsibilities for state, local, and (public and private sector) CIKR operators will flow out of the federal resilience goals effort. Federal infrastructure investment priorities drive state-level investment priorities and then private infrastructure owners.

> ***Recommendation:*** The federal government should find opportunities to support and collaborate with State and local governments on subsequent state and regional goals development.

Understanding of goals should be applied towards development of resilience metrics in each sector. Government should support development of voluntary metrics, but not apply the outcomes toward regulation. This process should be coordinated with the US Voluntary Private Sector Preparedness Accreditation and Certification Program, established under Title IX of the "Implementing Recommendation of the 9/11 Commission Act of 2007." This process should include consideration and development of appropriate recommendations for information sharing mechanisms with the private sector that will appropriately protect business confidential information.

> ***Recommendation:*** CIKR owners and operators and DHS should identify a mechanism to monitor and measure resilience at the CIKR sector level. This process should include establishment and support of a feedback mechanism to address CIKR owner and operator concerns in all critical infrastructure sectors and should specifically assess the adequacy of the supply chain to meet response and recovery needs. This process should be analogous to and in coordination with the NIPP annual reporting process.

In developing and operating CIKR both government and private sector need to consider ongoing funding for maintenance and sustainability, which can have a significant affect on the operations and resiliency of CIKR. In this current economic climate, funding for repair and maintenance is not always accounted for in the funding of new and ongoing CIKR projects. The U.S. Government should lead this effort by demonstrating a commitment to funding these type activities and recognizing that deterioration due to lack of maintenance can be more detrimental to critical infrastructure than a single catastrophic event. DHS should gain a better understanding of the impacts of improper funding of repair and maintenance can have on CIKR.

> ***Recommendation:*** Government should develop a better understanding on the role that repair and maintenance funding can have on CIKR and prioritize funding for these activities, both as a component of their resiliency activities as well as part of their broader funding support of public infrastructure.

4. Strengthen and leverage public-private partnership

Increased resilience is best achieved through direct collaboration between the government and critical infrastructure owners and operators. Reexamining relationships and partnerships between the public and private sectors as well as between the public sector at different levels (e.g., federal-state; state-local) is critical to developing goals, standards,

or regulations that are effective and achievable. In *The Resilience Imperative*, MIT said that it is essential for government to "change the way they prepare and partner" on resilience efforts, especially in our increasingly interconnected world.

Collaborations on resilience must be a true partnership of equals and not merely presented as an implicit threat of regulation. Such partnerships have proven successful. The Department of Energy's National SCADA Test Bed program gave vendors an opportunity to use cutting-edge cyber attack tools to test their control systems, and ultimately demonstrate the need for increased investment in more secure energy control systems. Efforts such as these help prevent disturbances such as the Blackout of 2003 and mitigate the consequences when a similar event occurs.

> ***Recommendation:*** Government should collaborate with CIKR executive decision-makers throughout the resilience policy development process. Development must be an iterative process, with bi-directional communication, and a clear understanding of how to reach consensus.

The best mechanism for engagement on resilience is the existing Sector Partnership Framework. The public private partnership for infrastructure protection, as established under HSPD-7 and the NIPP, is a valuable partnership mechanism and should be a part of the resilience policy development and implementation process. The National Infrastructure Protection Plan (NIPP) outlines the roles and responsibilities of public and private sector partners to “build a safer, more secure, and more resilient America.” It established the Sector Partnership Model to implement a public-private partnership to foster “integrated, collaborative engagement and interaction.” The model, as implemented in the Critical Infrastructure Partnership Advisory Council, consists of a series of parallel government and industry councils designed to encourage collaboration across the entire range of infrastructure protection activities. [See Appendix C for more information.]

Multiple sectors have addressed threats, incidents and vulnerabilities by working with DHS through CIKR Sector Councils and sector-specific Information Sharing and Analysis Centers (ISACs) where they exist. These mechanisms play a key role in developing operational business continuity plans and disaster response protocols for each sector. They work closely with DHS’s National Infrastructure Coordinating Center (NICC) and their respective Sector Specific Agencies (SSAs) to obtain real-time information, which helps DHS determine the cross-sector impact of standard operations as well as extraordinary events. This process was first utilized in the course of Hurricane Katrina, practiced during the NLE02-08 exercise, and executed successfully during the 2008 hurricane season.

> ***Recommendation:*** Government should use the existing Sector Partnership Model to plan and implement resilience efforts in coordination with, and addition to,

> current protection activities. The achievements of the past seven years have validated the promise of the public-private partnership framework as a highly effective strategy. The NIAC strongly recommends that this approach be strengthened to continue to build greater resilience in our society. In doing so, government should provide maximum flexibility for each sector to develop and adopt resilience strategies that match their business model, asset base, and risk profile.

An improved understanding of cross-sector interdependencies is essential to coordinate efforts toward improving resilience along supply chains and across sectors. Yet CIKR owners and operators remain reluctant to communicate risks and vulnerabilities out of a natural caution against sharing sensitive proprietary information and fear of widespread publication. They do not want to suffer a competitive disadvantage, increase their potential for litigation or insurance premiums, and do not trust that government will protect the information. Thus, two important enablers for the much-needed information sharing are 1) emphasis on the role that the government plays as a neutral catalyst for competitors to partner, and 2) the protection provided by the special exemption to the Federal Advisory Committee Act (FACA).

The NIAC found that several private sector partners from fairly concentrated industries indicated their companies had legal concerns about meeting with business competitors. Government presence, however, eases this concern. The exemption to FACA, pursuant to Section 871 of the Homeland Security Act of 2002, allows companies to conduct sensitive discussions with their government counterparts without the barrier to such discussion that would have been posed by the requirement of public disclosure of the details of these discussions without the FACA exemption. This was a key recommendation of the 2005 NIAC report on sector partnership model implementation that was successfully implemented by the government.

Information Sharing to Strengthen Resilience

The NIAC also learned that the United Kingdom has successfully accomplished the exchange of risk information, even among competitors. Their system uses Chatham House Rules, which requires that participants refrain from discussing who shared the risk information and instead focus on how to mitigate the risk. A similar set of rules would be effective for Protected Critical Infrastructure Information (PCII) program to dispel concerns that the information revealed will be leveraged against the entity that revealed it.

> ***Recommendation:*** Foster the government's role as a facilitator to enable companies to share information without fear of accidental release, misuse or issuer of anti-trust. Reexamine PCII and other information protections to encourage the private sector to share information on intrusions, threats, and vulnerabilities with the government. Acting as a contributing party, government

can facilitate conversations between and among sectors and companies that can better their infrastructure resilience and provide each stakeholder with a clear perspective of the risks they face. CIKR and government have a common interest in its ability to recover from an event and deliver goods and services. Leveraging that responsibility of all parties, government can enable CIKR to have full information on the risks their sector or specific entity faces.

Strengthening Incident Management and Response

Incident management response can incur huge litigation expenses, increased insurance rates, or other agency regulations, all of which impede on the ability for CIKR sectors to respond to the emergency. Most importantly, levels and agencies of government may have competing restrictions that in an emergency situation can limit CIKR sectors ability to respond. For example, states often have differing size and weight standards and restrictions for trucks. During the aftermath of Hurricane Katrina, not all states lifted their weight restrictions, and thus it was difficult or impossible for companies to deliver goods to New Orleans. CIKR sectors also face multiple credentialing requirements at every level of government, and often have difficulties getting emergency staff to a site to repair and restore services during an incident. Improved cooperation and communication between the private sector and relevant government authorities are critical to optimizing CIKR recovery during all phases of preparation and communication.

In the NIAC's *Framework for Dealing with Disasters and Related Interdependencies Study*, the NIAC explored potential avenues and solutions to improve CIKR recovery following a disaster event. The NIAC found many areas with significant potential for government to strengthen and improve CIKR response and recovery. Most significant among these were processes to address statutory and regulatory impediments to recovery, propagation of best practices among state and local operators, and also opportunities to improve cooperation and information sharing among actors involved in disaster recovery had the potential to significantly improve disaster response and recovery efforts. The recommendations in this report offer practical and detailed solutions for every level of government to improve incident management and response.

> ***Recommendation:*** DHS should implement the NIAC's recommendations contained within the *Framework for Dealing with Disasters and Related Interdependencies Report* that support needed changes for CIKR operator regulatory relief during a national crisis or incident, CIKR worker credentialing and access to a disaster area, and clarification of disaster recovery priorities and roles. This improved coordination among CIKR sectors and government will provide faster recovery times and more focus on restoring operations, order, and public safety.

Leveraging Trust and Relationships to Strengthen Resilience
Trusted executive relationships among CIKR sectors and government present an opportunity to strengthen incident response, share strategic level information, and get things done during a crisis.

The most successful partnerships have a strong commitment from senior government and corporate executives who are informed and engaged on infrastructure issues. Senior leadership is essential because it enables sectors to build key relationships, set priorities, take collective action, and commit resources to address infrastructure challenges. CEOs and senior government executives are uniquely positioned to offer both a strategic viewpoint and valuable resources to the public-private partnership for infrastructure protection. They are empowered to make immediate commitments of resources in a time of crisis. They also provide the vision needed for planning and strategy within the partnership, vital during the response to an event and in preparation for the future.

Protection and resilience in the Banking and Finance Sector has been enhanced through the establishment of regional Financial Industry Resilience through Security and Teamwork, or FIRST organizations. These private sector groups, including ChicagoFIRST and over a dozen similar organizations, are comprised of major financial institutions serving a mission to increase the resilience of the financial community in their respective geographic areas. FIRST organizations address business continuity and homeland security issues requiring a common or coordinated response. They coordinate regularly with local, regional and federal agencies, helping to build trusted relationships that will later allow them to get “beyond the yellow tape” in an emergency and provide expert timely assistance to first responders.

During a significant bank fire in the Chicago area, the public-private relationships established by ChicagoFIRST enabled bank employees to provide critical information to first responders, assisting the emergency response to the event. ChicagoFIRST has also established the Regional Partnership Council, or RPCfirst, to foster collaboration among the FIRST coalitions. The mission of RPCfirst is to share best practices regarding the building of relationships with the public sector, the development of credentialing programs, how to obtain seats in emergency operations centers, and the promotion of effective and efficient information sharing before, during, and after an event.

> ***Recommendation:*** Government needs to engage CIKR owners and operators in order to build institutional and personal relationships that can be leveraged to mitigate crisis situations. By incrementally building personal relationships across and among CIKR sectors, executive leaders will be able to use their established protocols and relationships with each other to access critical goods and services. Executive leaders in government will also be able to leverage their pre-established protocols and relationships with CIKR sectors to assure rapid response and recovery.

Government has an opportunity to partner with CIKR owners and operators to build resilience into the next generation of infrastructure. As the administration focuses on rebuilding and reconstituting the nation's infrastructure, there is a strong emphasis on moving toward efficiency. As this paradigm emerges, efforts to promote these goals have the potential to both enhance resiliency and leave critical infrastructure vulnerable to new threats. For example, the smart grid's multiple routing networks enhances resiliency, while multiple points of entry ease access for computer malware that could lead to cascading outages brought on by cyber attack. The same multiple connections that build redundancy to the system and prevent the possibility of single point failures could also become the catalyst for a widespread disruption.

> ***Recommendation:*** Government should endeavor to better understand the role of design and construction in infrastructure resilience. Application of this understanding will help to shape the policy, R&D funding, and incentives that can spur technological innovation as well as the robust design and construction of critical infrastructures needed for resilience.

5. Encourage Resilience Using Appropriate Market Incentives

In sectors such as telecom, banking & finance, water, and energy, market mechanisms mandate high levels of intra-sector cooperation, significant competition, customer demand for reliable services, and resilience-focused procurement practices. The government should further explore how resilience afforded by these market driven mechanisms can be applied to sectors where they are not currently present in order to achieve higher levels of resilience.

In sectors where the economic cost may exceed the perceived benefit, the government may use its own leverage in the marketplace to provide incentives for the adoption of more resilient best practices. For public infrastructure sectors where well-defined market mechanisms do not exist, surrogate approaches will be required.

Much like the way "green" practices and reporting of an industry's carbon footprint has increasingly become the norm, government has the leverage to create a similar market differentiator on resilience for investing and doing business. There are a variety of incentive mechanisms that could be explored without having to resort to regulation. Those include:

- Tax incentives
- Procurement practices
- Financial disclosure requirements
- Insurance-based incentives

- Increased funding for repair and maintenance

Recommendation: Government should partner with CIKR owners and operators to leverage their understanding of market forces, incentives, and disincentives in order to apply appropriate action that will strengthen infrastructure resilience.

6. Implement Government Enabling Activities & Programs in Concert with Critical Infrastructure Owners and Operators

Partnership and collaboration apply to specific programs as well. Cooperatively designed activities, including everything from studies to performance metrics to training, will yield better results when they are jointly created by the government and the CIKR owners and operators who know the nuance of their sector processes and will be held accountable for implementation.

While there are government programs that address resilience tangentially, government lacks a cohesive set of programs and activities that directly address CIKR resilience. [See Appendix B for more information.]

The DHS scenario exercise program does not reflect an infusion of the concept of resilience. As companies and sectors better understand how to manage their internal security risks, they are paying more attention to identifying and addressing cross-sector vulnerabilities. Resilience measurements are based on assumptions about cross-sector interdependencies; it is imperative to know if these assumptions are wrong. Assessing CIKR sectors individual and cross-sector resilience provides information they may otherwise not be able to access on how to prepare internally to mitigate possible disruptions and work across sectors to develop service contingency plans.

Recommendation: Engage CIKR owners and operators to conduct more cross-sector emergency planning exercises to identify interdependencies, improve preparedness, and establish relationships between sectors, local, state, and Federal government. Results of these exercises should be accessible to all related sectors and facets of government, regardless of whether or not they participated in the exercise, so that the full benefits of resilience and business continuity planning can be realized.

APPENDIX A: SUMMARY OF PREVIOUS NIAC RECOMMENDATIONS ON RESILIENCE

This appendix identifies the principal recommendations of several NIAC publications that relate to resilience, risk management, or information sharing. Each of the examined NIAC recommendations has been included in a transmittal letter to the President. The recommendations relating to resilience, risk management, and information sharing are based on the following seven NIAC documents:

- *Critical Infrastructure Partnership Strategic Assessment* (July 2008)
- *Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States* (January 2007)
- *Convergence of Physical and Cyber Technologies and Related Security Management Challenges* (January 2007)
- *Public-Private Sector Intelligence Coordination* (August 2006)
- *Workforce Preparation, Education, and Research* (July 2006)
- *Risk Management Approaches to Protection* (October 2005)
- *Implementation of the Sector Partnership Model* (October 2005)

Critical Infrastructure Partnership Strategic Assessment

Partnership between the public and private sectors is essential to communication and coordination in resilience, protection, and recovery efforts. The government should reinforce the partnership as a priority in order to increase participation throughout the public and private sectors, as well as require greater accountability of the partners. Utilizing the partnership to leverage relationships and maximize engagement is essential to ensuring the participation of business, state, local, and regional partners.

The NIAC advocates for the inclusion of a wide-range of entities with a stake in CIKR, such as existing sector-based organizations. In order to accommodate a diverse group of sectors, flexibility within the partnership can better meet their needs by diverting away from the “one-size-fits-all” approach that was previously taken.

As companies become more confident with their internal security plans, they are beginning to focus on the vulnerabilities that exist between sectors and throughout supply chains. Increased focus on cross-sector interdependencies within the partnership can facilitate supply chain resiliency.

Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States

The NIAC conducted this study to establish a framework for recovery in the event of a pandemic in the United States. Their findings and recommendations encompass key points relating to risk management and recovery. Cross-sector interdependencies improve pandemic planning and response, however throughout the study the NIAC uncovered numerous key interdependencies, which can negatively impact critical goods and services. By pre-defining a flexible pandemic communications plan and pre-positioning communications, government should be able to augment communications distribution to the critical workforce. Partnerships between the public and private sector are critical to refining existing communications plans, processes, and success metrics. In addition, the NIAC recommended that government develop innovative ways to identify priority workforce groups in the event of a pandemic.

Convergence of Physical and Cyber Technologies and Related Security Management Challenges

This study contains numerous recommendations that provide a framework and approach for improving Executive Leadership Awareness of the cyber threat to critical infrastructure control systems. Executive Awareness is critical to achieving all action for needed control systems cyber security. Seven detailed recommendations to improve information sharing regarding cyber risks to critical infrastructure control systems were included in this report.

Properly informed executive decision by infrastructure protection partners in the public and private sectors are dependent upon improved understanding and communication of information on threats, incidents, and vulnerabilities. The NIAC recommended improvements in government leadership priorities for strategic planning and coordination. DHS and the Sector Specific Agencies (SSAs), in coordination with the National Laboratories, are working to develop cyber security solutions for these systems, but strategic planning and coordination could benefit from higher-level agency coordination and private-sector feedback in the funding prioritization process. Also, a sector specific approach is suggested for developing and supporting appropriate market conditions to develop control systems cyber security technologies and products. The control systems market is distinctly different than the IT market, and it is in the early stages of a transition toward developing the needed market drivers for cyber security solutions. These goals and recommendations are needed to change the mindset of critical infrastructure operators, and establish cyber security as a critical aspect of their recognized operational goals of availability, reliability, and safety.

Public-Private Sector Intelligence Coordination

The NIAC recommended engaging senior CIKR CEOs in the intelligence sharing process, resolving private sector concerns over legality of cooperating with Intelligence Community (IC), utilizing existing sector partnership model to improve information flow between the IC and the CIKR, and improving sector understanding on the part of IC staff.

Workforce Preparation, Education, and Research

Government should designate and privately administer, public-private Information Assurance (IA) training certification body. This organization would standardize IA position descriptions, including required and recommended Knowledge, Skills, and Abilities (KSAs) for government jobs and review and reform IA testing procedures. A partnership between government, industry, and educators is needed to train a workforce capable of servicing the nation's critical infrastructure and cyber security and ensure U.S. competitiveness in the global marketplace.

Risk Management Approaches to Protection

Risk management is a complex endeavor, and expansion of its use in government will not be achieved without recalibrations, lessons-learned, and continuous improvement. The government should look to the private sector for guidance on this task because of its long-standing and matured processes in risk management. Establishing risk management leadership functions within all federal agencies will provide greater focus and accountability at senior levels of government, and will help to drive risk management structure and practice throughout government. To achieve this, cabinet-level departments should establish a Chief Risk Officer (CRO), a common element of successful risk management in the private sector.

In the private sector, risk management is most effective when corporate governance structures oversee the process in order to ensure accountability, promote standards, and prioritize resources against threats and vulnerabilities. Government would benefit from the establishment of similar risk management accountability and oversight structures. Government can learn from the private sector and the private sector is willing to cooperate with government to help it become more efficient.

Implementation of the Sector Partnership Model

After close consideration of the partnership's objectives, the NIAC determined that the Federal Advisory Committee Act (FACA) would effectively end the public-private collaboration needed to achieve the nation's security goals. Critical Infrastructure Protection (CIP) requires open dialogue between both public and private entities. Consequently, the NIAC recognized the importance of fostering the partnership and recommended that the operational framework of the Sector Partnership Model (SPM) should be based on the Section 871 exemption and be exempted from all requirements of the FACA.

APPENDIX B: GOVERNMENT POLICIES AND PROGRAMS SECTION

Given the definition developed by the NIAC and the broad and varying definitions for resilience applied across the infrastructure sectors and government, there are a wide variety of programs that can be characterized as critical infrastructure resilience-oriented. The following is a sampling of government and critical infrastructure sector programs that fit this description.

DHS Private Sector Voluntary Preparedness Certification Program

The one of the most significant resilience-oriented programs within DHS is the Voluntary Private Sector Preparedness Accreditation and Certification Program, which was mandated by the *Implementing Recommendations of the 9/11 Commission Act of 2007*. The intent of the program, which still under development, is to establish a common set of criteria for preparedness among private sector businesses, including disaster management, emergency management, and business continuity programs. It was designed as a voluntary program with the intention that participation would be market-driven and the result would enhance national resilience against all hazards by improving private sector preparedness for disruptive events. The program also involves an effort by DHS to promote the business case for participation and compliance with preparedness standards.

In the law, DHS was charged with a number tasks to establish the program, including designation of standards for assessing private sector preparedness; promoting the business case for preparedness standards; and monitoring the effectiveness of the program. Under the program, third-party certifying organizations will receive accreditation to conduct preparedness certifications from ANSI-ASQ National Accreditation Board (ANAB). Achievement of certification will establish that a company's emergency preparedness and business continuity management system has met the terms of an accepted standard. Organizations participating in the process will choose a selected standard and then become certified based on their compliance to that standard.

DHS Protective Security Coordination Division (PSCD)

Another resilience-focused program at DHS is the PSCD's Regional Resiliency Assessment Program (RRAP). RRAP is an effort conducted in cooperation with State and local governments and CIKR operators to assess CIKR risk on a regional level and coordinate protection efforts to enhance resiliency and address capability gaps of the surrounding first responder communities and region.

The RRAP concept evolved from a previous CIKR site and system assessment approach used by DHS, known as Comprehensive Review. The RRAP built upon these system-

and sector-based methodologies to include characteristics of resiliency as they pertain to the relevant geographic region. RRAP uses multiple vulnerability assessments, capabilities assessments, and infrastructure protection planning efforts to identify and analyze CIKR dependencies, interdependencies, resiliency characteristics, and regional capability and security gaps.

Following each assessment, DHS provides the resulting analysis to its owner or operator. At the conclusion of each RRAP, the resulting analysis of regional resiliency is provided to the State's homeland security agency in the form of an Integrated Protective Measures Analysis (IPMA) Report. The results are used to enhance the overall security posture of the facilities, the surrounding communities, and the geographic region using risk-based investments in equipment, planning, training, processes, procedures, and resources.

Federal Emergency Management Agency

The Federal Emergency Management Agency (FEMA) has developed the FEMA Emergency Management Training Program as part of an effort to build a pipeline of emergency management professionals. Resilient systems and enterprises require long-term investments and preparation and is one such long-term goal. This effort represents a long-term investment to strengthen resiliency strategies for CIKR in the future. FEMA's Exercise and Training Division program is a strong example of how government and the private sector can work together to better understand their relationships and responsibilities. The program facilitates public and private sector interaction on disaster response and recovery coordination efforts.

South East Region Research Initiative (SERRI)

The South East Region Research Initiative (SERRI) Program is managed by Oak Ridge National Laboratory (ORNL) for the US Department of Homeland Security. Its goal is to assist local, state, tribal and regional leaders in developing the tools, technologies, and systems required by communities, states, and regions to prepare for, respond to, and recover from the effects of a man-made or natural disaster. The Community and Regional Resilience Initiative (CARRI) is part of this effort and currently taking place in Gulfport, MS, Memphis, TN, and Charleston, SC. These partner communities are developing and sharing knowledge, best practices, tools and techniques to strengthen their communities' ability to withstand a major disaster event and minimize downtime of government and business services.

National Infrastructure Simulation and Analysis Center (NISAC)

The National Infrastructure Simulation and Analysis Center (NISAC), established in 2003, is a modeling, simulation, and analysis program within the U.S. Department of Homeland Security (DHS). The NISAC provides strategic, multi-disciplinary analyses of interdependencies and the consequences of infrastructure disruptions across all 18 CIKR sectors at national, regional, and local levels. NISAC's analyses assist in the understanding of infrastructure protection, mitigation, response, and recovery options.

Other Federal Agency and Sector Infrastructure Resilience Efforts

Outside of DHS, there are other federal regulatory agencies, who, in accordance with their mission and objectives, oversee regulations that strengthen the resilience of critical infrastructure. One such example is the Department of Energy and its programs that promote the reliability of the electrical grid. Under the goal of reliability, DOE works with operators in the electricity sector to make the grid more robust, improve incident reaction and response, and minimize service interruptions. All of these goals directly align with the resilience objectives outlined earlier in the report. Regulators in the banking and finance sector worked closely with operators through regulatory practices and programs to optimize continuity of services in this sector. Similarly, the DOT, DOE, and TSA collaborate with operators in the oil and natural gas sector to maintain continuity of services in this sector. In all of these cases, continuity of services is a critical mission for operators in these sectors, which significantly affects their approach to resilience as a strategy.

Banking and Finance Sector

The Financial and Banking Information Infrastructure Committee (FBIIC) is one example of the Banking and Finance Sector's resiliency based approach to risk management. FBIIC is chartered under the President's Working Group on Financial Markets, and is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. The committee works to identify critical infrastructure assets, their locations, potential vulnerabilities, and prioritize their importance to the financial system of the U.S; establish secure communications capability among the financial regulators and protocols for communicating during an emergency; and ensure sufficient staff at each member agency with appropriate security clearances to handle classified information and to coordinate in the event of an emergency.

Communications Sector

The federal government has worked closely with the Communications sector over many years to develop programs that promote resilience. The Telecommunications Service Priority (TSP) and Wireless Priority Services (WPS) programs are two examples of the government's efforts to partner with the sector and ensure continuity of services. TSP and WPS are Federal Communications Commission (FCC) programs used to identify and prioritize telecommunication and cellular services that support national security or emergency preparedness (NS/EP) missions. The programs direct telecommunications and cellular service providers to give priority to users enrolled in the programs when they need to add lines or have their lines restored, or receive calling queue priority following a disruption of service, regardless of the cause. The programs are always in effect and their operation is not contingent on a major disaster or attack taking place. The FCC sets the

rules and policies for both the TSP and WPS programs; the National Communications System, a part of DHS, manages the programs.

Electricity Sector

The Electricity Sector is focused on providing continuity of services to its customers. The Office of Electricity Delivery and Energy Reliability (OE) works to ensure that the energy delivery system is secure, resilient and reliable. The Office leads national efforts to modernize the electric grid; enhance security and reliability of the energy infrastructure; and facilitate recovery from disruptions to energy supply. OE collaborates with DHS and others to bolster the resiliency of the grid and assist with restoration when major energy supply interruptions occur. OE also coordinates with national, regional, state, and local organizations and utilities to develop effective solutions to increasing the reliability and efficiency of electric market operations.

The North American Electric Reliability Council (NERC) is another organization in the Electricity Sector that works to ensure the reliability of the bulk power system in the U.S. NERC develops and enforces reliability standards; assesses reliability annually via 10-year and seasonal forecasts; monitors the bulk power system; and educates, trains, and certifies industry personnel. NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada. NERC also established Cyber Security standards for SCADA and control systems to improve reliability in recent years. The standards require utilities responsible for delivering bulk electricity to the North American electrical grid to identify and protect critical cyber assets. The Federal Energy Regulatory Commission oversees the power industry, and has delegated responsibility for maintaining and complying with standards to NERC.

Oil and Natural Gas Sector

The Oil and Natural Gas Sector has a significant amount of redundancy and robustness built into the system. The Federal Energy Regulatory Commission (FERC) is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. FERC also reviews proposals to build liquefied natural gas (LNG) terminals and interstate natural gas pipelines as well as licensing hydropower projects. The Energy Policy Act of 2005 gave FERC additional responsibilities as outlined in FERC's Top Priorities which includes promoting the development of a strong energy infrastructure.

The Department of Transportation's (DOT) Pipeline and Hazardous Material Safety Administration (PHMSA), acting through the Office of Pipeline Safety (OPS), administers the Department's national regulatory program to assure the safe transportation of natural gas, petroleum, and other hazardous materials by pipeline. OPS develops regulations and other approaches to risk management to assure safety in design, construction, testing, operation, maintenance, and emergency response of pipeline facilities.

The Transportation Security Administration (TSA) is responsible for pipeline security in the ONG Sector. The TSA has developed security guidelines in cooperation with industry associations and operators that address elements of resiliency. Per the Implementing Recommendations of the 9-11 Commission Act of 2007, TSA is also required to conduct security inspections of the top 100 systems, based upon system throughput. Under the same law, the TSA is required to prepare a Pipeline Incident Recovery and Protocols Plan, which directly affects system resiliency.

APPENDIX C: SUMMARY OF THE SECTOR PARTNERSHIP MODEL

The National Infrastructure Protection Plan (NIPP) establishes a framework for government and the private sector to collaborate on CI/KR issues. To this end, the NIPP offers a comprehensive risk management framework with defined roles and responsibilities for the Department of Homeland Security (DHS), Federal Sector Specific Agencies (SSAs) and other Federal, State, local, tribal, and private sector security partners. This approach is facilitated by the Critical Infrastructure Partnership Advisory Council (CIPAC), Sector Coordinating Councils (SCCs), and Government Coordinating Councils (GCCs).

HSPD-7

Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, provides for a central source in coordinating uniform security practices and harmonizing security programs across and within government agencies. The directive identifies seventeen CI/KR sectors. It directs the DHS and other Federal agencies to "collaborate with the private sector and continue to support sector-coordinating mechanisms: (a) to identify, prioritize, and coordinate the protection of CI/KR; and (b) to facilitate the sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."

Under HSPD-7, the DHS is responsible for leading, integrating, and coordinating the overall effort to enhance CI/KR protection including collaborative development of the NIPP. The primary organizational structure relied upon by the NIPP for this purpose is the Sector Partnership Model.

Sector Partners

DHS developed a Sector Partnership Model to facilitate an unprecedented level of cooperation throughout all levels of government, industry, and institutions for protection of CI/KR. Under the Sector Partnership Model, each of seventeen sectors identified in HSPD-7 as CI/KR is designated to a corresponding federal "partner" or Sector Specific Agency (SSA). An eighteenth sector, Critical Manufacturing, was established in 2008, by the Secretary for Homeland Security exercising his authority under HSPD-7.

The partnership structure recognizes a private Sector Coordinating Council (SCC) and a corresponding Government Coordinating Council (GCC) for each sector. CIPAC enables SCC and GCC members to engage in intra-government and public-private cooperation and information sharing across the entire range of CI/KR activities.

Partner Roles and Responsibilities

Federal. According to HSPD-7, DHS is responsible for leading, integrating, and coordinating the overall effort to enhance CI/KR protection. SSAs work with DHS to implement the NIPP sector partnership model, develop protective programs and related requirements, provide sector-level CI/KR protection guidance, and encourage sharing of security-related information, when appropriate, among private entities within the sector and between the public and private sectors. Additionally, SSAs collaborate with security partners to develop Sector Specific Plans (SSPs) and sector-level performance feedback to DHS for cross-sector gap analysis assessments. DHS serves as the SSA for 11 of the 18 CI/KR sectors identified in HSPD-7.

Sector Specific Agencies

Sector	Sector-Specific Agency (SSA)
Agriculture & Food	Departments of Agriculture, Health and Human Services, Food and Drug Administration
Banking and Finance	Department of the Treasury
Chemical	Department of Homeland Security, Infrastructure Protection
Commercial Facilities	Department of Homeland Security, Infrastructure Protection
Communications	Department of Homeland Security, Cyber Security and Communications
Critical Manufacturing	Department of Homeland Security, Infrastructure Protection
Dams	Department of Homeland Security, Infrastructure Protection
Defense Industrial Base	Department of Defense
Drinking Water & Water Treatment Systems	Environmental Protection Agency
Energy	Department of Energy
Emergency Services	Department of Homeland Security, Infrastructure Protection
Government Facilities	Department of Homeland Security, Immigration and Customs Enforcement, Federal Protective Service
Information Technology	Department of Homeland Security, Cyber Security and Communications
National Monuments and Icons	Department of the Interior
Nuclear Reactors, Materials, and Waste	Department of Homeland Security, Infrastructure Protection

Sector Specific Agencies

Sector	Sector-Specific Agency (SSA)
Postal and Shipping	Department of Homeland Security, Transportation Security Administration
Public Health & Healthcare	Department of Health and Human Services
Transportation Systems	Department of Homeland Security, Transportation Security Administration and U.S. Coast Guard

State. As outlined in the NIPP, states are primarily responsible for developing and implementing statewide/regional CI/KR protection programs. To effectively implement CI/KR protection programs, states should establish security partnerships, facilitate coordinated information sharing, coordinate regional and local efforts with the private sector, and cut across all sectors present within the state to support national, State, and local priorities.

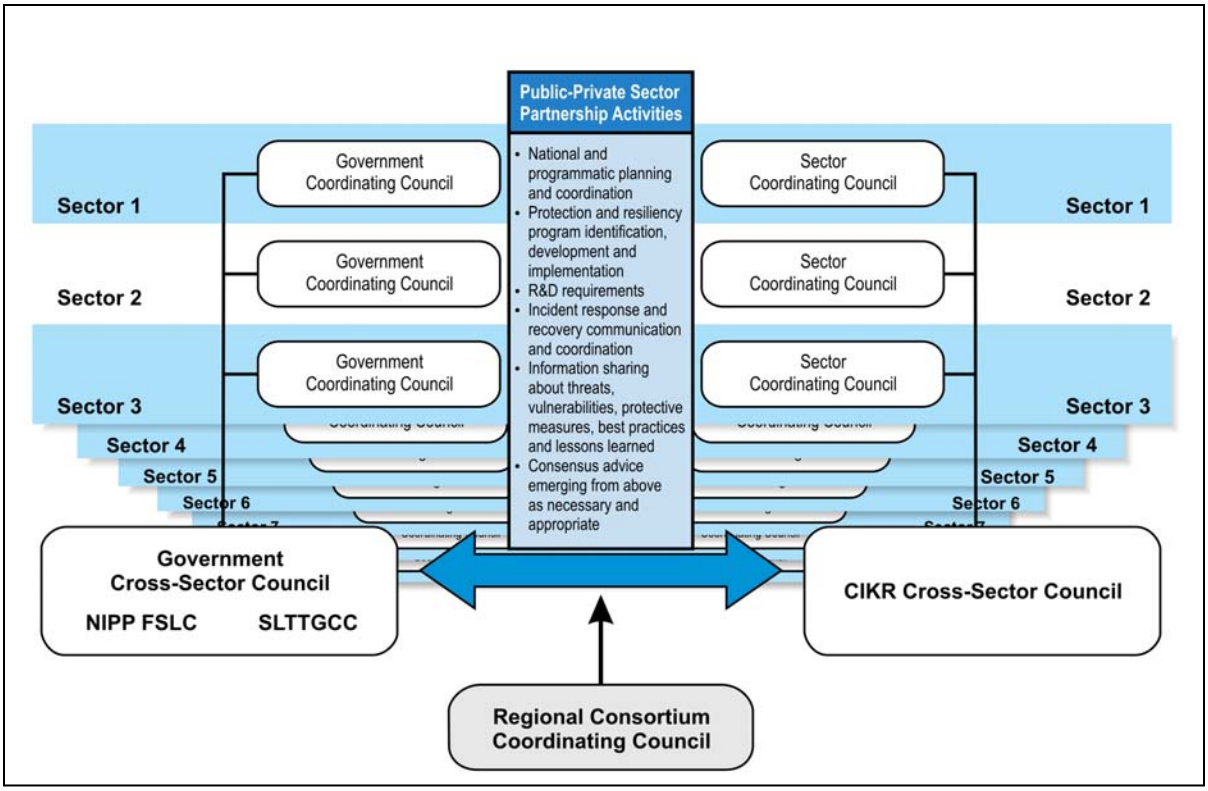
Local. Local entities provide critical public services in conjunction with private sector owners and operators, and thus they drive emergency preparedness and local participation in NIPP and SSP implementation. As a NIPP partner, local governments:

- Facilitate the exchange of information among and between public and private entities;
- Apply documented lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents to CI/KR protection; and
- Act as a focal point for protective and emergency response activities, preparedness programs, and resource support among local agencies, business and citizens.

Regional. Regional security partnerships include a variety of public-private sector initiatives that cross jurisdictional and/or sector boundaries and focus on homeland security preparedness, protection, response, and recovery within or serving the population of a defined geographical area. Regional partners collaborate to implement NIPP-related CI/KR risk assessment and protection activities, promote education and awareness of CI/KR protection efforts occurring within their region, and coordinate regional exercise and training programs.

Private Sector. Private sector owners and operators are responsible for supporting risk management planning and investments in security as a necessary component of prudent business planning and operations. The CI/KR protection responsibilities of specific owners or operators vary widely within and across sectors. Some sectors have regulatory or statutory frameworks that govern private sector security operations within the sector; however, most are guided by voluntary security regimes or adherence to industry-

promoted best practices. Fortifying CI/KR security within this diversity of sectors requires implementing protective actions and programs to reduce identified vulnerabilities appropriate to the level of risk presented; developing and coordinating CI/KR protective and emergency response actions, plans, and programs with appropriate



Federal, State, and local governments; and participating in the NIPP Sector Partnership Model.

Sector Coordinating Councils

SCCs are self-organized, representative bodies broadly inclusive of owners, operators, and trade associations within a particular sector. They assume the responsibility of coordinating sector-wide activities and initiatives focused on improving homeland security and critical infrastructure protection.

According to the NIPP, SCCs are also a primary point of entry into their respective sectors, providing a communication and coordination channel between the sector and DHS, SSAs, and their counterpart GCCs. This range of coordination is designed to facilitate:

- National planning on protection and resiliency;
- Identification and prioritization of sector risk management activities;

- Information sharing related to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and effective security practices; and
- Collaboration among and between public and private sector CI/KR security partners on strategic communication, coordination, and procedures during response and recovery activities.

Cross-sector issues and interdependencies between the SCCs are addressed through a Private Sector Cross-Sector Council, currently housed within the privately organized Partnership for Critical Infrastructure Security (PCIS).

Government Coordinating Councils

GCCs serve as a counterpart to the SCC for each CI/KR sector. They bring together diverse Federal, State, local, and tribal interests to identify and develop collaborative strategies for the advancement of CI/KR protection. GCCs support the efforts of SCCs to plan, implement, and execute sector-wide security initiatives, leveraging complementary resources within government and between CI/KR owners and operators to enhance sector security.

According to the NIPP, GCCs further CI/KR sector security by supporting:

- Interagency coordination for CI/KR strategies, programs, initiatives, activities, policies, and communications;
- SCC planning, implementation, and execution of sector-wide security initiatives;
- Identification of gaps in plans, programs, policies, procedures, and strategies;
- Forums with the private sector to develop, implement, and maintain SSPs and programs; and
- Information sharing and coordination during events of national emergency or significance and augmentation of existing emergency operation channels within Federal, State, local, Territorial, and tribal governments and with industry.

Cross-sector issues and interdependencies between the GCCs are addressed through the Government Cross-Sector Council and its two subcouncils. The NIPP Federal Senior Leadership Council (FSLC) drives enhanced communications and coordination between and among Federal departments and agencies with a role in implementing the NIPP and HSPD-7. The State, Local, Tribal and Territorial Government Coordinating Council (SLTGCC) provides an organizational structure to provide perspective from senior homeland security officials and coordinate across jurisdictions on State and local levels.

Critical Infrastructure Partnership Advisory Council (CIPAC)

CIPAC is a non-decisional body, tasked with determining national priorities and resource requirements for the protection of CI/KR against threats and providing recommendations to DHS, SSAs, and other Federal departments as directly related to the critical infrastructure areas outlined in HSPD-7.

Due to the often sensitive nature of CI/KR operations, it is necessary for owners and operators to, in confidence, share information and advice regarding threats, vulnerabilities, protective measures, and lessons learned. CIPAC provides an operational mechanism for government and private sector partners in the Sector Partnership to engage in a wide range of activities including: planning, coordination, implementation, and operational issues; implementation of security programs; operational activities related to CI/KR protection including incident response, recovery, and reconstitution; and development and support of national plans, including the NIPP and Sector-Specific Plans.

CIPAC, which has been exempted from the requirements of the Federal Advisory Committee Act (FACA), is designed to allow meaningful dialogue on CI/KR protection issues while facilitating mutual action between government entities and owners and operators.

APPENDIX D: REFERENCES

Akay, Adnan and Judy Raper. *Complex Engineered and Natural Systems.* National Science Foundation Directorate for Engineering, 2008. http://www.nsf.gov/attachments/103193/public/8Akay.ppt (accessed June 2009)

Alesh, Daniel and James Holly. "Tight Coupling, Open Systems, and Losses from Extreme Events." https://www.riskinstitute.org/peri/images/file/Alesch_Tight_Coupling_Open_Systems_and_Losses_From_Extreme_Events.pdf (accessed June 2009)

American Society for Civil Engineers. *Report Card for America's Infrastructure.* Washington, DC: American Society for Civil Engineers, 2005. http://www.asce.org/files/pdf/reportcard/2005_Report_Card-Full_Report.pdf (accessed June 2009)

American Society for Civil Engineers. *2009 Report Card for America's Infrastructure.* Washington, DC: American Society for Civil Engineers, 2009. http://www.infrastructurereportcard.org/sites/default/files/RC2009_full_report.pdf (accessed June 2009)

American Society for Industrial Security (ASIS) International. *Organizational Resilience: Security, Preparedness and Continuity Management Systems - Requirements with Guidance for Use*. Alexandria, VA: ASIS International, 2009. http://www.asisonline.org/guidelines/ASIS_STD_SPC.1-2009_Item_1842.pdf (accessed June 2009)

Archuleta, Edmund; James Nicholson; Tim Pawlenty. "The Framework for Dealing with Disasters and Related Interdependencies Working Group." Presented to the DHS National Infrastructure Advisory Council, 14 October 2008.

Auerswald, Philip and Debra van Opstal. *Coping with Turbulence: The Resilience Imperative. Innovations*. MIT Press, 2009. http://www.compete.org/images/uploads/File/PDF%20Files/INNOVATIONS-Davos-2009_Auerswald-vanOpstal.pdf (accessed June 2009)

Briggs, Rachel and Charlie Edwards. *The Business of Resilience: Corporate security for the 21st century.* London, UK: Demos, 2006. http://www.demos.co.uk/files/thebusinessofresilience.pdf (accessed June 2009)

Bush, George W. “Protect the American People, Critical Infrastructure, and Key Resources.” Washington, D.C.: The White House, 2007. http://georgewbush-whitehouse.archives.gov/infocus/homeland/nshs/2007/sectionVI.html (accessed June 2009)

Bush, George W. “Public Health and Medical Preparedness.” *Homeland Security Presidential Directive/Hspd-21*. Washington, D.C.: The White House, 2007. http://georgewbush-whitehouse.archives.gov/news/releases/2007/10/20071018-10.html (accessed June 2009)

The Centre for Community Enterprise. *The Community Resilience Manual: A Resource for Rural Recovery & Renewal*. Port Alberni, British Columbia: The Centre for Community Enterprise, 2000.

The Centre for Community Enterprise. *Section 2: The Workbook to the Community Resilience Manual*. Port Alberni, British Columbia: The Centre for Community Enterprise, 2000.

The Centre for Community Enterprise. “Center for Community Enterprise: The Community Resilience Project: A Resource that Links Rural Revitalization to CED Best Practice.” Port Alberni, British Columbia: The Centre for Community Enterprise, 2000. http://www.cedworks.com/communityresilience02.html (accessed June 2009).

Center for Strategic and International Studies. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC: Center for Strategic and International Studies, 2008. http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed June 2009)

The Conference Board of Canada. *Building Resilience: Cooperation and Coordination for an Effective Response.* Ottawa, Canada: The Conference Board of Canada, 2009.

Council on Competitiveness. *Prepare. Briefing Materials: Workshop on Risk Intelligence and Resilience.* Washington, DC: Council on Competitiveness, 2008. http://www.compete.org/images/uploads/File/PDF%20Files/Prepare%20112008.pdf (accessed June 2009)

Council on Competitiveness. *Transform. The Resilient Economy: Integrating Competitiveness and Security*. Washington, DC: Council on Competitiveness, 2007.

http://www.tisp.org/index.cfm?pk=download&id=11018&pid=10261 (accessed June 2009)

Council on Competitiveness. *The Value of Resilience: Security and Shareholder Value*. Washington, DC: Council on Competitiveness, 2006.

Critical Infrastructure Partnership Advisory Council (CIPAC). *Critical Infrastructure Partnership Advisory Council Annual.* Washington, DC: U.S. Department of Homeland Security, 2008.

Critical Infrastructure Protection Program (CIPP), *CIPP Resilience Series Monograph: Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*. George Mason University School of Law, 2007. http://cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf (accessed June 2009)

Edwards, Charlie. *Resilient Nation*. London, UK: Demos, 2009. http://www.demos.co.uk/files/Resilient_Nation_-_web-1.pdf?1242207746 (accessed June 2009)

Electric Power Research Institute (EPRI), Inc. *IntelliGrid: Smart Power for the 21st Century.* Palo Alto, CA: EPRI, 2005. http://my.epri.com/portal/server.pt?Product_id=000000000001012094 (accessed June 2009)

Ferriere, Dale, National Infrastructure Institute, Center for Infrastructure Expertise. "Maritime Transportation Infrastructure Resiliency, Redundancy, Readiness, Recovery, Restoration" Presented at 2nd Annual Infrastructure Protection and Security Forum. Melbourne, Victoria, Australia. 30th & 31st July 2007. http://www.ni2cie.org/downloads/Presentation2-MaritimeTransportationInfrastructureResilience.pdf (accessed June 2009)

Flynn, Stephen E. "America the Resilient: Defying Terrorism and Mitigating Natural Disasters." *Foreign Affairs*, March/April, 2007 http://www.nyu.edu/intercep/lapietra/Flynn_AmericatheResilient.pdf (accessed June 2009)

Fowler, Daniel. "Advisory Council Reports a 'Cliffs Notes' Guide for the Next Administration." Washington, DC: CQ Homeland Security, 2008.

Fowler, Daniel. "Infrastructure Protection Chief Demurs on Resiliency Focus." Washington, DC: CQ Homeland Security, 2008.

Fowler, Daniel. “Reform Institute Study Builds Case for Resiliency.” Washington, D.C.: CQ Homeland Security, 2008.

Gaynor, Jeff. “The Resilience Imperative.” 2008 TISP Corporate, Community, and Government Resilience Day. Reston, VA: The Infrastructure Security Partnership (TISP). http://www.tisp.org/index.cfm?pk=download&id=11040&pid=10261 (accessed June 2009)

Gould, W. Scott, Daniel B. Prieto, and Jonah J. Czerwinski, *Global Movement Management: Strengthening Commerce, Security and Resiliency in Today’s Networked World*. Somers, NY: IBM, 2008. http://www-03.ibm.com/industries/global/files/gov_gmm_v.2.0_final.pdf (accessed June 2009)

Gurwitch, Robin, Betty Pfefferbaum, Juliann Montgomery, Richard Klomp, and Dory Reissman. *Building Community Resilience for Children and Families*. Oklahoma: Terrorism and Disaster Center, University of Oklahoma Health Services Center, 2007. http://www.nctsnet.org/nccts/asset.do?id=1065 (accessed June 2009)

Harwood, Matthew. “U.S. Must be More Resilient to Disasters and Terrorism, Experts Explain.” *Security Management: Security’s Web Connection.* Securitymanagement.com, 6 June 2008. http://www.securitymanagement.com/news/u-s-must-be-more-resilient-disasters-and-terrorism-experts-explain (accessed June 2009)

Heyman, David, James Carafano. *Homeland Security 3.0: Building a National Enterprise To Keep America Free, Safe, and Prosperous*. Washington, DC: Center for Strategic and International Studies, 2008. http://www.csis.org/media/csis/pubs/080918_homeland_sec_3dot0.pdf (accessed June 2009)

Homeland Security Advisory Council. *Report of the Critical Infrastructure Task Force*. Washington, D.C.: U.S. Department of Homeland Security, 14 February 2006. http://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf (accessed June 2009)

IBM. Security & Society. Armonk, NY: IBM, 2008. http://www.ibm.com/ibm/gio/media/pdf/gio_s_s_report.pdf (accessed June 2009)

IBM. Supply Chain Risk Management: A Delicate Balancing Act. Somers, NY: IBM, 2008. ftp://ftp.software.ibm.com/common/ssi/rep_wh/n/GBW03015USEN/GBW03015USEN.PDF (accessed June 2009)

The Infrastructure Security Partnership (TISP). *Regional Disaster Resilience: A Guide for Developing an Action Plan*. Reston, VA: The American Society of Civil Engineers, 2006. http://tisp.org/index.cfm?cdid=10962&pid=10261 (accessed June 2009).

Kagan, Frederick. "Two Decades Late." Washington, D.C.: American Enterprise Institute for Public Policy Research, 2008. http://www.aei.org/docLib/20080612_2923203OTIKagan_g.pdf (accessed June 2009)

Kelly, Sheila. "Personal and Community Resilience: Building It and Sustaining It." Bureau for Behavioral Science and Health Facilities, 2007. www.wvdhhr.org/healthprep/common/resiliency.ppt (accessed June 2009).

Korade, Matt. "Resiliency Hearings Spark Fireworks Between Panel, Administration." Washington, D.C.: CQ Homeland Security, 6 May 2008.

Korade, Matt. "Without a Guard at Every Door, 'Resiliency' Becomes the New Buzzword." Washington, D.C.: CQ Homeland Security, 9 January 2008.

Laws, John. U.S. Department of Homeland Security. *TSIP Forum: Security of Water and Wastewater Critical Infrastructure*. Washington, D.C.: Department of Homeland Security, 29 October 2008.

The Manufacturing Institute. *Innovators in Supply Chain Security: Better Security Drives Business Value*. Stanford University, 2006. http://www.nam.org/supplychainsecurity (accessed June 2009)

Margetta, Rob. "Committee Leaders Pleased With Month of Hearings on Resiliency." Washington, D.C.: CQ Homeland Security, 23 May 2008.

Margetta, Rob. "Making Mr. Secretary: Experts Weight In on Skills Needed by the Next DHS Chief." Washington, D.C.: CQ Homeland Security, 30 September 2008.

Margetta, Rob. "Lack of Campaign Focus on Homeland Security Could Leave Winner Unprepared." Washington, D.C.: CQ Homeland Security, 15 October 2008.

Morrison, David C. "Behind the Lines: Our Take on the Other Media's Homeland Security Coverage." Washington, D.C.: CQ Homeland Security, 26 September 2008.

Muccio, Amelia. “NJPAC: Be Ready to Rise to the Challenge: Introduction to the National Infrastructure Protection Plan IS 860.” New Jersey Primary Care Association, 2008. http://www.nj-ptc.org/training/materials/NJPCA/IntroNatlInfrastructure.ppt (accessed June 2009).

National Infrastructure Advisory Council. *Best Practices for Government to Enhance the Security of National Infrastructures*. Washington, D.C.: U.S. Department of Homeland Security, 13 April 2004. http://www.dhs.gov/xlibrary/assets/niac/NIAC_BestPracticesSecurityInfrastructures_0404.pdf (accessed June 2009)

National Infrastructure Advisory Council. *Risk Management Approaches to Protection: Final Report and Recommendations by the Council*. Washington, D.C.: U.S. Department of Homeland Security, 11 October 2005. http://www.dhs.gov/xlibrary/assets/niac/NIAC_RMWG_-_2-13-06v9_FINAL.pdf (accessed June 2009)

National Infrastructure Advisory Council. *Critical Infrastructure Protection Strategic Assessment Final Report and Recommendations*. Washington, D.C.: U.S. Department of Homeland Security, 14 October 2008. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf (accessed June 2009)

National Infrastructure Advisory Council. “Critical Infrastructure Partnership Strategic Assessment: Study Overview.” Washington, D.C.: U.S. Department of Homeland Security, 2008.

Norris, Fran H. and B. Pfefferbaum. “Assessing Community Resilience.” Presented at the START Research Symposium, College Park, Maryland, 28 June 2006. http://www.start.umd.edu/start/publications/START_Community_Resilience_062706_HO.ppt (accessed June 2009).

O’Rourke, T.D. “Critical Infrastructure, Interdependencies, and Resilience. *The Bridge*. Vol. 37, No.1. National Academy of Engineering, 2007. http://www.nae.edu/nae/bridgecom.nsf/weblinks/CGOZ-6ZRLSP/$FILE/Bridge-v37n1.pdf?OpenElement (accessed June 2009)

O’Rourke, T.D., Briggs, T.R.. “Modern Approaches to Infrastructure Resilience.” University of Canterbury, Cornell University, 2007. http://www.caenz.com/info/RINZ/downloads/Prestige.pdf (accessed June 2009)

Perelman, Lewis J. “The Resilience Imperative.” 2008 TISP Corporate, Community, and Government Resilience Day. Reston, VA: The Infrastructure Security Partnership (TISP). http://www.tisp.org/index.cfm?pk=download&id=11040&pid=10261 (accessed June 2009)

Prieto, Robert. *The 3Rs: Lessons Learned from September 11th*. London, England: The Royal Academy of Engineering, 2002. http://www.raeng.org.uk/news/releases/attach/154.pdf (accessed June 2009)

Prieto, Robert. “The Built Environment: A systems perspective from 9/11.” Washington, DC: The Infrastructure Security Partnership (TISP), 2002.

Prieto, Robert. “Vulnerability of Public Infrastructure: A systems perspective.” Presented at the Homeland Security Summit, Washington, DC, 6-7 June 2002.

Prieto, Robert. “Infrastructure Resiliency: Do We Have The Focus Right?” Fluor Corporation, 2008.

Prieto, Robert. “Personal Perspective: Program management and events of scale.” PM World Today, July 2008. http://www.pmforum.org/library/papers/2008/PDFs/Prieto-7-08.pdf (accessed June 2009).

Project on National Security Reform. *Forging a New Shield*. Washington, DC: Center for the Study of the Presidency, 2008. http://www.pnsr.org/data/files/pnsr%20forging%20a%20new%20shield.pdf (accessed June 2009)

Raisch, William. The Business Case for Enterprise Resilience: Significant Risks, Substantial Rewards. New York: International Center for Enterprise Preparedness, New York University, 2007. http://www.nyu.edu/intercep/research/pubs/Business%20Case%20for%20Enterprise%20Resilience%201.5.07.pdf (accessed June 2009)

The Reform Institute. *Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy.* Alexandria, VA: the Reform Institute, 2008. http://www.reforminstitute.org/uploads/publications/Building_Resilience_SEPT25.pdf (accessed June 2009)

The Reform Institute. *Summary of Session 4: Securing the Energy Markets; from Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy.* Hosted by the Reform Institute and Sponsored by the McCormick Tribune Foundation. New York: New York Yacht Club, 28 March 2008.

The Reform Institute. *Policy Forum Transcript: A Resilience Metric: Measuring Preparedness before Disaster Strikes.* Alexandria, VA: the Reform Institute, 2009. http://www.reforminstitute.org/uploads/publications/Resilience_Metric_Edited_Transcript_4-27-09.pdf (accessed June 2009)

Sheffi, Yossi. "Building a Resilient Organization." *The Bridge.* Vol. 37, No.1. National Academy of Engineering, 2007. http://www.nae.edu/nae/bridgecom.nsf/weblinks/CGOZ-6ZRLSP/$FILE/Bridge-v37n1.pdf?OpenElement (accessed June 2009)

Sheldon, Frederick and Stephen Batsell. "Position Statement: Methodology to Support Dependable Survivable Cyber-Secure Infrastructures." Presented at the 38th Hawaii International Conference on System Sciences, Waikoloa, Hawaii, 2005. http://www.csm.ornl.gov/%7Esheldon/public/SheldonFT-HICSS38v9c.pdf (accessed June 2009)

U.S. Congress. House. Committee on Homeland Security. U.S. Department of Homeland Security. 110th Cong., 1st sess. Statement by Jeff Gaynor. 25 July 2007. http://homeland.house.gov/SiteDocuments/20070725111505-98643.pdf (accessed June 2009)

U.S. Congress. House. Committee on Homeland Security. Statement by Randy Beardsworth, Former Assistant Secretary for Strategic Plans, U.S. Department of Homeland Security. 110th Cong., 1st sess. 25 July 2007. http://homeland.house.gov/SiteDocuments/20070725111424-25359.pdf (accessed June 2009)

U.S. Congress. House. Committee on Homeland Security. Statement by Susan R. Bailey, PhD., Vice President, Global Network Operations Planning, AT&T Inc. 110th Cong., 2nd sess. 6 May 2008. http://homeland.house.gov/SiteDocuments/20080506102203-38323.pdf (accessed June 2009)

U.S. Congress. House. Committee on Homeland Security. "The Resilient Homeland—Broadening the Homeland Security Strategy." Statement by Mary Arnold, Vice President, Government Relations, SAP. 110th Cong., 2nd sess. 6 May 2008. http://homeland.house.gov/SiteDocuments/20080506102152-56352.pdf (accessed June 2009)

U.S. Congress. House. Committee on Homeland Security. "The Resilient Homeland—Broadening the Homeland Security Strategy." Statement by Erroll G.

Southers, Assistant Chief, Homeland Security & Intelligence Division, Los Angeles World Airports Police Department, Associate Director for Educational Programs, Homeland Security Center for Risk and Economic Analysis of Terrorism Events, University of Southern California. 110th Cong., 2nd sess. 6 May 2008. http://homeland.house.gov/SiteDocuments/20080506102233-79198.pdf (accessed June 2009)

U.S. Congress. House. Committee on Homeland Security. "Partnering with the Private Sector to Secure Critical Infrastructure: Has the Department of Homeland Security Abandoned the Resilience-based Approach?" Statement by Jonah J. Czerwinski, Senior Fellow, Homeland Security, IBM Global Leadership Initiative, Managing Consultant, IBM Global Business Services. 110th Cong., 2nd sess. 14 May 2008. http://homeland.house.gov/SiteDocuments/20080514143358-14814.pdf (accessed June 2009)

U.S. Congress. House. Committee on Homeland Security. "GAO Responds to Gregg and Thompson's Call For Evaluation Of Pandemic Preparedness." 1 November 2007. http://homeland.house.gov/issues/index.asp?ID=293&SubSection=0&Issue=0&DocumentType=0&PublishDate=0 (accessed June 2009).

U.S. Congress. House. Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security. Carafano, James J. "Risk and Resiliency: Developing the Right Homeland Security Public Policies for the Post-Bush Era." 110th Cong., 2nd sess. Washington, D.C.: The Heritage Foundation, 24 June 2008. http://homeland.house.gov/SiteDocuments/20080625151302-26534.pdf (accessed June 2009)

U.S. Congress. House. Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security. "Partnering with the Private Sector to Secure Critical Infrastructure: Has the Department of Homeland Security Abandoned the Resilience-based Approach?" Statement by Jonah J. Czerwinski, Senior Fellow, Homeland Security, IBM Global Leadership Initiative, Managing Consultant, IBM Global Business Services. 110th Cong., 2nd sess. Washington, D.C, 14 May 2008. http://homeland.house.gov/SiteDocuments/20080514143358-14814.pdf (accessed June 2009)

U.S. Congress. Senate. Committee on Homeland Security and Government Affairs. Statement by Michael Chertoff, Secretary, United States Department of Homeland Security. 110th Cong., 2nd sess. 14 February 2008. http://hsgac.senate.gov/public/_files/021408Chertoff.pdf (accessed June 2009)

U.S. Congress. Senate. Committee on Homeland Security and Government Affairs. Statement by Testimony of Jane Bullock, Principal, Bullock & Haddow, LLC and former Chief of Staff, Federal Emergency Management Agency (FEMA) Ad Hoc Committee on State, Local and Private Sector Preparedness and Integration. 24 September 2008. http://hsgac.senate.gov/public/_files/Bullocktestimony.pdf (accessed June 2009)

U.S. Congress. Senate. Subcommittee on State, Local, & Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs. Statement by Dennis Schrader, Deputy Administrator, National Preparedness Directorate, Federal Emergency Management Agency, Department of Homeland Security. 110th Cong., 2nd sess. 5 June 2008. http://hsgac.senate.gov/public/_files/Schraderrevisedtestimony000.pdf (accessed June 2009)

U.S. Congress. Senate. Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs. Statement by Robert B. Stephan, Assistant Secretary, Infrastructure Protection, National Protection and Programs Directorate, Department of Homeland Security. 110th Cong., 1st sess. 12 July 2007. http://hsgac.senate.gov/public/_files/TestimonyRobertStephan.pdf (accessed June 2009)

U.S. Department of Homeland Security. *National Incident Management System.* Washington, DC: U.S. Department of Homeland Security, 2004. http://www.dhs.gov/xlibrary/assets/NIMS-90-web.pdf (accessed June 2009)

U.S. Department of Homeland Security. *Homeland Security Advisory Council: Report of the Critical Infrastructure Task Force.* Washington, D.C.: U.S. Department of Homeland Security, 2006. http://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf (accessed June 2009)

U.S. Department of Homeland Security. *National Infrastructure Protection Plan.* Washington, D.C.: U.S. Department of Homeland Security, 2006.

U.S. Department of Homeland Security. *Communications: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan.* Washington, D.C.: Department of Homeland Security, 2007. http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications.pdf (accessed June 2009)

U.S. Department of Homeland Security. *Target Capabilities List: A Companion to the National Prepareness Guidelines.* Washington, DC: Department of Homeland Security, 2007. http://www.fema.gov/pdf/government/training/tcl.pdf (accessed June 2009)

U.S. Department of Homeland Security. *National Incident Management System.* Washington, DC: U.S. Department of Homeland Security, 2008. http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf (accessed June 2009)

U.S. Department of Homeland Security. *National Response Framework.* Washington, D.C.: U.S. Department of Homeland Security, 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (accessed June 2009)

U.S. Department of Homeland Security. 2008. *National Response Framework Emergency Support Function Annexes.* Washington, D.C.: U.S. Department of Homeland Security, 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-esf-all.pdf (accessed June 2009)

U.S. Department of Homeland Security. *Overview: ESF and Support Annexes Coordinating Federal Assistance In Support of the National Response Framework.* Washington, D.C.: U.S. Department of Homeland Security, 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-overview.pdf (accessed June 2009)

U.S. Department of Homeland Security. *Risk Lexicon.* Washington, D.C.: U.S. Department of Homeland Security, 2008. http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf (accessed June 2009)

U.S. Department of Homeland Security. *Voluntary Private Sector Preparedness Accreditation and Certification Program.* Washington, D.C.: U.S. Department of Homeland Security, 2008. http://www.fema.gov/media/fact_sheets/vpsp.shtm (accessed June 2009)

U.S. Department of Homeland Security. *Voluntary Private Sector Preparedness Accreditation and Certification Program: Proposed Target Criteria for Preparedness Standard.* Washington, D.C.: U.S. Department of Homeland Security, 2008. http://www.fema.gov/media/fact_sheets/vpsp.shtm (accessed June 2009)

U.S. Department of Homeland Security. *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency.* Washington, D.C.: U.S. Department of Homeland Security, 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed June 2009)

U.S. Department of Transportation Research and Special Programs Administration. "Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout New York City." Cambridge, MA: U.S. Department of Transportation ITS Joint Program Office and Federal Highway Administration Office of Transportation Operations, 2004. http://ntl.bts.gov/lib/jpodocs/repts_te/14023_files/14023.pdf (accessed June 2009)

U.S. The White House. *National Strategy for Homeland Security.* Washington, D.C.: U.S. The White House, 2002.. http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf (accessed June 2009)

U.S. The White House. *Homeland Security Presidential Directive 7.* Washington, D.C.: U.S. The White House, 2003. http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm (accessed June 2009)

U.S. The White House. *Homeland Security Presidential Directive 8.* Washington, D.C.: U.S. The White House, 2003. http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm (accessed June 2009)

U.S. The White House. *National Strategy for Homeland Security.* Washington, D.C.: U.S. The White House, 2007. http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed June 2009)