National Infrastructure Advisory Council

Optimization of Resources for Mitigating Infrastructure Disruptions Study

Final Report and Recommendations by the Council

October 19, 2010

Margaret Grayson
Working Group Co-Chair
President
Grayson & Associates

Tom Noonan
Working Group Co-Chair
Former General Manager
IBM Internet Security Systems

Table of Contents

Acknowledgements

NIAC Working Group Members

Margaret Grayson, President, Grayson & Associates
Tom Noonan, Former General Manager, IBM Internet Security Systems

Study Group Members

Peter Allor, Senior Security Strategist, IBM Corporation
Cherrie Black, State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) Co-Chair and Chair, Regional Partnership Working Group
Lt. Gen. (ret.) Albert J. Edmonds, Chairman and Chief Executive Officer, Edmonds Enterprise Services, Inc.
Patrick Gray, Principal Security Strategist, CISCO Systems
David Kepler, Executive Vice President, Chief Sustainability Officer, Chief Information Officer, Corporate Director of Shared Services, Dow Chemical
James B. Nicholson, President and Chief Executive Officer, PVS Chemicals, Inc.
Ulie Seal, SLTTGCC Chair

Support Staff

Robert Briggs, SRA International
Jim Carey, Energetics Incorporated
Kate Finnerty, Energetics Incorporated
Melissa Hill, SRA International
Marc Sigrist, Energetics Incorporated

Executive Summary

Study Overview

Within national policy, the infrastructure sectors, and the communities they serve, there is a growing awareness of, and focus on, the need and opportunity for enhanced collaboration in understanding and planning for resilient communities. Collaboration among public and private partners is essential to *keep communities above water*—literally and economically.

To address this critical intersection between infrastructure resilience and the communities they serve, the National Infrastructure Advisory Council (NIAC) undertook this *Optimization of Resources for Mitigating Infrastructure Disruptions* study with the objective of identifying how the capabilities and resources that support infrastructure resilience can *better contribute* to community resilience. Two key questions frame the study:

- What are the potential enablers of infrastructure resilience that can support and strengthen community resilience?
- Are there significant weaknesses in infrastructure resilience that limit the ability of communities to achieve resilience?

NIAC members represent extensive infrastructure expertise and knowledge—in the challenges and opportunities for infrastructure protection and resilience, and the benefits of the Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) public-private partnership model in deriving shared outcomes. This study extends the work done in the NIAC 2009 *Critical Infrastructure Resilience* study by providing a framework for how and where the infrastructure protection and resilience mission can better support the broad national mission of community resilience.

The National Policy Framework

With the publication of the DHS *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland (QHSR)* in February 2010, the Administration established a new strategic framework for DHS. The QHSR defines the homeland security "enterprise" as the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. It connotes a broad-based community with a common interest in the safety and well-being of America and American society.

In accordance with this framework, the QHSR established two core resilience objectives:

- An objective of ensuring *broad-based* resilience: "Improve capabilities of families, communities, private sector organizations, and all levels of government to sustain essential services and functions."
- An objective of ensuring *infrastructure* resilience: "Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions."

This study and its 2010 companion study*, A Framework for Establishing Infrastructure Resilience Goals,* directly address these two QHSR objectives.

Findings

The NIAC has four general observations that result from this study. These observations underpin the specific findings of the study. First, the NIAC recognizes the important role played by leadership—public and private alike—in community resilience. Second, we believe that personal responsibility plays a key role in the nexus between community resilience, critical infrastructure, and resource optimization. Third, public and private sector infrastructure service providers clearly (and obviously) play a major role in communities, not just as service providers but as employers, individuals, families, community members, volunteers, and neighbors. Finally, as noted in the 2009 *Critical Infrastructure Resilience* study, there are critical sectors and all levels of government that have long-established, well-proven programs and processes for sharing resources; e.g., mutual aid agreements and prepositioning of material. In general, there are excellent sources available for lessons learned and models of resilience.

There are nine major findings:

The resilience component of the National Infrastructure Protection Plan (NIPP) is not well understood. There is presently no widely shared understanding, among public and private partners alike, of (1) what infrastructure resilience activities are and (2) how they contribute to community resilience.

At the community level, interdependencies—among infrastructure sectors and within and across communities—are often not well defined or understood. Although there is *awareness* that interdependencies are critical and should be addressed, the *tools and knowledge base* needed to support this effort are generally not available.

Stakeholder education is critical and can be enhanced. Communication within and across communities is always challenging; however, a common understanding of community and infrastructure risks, consequences, and resilience capabilities—and limitations—is critical to building a future in which mutual resilience is better assured.

In general, many infrastructure systems are designed to be resilient in order to satisfy customer demands for service availability. These systems are designed to work as a whole to achieve service delivery, both to ensure steady-state operations and in many cases to respond to disruptions.

Early development and deployment of structured relationships and processes between critical infrastructures and the communities they serve is necessary. Planning and response agreements are valuable tools that can provide a more robust foundation for enhancing community resilience.

Testing plans and processes and conducting exercises are critical to resilience. Evaluating relationships, processes, and tools will contribute to identifying and refining *which* resources are critical to resilience and *how* they can best be applied.

Existing information-sharing mechanisms can be effective models for improving communications and understanding across sectors and communities. Building on existing models to improve the integration of community-level information with that of infrastructure service providers can enhance planning and response capabilities.

Mutual aid agreements and other existing sector and government mechanisms for resource management can be effective tools to aid community resilience. Broader application of such agreements—across sectors, across communities, and between sectors and communities—can provide a more flexible, better resourced, and timelier basis for allocating shared resources to best effect infrastructure service delivery and community recovery.

The legal and regulatory environment can vary significantly across different service areas and may hamper the ability of infrastructure service providers to bring to bear additional resources during times of service disruption. The lack of commonly and broadly accepted agreements across jurisdictions hampers the ability of infrastructure service providers to deliver all of the resources that are necessary to restore services and thus enable communities to recover.

Combined, these findings demonstrate that there is much to build upon, including lessons learned and model approaches to resilience; private and public leadership in planning and response for service restoration; and an evolving understanding of interdependencies, vulnerabilities, and options for resilient capabilities.

Recommendations

The NIAC has six major recommendations. These address (1) improving the understanding of resilient activities across and among infrastructures and communities; (2) enhancing regional and community-level information exchange; (3) expanding the availability of low-cost, scalable tools and techniques; (4) enhancing the transfer of expertise and lessons learned from national-level infrastructure planning and analysis to regional and community-level systems; (5) identifying the impact on critical infrastructure services that result from changes in the Threat Condition under the Homeland Security Advisory System; and (6) removing cross-jurisdictional and other impediments to the transportation and use of outside assets during an emergency.

1. **The DHS Office of Infrastructure Protection (DHS-IP) should lead a national effort to improve the understanding of resilient activities and how they are implemented in support of combined infrastructure and community resilience.** Such an effort requires the establishment of a widely shared, well-understood description of the elements of infrastructure resilience and how they can contribute to community resilience. As part of a revised NIPP or as a separate supporting document, DHS-IP should develop—in collaboration with critical infrastructure stakeholders both within and outside of government—a common framework to enable infrastructure and community partners to identify, plan, implement, and assess the various resilience activities.

2. **DHS-IP should take a leadership role in an initiative to enhance regional and community-level information exchange through the increased availability of data, information, tools, and techniques that may bear upon critical infrastructure protection and resilience. The NIAC especially recommends that this information exchange be expedited through the wider use of fusion centers, and that the NIAC should examine how to enhance infrastructure owner/operator participation in, and contributions to, fusion-center effectiveness in community/infrastructure resilience.** The ability for non-Federal entities to plan and execute resilience activities is dependent on good information *and* the tools and techniques to apply this information to good effect. The transfer of lessons learned and proven technology and organizational-approach models from infrastructure collaborations in Federal information sharing can provide a valuable tool kit for community-level improvements in information sharing.

3. **DHS-IP should expand the provision of scalable, low-cost tools and techniques for community-level identification and assessment of infrastructure interdependencies.** There are many effective tools and techniques that are widely used on a national level to assess interdependencies and their potential impacts. Further development and transfer of infrastructure-based tools for applications such as dependency analysis and cybersecurity assessment could demonstrably increase the ability of communities to establish an improved baseline of infrastructure assets and their relationship to individual communities or groups of communities. Knowledge of these interdependencies can in turn improve the planning for and use of resources by critical infrastructure operators and the local community.

4. **DHS-IP should lead a continuing effort to enhance the transfer of expertise and lessons learned from national-level infrastructure planning and analysis to regional and community-level systems.** There is a wide range of valuable expertise and knowledge within Federal, State, and local governments that could, if made available in an appropriate format, bolster community understanding of, and planning for, resilience. The NIAC also encourages the individual sectors, acting through their representative Sector Coordinating Councils or other channels, to identify and make available to local communities tools, techniques, and lessons learned that could enhance local and regional resilience. The NIAC especially encourages larger commercial distribution industries to consider how their supply chain expertise might be applicable to the optimization of resources during an emergency.

5. **DHS-IP should develop a national "playbook" to be used by DHS to clearly identify the impact on critical infrastructure services that result from changes in the Threat Condition under the Homeland Security Advisory System.** In its discussions, the NIAC found that, when the national threat level is elevated, the protective measures associated with this change may have unanticipated consequences on the ability of infrastructure providers to deliver needed services at the regional and community level. To help maintain a community's resilience, infrastructure providers need a clear "playbook" of what actions the Federal government is expected to take with a given change in threat level. In turn, such a playbook will enable infrastructure owners and operators to provide both DHS and their customers with an improved picture of the actions industry will take under the various threat levels and more clearly spell out the implications for service delivery. Ideally, the playbook would address national, regional, community, and sector-specific threat-level changes.

6. **The NIAC should prepare a follow-up report to the July 2009 *Framework for Dealing with Disasters and Related Interdependencies* report to determine the implementation status of recommendations to remove cross-jurisdictional and other impediments to the transportation and use of outside assets during an emergency. It is recommended that this follow-up report also explore the possibility of implementing standard approaches and agreements to alleviate these constraints.** Although infrastructure operators generally have well-established processes for working with government within their service areas, moving and applying assets from outside the affected jurisdiction(s) often face significant constraints. A consolidated effort of government and infrastructure service providers, working through appropriate public-private sector partnership mechanisms, should focus on (1) identifying key cross-jurisdictional bottlenecks and (2) implementing standard approaches to remove these impediments for the purposes of optimizing the sharing of resources during major disruptions. One example is the development of credential standards needed to respond to all hazards, as directed by the *Post Katrina Emergency Management Reform Act of 2006*.

The NIAC believes these recommendations address significant gaps in the present resilience planning and implementation framework, and if acted upon, can help enable substantive improvements in optimizing resources for improved infrastructure and community resilience. Just as "a rising tide floats all ships," collaboration among public and private resources can contribute to keeping communities above water—literally, socially, and economically. The Council believes that enhancements to joint infrastructure and community resource management *can* contribute substantially to this shared outcome.

1.0 Introduction

There is a growing awareness and focus—within national policy, the infrastructure sectors, and the communities they serve—of the need and opportunity for enhanced collaboration in the understanding of, and planning for, resilient communities. To address this critical intersection between infrastructure resilience and the communities they serve, the National Infrastructure Advisory Council (NIAC) undertook this study with the objective of **identifying how the capabilities and resources that support infrastructure resilience can *better contribute* to community resilience.**

In October 2009, the NIAC delivered a study, *Critical Infrastructure Resilience*, which specifically examined the ways in which infrastructure could become more resilient. The study was a leading voice in establishing resilience as a fundamental concept for sustaining and enhancing infrastructure capability. It defined the core elements of infrastructure resilience and how they contribute to the Nation's security and our quality of life.

With the publication of the Department of Homeland Security (DHS) *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland (QHSR)* in February 2010, the Administration established a new strategic framework for DHS. This framework established resilience as one of three core concepts in a comprehensive approach to homeland security:

- Security: Protect the United States and its people, vital interests, and way of life
- Resilience: Foster individual, community, and system robustness, adaptability, and capacity for rapid recovery
- Customs and Exchange: Expedite and enforce lawful trade, travel, and immigration

The concept of resilience encompasses mitigating risk to communities, enhancing recovery capabilities, and ensuring continuity of essential services and functions. Accordingly, the QHSR established two core resilience objectives:

- An objective of ensuring *broad-based* resilience: "Improve capabilities of families, communities, private sector organizations, and all levels of government to sustain essential services and functions."
- An objective of ensuring *infrastructure* resilience: "Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions."

The Optimization of Resources for Mitigating Infrastructure Disruptions study is one of two 2010 NIAC studies. This study, along with its companion study*, A Framework for Establishing Infrastructure Resilience Goals,* directly address these two QHSR objectives. They extend the work done in the NIAC's 2009 *Critical Infrastructure Resilience* study by assessing the infrastructure-community interface and establishing a model for infrastructure resilience goals.

2.0 Study Context: Resilience Today

Although the NIAC mission is to help meet the challenge of infrastructure protection and resilience, the members understand that to be most effective, infrastructure progress must be integrated with efforts in the communities they serve and other aspects of homeland security. The QHSR states that DHS should: ". . . delineate a homeland security strategy, including an outline of priority mission areas, not simply for DHS, but for the homeland security enterprise as a whole—embracing Federal, State, local, tribal, and territorial governments, nongovernmental organizations, the private sector, as well as individuals, families and communities."

This new strategic framework envelops the entire "ecosystem" of infrastructure-related services and products—both the service providers and those who rely on these services at the individual, family, and community level. It clearly ties infrastructure resilience to the broad-based resilience of communities and their constituents. The NIAC embraces this inclusive context and the importance of understanding resilience from multiple perspectives. Accordingly, the following sections provide a sampling of related information and perspectives—about infrastructure owners and operators, Federal programs, communities, and prior NIAC studies—that are germane to the study.

2.1 Resilience in Infrastructure Systems and Services

The 2009 NIAC *Critical Infrastructure Resilience* study stated that "Resilience has become an important dimension of the critical infrastructure protection mission, and a key element of the value proposition for the partnership with the government because it recognizes both the need for security and the reliability of business operations." The context of infrastructure security efforts is continuously evolving, both to better recognize and enhance *current* resilient activities and to establish *new* models for resilience, exemplified in the 2010 NIAC study on a framework for resilience goals. This evolution crosscuts all aspects of the business enterprise: management of physical and cyber systems and assets; plans and processes for service delivery; and the organizational relationships among providers, customers, and government.

It is important to note, however, that resilience is already embedded in many current infrastructure practices. The 2009 study elaborates: "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."

Within this broad context, the size, reach, resources, and sophistication of infrastructure service providers varies greatly, both within individual sectors and across the 18 critical sectors. From the 2009 study: "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-sized businesses, for example, may lack sophisticated continuity of operations plans and may not have the resources to continually monitor the risk landscape."

The NIAC reaffirms this characterization and believes that there are parallels between these characteristics and the associated characteristics demonstrated across a wide diversity of communities. There are other relevant recommendations from prior NIAC studies, specifically including cybersecurity, which this study strongly endorses. Appendix C presents a summary of relevant recommendations from the 2009 resilience study and earlier NIAC studies.

2.2 Current DHS Resilience Programs

To implement the homeland security mission, Federal Government agencies and critical infrastructure sectors are developing and deploying programs related to resilience as delineated in the NIPP, these programs are implemented to support an approach that is comprehensive, coordinated, and cost effective in order to help reduce or manage the risks to the Nation's most critical assets, systems, and networks. During interviews for this study, subject matter experts cited various federally sponsored programs implemented by State and local jurisdictions. These programs are consistent with the focus of this study and they exhibit the following positive characteristics:

- Enhancement of the identification and understanding of interdependencies
- Improvement of the Federal Government's coordination with other levels of government
- Institutionalization of relationships and processes among partners
- Sharing and use of available technologies and tools

For example, the Regional Resilience Assessment Program (RRAP) is conducted in cooperation with State and local governments and critical infrastructure owners and operators to assess critical infrastructure risk on a regional level, address capability gaps of the surrounding communities and region, and coordinate associated protection activities. Multiple tools—including vulnerability assessments, capabilities assessments, and infrastructure protection planning efforts—are used to identify and analyze critical infrastructure dependencies, interdependencies, capabilities, and security gaps. A listing and description of current DHS programs supporting the resilience mission is presented in Appendix B.

Exhibit 2.1 RRAP: A Model for Integrating Regional Resilience Planning

The Regional Resiliency Assessment Program (RRAP) is viewed in the field as a model example of collaboration for two primary reasons: it incorporates key partners from the beginning of the assessment process and maps a DHS-provided capability to needs identified by participating private and public sector partners. RRAP provides integrated, interagency assessment of specific critical infrastructure and regional analysis of the surrounding infrastructure, including key interdependencies. The RRAP incorporates vulnerability and capability assessments with infrastructure protection planning efforts to assemble a comprehensive analysis of a region's critical infrastructure and prevention and protection capabilities.

Five RRAPs were performed in Fiscal Year 2009 (FY 2009) in the Chicago Financial District; Raleigh-Durham, NC Research Triangle; the Exit 14 Chemical Corridor of the New Jersey Turnpike; New York State Bridges; and the Tennessee Valley Authority. These pilot projects provide State and local stakeholders with a comprehensive understanding of a region's vulnerabilities, and provide critical risk-based information on how to apply the most cost-effective protective measures to the most vulnerable regional assets. In FY 2010, RRAPs are being performed in the six regions of Atlanta, the Las Vegas Strip, Massachusetts, Seattle, Texas, and West Virginia.

The RRAPs represent a critical step forward in understanding and identifying the nature and functions of critical infrastructure within these specific regions. For example, in Atlanta, the RRAP's primary focus on the Commercial Facilities Sector and secondary focus on Energy, Water/Wastewater, and Transportation Sectors revealed significant common security and resiliency vulnerabilities. Assessments included 12 Enhanced Critical Infrastructure Protection, 10 Site Assistance Visits, 7 Consequence-Based Assessment Tools, and 3 Buffer Zone Plans assessments.

Sources: "Regional Resiliency Assessment Program," Presented by Charles Hamilton, PSA (El Paso) and James Hardy, PSA (Atlanta), at the 2010 UASI Conference in New Orleans on June 23, 2010 and "Regional Resiliency Assessment Program Fact Sheet," DHS IP Protective Security Coordination Division, October 2009.

2.3 Non-Federal Community Resilience Actions

Across the Nation, State and local governments recognize the complexity of resilience and are taking steps to define and plan for community resilience. These leaders already know that emergencies and disasters know no political boundaries. Collaborative efforts —regular contact with critical infrastructure owners and operators, workshops and conferences, training and exercises, applying lessons learned— are tools used by the jurisdictions and regions that are actively planning for the resilience of their jurisdictions and regions. Additionally, increased collaboration with the Federal Government, issuance of national plans, and availability of Federal resources are leading to many accomplishments in support of community resilience. These include an increased awareness of critical infrastructure issues by non-Federal entities, enhanced identification of critical sites and networks, establishment of additional partnerships, and an evolved dialogue that spans protection, resilience, and interdependencies. As the resilience and community resilience debate continues, organizations such as the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) are particularly germane in providing substantive input to the Federal Government on issues of importance or concern to communities across the Nation. This will ensure that non-Federal partners are active and integrated into the national resilience mission in order to inform and improve national efforts to increase protection and resilience at all levels.

2.4 A Viewpoint of Community Resilience

Communities are considered to be essential partners in the homeland security enterprise. Their involvement is accomplished through the awareness and empowerment of the public in terms of their own preparedness and through planning and response by government agencies and industry within the community. By recognizing that there are vast differences in types of communities, the NIAC does not posit a concrete definition of community. Further, the study recognizes that community resilience is not simply an end point, but is one element of a comprehensive preparedness and response spectrum.

Therefore, a community's preparedness and steady-state health is just as important to its resilience as its capability in incident response.

In practicality, it is difficult to identify the boundaries of a community, in part because proximity and jurisdictional boundaries alone do not always define a true community. From the perspective of resilience, a community in its simplest terms is one that collectively deals with a significant disruption to its social and economic life.

A resilient community is a complex and multifaceted concept. In general terms, the concept refers to the capacity of a community to bounce back from an event by mounting a collective response. Factors that contribute to community resilience include the following:

- A ***mindset of self-reliance*** among community members fosters responsibility for each other, a commitment to the community, and the mobilization to come together as needed to overcome obstacles.
- ***Well-established working relationships*** facilitate the mutual trust and communications needed for effective cooperation.
- ***Community-based organizations*** and institutions are positioned and willing to mobilize, work together, and step in as needed to protect and preserve public health and safety.
- ***Emergency plans*** are pre-established and exercised.
- ***Community preparedness*** programs are an integral part of public outreach and serve to educate the public on expectations and how to protect themselves.
- The ability to ***adapt to changing conditions*** by adjusting plans and actions enables the mitigation of impacts and restoration of critical services.

Additionally, the wide diversity of communities must be recognized. This diversity is reflected in a variety of factors—size, predisaster economic vitality, the degree of prior experience in collaborating with multiple public and private partners, and others. In some communities a company, or a handful of companies, is the heart and soul of the community—if these companies cannot rebound from disaster, the entire community is at risk.

3.0 Study Structure

3.1 Objective and Scope

The objective of this study is to identify how the capabilities and resources that support infrastructure resilience can *better contribute* to community resilience. Two key questions frame the study:

- What are the potential enablers of infrastructure resilience that can support and strengthen community resilience?
- Are there significant weaknesses in infrastructure resilience that limit the ability of communities to achieve resilience?

As owners and operators of the Nation's infrastructure, NIAC members represent extensive infrastructure expertise and knowledge—in the challenges and opportunities for infrastructure protection and resilience, and in the benefits of the public-private partnership model in deriving shared outcomes. Nonetheless, in serving communities across the Nation, the infrastructure mission is to keep the lights on, not to ensure that there is a *viable community to shine the lights on*. However, critical infrastructure owners and operators recognize their dependency on healthy communities to maintain the health of their businesses. This study provides a framework for how and where the infrastructure mission can better support the broader mission of community resilience.

The study scope covered three primary topics: functions, resources, and government policy and programs. With respect to functions, the study addresses the following considerations:

- What are current practices in aligning infrastructure resilience with community resilience?
- Are there existing success models in public-private partnerships that can guide improvements in infrastructure and community resilience?
- Where are the best areas of opportunity for achieving synergies among communities and sectors?

With respect to resources, the study considers the following:

- Are there key weaknesses in resource management and sharing?
- Are there applicable models for resource management that build synergies across the public-private enterprise?
- What opportunities are there to enhance collaborative resource planning and management?

With respect to government policy and programs, the study considers the following:

- How do existing government programs help or hinder synergies in these areas?
- What steps might the government take to encourage the contribution of infrastructure resilience to community resilience?

3.2 Key Aspect: Enhancing the Synergy between Infrastructure Resilience and Community Resilience

> **From the QHSR:**
>
> The homeland security "enterprise" refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. It connotes a broad-based community with a common interest in the safety and well-being of America and American society.

As previously noted, the QHSR has delineated infrastructure resilience and community resilience as two core and complementary objectives. These objectives fit within a unified homeland security "enterprise." The National Infrastructure Protection Plan (NIPP) supports the QHSR framework, defining resilience as the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions. The NIAC definition from the 2009 *Critical Infrastructure Resilience* study aligns closely with this definition, identifying infrastructure resilience as the ability to reduce the magnitude and/or duration of disruptive events. It is the ability to *anticipate, absorb, adapt to, and/or rapidly recover* from a potentially disruptive event.

Within the QHSR context, community resilience is the capability to return citizens to work, reopen businesses, and restore the basic services and economic stability of a community or a linked group of affected communities.

Key aspects of infrastructure and community resilience that are shared include identification and understanding of interdependencies—across communities, across services —and the availability, timing, and coordination of resources—local, regional, and national in scope. Both considerations were prevalent themes throughout the study.

3.3 Approach

To conduct the study, a NIAC Working Group convened a Study Group consisting of senior executives and subject matter experts (SMEs) with extensive experience and leadership (1) across critical infrastructures and State, local, regional, and community governments and (2) with expertise in topics such as emergency preparedness and response. As noted, the study input came from roundtable and individual discussions with leaders and experts in government *and* industry, infrastructure *and* communities, as well as supporting research on existing policies, programs, and practices. The study was conducted in four phases:

- *Phase 1: Capturing community perspectives and insights.* This phase established a community-focused information baseline that crosscuts infrastructure sectors and service-delivery areas. Activities included roundtable discussions with the SLTTGCC and the Regional Consortium Coordinating Council (RCCC), discussions with community-focused service organizations, and interviews with SMEs.
- *Phase 2: Engaging infrastructure service providers to capture their perspectives on community resilience.* This phase shared results of the first phase with infrastructure owners and operators and elicited infrastructure perspectives in order to build a joint picture of how infrastructure and community resilience interrelate. Activities included interviews and discussions with executives and SMEs from key sectors.

- *Phase 3: Comparing community and owner and operator perspectives.* This phase identified gaps and opportunities for enhancing community resilience. Activities included follow-up engagements to clarify and expand on identified issues, improving joint understanding of problems *and* potential solutions.
- *Phase 4: Identifying and clarifying key findings and recommendations.* This final phase compared current capabilities for resilience with the QHSR and NIPP objectives; identified apparent gaps in resource management; and identified potential improvements in identifying, sharing, and applying resources.

The Study Group gathered information from five main categories of sources:

- Executive interviews in key sectors to gain strategic perspectives on interdependencies among sectors and communities
- Panel discussions with SLTTGCC and RCCC members to assess the intersection of infrastructure and community resilience
- Interviews with SMEs to examine practices, interdependencies, and the associated effects on the community
- Review of government policies and programs to identify current resilience practices at the Federal, State, local, and regional levels
- Review of infrastructure and community resilience studies and literature to identify case studies and best practices

Of particular note is the engagement with members of the SLTTGCC, the RCCC, and others groups representing communities across the Nation. By reaching out beyond the immediate NIAC community, the study benefited from a wide range of community-based perspectives and insights.

4.0 Findings

In its data-gathering and analysis efforts, the study absorbed information from a very broad range of sources in infrastructure resilience and community resilience. When analyzed, the information yielded findings that are *highly* consistent across different sources. The following are general observations and key findings.

4.1 General Observations

There are four general observations that result from this study. These observations underpin the specific findings of the study.

First, the NIAC recognizes the important role played by leadership, from the public and private sectors alike, in community resilience. Business leaders and elected officials—as well as directors of law enforcement, emergency preparedness, and other service organizations—must be involved in coordinated planning at the community level to ensure that their communities are as resilient as possible. The engagement of senior public-private sector leadership in critical infrastructure protection and resilience is a recurrent theme in NIAC studies.

Second, we believe that personal responsibility plays a key role in the nexus between community resilience, critical infrastructure, and the optimization of resources. The cornerstone of community resilience is individual and household readiness. The NIAC applauds the efforts of the Federal Emergency Management Agency (FEMA) Citizen Corps and similar organizations that promote community resilience and offer practical suggestions as to how individuals and communities can enhance their own readiness. Readiness at the individual and community levels directly supports the goal of optimizing the use of resources for the purposes of resilience. The acceptance of personal and community responsibility for local resilience is a cornerstone for a culture of resilience that makes the Nation stronger and more prepared for any manmade or natural disaster. Given this, infrastructure service providers can engage their customers to mutual benefit in planning for resilience.

Third, public and private sector infrastructure service providers clearly (and obviously) play a major role in communities. We note that they contribute not simply as service providers, but as employers, individuals, families, community members, volunteers, and neighbors. By the very nature of their jobs, many individuals in key sectors are well prepared and resilient—their jobs and organizations depend on it.

Finally, as noted in the 2009 *Critical Infrastructure Resilience* study, some critical infrastructure sectors, and all levels of governments, have long-established, well-proven programs and processes for resource sharing (e.g., mutual aid agreements and prepositioning of material). For many key sectors, these factors combine preparedness and resilience and are simply the accepted way of ensuring business and service continuity. Similarly, for State and local governments, it is often the successful path to sustaining healthy, viable communities. We are reminded that resilience is part of a *systematic,* rather than stand-alone, approach to risk management; communities that are not prepared are not likely to be resilient.

Combined, these factors demonstrate that there is much to build upon. This includes lessons learned and model approaches to resilience; public and private leadership in planning and response for service restoration; and understanding of interdependencies, vulnerabilities, and options for resilience capabilities.

4.2 Specific Findings

There are nine major findings:

1. **The resilience component of the NIPP is not well understood.** Presently, there is no widely shared understanding at the community level of (1) what infrastructure resilience activities are and (2) how they contribute to community resilience. To support its mission of enhancing cooperation between the public and private sectors, the NIAC has developed its definition of infrastructure resilience, as described in Section 2. The NIPP provides a similar definition. Improved communication of a resilience-planning framework at the community level would help infrastructures and the communities they serve to jointly identify and manage where and how resources might be leveraged.

2. **At the community level, interdependencies—among infrastructure sectors, and within and across communities—are often not well defined and understood.** Although there is *awareness* that interdependencies are critical and should be addressed, the *tools and knowledge base* to support this effort are generally not available. The challenges of understanding interdependencies are equally important for national resilience and community resilience.

3. **Stakeholder education is critical and can be enhanced.** Although communication within and across communities is always challenging, a common understanding of community and infrastructure risks, consequences, and resilience capabilities—and limitations—is critical to building a future where mutual resilience is better assured. A shared understanding of what each party has to contribute—among the public, public servants, and service providers alike—is necessary to best identify and plan how resources can be shared for mutual benefit.

4. **In general, many infrastructure systems are designed to be resilient in order to satisfy customer demands for service availability.** They are classic systems (i.e., composed of physical and cyber subsystems and components designed to work as a whole to achieve service delivery). In contrast, the "systems" of roles and responsibilities across different communities may be less structured, with unknown or misunderstood interdependencies.

5. **Early development and deployment of structured relationships and processes between critical infrastructures and the communities they serve is necessary.** Today, many infrastructure sectors employ planning and response agreements with their service communities that define key relationships and processes such as points of contact, communication protocols, expectations for response, and the availability of infrastructure resources to aid in general community response and recovery. Such agreements are highly useful tools that can provide a more robust foundation for enhancing community resilience.

Exhibit 4.1 Coordination among Partners and Customers: Memphis Adapts after Summer Storm of 2003

On July 22, 2003, a severe summer storm impacted southwestern Tennessee, particularly Shelby County and the City of Memphis. Commonly referred to as "Hurricane Elvis," its winds reached the levels of a Category 2 hurricane. The storm caused seven deaths and damage costs exceeding $525 million in Shelby County alone. The event left 339,000 electrical customers affected, which represented over 80 percent of Memphis Light, Gas and Water (MLGW) Division customers. Additionally, the storm affected eight water pumping stations, impacting more than 70 percent of MLGW customers.

Although the region averted a major water crisis through water conservation and survived without any major transmission damage, a need for major improvements in the Division's disaster preparedness and response framework was revealed. Through lessons learned in the storm, the Division revised its Emergency Response Plan (ERP) to better adapt to a wide range of hazards and adapted its use of resources. The Division added an ERP Coordinator position and adjusted restoration priorities—with a primary focus on restoring service to hospitals, water pumping facilities, public sewage, and airport. Additionally, the Division adapted to National Incident Management System compliance and developed a model to estimate outage duration. The Division has ongoing objectives to mitigate weakness (such as Smart Grid), reduce a major event down to between 7 and 9 days before total restoration, increase customer awareness, and provide customers with a satisfactory response.

As part of their outreach efforts, the Division added new methods of communicating with its crew and customers. The Division opened a Customer Care Center, with a staff of 70 agents, to assist customers in the preparation and response efforts following a major disaster, in addition to daily administrative duties. The Division also set up a Commercial Resource Center, staffed by 10 agents, to assist business customers in emergencies and offer numerous services, ranging from publications to online reference libraries.

Sources: "Disaster Recovery Planning for High Consequence Events," Presented by Richard Bowker at the 2010 Media Disaster Preparedness Conference," April 27, 2010 and "Memphis Summer Storm of 2003," Wikipedia. Available at http://en.wikipedia.org/wiki/Memphis_Summer_Storm_of_2003.

6. **Testing plans and processes and conducting exercises are critical to resilience.** Established plans are necessary, but they are not sufficient. Evaluating relationships, processes, and tools will contribute to identifying and refining *which* resources are critical to resilience and *how* they can best be applied. Infrastructures and communities should have systems that are tested and proven, both to deal with known threats through scenario testing and to adapt to new conditions and threats. Practice, if not necessarily making things perfect, is vastly better than the alternative.

7. **Existing information-sharing mechanisms can be effective models for improving communications and understanding across sectors and communities.** There are fusion centers that are models in aligning community-level information sharing with broader (regional and national) information content. Similarly, there are established sector-specific mechanisms that share time-sensitive information critical to maintaining or reestablishing infrastructure services. Building on these models to improve integration of community-level information with that of infrastructure service providers could enhance both planning and response capabilities.

Exhibit 4.2 Fusion Center Stimulates Vital Information Sharing Link

The DHS Office of Infrastructure Protection (IP) has partnered with the Northern California Regional Intelligence Center (NCRIC) to bolster information-sharing efforts among the region's various levels of government and critical infrastructure owners and operators. The NCRIC, formed to provide comprehensive intelligence products to public safety agencies and corporate partners, has engaged both the public and private sectors to ensure heightened vigilance and collaboration. In a recent example, the NCRIC teamed up with the private sector to provide businesses and local public safety agencies with situational awareness in downtown Oakland in advance of a controversial trial verdict of a former Bay Area Rapid Transit (BART) officer.

Oakland's preparation for riots during the trial of a BART police officer, who was accused of murdering an unarmed African-American male on January 1, 2009, posed a direct challenge to the partnership between the NCRIC and the region's business community. City and private sector officials were concerned about potential reprisal of previous riots that followed the release of a cell-phone video of the shooting.

As a model of the partnership in action, the Regional Incident Discussion Board on Homeland Security Information Network-NCRIC provided a vital link between infrastructure owners and operators, the fusion center, and the respective emergency operations centers activated in advance of the trial verdict. The collaboration proved necessary as riots erupted in downtown Oakland. The rapid communications enabled through HSIN-NCRIC led to the safe closure and restoration of businesses in the downtown Oakland area, minimizing the riot's effect on local business continuity.

Sources: "Regional and Local Information Sharing Enhancement," *Homeland Security NIPP News,* Issue 54: July-August 2010; and McKinley, Jesse. "Officer Guilty in Killing that Inflamed Oakland," *New York Times*, Published July 8, 2010. Available at http://www.nytimes.com/2010/07/09/us/09verdict.html; and The Northern California Regional Intelligence Center Web site, www.ncric.org (Accessed on August 24, 2010).

8. **Mutual aid agreements and other existing sector and government mechanisms for resource management can be effective tools to aid community resilience.** Many infrastructure sectors and governments routinely employ mutual aid agreements to plan and implement resource sharing within and across sectors and jurisdictions during times of duress. Broader application of such agreements—across sectors, across communities, and between sectors and communities—can provide a more flexible, better resourced, and timelier basis for allocating shared resources to best effect infrastructure service delivery and community recovery.

9. **The legal and regulatory environment can vary significantly across different service areas and may hamper the ability of infrastructure service providers to bring additional resources to bear during times of service disruption**. Whenever a disruption involves multiple jurisdictions, there is always the potential for constraints on the ability to move quickly and apply the resources needed to restore services. The lack of commonly and broadly accepted agreements across jurisdictions (such as credentialing for ingress and egress) hampers the ability of infrastructure service providers to deliver the resources necessary to restore services and enable communities to recover.

5.0 Recommendations

The NIAC has six major recommendations. These address the following: (1) improving the understanding of resilient activities across and among infrastructures and communities; (2) enhancing regional and community-level information exchange; (3) expanding the availability of low-cost, scalable tools and techniques; (4) enhancing the transfer of expertise and lessons learned from national-level infrastructure planning and analysis to regional and community-level systems; (5) identifying the impacts on critical infrastructure services that result from changes in the Threat Condition under the Homeland Security Advisory System; and (6) removing cross-jurisdictional and other impediments to the transportation and use of outside assets during an emergency. These six recommendations and associated actions are discussed below.

1. **DHS-IP should lead a national effort to improve the understanding of resilient activities and how they are implemented in support of combined infrastructure and community resilience.** Such an effort requires the establishment of a widely shared, well-understood description of the elements of infrastructure resilience and how they can contribute to community resilience. As part of a revised NIPP or as a separate supporting document, DHS-IP should develop—in collaboration with critical infrastructure stakeholders within and outside of government—a common framework to enable infrastructure and community partners to identify, plan, implement, and assess various resilience activities. The broadest, most effective contributions of infrastructure activity to community resilience can be achieved only when the baseline definition and framework are commonly understood and applied. It is also essential that the various stakeholders in infrastructure and community resilience clearly understand their respective roles and responsibilities. The delineation of these roles, although mostly voluntary for non-Federal government entities, should be the responsibility of DHS-IP.

    - As the resilience framework is developed and the NIPP evolves to emphasize critical infrastructure and key resources (CIKR) resilience further, DHS should document agency roles and responsibilities in supporting CIKR resilience, particularly the roles and responsibilities for the Office of Infrastructure Protection and FEMA, and the roles of the Sector-Specific Agencies (as identified in Homeland Security Presidential Directive 7) and subsequent directives.
    - Federal programs in support of community resilience should be tailored to each jurisdiction's needs, resources, and current capabilities. DHS-IP should offer further assistance to local communities in identifying their interdependencies, both with local critical infrastructure as well as resources outside of the community jurisdictional boundaries. DHS-IP should work closely with State, local, tribal, territorial governments, and FEMA to develop guidelines for community resilience that could be shared with community organizations, such as Chambers of Commerce, for distribution to their members as part of their outreach to small businesses.
    - DHS-IP collaborating with FEMA should encourage regional organizations to develop Regional Infrastructure Protection Plans (RIPP) to support the coordination of regional all-hazards planning for catastrophic events. Regional plans should include the development of integrated protocols and procedures to manage a catastrophic event. An important component of regional plans should be the linkage of response operations and available resources. The NIAC encourages regional organizations to seek funding for RIPPs through the DHS Regional Catastrophic Preparedness Grant Program.

- Regions of the Nation that have already developed RIPPs should establish Regional Catastrophic Planning Teams tasked with the responsibility of testing regional and community emergency plans to ensure acceptable levels of resilience within specific geographic regions. These recurring tests can focus on different critical infrastructure and/or community assets for the purpose of optimization of resources, as well as on the various stages of response, restoration, and recovery. The NIAC strongly recommends that these tests include all key stakeholders and that lessons learned be documented and shared within the region so that all infrastructures and communities can benefit.
- Local communities should develop an Emergency Response Plan (ERP) to better adapt to all hazards and optimally use available resources. Where appropriate, the ERP should be compliant with the National Incident Management System and follow the guidelines established in the National Response Framework. The DHS Protective Security Advisor (PSA) and RRAP programs should be made available to assist those communities that wish to develop, modify, or improve local ERPs. The NIAC strongly recommends that, in developing ERPs, local communities include all major emergency preparedness stakeholders in their planning; this includes local law enforcement; other emergency response organizations; nonprofit organizations; owners and operators of local critical infrastructure; and local, regional, and/or State government officials. The NIAC further recommends that, as part of the ERP, processes be developed to periodically update the plan based on tests and exercises and the associated lessons learned.

2. **DHS-IP should take a leadership role in an initiative to enhance regional and community-level information exchange through the increased availability of data, information, tools, and techniques that bear upon critical infrastructure protection and resilience. The NIAC especially recommends that this information exchange be expedited through the wider use of fusion centers, and that the NIAC should examine how to enhance infrastructure owner/operator participation in, and contributions to, fusion-center effectiveness in community/infrastructure resilience.** The ability for non-Federal entities to plan and execute resilience activities is dependent on good information *and* the tools and techniques needed to apply this information to good effect. The transfer of lessons learned and proven technology and organizational-approach models from infrastructure collaborations in Federal information sharing can provide a valuable tool kit for community-level improvements in information sharing, which contribute to their resilience.
    - DHS-IP should partner with the Nation's fusion centers to ensure that critical infrastructure owners and operators are participating in fusion center information sharing. The co-location of business representatives and fusion center personnel can increase the flow of actionable information and lead to enhanced community resilience, especially during local and regional emergencies. The NIAC considers such co-location to be an essential element in the optimization of community resilience resources.
    - DHS should support the further development of regional fusion centers or the linking of multiple local fusion centers to enhance regional situational awareness. These regional centers can become the hub for co-location of the most advanced data collection and analysis tools available to the Nation. DHS should support the inclusion of a commitment to community resilience in the mission statements of these regional fusion centers, and part of their tasking should be the identification of how available resources in the region might best be distributed during various disaster scenarios.

- DHS should take the lead within the Federal Government to ensure that critical infrastructure owners and operators are regularly invited to participate in various scaled exercises around the Nation. One important lesson learned from previous tabletop exercises and workshops is that such exercises are often the best way to exchange information between government and private sector stakeholders. In collaboration with FEMA, DHS might help fund such exercises as appropriate, and encourage all sponsors of the exercises to record the findings and make them available to as wide an audience as possible in order to maximize the dissemination of lessons learned.

3. **DHS-IP should expand the provision of scalable, low-cost tools and techniques for community-level identification and assessment of infrastructure interdependencies.** Many effective tools and techniques are widely used on a national level to assess interdependencies and their potential impacts. Further development and transfer of infrastructure-based tools could demonstrably increase the ability of communities to establish and maintain an improved understanding of infrastructure assets and the associated community and infrastructure interdependencies. In turn, understanding of these interdependencies can improve the planning and use of resources in the event of disruptions.

    - DHS-IP should champion the development and transfer of infrastructure-based tools for applications such as dependency analysis and cybersecurity assessment. Although regional and community-level tools are not necessarily as robust, they can build on the structure and content of tools that have been tested and proven at the national level.

    - As part of their community resilience efforts, local governments and industries should contact their local PSA for a briefing on the various tools available from DHS and other Federal Government entities. PSAs should encourage local government and business leaders to look into the RRAP program as an effective way to apply these tools directly to community needs.

    - DHS-IP should expand the RRAP program as quickly as feasible to enhance the level of local, community, and regional resilience. The NIAC recognizes that one of the principal benefits of the RRAP is that it results in an integrated view of the close interdependencies of critical infrastructure and their surrounding communities. Such a view enhances security and resilience; moreover, the combination of multiple assessments achieved through the RRAP process reveals many areas in which resources can be better utilized to mitigate risk and increase resilience.

4. **DHS-IP should lead a continuing effort to enhance the transfer of expertise and lessons learned from national-level infrastructure planning and analysis to regional and community-level systems.** There is a wide range of valuable expertise and knowledge within Federal, State, and local governments that could, if made available in an appropriate format, bolster community understanding of, and planning for, resilience. The NIAC also encourages the individual sectors, acting through their representative Sector Coordinating Councils or other channels, to identify tools, techniques, and lessons learned that could enhance local and regional resilience and make them available to local communities. The NIAC especially encourages larger commercial distribution industries to consider how their supply-chain expertise might be applicable to the optimization of resources during an emergency.

    - DHS-IP should sponsor a series of regional exercises devoted specifically to the issue of the distribution of goods and services during a major event affecting community resilience. The purpose of these exercises is to bring together officials at all levels of government and private sector owners and operators to identify the specific resources that may be needed in such an

event, where the resources may be available, and how they are to be distributed under emergency conditions. The results of these exercises should be compiled into a report and widely distributed as part of FEMA's community outreach program to aid in community resilience planning.

- DHS-IP should develop nontraditional opportunities for communities to take advantage of federally provided training through venues, such as Webinars, that are practical, interactive, and accessible by public and private sector stakeholders. These easily accessible training tools can effectively transfer key lessons learned to a broad audience.

5. **DHS-IP should develop a national "playbook" to be used by DHS to clearly identify the impact on critical infrastructure services that result from changes in the Threat Condition under the Homeland Security Advisory System.** In its discussions, NIAC found that when the national threat level is elevated, the protective measures associated with this change may have unanticipated consequences on the ability of infrastructure providers to deliver needed services at the regional and community levels. To help maintain a community's resilience, infrastructure providers need a clear "playbook" of what actions the Federal Government is expected to take with a given change in threat level. In turn, such a playbook will enable infrastructure owners and operators to provide DHS and their customers with an improved picture of the actions industry will take under the various threat levels, and more clearly spell out the implications for service delivery. Ideally, the playbook would address national, regional, community, and sector-specific threat-level changes.

   - DHS-IP should encourage the participation of other Sector-Specific Agencies in the development of the playbook. For example, the Department of Energy might increase its role in the collection and dissemination of information during a storm response by preparing a daily impact status report on affected areas. Such information would enable power companies and local governments to collaborate on identifying which resources must be freed up or saved and which locations should be given priority for power restoration during a particular event.

   - As part of these playbooks, both government officials and private sector owners and operators should carefully consider and develop communications protocols for public information before, during, and after an event. When a disaster occurs, accurate and actionable information is vital for both emergency responders and the impacted community. Government and industry officials responsible for conveying this information to the public must be knowledgeable of the resources and capabilities available during an emergency and report information factually, so as not to inflate public expectations over timing for the recovery.

6. **The NIAC should prepare a follow-up report to the July 2009 *Framework for Dealing with Disasters and Related Interdependencies* to determine the implementation status of recommendations to remove cross-jurisdictional and other impediments to the transportation and use of outside assets during an emergency.** It is recommended that this follow-up report also explore the possibility of implementing standard approaches and agreements to alleviate these constraints. Although many infrastructure operators have well-established processes for working with government within their service areas, moving and applying assets from outside the affected jurisdiction(s) often faces significant constraints. A consolidated effort of government and infrastructure service providers, working through appropriate public-private sector partnership mechanisms, should focus on (1) identifying key cross-jurisdictional bottlenecks and (2) implementing standard approaches to remove these impediments for the purposes of optimizing the sharing of resources during major

disruptions. One example is the development of credential standards needed to respond to all hazards, as directed by the *Post Katrina Emergency Management Reform Act of 2006*.

- The NIAC encourages close collaboration between the Federal Government and State organizations such as the National Governors Association, Council of State Governments, and National Council of State Legislatures to develop model State legislation to ease the restoration of a community following an emergency or disaster. Part of this effort should be to ensure that, as States increasingly contract out services for emergency response, contractors are held to common standards so they can handle a regional response where multiple jurisdictions are requesting services or equipment.
- DHS should encourage State and local officials to identify and track available community-level resources that may be required for emergency response. Such activity would provide a significant opportunity for relationship building and coordination of resource allocation in any potentially affected areas. This database should also be shared with neighboring communities to ensure that available, convenient resources are not neglected, and resource allocations are not duplicated.
- The NIAC encourages the use of Federal assessment programs to assess the state of the Nation's aging infrastructure from the standpoint of ensuring community resilience. Damage to bridges and overpasses, for example, can severely impact the delivery of essential goods and services in the aftermath of a severe earthquake or hurricane. Given the assessment of the American Society of Engineers in their 2009 *Report Card for America's Infrastructure* that one in four rural bridges and one in three urban bridges were deficient, alternative routing for the delivery of essential goods and services must be part of all optimization of resource planning by local communities.

The NIAC believes these recommendations address significant gaps in the present resilience planning and implementation framework, and if acted upon, can help enable substantive improvements in optimizing resources for improved infrastructure and community resilience. Collaboration among public and private resources is essential to *keep communities above water*—literally and economically. In a world of *successful* community resilience, "normal life" is more than just a fond memory. Businesses can operate, people can work, children can go to school, and the economy can flourish. The NIAC believes that the enhancements to joint infrastructure and community resource management outlined in this study can substantially contribute to this shared outcome.

Exhibit 5.1 A Planning and Coordination Model: Four States Collaborate in Regional Emergency Planning Efforts

The New York City and Northern New Jersey Urban Area Working Groups and 30 counties forming the NYC-Northern New Jersey Combined Statistical Area are participating with government and industry members from Connecticut, New Jersey, New York, and Pennsylvania to engage in the development of a Regional Infrastructure Protection Plan (RIPP). The purpose of the RIPP is to support the coordination of regional all-hazard planning for catastrophic events, including the development of integrated planning communities, plans, protocols, and procedures to manage a catastrophic event. Funded by the DHS Regional Catastrophic Preparedness Grant Program, the mission is to fix shortcomings in existing plans, to build regional planning processes and planning communities, and to link operational and capabilities-based planning for resource allocation. Given that the region represents 1 out of every 14 Americans, the regional planning and coordination effort is critical to protecting and building up the resilience of a significant percentage of the Nation's population and critical infrastructure.

The NY-NJ-CT-PA Regional Catastrophic Planning Team, in support of its development of the RIPP, permitted the limited release of a report outlining its findings from a study simulating a high-impact low-frequency catastrophic incident affecting the electrical grid in the New York metropolitan area. Participants included government executives and operational leadership from electric power industry stakeholders, critical infrastructure facilities, and government agencies. The study's findings documented the actions taken during the post-incident phases—response, restoration, and recovery—through the lenses of the key stakeholders. Three workshops guided the study. Utility companies participated in two workshops on "Coordination of Emergency Response and Restoration" and "Supply Chain Challenges," and the third workshop fully considered the utility companies' actions and challenges to developing a better-informed government response. The study produced a set of lessons learned, including the present state of transformer manufacturing in the United States, and key steps to expedite the manufacturing of key grid restoration elements, thus providing new insight into electric grid security.

The study issued several recommendations, including the following:

- Government agency decision makers and key staff should receive training on electric power infrastructure and associated decision-making during emergencies, similar to a course already offered by some utility companies.
- Government should become more involved in the Spare Transformer Programs, potentially through incentivizing participation to improve the availability of spare transformers.
- Increased resilience of the supply chain would be aided by the inclusion of interoperability requirements into the transformer supply chain, such as support for standardized minimum design specifications for large transformers, to speed up the restoration process.
- Public-private sector efforts related to credentialing and access control should address the needs of the RIPP, aided by the identification of the current capabilities and limitations of real-time credentialing systems.

Sources: "Regional Infrastructure Protection Plan: Baseline Prioritization Report," Prepared for the New York City Office of Emergency Management and the NY-NJ-CT-PA Regional Catastrophic Planning Team, Public Health Solutions, Prepared by ICF International, August 27 2010; "Governor Patterson Announces More than $283 Million in Homeland Security Funding for New York State," New York State Press Release, June 18 2009, available at http://www.state.ny.us/governor/press/press_0618091.html; and "Regional Mass Fatality Response System," presented by Erin McLachlan, Mass Fatality Project Manager, on March 4 2010 at the Emergency Management Summit, available at http://www.ehcca.com/presentations/emsummit4/1_01.pdf

Appendix A About the NIAC

NIAC Members

Chair - Mr. Erle A. Nye, Chairman Emeritus, TXU Corp.

Vice Chair - Mr. Alfred R. Berkeley III, Chairman, Pipeline Financial Group, LLC *(Vice Chairman (retired) NASDAQ)*

Mr. David J. Bronczek, President and CEO, FedEx Express

Mr. Wesley Bush, Chief Executive Officer and President, Northrop Grumman

Lt. Gen. Albert J. Edmonds (ret.), Chairman and Chief Executive Officer, Edmonds Enterprise Services, Inc.

Chief Gilbert L. Gallegos (ret.), Chief of Police, City of Albuquerque, New Mexico

Ms. Margaret E. Grayson, President, Grayson & Associates

Mr. Philip G. Heasley, President and CEO, ACI Worldwide

Commissioner Raymond W. Kelly, Police Commissioner, New York Police Department

Mr. David Kepler, Executive Vice President, Chief Sustainability Officer, Chief Information Officer, Dow Chemical

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, Chief Executive Officer, News Distribution Network, Inc.

Mr. James A. Reid, President, Eastern Division, CB Richard Ellis

Mr. Bruce Rohde, Chairman and Chief Executive Officer Emeritus, ConAgra Foods, Inc

Dr. Linwood H. Rose, President, James Madison University

Mr. Matthew K. Rose, Chairman, President, and Chief Executive Officer, BNSF Railway Company

Mr. Michael J. Wallace, Vice Chairman and COO, Constellation Energy; Chairman, UniStar Nuclear Energy; Chairman, Constellation Energy Nuclear Group

Mr. Greg Wells, Senior Vice President-Operations, Southwest Airlines

Ms. Martha B. Wyrsch, President, Vestas Americas / Vestas Wind Systems, NA

NIAC Purpose and Structure

The National Infrastructure Advisory Council (NIAC) provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructures, both physical and cyber, supporting sectors of the economy. The NIAC also advises the lead Federal agencies that have critical infrastructure responsibilities and industry sector coordinating mechanisms. Specifically, the Council is charged with the following:

- 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.

The Council is composed of a maximum of 30 members, appointed by the President. The members of the NIAC are selected from the private sector, generally chief executive officers or their equivalent, including industry and academia, as well as public sector employees representing State and local governments. The members of the NIAC have expertise relevant to the functions of the NIAC with responsibilities for the security and resilience of critical infrastructure supporting key sectors of the economy, including agriculture, banking and finance, chemical, commercial facilities, critical manufacturing, dams, defense industrial base, government facilities, nuclear, postal and shipping, public health, transportation, energy, emergency services, and water.

Each year the NIAC undertakes several major studies in support of its mission. These studies focus on key topics selected by the NAC to inform the President on emerging issues, developments, and trends related to infrastructure protection and resilience. Its reports have drawn public and private sector interest with regular requests from Congressional committees for copies. The NIAC meets publicly four times a year, hosted in Washington, D.C., in a venue open to the public.

Appendix B DHS Programs Contributing to Resilience

Automated Critical Asset Management System (ACAMS)—A non-regulatory, Web-enabled information services portal that helps State and local governments build critical infrastructure protection programs in their local jurisdictions. ACAMS provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel collect and use asset data, assess vulnerabilities, develop all-hazards incident response and recovery plans, and build public-private partnerships.

Buffer Zone Protection Plan (BZPP)—BZPP is a targeted infrastructure protection grant program that provides funding to first responders for equipment acquisition and planning activities. The funding allows first responders to address gaps and enhance capabilities in protecting the highest risk critical infrastructure sites. BZPP funding has supported the Regional Resilience Assessment Program in fiscal year 2010.

Chemical Sector Security Seminar and Exercise Series—DHS collaborates with State chemical industry councils to provide facilitated tabletop exercises to simulate security incidents or natural disasters and engage chemical facility managers and emergency responders in interactive discussions on how to prepare for, respond to, and recover from such events. Each exercise is designed to improve the protection and resilience of the Chemical Sector by allowing sector partners to test their critical thinking, discuss how to coordinate procedures and communication, and strengthen security plans.

Citizen Corps Program (CCP)—CCP supports Citizen Corps Councils' efforts to engage citizens in personal preparedness, exercises, ongoing volunteer programs, and surge capacity response. The program is intended to better prepare citizens to be fully aware, trained, and practiced on how to respond to all threats and hazards. The program provides funding by formula basis to all 56 States and Territories.

Critical Infrastructure and Key Resources Information Sharing Environment (CIKR ISE) – The CIKR ISE enables informed decisions and timely actions among the CIKR Sectors as they execute infrastructure protection and resilience activities. Specifically, the CIKR ISE provides the procedures, content, and tools needed to enable security partners to share the vital information needed to manage their critical infrastructure security and risk, respond to events, and enhance resilience. Currently, the CIKR ISE's primary information sharing platform is the Homeland Security Information Network – Critical Sectors.

Enhanced Critical Infrastructure Protection (ECIP) Assessment—The ECIP program and associated tools deployed in the field by Protective Security Advisors (PSAs) can substantially enhance State and local understanding of the characteristics of assets and systems.

Integrated Common Analytical Viewer (iCAV)—A secure, Web-based, geospatial visualization suite of tools that integrates commercial and government-owned data and imagery from multiple sources to enable situational awareness. iCAV users can view the impact of threats, natural and manmade disasters, population centers that could be impacted, and the resources available to respond to and recover from an event.

National Exercise Program (NEP)—The NEP provides a framework for prioritizing, coordinating, and aligning Federal, regional, and State exercise activities. This alignment is achieved by issuing annual NEP exercise planning guidance derived from a strategic review of risks (threats, hazards, vulnerabilities, and operational risks), and by outlining a 5-year schedule of NEP tiered exercises.

National Infrastructure Simulation and Analysis Center (NISAC)—Analyzes and monitors risk to the Nation's critical infrastructure and provides key public and private sector decision makers with risk-informed, analytic products that influence the prioritization of risk-reduction strategies.

Pre-Disaster Mitigation (PDM)—The Pre-Disaster Mitigation (PDM) program provides funds to States, Territories, Indian tribal governments, communities, and universities for hazard mitigation planning and the implementation of mitigation projects prior to a disaster event. PDM grants are to be awarded on a competitive basis and without reference to State allocations, quotas, or other formula-based allocation of funds.

Protective Security Advisors (PSAs)—Trained critical infrastructure protection and vulnerability mitigation subject matter experts that advise and assist State, local, and critical infrastructure facility owners and operators on training, grants, and vulnerability assessments. The PSA program is viewed in the field as a success because it does not enforce regulations—a characteristic that fosters true partnerships—and has the ability to deliver Federal products and tools of significant value to State and local governments and critical infrastructure owners and operators.

Regional Catastrophic Preparedness Grant Program—The purpose of RCPGP is to enhance catastrophic incident preparedness in selected high-risk, high-consequence urban areas and their surrounding regions. RCPGP is intended to support coordination of regional all-hazards planning for catastrophic events, including the development of integrated planning communities, plans, protocols, and procedures to manage a catastrophic event. The deliverables from the RCPGP are made available throughout the country to enhance national resilience.

Regional Resilience Assessment Program (RRAP)—An effort conducted in cooperation with State and local governments and critical infrastructure owners and operators to assess critical infrastructure risk on a regional level, address capability gaps of the surrounding communities and region, and coordinate associated protection activities. Multiple tools—including vulnerability assessments, capabilities assessments, and infrastructure protection planning efforts—are used to identify and analyze critical infrastructure dependencies, interdependencies, capabilities, and security gaps. RRAP is viewed in the field as a model example of collaboration for two primary reasons: it incorporates key partners from the beginning of the assessment process and maps a DHS-provided capability to needs identified by participating private and public sector partners.

Appendix C Contributing Recommendations from Prior NIAC Studies

Previous National Infrastructure Advisory Council (NIAC) reports with recommendations related to infrastructure resilience examined the increased interdependencies between sectors, the reliance of systems on the Nation's cyber infrastructure, and the associated impacts of disruptions on key business functions and the national economy. Two primary infrastructure resilience reports include the 2009 *Critical Infrastructure Resilience* report and the 2009 *Framework for Dealing with Disasters and Related Interdependencies* report, both of which are summarized below. As noted earlier in this report, the scope and focus of previous NIAC reports has been on infrastructure resilience, and not on the intersection with community resilience. In addition, findings and recommendations on cybersecurity apply from several NIAC studies.

Critical Infrastructure Resilience[1]

The *Critical Infrastructure Resilience Report* originated from a recommendation by the preceding NIAC *Critical Infrastructure Partnership Strategic Assessment Study* (2008), which emphasized the importance of critical infrastructure resilience as necessary for government and business to create a comprehensive risk-management strategy. To address the gap between private sector business practices and protection-focused government policies, the *Critical Infrastructure Resilience Report* sought to identify and address key questions about the role of resilience in the public-private partnership for infrastructure protection. Specifically, the report included the following recommendations:

- Increase coordination among all levels of government and critical infrastructure and key resources (CIKR) owners and operators to mitigate the potentially detrimental effects of competing regulations and standards across regions, States, and local entities.
- Clarify roles and responsibilities of critical infrastructure partners to provide Federal, State, and local entities with better understanding of the components of resilience during an event and allow for increased information sharing. This clarification of roles should include a review of current incident management documents to identify opportunities to expand training and outreach activities to the CIKR owners and operators.
- Strengthen and leverage the public-private partnership by making full use of existing 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.

Framework for Dealing with Disasters and Related Interdependencies Report[2]

The NIAC *Framework for Dealing with Disasters and Related Interdependencies Report* sought to identify the following: areas of policy, law, and regulation that impede or constrain disaster recovery efforts of critical infrastructure owners and operators; policy-level approaches and solutions to identified impediments; and improvements to the challenge of deploying needed Federal resources to disaster

[1] See "Critical Infrastructure Resilience," *NIAC,* September 8, 2009, www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.
[2] See "Framework for Dealing with Disasters and Related Interdependencies Report," *NIAC,* July 14, 2009, www.dhs.gov/xlibrary/assets/niac/niac_framework_dealing_with_disasters.pdf.

areas. The report found many areas with significant potential for government to strengthen and improve critical infrastructure 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 opportunities to improve cooperation and information sharing among actors involved in disaster recovery.

The *Critical Infrastructure Resilience Report* found that the recommendations in the *Framework Report* offered practical, detailed solutions for every level of government to improve incident management and response. It further recommended that DHS should implement the *Framework* recommendations that support needed changes for critical infrastructure operator regulatory relief during a national crisis or incident, worker credentialing and access to a disaster area, and clarification of disaster recovery priorities and roles. The NIAC posited that this improved coordination among the sectors and government will provide faster recovery times and more focus on restoring operations, order, and public safety.

Cybersecurity Findings and Recommendations (Multiple Studies)

The following highlights cybersecurity findings and recommendations, relevant to community resilience, from four previous NIAC reports. Focus areas of the findings and recommendations include interdependencies, improved information sharing, benefits of public-private partnerships, incident response, and worker education programs.

- Dependency on network-based systems is pervasive across all sectors; critical components of our national infrastructure rely on a variety of network-based systems.[3]
- Improved information sharing regarding control systems threats, vulnerabilities, consequences, and solutions is vital to a properly informed and measured response to the threat to critical infrastructure control systems.[4]
- Sound business continuity practices, as well as information technology and cybersecurity best practices, provide some protection.[5]
- The DHS Secretary and the Sector-Specific Agencies should emphasize distinct private sector issues and priorities, such as the need for insightful threat information, cybersecurity improvements, or cross-sector initiatives to address interdependencies.[6]
- Government actions could benefit from private sector feedback and from higher-level interagency coordination and strategic planning to best address the cyber threat to control systems.[7]
- The Stafford Act's definition of "major disaster" should be amended to include chemical, biological, radiological, and cyber events.[8]

---

[3] "Convergence of Physical and Cyber Technologies and Related Security Management Challenges," *NIAC*, January 16, 2007, page 8–9. http://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport-011607.pdf.
[4] Ibid, page 6.
[5] Ibid, page 8–9.
[6] "Critical Infrastructure Partnership Strategic Assessment," *NIAC*, October 14, 2008, page 36. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf.
[7] "Convergence of Physical and Cyber Technologies and Related Security Management Challenges," *NIAC,* January 16, 2007, page 5.
[8] "Framework for Dealing with Disasters and Related Interdependencies," *NIAC,* July 14, 2009, page 21.

- To improve CIKR worker ethics, accountability, and understanding of appropriate information technology network conduct, secondary education training on ethics and awareness of the real consequences of cyber actions is needed for future workers.[9]

The NIAC considers these previous findings and recommendations to be highly germane and important to this study.

[9] "Insider Threat to Critical Infrastructures," *NIAC,* April 8, 2008, page 7, http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf.

Appendix D References

Advisory Committee on Earthquake Hazards Reduction, *White Paper on Achieving National Disaster Resilience through Local, Regional, and National Activities*, Reston, VA: National Earthquake Hazards Reduction Program, February 2010.

Alesch, Daniel J. and James N. Holly, *Tight Coupling, Open Systems, and Losses from Extreme Events*, Fairfax, VA: Public Entity Risk Institute, https://www.riskinstitute.org/peri/images/file/Alesch_Tight_Coupling_Open_Systems_and_Losses_From_Extreme_Events.pdf.

American Society of Civil Engineers, *2009 Report Card for America's Infrastructure*, Reston, VA: American Society of Civil Engineers, March 25, 2009, http://www.infrastructurereportcard.org/sites/default/files/RC2009_full_report.pdf.

Barnes, Paul and Akira Nakamura, eds., *Resilience and Crisis Planning in Mega-Cities: Issues, Opportunities and Uncertainties*, Northampton, MA: Edward Elgar Publishing, 2010.

Burdette, Mac, "Leading the Way: Increasing the Resilience of Local Government," presented at the CARRI Community Resilience Forum, April 28, 2009, http://www.resilientus.org/library/Mac_Burdette_1246387383.pdf.

Cabinet Office of the United Kingdom, United Kingdom Resilience Web page, "Community Resilience," July 1, 2010, www.cabinetoffice.gov.uk/ukresilience/communityresilience.aspx.

Canadian Centre for Community Renewal, "Community Resilience Manual," www.cedworks.com/communityresilience01.html.

Canadian Community Resilience Project Team, *The Community Resilience Manual*, Canadian Center for Community Renewal, 2000, 10–14, www.cedworks.com/files/pdf/free/MW100410.pdf.

Colten, Criag E., Robert W. Kates, and Susan B. Laska, *Community Resilience: Lessons from New Orleans and Hurricane Katrina*, Oak Ridge, TN: Community and Regional Resilience Institute, September 2008, www.resilientus.org/library/FINAL_COLTEN_9-25-08_1223482263.pdf.

Colten, Criag E., Robert W. Kates, and Shirley B. Laska, "Three Years after Katrina: Lessons for Community Resilience," *Environmental Magazine* 50(5) (September–October 2008).

Comfort, Louise K., Arjen Boin, and Chris C. Demchak, *Designing Resilience: Preparing for Extreme Events*, Pittsburgh, PA: University of Pittsburgh Press, 2010.

Cutter, Susan L., Lindsay Burnes, Melissa Berry, Christopher Burton, Elijah Evans, Eric Tate, and Jennifer Webb, "A Place-based Model for Understanding Community Resilience to Natural Disasters," *Global Environmental Change* 18(4)(October 2008): 598–606.

Cutter, Susan L., Lindsay Burnes, Melissa Berry, Christopher Burton, Elijah Evans, Eric Tate, and Jennifer Webb, *Community and Regional Resilience: Perspectives from Hazards, Disasters and Emergency Management*, Oak Ridge, TN: Community and Regional Resilience Institute, 2008.

Emergency Management and Response Information Sharing and Analysis Center, "The Concept of Resiliency," *EMR-ISAC Infogram 16-10* (April 22, 2010) www.usfa.dhs.gov/downloads/pdf/infograms/16_10.pdf.

Flynn, Stephen E., *The Edge of Disaster: Rebuilding a Resilient Nation*, New York: Random House, 2007.

Geis, Don, and Tammy Kutzmark, "Developing Sustainable Communities: The Future Is Now," *Public Management Magazine*, www.freshstart.ncat.org/articles/future.htm.

George Mason University School of Law, Critical Infrastructure Protection Program, *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, Fairfax, VA: George Mason University, February 2007, http://cip.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf.

Gooch, Margaret, and Jeni Warburton, "Building and Managing Resilience in Community-Based NRM Groups: An Australian Case Study," *Society & Natural Resources* 22(2)(2009).

Graham, Mary, *Community Resilience and Rapid Recovery of the Business Sector*, Oak Ridge, TN: Community and Regional Resilience Institute, April 2009, www.resilientus.org/library/Mary_Graham_1246387237.pdf.

Gunderson, L., *Comparing Ecological and Human Community Resilience*, Oak Ridge, TN: Community and Regional Resilience Institute, January 2009, www.resilientus.org/library/Final_Gunderson_1-12-09_1231774754.pdf.

Gurwitch, R.H., B. Pfefferbaum, J.M. Montgomery, R.W. Klomp, and D.B. Reissman, *Building Community Resilience for Children and Families*, Norman, OK: Terrorism and Disaster Center, University of Oklahoma, 2007, www.nctsnet.org/nctsn_assets/pdfs/edu_materials/BuildingCommunity_FINAL_02-12-07.pdf.

Jackson, Scott, *Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions*, Hoboken, NJ: John Wiley and Sons, 2010.

Lansford, Tom, *Fostering Community Resilience: Homeland Security and Hurricane Katrina*, Burlington, VT: Ashgate, 2010.

Mclachlan, Erin, "Regional Mass Fatality Response System," presented at the Emergency Management Summit, Seattle, March 4, 2010, www.ehcca.com/presentations/emsummit4/1_01.pdf.

Monday, Jacquelyn L, "Building Back Better: Creating a Sustainable Community After Disaster," *National Hazards Informer* 3(February 2002) www.colorado.edu/hazards/publications/informer/infrmr3/informer3b.htm.

Monday, Jacquelyn L., and Mary Fran Myers, "Coping with Disasters by Building Local Resiliency," National Hazards Research and Applications Information Center, University of Colorado, n.d.

National Fire Protection Association, *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, 2010 Edition*, Quincy, MA: National Fire Protection Association, 2010, www.nfpa.org/assets/files/PDF/NFPA16002010.pdf.

National Governors Association Center for Best Practices, *A Governor's Guide to Homeland Security*, Washington, D.C.: National Governors Association, 2007, www.nga.org/Files/pdf/0703GOVGUIDEHS.PDF.

National Governors Association Center for Best Practices, *Issue Brief: 2009 State Homeland Security Advisors Survey*, Washington, D.C.: National Governors Association, October 2009, www.nga.org/Files/pdf/1002HSASURVEY.PDF.

National Governors Association Center for Best Practices, *Issue Brief: Governors' Use of Executive Orders in Disaster Response*, Washington, D.C.: National Governors Association, October 2009, www.nga.org/Files/pdf/0910DISASTERRESPONSE.PDF.

National Infrastructure Advisory Council, *Best Practices for Government to Enhance the Security of National Critical Infrastructures: Final Report and Recommendations by the Council*, Washington, D.C.: National Infrastructure Advisory Council, April 13, 2004, www.dhs.gov/xlibrary/assets/niac/NIAC_BestPracticesSecurityInfrastructures_0404.pdf.

National Infrastructure Advisory Council, *Critical Infrastructure Resilience: Final Report and Recommendations*, Washington, D.C.: National Infrastructure Advisory Council, September 8, 2009, www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

National Infrastructure Advisory Council, *Cross Sector Interdependencies and Risk Assessment Guidance: Final Report and Recommendations by the Council*, January 13, 2004.

National Infrastructure Advisory Council, *Framework for Dealing with Disasters and Related Interdependencies: Final Report and Recommendations by the Council*, Washington, D.C.: National Infrastructure Advisory Council, July 14, 2009, www.dhs.gov/xlibrary/assets/irawgreport.pdf.

National Research Council of the National Academies, *Private-Public Sector Collaboration to Enhance Community Disaster Resilience: A Workshop Report*, Washington, D.C.: The National Academies Press, 2010.

New York City Office of Emergency Management and the NY-NJ-CT-PA Regional Catastrophic Planning Team, prepared by ICF International, *Regional Infrastructure Protection Plan: Baseline Prioritization Report*, August 27, 2010.

New York State Governor's Office, "Governor Patterson Announces More than $283 Million in Homeland Security Funding for New York State," Albany, NY: State of New York, June 18, 2009, www.state.ny.us/governor/press/press_0618091.html.

Norris, Fran H., and Betty Pfefferbaum, "START Community Resilience," presented at the Start Research Symposium at the University of Maryland College Park, June 28, 2006.

O'Donnell, Ian, Kristin Smart, and Ben Ramalingam, *Responding to Urban Disasters: Learning from Previous Relief and Recovery Operations*, London: ALNAPLessons, July 2009, www.proventionconsortium.org/themes/default/pdfs/alnap-provention-lessons-urban.pdf.

Provincial Emergency Program, Ministry of Public Safety and Solicitor General, *Critical Infrastructure Rating Workbook*, Surrey, B.C.: Government of British Columbia, May 2007, www.pep.bc.ca/Community/CI-RatingsWkbk.pdf.

Schoch-Spana, Monica, "Community Resilience for Catastrophic Health Events," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 6(2)(2008).

Seville, Erica, Andre Dantas, Jason Le Masurier, John Vargo, David Brunsdon, Suzanne Wilkinson, "Organisational Resilience: Researching the Reality of New Zealand Organisations," *Journal of Business Continuity and Emergency Planning* 2(3)(April 2008): 258–266.

Sheffi, Yossi, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, Cambridge, MA: MIT Press, 2005.

Stargel, Jocelyn, "Sustaining the Workforce and Infrastructure Through Catastrophe," Presented to National Governors Association, www.nga.org/Filwww.pep.bc.ca/Community/CI-RatingsWkbk.pdfes/pdf/0910HSTROUNDTABLESTARGEL.PDF.

Steward, Geoffrey T., Ramesh Kollura, and Mark Smith, "Leveraging Public-Private Partnerships to Improve Community Resilience in Times of Disaster," *International Journal of Physical Distribution & Logistics Management* 39(5)(2009).

Tierney, Kathleen, *Disaster Response: Research Findings and Their Implications for Resilience Measures*, Oak Ridge, TN: Community and Regional Resilience Initiative, March 2009, www.resilientus.org/library/Final_Tierney2_dpsbjs_1238179110.pdf.

The Infrastructure Security Partnership, "White Paper on Infrastructure Security Partnership, Infrastructure Resilience, and Interdependencies," Alexandria, VA: The Infrastructure Security Partnership, March 2010, www.drs-international.com/uploads/WH_OCIP_Recommendation_letter_March_2010%5B1%5D.pdf.

University of North Carolina Web page, "National Center for Natural Disasters, Coastal Infrastructure and Emergency Management (DIEM)," http://hazardscenter.unc.edu/diem/.

U.S. Congress, House, Committee on Homeland Security, Subcommittee on Emergency Communications, Preparedness, and Response, *Preparedness: State of Citizen and Community Preparedness*, 111th Cong., 1st sess., 2009, http://homeland.house.gov/Hearings/index.asp?ID=215.

U.S. Congress, House, Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, *Hearing on Post-Katrina: What it Takes to Cut the Bureaucracy and Assure a More Rapid Response After Catastrophic Disaster*, 111th Cong., 1st Sess., July 27, 2009.

U.S. Congress, Senate, statement of John R. Harrald before the Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration of the Homeland Security and Governmental Affairs Committee, *Hearings on New Paradigms for Private Sector Preparedness*, 111th Cong., 2nd Sess., March 4, 2010.

U.S. Congress, Senate, testimony of Juliette Kayyem before the Committee on Homeland Security and Governmental Affairs, *Deep Impact: Assessing the Effects of the Deepwater Horizon Oil Spill on States, Localities and the Private Sector*, 111th Cong., 2nd Sess., June 10, 2010.

U.S. Congress, Senate, testimony of Stephen Flyn to the Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration of the Homeland Security and Governmental Affairs Committee, *Building a More Resilient Nation by Strengthening Private-Public Partnerships*, 11th Cong., 2nd Sess., March 4, 2010.

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, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, Washington, D.C.: DHS, February 2010, http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

U.S. Department of Homeland Security, Federal Emergency Management Agency, National Response Framework, "Emergency Support Function #14: Long-Term Community Recovery Annex," Washington, D.C.: U.S. Department of Defense, August 2009, www.fema.gov/pdf/emergency/nrf/nrf-esf-14.pdf.

U.S. Department of Homeland Security, Federal Emergency Management Agency Web page, "National Incident Management System," www.fema.gov/emergency/nims/.

U.S. Department of Homeland Security, Federal Emergency Management Agency Web page, National Response Framework, "NRF Resource Center," www.fema.gov/emergency/nrf/.

U.S. Department of Homeland Security, Federal Emergency Management Agency Web page, "Federal Emergency Management Agency," www.fema.gov/index.shtm.

U.S. Department of Homeland Security, Federal Emergency Management Agency, Community Preparedness Division, "Update on Citizen Preparedness Research," *Citizen Preparedness Review* (5)(Fall 2007).

Woodrow Wilson International Center for Scholars, *Community Resilience: A Cross-Cultural Study*, Washington, D.C.: Woodrow Wilson International Center for Scholars, 2009, http://wilsoncenter.org/topics/pubs/CommunityResilience.pdf.